Von der Unmöglichkeit der Freiheit

Zum „Ökosystem Smartphone“

> Als uns die Redaktion der RHZ fragte, ob wir zum Schwerpunkt dieser Ausgabe einen Artikel zum Verschlüsseln von bzw. auf Smartphones beisteuern könnten, haben wir ein wenig überlegt. Sollen wir ein paar Wischanleitungen für, sagen wir, Signal oder k9mail zusammenstöpseln? Recherchieren, wie oft die deutsche Polizei Google-Terminkalender abgegriffen hat? Am Schluss haben wir vor der Herausforderung „Smartphone sichern“ kapituliert. Ja, das heißt Kapitulation vor der Art, in der die breite Mehrheit der „Verbraucher_innen“ heute Computer konsumiert. Und weil uns das eigentlich etwas peinlich ist, wollen wir diskutieren, warum wir bei dem Thema die weiße Fahne hissen.

Die Ultrakurzfassung ist: Das „Absichern“ eines Smartphones macht das Ding zu einem Computer Und damit für Zwecke des Smartfonierens kaputt.

Ein Smartphone nämlich ist gebaut und entworfen als Ausspielweg für „Content“ aller Art: Karten oder Kontakte, Trailer oder Termine, Facebook oder Fitnessgraphen. Damit das für beide Seiten einfach und für die Hersteller monetarisierbar geht, muss das Gerät möglichst weitgehend von den verschiedenen Content-Lieferanten kontrollierbar sein und mithin möglichst wenig von den Nutzer_innen, die wir in dieser Welt lieber mit dem schön-doppeldeutigen Wort „Bediente“ bezeichnen.

Aus diesem Design erklären sich all die Jails, die Appstores, die die Bedienten aussperrende Krypto, die Möglichkeiten für Infrastrukturprovider, Content (und mithin auch Software) „over the air“ auf die Geräte zu bringen oder wieder von den Geräten zu entfernen (früher Höhepunkt: Amazon löscht Orwells 1984 von seinen an Bediente verteilten Kindles – true story!).

Klar kann mensch Telefone jailbreaken, die verschiedenen Ausspielinfrastrukturen entfernen, vielleicht sogar durch Freie Alternativen ersetzen. Aber das Ergebnis davon ist etwas, das erstmal nichts weiß von Pizzerien innerhalb von 500 m um den aktuellen Standort oder den Foursquarerern in der Kneipe hier. Dem Ding sowas beibringen ist meist mühsam und setzt etwas Verständnis dafür voraus, was da im Hintergrund alles übertragen und verarbeitet wird. Das schöne Smartphone ist damit, wie gesagt, kaputt. Für die Contentlieferanten und mithin die Behörden (das war ja das Etappenziel). Aber eben auch für die Bedienten.

Und so malen wir hier nur das graue Protestantorama aus RHZ 1/15 („Hämmer haben keine Augen“) weiter. Damals war das Hauptthema die Nutzung von freiheits- und mithin privatsphäreraubenden „Plattformen“ (Facebook, Skype, WhatsApp...), statt derer wir lieber die Nutzung offener Standards sehen würden. Lest die Archivkopie (vgl. unten) einfach nochmal als Teil des Schwerpunkts dieser RHZ.

Vier Freiheiten

In diesem Artikel nun würden wir gerne eine Art Checkliste liefern, wie viele Freiheiten euch ein bestimmtes Stück Software lässt. Gerade „Apps“ schneiden da häufig noch schlechter ab als klassische Computerprogramme, und das, obwohl erstere gerne mit noch heikleren Daten hantieren. Und klar ist, dass die Übergriffe eben nicht nur den „Kernbereich der privaten Lebensgestaltung“ verletzen; all die Daten, die bei den Content-Lieferanten liegen, sind für den Staat relativ einfach zugänglich, schon rechtlich geschützt mit weniger dem Postgeheimnis, und wenigstens die NSA hat klar angesagt, dass sie damit Massenüberwachung veranstalten will und das in relativ geringem Umfang auch schon tut. Die hier diskutierten Freiheiten schützen also nicht nur die *Privat*-Sphäre, sondern auch die, sagen wir, Politsphäre.

