Hämmer haben keine Augen

Zum verantwortungsvollen Umgang mit Technologie in der Linken

> Der Schwerpunkt der RHZ 4/2014 drehte sich um die Folgen der Nutzung von Facebook, Twitter und Co im Politbereich – unser Beitrag wäre in etwa der Aufruf gewesen, wenigstens ein wenig Nerd zu werden. Das haben wir uns nicht getraut, denn die Reaktionen auf unsere Argumentationslinien sind zwar recht divers, aber ziemlich durchweg negativ. Am Ende fanden wir aber, dass Fragen der Infrastruktur – wer hat sie in der Hand? Und warum sind die Dinge so scheiße, wie sie gerade sind? – im Schwerpunkt doch zu kurz kamen. Und so wollen wir uns jetzt doch unbeliebt machen.

Ausgangspunkt unserer Argumentation ist, dass linke Organisationen im Allgemeinen keine Geheimdienste sind und das auch nicht sein *dürfen*. Gut, klar gibt es Aktions- und vielleicht sogar Organisationsformen, die ein hohes Maß an Konspirativität brauchen, aber die politischen Aktivitäten der meisten von uns gehören jedenfalls nicht dauerhaft in diese Kategorie.

Für diesen großen Rest gilt: Ein wichtiger Teil unserer Arbeit ist politische Sozialisation, also die Wandlung von Staatsbürger_innen in (revolutionäre oder sonstige) Subjekte. Wer will, kann das Agitation nennen. Jedenfalls klappt das nicht, wenn wir schweigen, uns tarnen, abschirmen, verschwinden. Es klappt aber weit besser, wenn unsere Strukturen, soweit irgend möglich, offen, freundlich, "welcoming" sind. Auch intern bedeutet breite Partizipation – die hier mal als strömungsübergreifend erstrebenswert unterstellt ist – größtmögliche Transparenz. Für EDV heißt das schon mal: Ziel kann im Allgemeinen nicht perfekte "Sicherheit" sein (zumal wir beim Versuch, dorthin zu kommen, nicht mehr viel anderes tun würden).

Allerdings agieren wir natürlich auch unter einer Obrigkeit, die keine große Lust hat, dermaleinst von lauter emanzipierten Untertanen gestürzt zu werden, und in unserer Umgebung tummeln sich Chefs und Nazis, die uns das Leben zusätzlich schwer machen können. Entsprechend ist die Frage, welche Nachrichten wir an wen schicken, wer sie lesen kann und was an ihnen dranhängt, höchst relevant für das, was wir uns trauen können, vor allem aber auch dafür, wie viel Vertrauen Menschen, die sich auf dem Weg zu uns befinden, in uns setzen können.

Ein ganz plattes Beispiel: Ein EA macht eine Erklärung zur Polizeigewalt auf einer Demo. Klar wollen wir, dass die gelesen wird. Aber schon von wem die genau kommt, sollte eigentlich nicht nachvollziehbar sein, und noch weniger, wer sie liest, wie lange Leute sie sich ansehen, wie die Leute auf die Erklärung gekommen sind, was sie danach gemacht haben und so weiter und so fort.

Die Vertrauensfrage ist also: Werden Informationen dieser Art gespeichert, welche genau sind das, wer kommt an sie ran? Wenn wir mit einiger Zuversicht Antworten geben wollen, hilft nur eins: Die Infrastruktur muss von vertrauenswürdigen Menschen betrieben werden, und diese müssen sie durchschauen können. Google, Facebook und Co kommen dafür nicht in Frage, schon, weil sie alle ein gedeihliches ökonomisches Umfeld und mithin ein konstruktives Verhältnis zu den Autoritäten brauchen.

Was, sagt ihr, wie soll ich denn Facebook laufen lassen? Exakt da liegt das ganz große, garstige Problem von Web 2.0, Cloud, Social Network oder wie immer ihr das Kommerznetz so nennen wollt: Firmen bauen da Systeme, die ihre Nutzer_innen einsperren: Apps fürs iphone gibts nur bei Apple, Facebook-Nachrichten können nur aus Facebook kommen, mit Leuten auf Skype oder Whatsapp kann ich nur reden, wenn ich selbst Skype oder Whatsapp "mache" – ihr erkennt das System (das, nebenbei bemerkt, bei Twitter und verschiedenen Google-Diensten eingestandenermaßen etwas subtiler abläuft).

