Chatgruppen sind mittlerweile auch im anarchistischen Milieu das Mittel der Wahl zur Koordination und Mobilisation. Kritische Stimmen dem gegenüber werden zunehmend leiser. Die beiden Texte in dieser Broschüre behandeln Ermittlungsverfahren der letzten Jahre und die praktischen Folgen, wenn Chatgruppen zur politischen Organisierung benutzt werden.

Tod den Chats!

Es lebe die soziale Beziehung!

Wider den chattenden Verhältnissen

Kritische Betrachtungen
zur Verwendung von Chatgruppen

Wien
Mai 2022

mehr auf: librifelis.noblogs.org

Wider den chattenden Verhältnissen

Kritische Betrachtungen
zur Verwendung von Chatgruppen

Inhalt

Entnommen:

autonomes Blättchen
Nr. 48
März-Mai 2022

P.S.: Wir sind nicht nur ein paar Unzufriedene, sondern mehr als 30 Leute, die sich über die Themen dieses Textes lange Gedanken gemacht haben. Wir haben in echt und von Angesicht zu Angesicht diskutiert und analysiert und sind zu diesem politischen Schritt gemeinsam gelangt.

Wir halten die aufgeklärte und disziplinierte Nutzung eines Tails-Computer ohne Festplatte etc. und die Nutzung von Jabber über einen Tails-Computer für weiterhin einigermaßen sicher. Unter: https://capulcu.blackblogs.org/ findet ihr alles, was ihr dafür braucht. Es gilt aber auch hier: Die ganz spannenden Sachen nur von Angesicht zu Angesicht! Updates! Immer schön ausschalten! Und so wenig wie möglich, besser gar nichts, speichern! Keine Namen, keine Strukturen! Verifikationsmethoden und Vertrauensnetzwerke nutzen!

Ein Plädoyer gegen Chats

Es sind die mitunter größten Razzien der Polizeigeschichte: International koordinierte Hausdurchsuchungen in dutzenden Ländern, Hunderte Tonnen sichergestellte Drogen, Millionen an Bargeld, etliche Waffen und tausende Haftbefehle. Was sich in den letzten zwei Jahren an Entschlüsselungen und Infiltrierungen in vermeintlich verschlüsselte Chats und Krypto-Handy-Software ereignet hat, wirft ein Licht auf Polizeiarbeit im 21. Jahrhundert. Doch der Reihe nach:

Von EncroChat...

EnroChat war ein Unternehmen, welches von 2018 verschlüsselte Handys an Kunden in über 140 Ländern verkaufte. Extrem teure Preise sollten der Garant für extrem sichere Verschlüsselung sein, einschließlich der Option bei Bedarf den kompletten In-

halt des Handys zu löschen. EncroChat-Phones waren stinknormale Smartphones, allerdings ohne GPS, Mikrofon, Kamera etc. Bei Bedarf konnte man mit einem Passwort den verschlüsselten Chat öffnen – und diesen gegebenefalls komplett löschen. Jedoch schafften es die französischen Bullen den Chatdienst mit Schadsoftware zu infiltrieren. Die EncroChat-Betreiber bemerkten die Malware und versuchten die Software zu modifizieren, jedoch verhärtete sich der Verdacht, dass es sich um Behörden handelte und deswegen forderte Encro seine 60.000 Nutzer auf jeglichen Inhalt der Handys zu löschen und die Geräte zu zerstören. Doch zu spät… zwanzig Millionen Chat-Daten waren bereits abgefangen und es kam zu mehr als tausend Festnahmen, hauptsächlich in Frankreich, den Niederlanden, Belgien und England. Während sich die Behörden rühmten, endlich einmal nicht nur die Handlanger der Organisierten Kriminalität erwischt zu haben, wurden manche Nutzer auch nicht verhaftet, da sie nicht so blöd waren Photos, Geburtstagsglückwünsche und

Schluss

Wir halten es dennoch für legitim auf Reichweite von Informationen und auf „Masse“ zu setzen. Auf uns müsst ihr aber verzichten, wenn ihr den Weg des arbeitssparenden Technologieeinsatzes wählt, der die Anwendung und ihre Folgen nicht wirklich mitdenkt, geschweige denn sich zu diesen verhält. Lieber würden wir in Euch Vertrauen setzen und in Zukunft gemeinsam mit Euch kämpferisch durch die Straßen ziehen. Dafür benötigt es aber gute reale Beziehungen untereinander. Die wachsen langsamer als eure Signal-Kontaktlisten, überstehen dafür aber auch die schweren Schläge der Repression und des Lebens.

Bildet Banden und vernetzt euch im Real-Life, dann könnt ihr auch auf Signal im politischen Gebrauch verzichten!