Freie (mit großem F) Software und Daten sind welche, die ihren Nutzer_innen vier Freiheiten einräumen (in ein paar Details werden bei Profis Programme und

Daten – stellt euch da z.B. Landkarten, aber auch Bücher oder Musik vor – noch etwas unterschieden, aber das muss uns hier nicht kümmern):

- Nutzung (ich kann Programme und Daten auf den Kisten, die ich habe, ausführen bzw. lesen, wann ich will und solang ich will)
- Untersuchung (ich kann mir ansehen, wie Programme funktionieren und was den Daten zugrundeliegt. Das setzt in der Regel lesbaren Quelltext voraus)
- Verbessern (ich kann Fehler beseitigen, Daten ergänzen, den Kram auch komplett umbauen oder was immer)
- Weitergeben (etwa, weil wer anders das Ding braucht, oder auch, um meine Verbesserungen zu verbreiten)

Die meisten modernen Desktop-Systeme abseits von MacOS und Windows geben ihren Nutzer_innen für fast alle installierte Software diese Freiheiten. Das hat übrigens auch Schattenseiten, denn ohne die Freiheiten, die GNU und Linux auch den Imperien von Google, Facebook und Whatsapp geben, gäbe es die Imperien nicht. Aber so ist das mit Freiheit: Wenn *nur* die Falschen sie nutzen, kommt eine fiese Klassengesellschaft raus.

Übliche kommerzielle Software schränkt einige der vier Freiheiten in verschiedenen Weisen ein: Es gibt einen Haufen „kostenlose“ Software, die ohne Quelltext kommt (nix untersuchen, nix verbessern, nur dort laufen lassen, wo es der Hersteller erlaubt), allerlei Inhalte kommen kaum noch nützlich festgebacken (Karten als Bilder z.B.) und mit Lizenzen oder technischen Maßnahmen, die eine selbstbestimmte Nutzung ausschließen (DRM-belastete Bücher oder Musik sind da Beispiele). Und natürlich dürft ihr fast alle Software, die ihr von Firmen kriegt, bezahlt oder nicht, per Lizenz eigentlich nicht weitergeben.

Stufen der Knechtschaft

Schon auf konventionellen Computern aber sind viele Hersteller dazu übergegangen, die Freiheit ihrer Nutzer_innen noch über das von Word und Co gewohnte Maß hinaus einzuschränken. Dazu gehört etwa die Kopplung an irgendwelche Online-Ressourcen, seien es Lizenzserver (das Programm startet nicht, wenn nicht regelmäßig Gebühren bezahlt werden) oder Onlinedienste wie etwa bei vielen Computerspielen. Damit kann der Hersteller zu jeder Zeit auch die Freiheit der Nutzung auf eigentlich vorgesehenen Plattformen verwehren.

Der nächste Schritt ist dann das permanente Nach-Hause-Telefonieren, um etwa zu melden, was Leute so mit der Software machen. Das ist schon nicht mehr in den vier Freiheiten zu messen. Diese Programme haben schlicht eine eingebaute Überwachungs-Infrastruktur.

Aber selbst bei lückenlos berichtender Software könnten Nutzer_innen immer noch ihre Daten nehmen und vielleicht, *vielleicht* mit anderen, freieren Programmen weiterwursteln. Wer will, kann das als fünfte Freiheit, die zum Weglaufen, fassen, und eine Art, sie einzufordern ist das Bestehen auf den offenen Standards aus RHZ 1/15. Die Kontrolle über die Bedienten und das, was sie tun, ist dennoch erst dann perfekt, wenn auch deren Daten „in der Cloud“ liegen, physisch also beim Content-Provider. Wer die Plattform wechselt verliert seine_ihre Daten. Perfekt. Für die eine Seite des Deals.