Das muss nicht sein, jedenfalls nicht in dem Ausmaß. Bei der alten E-Mail erwartet jedeR, dass ei-

ne Mail, die ein Thunderbird bei riseup.net eingeliefert hat, auch bei gmail.com gelesen werden kann, und trotz einiger Sabotageversuche ("embrace and extend") klappt das im Wesentlichen auch. Wenn ihr eine Webseite anguckt, geht das weitgehend unabhängig von eurer Wahl von Browser, Computer und Betreiber der Seite (es sei denn, letztere hätten auf Ekel-Technologien wie Flash gesetzt). Wenn ihr eure Kurznachrichten über XMPP ("jabber") verbreitet, könnt ihr nicht nur 1a Verschlüsselung haben, sondern könnt euch aussuchen, auf welchem Server ihr sein wollt und welches Programm ihr nehmen wollt. Wenn ihr über SIP und RTMP telefoniert statt mit Skype, habt ihr eine breite Auswahl von Programmen, und ihr könnt bestimmen, wo euer "Telefon im Netz" stehen soll.

Und in all diesen Fällen könnt ihr, ein paar technische Kenntnisse und einen Computer im Internet vorausgesetzt, die netzseitigen Teile (eben die "Server") selbst laufen lassen. Das liegt an einem Umstand: Es gibt *offene Standards* dafür, in transparenten Verfahren erarbeitete Übereinkünfte, wie Rechner über bestimmte Sorten von Daten reden, wie die Daten repräsentiert werden und mehr komplizierte Nerddinge.

Das ist unsere erste Nachricht: Wenn ihr Technologie einsetzt, seht nach, ob ihr damit in den "ummauerten Garten" eines Unternehmens geht oder ob die Infrastruktur, auf die sie aufsetzt, auch von netten Leuten bereitgestellt werden könnte (oder noch besser schon wird), ob ihr im Idealfall selbst machen könnt, ob sie eben auf offenen Standards beruht, von denen wir oben die derzeit für die Kommunikation über Rechner relevantesten aufgezählt haben.

Klar eliminieren offene Standards nicht jede Sorte Überwachung – insbesondere wird das Netz selbst in absehbarer Zeit nicht von netten Leuten betrieben werden, und darauf sitzt der Staat ganz massiv. Beim Entwurf von Standards wird aber heute meist mitgedacht, wie genau diese Sorte feindseliger Leitung ausgespielt werden kann, und das klappt häufig recht weitgehend, wenn auch gerade die kritischen "Verbindungsdaten", um die es bei der Vorratsdatenspeicherung geht, meist ein Problem bleiben. Den politischen Kampf gegen die Staatssicherheitsbehörden werden wir also auch mit offenen Standards nicht liegen lassen können Ein Teil dieses Kampfes kann und sollte aber sein, dass wir ihnen ihr Geschäft schon mit technischen Mitteln so schwer wie möglich machen.

Dazu gehört, ihre Handlanger nicht zu bedienen, eben die Unternehmen, die die Daten aggregieren, aufgrund derer wir später auf den Kopf bekommen (könnten). Eigene, möglichst verteilte, Infrastruktur verhindert zentrale Angriffspunkte wie Facebook, die Überwacher anlocken wie ein plattgefahrener Igel die Fliegen, sie schafft Transparenz von "unten" nach "oben", und sie schafft die Möglichkeit, auf den Standards aufbauend weiterzubasteln – wie das etwa bei wirksamer Verschlüsselung (OTR, PGP) für Instant Messaging mit XMPP passiert ist.

Leider hat die Freiheit einen Preis: Ohne potente Geldgeber und meist ohne zentrale Punkte sind freie und offene Lösungen in aller Regel nicht so bunt und vor allem nicht so "einfach" wie das, was es kommerziell und zentralisiert gibt – für den Begriff von "einfach", nach dem eine moderne Glotze einfach ist: Mensch kann durch Knöpfchendrücken irgendwas erzielen, was ein gutes Gefühl gibt und braucht nichts lesen oder verstehen. Dass diese Sorte Einfachheit durch große Komplexität hinter den bunten Pixeln erkauft wird, gibt gleich das nächste Problem im Kampf gegen Massenüberwachung: Eben weil diese Kisten furchtbar viel automatisch machen müssen, ist auch für technisch versierte Menschen kaum zu durchblicken, was auf diesen "smart appliances" so passiert, zumal sich die Hersteller typischerweise auch noch Mühe geben, das zu verschleiern.

Zusammengefasst: Verantwortungsvoller, wenigestens ansatzweise selbstbestimmter Umgang mit dem, was wir heute als Informationstechnik auf Tischen und in Taschen haben, setzt die Nutzung offener Standards voraus. Die wiederum gibts nicht ohne eine Auseinandersetzung mit der Technik selbst, ohne den Beschluss, dass Dinge auch mal ein wenig ruckeln dürfen, dass mensch einen Klick mehr brauchen darf, um ein Video zu sehen, dass mensch halt mal eine halbe Stunde irgendwas lesen muss, bevor was so geht, wie es auch mit der schicken, kostenlosen App aus dem Store ginge, ohne dass damit spürbar Arbeit verbunden wäre. Diese Nachricht, dargeboten in graugrauem Protestantorama, ist das, was wir uns in der letzten Nummer nicht zu sagen trauten.