Solidarische Grüße
die Freund_innen von Tails und Jabber

Parallel dazu sehen wir, wie mit zunehmender Repression die Antirepressionsarbeit vernachlässigt wird bzw. sie nicht Schritt hält. Schnelle Mobilisierung bedeutet in den meisten Fällen auch mangelnde Antireparbeit, weil die menschliche, soziale Struktur, aus der sich die solidarischen Antirepressionsgruppen bilden, gar nicht erst entsteht, weil zwischen den Menschen ein Smartphone hockt. Daher halten wir das Reichweiten-Argument für unverantwortlich und kontraproduktiv. Gerade angesichts der Tonnen an Repression und dem Mangel an solidarischen Strukturen in dieser Stadt.

An dieser Stelle Danke an alle, die bei den Hausdurchsuchungen vor Ort sind, denjenigen die nachts Stunden vor der GeSa warten, die alle möglichen Arbeiten für Repressierte übernehmen und sie emotional, sozial und ökonomisch stützen, damit sie bald wieder Seite an Seite mit uns kämpfen können.

andere personalisierte Daten hin und her zu schicken. Die Ermittlungen dauern allerdings an und alleine in Deutschland sitzen circa 1000 Leute wegen Encro in U-haft, es laufen 2.700 Ermittlungsverfahren [Stand: Januar 2022]. Damit die von französischen Bullen erhobenen Daten von den zu diesem Zeitpunkt nichts ahnenden deutschen Behörden nun verarbeitet werden dürfen, mussten auf diesen Präzedenzfall hin ersteinmal ein paar Paragraphen ein bisschen uuuuuuumgebogen werden... und nun laufen bereits Verhandlungen auf Grundlage der Daten und es wurden auch schon Leute verurteilt. Anscheinend versucht das BKA in den Akten die Herkunft der Datensätze zu verschleiern, da das alles rechtlich nicht ganz koscher abgelaufen sein dürfte.

...zum SkyEcc...

Doch der Entschlüsselungsspaß der Behörden kam durch EncroChat erst so richtig in Schwung. Anscheinend stiegen viele Kriminelle von EncroChat auf das Kyrptohandy SkyEcc um. Ende 2020 knackten belgische Bullen in Zusammenarbeit mit den Niederlanden und Frankreich in einer gemeinsamen Europol-Operation das Kryptohandy SkyEcc, was anscheinend Server in den USA, Kanada und Europa betreibt und international ca. 170.000 Nutzer hatte. Obwohl 700 Verhaftungen und etliche Hausdurchsuchungen folgten (einschließlich 17 Tonnen sichergestelltes Kokain) und die Behörden behaupten, dass sie diesmal eine Datenmenge sichergestellt hätten, die vier mal so groß wie die von EncroChat ist, beteuert SkyEcc dass sie nicht gehackt wurden und ihre Handys weiterhin sicher sind. Wenn ich richtig verstehe, kann man weiterhin SkyEcc-Handys kaufen und SkyEcc behauptet, die entschlüsselten Handys seien Fake-Sky-Handys gewesen, die von nicht-

wissen, was für ein Strafmaß das Ganze mit sich bringt, da die Einladung nicht mehr auf Vertrauensnetzwerken basiert.

Smartphones und ihre Software sind sowohl zum Weiterleiten und Teilen, als auch zum Aushorchen und zum Überwachen gebaut worden. Und so sind sensible Nachrichten schnell bei irgendwem, der es an irgendjemanden weiterleitet. Zur Erinnerung: EIN unsicheres Smartphone reicht! Und alle müssen mit den Konsequenzen leben. Vertrauensnetzwerke, die sich gemeinsam über präventive Abwehr und Antirepressionsarbeit Gedanken machen, sind das nicht mehr. Ankündigungen für gemeinsam begangene Straftaten werden auf offensichtlich viel zu viele Smartphones in der Stadt gesendet.

Das geschieht unserer Ansicht nach unbeabsichtigt, aber in voller politischer Ignoranz dessen, was das für Folgen hat und haben könnte (Repression, Repression, Repression, sozialer Abstand, Abstand, Abstand).

(Un-)Sicherheit

Angesichts der oben genannten Punkte halten wir die Signal-Spontis für sehr unsicher. Daher haben wir entschieden, nicht mehr an Spontis teilzunehmen, die über Signal mobilisiert wurden. Auch wir gehören zur Krawall- und Remmidemmi-Fraktion und freuen uns über jeden größeren Haufen. Unsere Haut ist uns zu schade, als das wir auf alle Sicherheitsstandards scheißen für schlecht vorbereitete Spontis mit ungewissen Ausgang ohne politisch durchdachte Wirkung. Auch so eine Sache, die sich erst richtig entfaltet, wenn sich von Angesicht zu Angesicht organisiert wird.