Dieses letzte Modell, jederzeit zurückrufbare Software, deren Aktionen durchweg beim Hersteller nachvollzogen werden können und deren Daten auch gleich dort liegen: Das ist das Modell der typischen Smartphone-App. Es ist geradezu das definierende Moment des ganzen Ökosystems. Und das ist der Hintergrund der Unersetzbarkeit der Schnüffel-Infrastruktur, die wir eingangs bejammert haben. Wer diese Welt verlassen will, muss alles zurücklassen.

Die Wandlung eines Smartphones in einen nur überschaubar ausforschbaren Computer ist übrigens auch weit mehr Arbeit, als sich halt gleich einen nicht allzu großen Computer zu besogen und da irgendein halbwegs freies System draufzubügeln. Wers ordentlich haben will, kann zu TAILS greifen und bei der Gelegenheit *beide* Capulcu-Broschüren lesen[1].

Ja, mit so einem Ding steht es sich nicht gut in der U-Bahn, mal eben kurz etwas tindern vielleicht. That's not a bug, that's a feature.

Netzwerken

Denn das wäre unser zweiter Schmerzpunkt beim Smartphone: Das Chatten (oder Blogs lesen oder Twittern oder Siri fragen) in der U-Bahn geht nur, weil so ein Gerät wann immer es kann eine Internet-Verbindung hält. Das heißt, dass das Netz im Wesentlichen immer eine recht gute (bei LTE im Prinzip auf ein paar Dutzend Meter genaue) Vorstellung davon hat, wo das Telefon und mithin in der Regel sein_e

Eigentümer_in ist. Damit wird in jedem Fall mal die einstmals gefürchtete „stille SMS“ obsolet, denn sie diente allein dazu, dass sich das Telefon mal kurz beim Netz rührte. Das wiederum war nötig, damit das Netz das Telefon nicht nur auf einige 10 km, sondern auf wenige 100 m genau lokalisieren konnte.

Wer also nicht im Effekt permanent stille SMS an sich selbst schicken will, kann nicht mobiles Internet als Dauerzustand haben. Andererseits besteht noch ein wenig Entwarnung auf der Zeitschiene: Bewegungsprofile in dieser Qualität werden zumindest vorläufig nicht vorratsgespeichert, denn §113b Abs. 4 Telekommunikationsgesetz will nur die Speicherung der Funkzelle, in der eine Internetverbindung aufgenommen wurde. Das ist zwar speziell im LTE-Netz (da ist die Einbuchung des Telefons bereits die Internet-Verbindung) keine wirklich verständliche Anweisung, weshalb die Praxis uneinheitlich sein dürfte. In jedem Fall hängt stark von Netzabdeckung und Empfangsbedingungen ab, wie viele Punkte wirklich gesetzt und vier Wochen lang zur Nutzung der Behörden gespeichert werden. Lückenlose Bewegungsprofile, wie sie die Technik hergeben würde, dürften aber nur unter ganz extremen Umständen rauskommen (und in denen macht das Smartphone sicher keinen Spaß mehr).

Und dennoch: Eröffnete schon die weite Verbreitung der alten Sprach-Mobiltelefone eine neue Liga der Überwachung, macht Always-On-Internet die live den Helden und Monstren folgenden Punkte auf Bildschirmkarten in SciFi-Actionreißern zu einer ermittlungstechnischen Realität. Dagegen gibt es prinzipbedingt keinen Schutz, und wer das nicht haben will, hat die Wahl zwischen GSM-Fon oder, gasp, gar keinem.

Ja, wir meinen das ernst: beim Smartphone ist mit Freiheit, Selbstbestimmung und Behördenaussperren fast nichts zu holen. Tut uns leid.

Der Ablass für ein Jahr Smartfonieren liegt derzeit bei 150 Euro Extraspende an die RH.

Datenschutzgruppe der Roten Hilfe Heidelberg

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

PGP Fingerprint: 4FD3 B3EE 7FCE 9FFD EC75 CAF9 4847 5F52 5C0C 5DB1

[1] https://capulcu.blackblogs.org/, auf Papier beim Literaturvertrieb