Nebenbei gilt das noch unausweichlicher für alles, was mit Verschlüsselung zu tun hat. Wenn ihr nicht wisst, was Schlüsselmanagement ist und wie das für eure Verschlüsselungstechnologie funktioniert, ist eure Verschlüsselung nur Verschleierung: Besser als gar nichts, aber schon durch relativ fantasielose Angriffe zu brechen.

"Aber benutze meinen Computer doch nur als Werkzeug," ruft ihr da. Nun, erstens mahnen wir auch Nutzer_innen von Kettensägen und Presslufthämmern, sich vorm Anwerfen etwas mit ihrer "Technologie" und den Eigenschaften der bearbeiteten Umwelt auseinanderzusetzen. Zweitens aber, und viel wichtiger, ist der Computer kein Werkzeug, und mensch muss nicht lange rätseln, was ihn zu was anderem macht: Eine Säge führt keine Programme aus, ein Schraubenschlüssel speichert keine E-Mails, ein Hammer hat keine Augen, und der Hobel sendet nicht eure Position raus. Brechstangen schließlich dürften nur für die wenigsten von euch einen großen Teil der Kommunikation mit anderen Menschen vermitteln.

Dazu tritt, dass inzwischen die meisten von euch vermutlich deutlich mehr Zeit mit Digitalplunder verbringen als mit tatsächlicher sozialer Interaktion – das mag Maurern mit ihrer Kelle ähnlich gehen, ist aber trotzdem nicht typisch für Werkzeugnutzung. Mit Computern als "Werkzeug" umgehen ist nach dieser Abwägung in etwa so verwantwortlich wie in der Steuerzentrale eines AKW zu stehen und zu verkünden: "Ich will hier doch nur wohnen, ich mag die bunten Lichter."

Als hätten wir noch nicht genug die Nerdkeule geschwungen, kommt hier noch eine dritte Nachricht: Unter Umständen hilfts auch noch nichts, offene Standards zu verwenden, manchmal gilt es, auch bei der Wahl der Infrastruktur vorsichtig zu sein – und zwar nicht nur für euch, sondern auch für die, die mit euch zu tun haben. Beispiel E-Mail: Seht mal in eure Mailbox und zählt, wie viele Mails da schon offensichtlich von den verschiedenen Inkarnationen von Google Mail kommen. Dazu kommen dann noch ein Haufen versteckte Mails von Googles Servern, weil immer mehr Behörden, Unis und Firmen ihre Mail-Infrastruktur an Google übergeben. Das ist der Anteil eurer Mails, die Google kennt (minus dem, was PGP-verschlüsselt war, aber dann kennt Google immerhin noch die Metadaten) – und das völlig unabhängig von eurer Entscheidung, ob ihr für das so atemberaubend tolle Gmail-Interface einige Freiheiten aufgebt oder nicht.

Ganz allgemein trefft ihr eure Entscheidungen bezüglich der Nutzung von Technologien nicht in einem Vakuum, sie beeinflussen ganz direkt die Freiheit anderer Menschen. Ein anderes Beispiel ist Internet-Telefonie – die rabiaten Methoden, mit denen Skype Firewalls und andere Internetschäden überwindet, und die schon mangels zentraler Server von freien Projekten nicht imitiert werden können, sorgen dafür, dass Netzbetreiber und Routerhersteller die vertretbaren Arten, auf der eigenen Kiste Internet-Telefonie zu machen, blockieren können: "Wenn du sowas machen willst, nimm halt Skype". An der Stelle sagen: "Nein, in deinem Netz gehen die vereinbarten Standardprotokolle für dies oder jenes nicht, und das ist ein Scheiß" – das ist ein kleiner Schritt in Richtung schwerer kontrollierbares, freieres, nutzer_innenbestimmtes Netz.

Die unbequeme Synthese aus den Nachrichten ist: Macht euch wenigstens rudimentär schlau über das, was ihr mit euren Kisten treibt. Ein paar Prozent der Zeit, die ihr mit ihnen verbringt, für einschlägige Fortbildung zu verwenden, würde da überallhin reichen. Zu fast allem gibts irgendwo im Netz lesenswerte Texte, die Wikipedia ist meist kein schlechter Ausgangspunkt, Freie Systeme haben ihre manpages, und es gibt natürlich Bücher. Wenigstens Anstöße können auch auch wir als Datenschutzgruppe in Veranstaltungen geben.

Und weil das alles eingestandenermaßen eine Zumutung ist: erstrebenswertes Ziel unserer Praxis sollte natürlich auch die Wahlfreiheit sein, mit dem ganzen Mist gar nichts zu tun haben zu müssen. Denn auch Fixogum hat keine Augen.

Datenschutzgruppe der Roten Hilfe Heidelberg

Kontakt und Artikel-Archiv: https://datenschmutz.de

PGP Fingerprint: a3d8 4454 2e04 6860 0a38 a35e d1ea ecce f2bd 132a