Das oft gehörte und einzige Argument für die Nutzung von Signal ist die potentielle Reichweite. Eine Signalnachricht ist schnell weiterverbreitet, das Smartphone lädt dazu ein, schnell und nebenbei Nachrichten (z.B. Spontimobilisierungen) weiterzuleiten. In solche Aktionen werden dann aber Personen hineingezogen, die nicht wissen, was für Sachen wie vorbereitet werden, die nicht

authorisierten Resellern verkauft wurden und dass ihre Kommunikation immer noch sicher sei. Jedenfalls waren sich die belgischen Cops, die hauptsächlich hinter der ganzen Aktion steckten, ihrer Sache so sicher, dass sie die Daten ihre eigene Kontoverbindung an SkyEcc schickten, um sie aufzufordern ihnen die Prämie zu überweisen, die SkyEcc für erfolgreiche Entschlüsselung an Hacker verspricht. Wie dem auch sei, entschlüsseltes Sky oder entschlüsseltes Fake-Sky-Phone, die deutschen Behörden meinen, sie warten noch, dass ihnen die Millionen Sky-Datensätze ausgestellt werden. Anscheinend laufen auch Verfahren gegen die Betreiber der Firma Drogen- und Waffenhandel zu ermöglichen, obwohl diese beteuern nichts von laufenden Verfahren zu wissen und einen legalen Service anzubieten.

...zu Anom...

Nach dem Schlag gegen Sky, vereinte Interpol seine Kräfte und holte zum Riesenschlag gegen die organisierte Kriminalität aus. Doch von Anfang an: Bereits 2018 nahm das FBI einen anderen kleineren KryptoPhone-Anbieter namens „Phantom Secure“ hoch, ansässig in Kanada mit circa 20.000 Nutzern. Der angeblicher Chef hinter Phantom Secure kooperierte bei seiner Festnahme in den USA nicht mit den Bullen und ging für neun Jahre hinter Gittern. In diesem Kontext konnte das FBI einen Informanten und Krypto-App-Entwickler anwerben, der im Kuhhandel für Straffreiheit und 120.000 Dollar zusammen mit dem FBI eine App verkaufen sollte, die er ohnehin gerade entwickelte: ANOM. Das FBI gründete also eine Firma in Panama und verkaufte ab 2020 von dort aus 12.000 angeblich sichere Geräte, die in Wahrheit alles direkt an die Behörden weiterleiteten. 18 Monate lang fingen das FBI 27 Millionen Nachrichten in einhundert Ländern ab und schlug dann in der „Operation

Die Presse

Nicht nur die Cops waren zu oft schon erstaunlich früh dabei. Bei den letzten Spontis ist uns aufgefallen, dass stets L-IZ-Journalist_innen von Anfang an anwesend waren. Zum Einen ist die L-IZ ein liberales Drecksblatt, das sind keine Genoss_innen oder Freunde_innen, denen wir vertrauen. Zudem gab es in der Vergangenheit L-IZ Journalist_innen, die drohten Bilder von Demo-Teilnehmern_innen zu veröffentlichen. Die Presse ist nicht unsere Verbündete. Die Journalist_innen (auch der L-IZ) werden immer zuerst sich selbst schützen und ihr Material an die Schweine weitergeben, bevor sie ihren Lebensunterhalt riskieren. Entweder gibt es einen Kreis, der die Jornalist_innen einlädt oder wir könnten auch hier davon ausgehen, dass eben diese Jornalist_innen mit in den Signal-Netzwerken hängen.

Konfrontation (z.B. mit den Cops) zu gehen. Es kommt doch hoffentlich auch niemand auf die Idee eine nächtliche militante Kleingruppen-Aktion über Signal zu koordinieren. Warum dann Spontis?

Machen wir uns nichts vor. Die Zeiten in denen es funktionierte, sich vorher zu überlegen, welches Strafmaß oder welche Folgen Eine_n im dümmsten Falle so blühen könnte, sind in dieser Stadt vorbei. Auch wenn es um die Abgabe von DNA geht, braucht es dafür schon lange keine brennenden Karren oder schwerverletzten Nazis mehr. Die Teilnahme an einer solchen Sponti und schon geringeres sind ausreichend, um schwerwiegende Repressionsmaßnahmen auszulösen. Dies steht im Widerspruch dazu, dass die Sicherheitsstandards der Szene (z.B. durch Smartphones) gesenkt werden.

Trojan Shield“ genannten Aktion in Zusammenarbeit mit 16 anderen Ländern zu. 700 Hausdurchsuchungen und bereits zu Beginn 800 Verhaftungen folgten, 50 Millionen beschlagnahmte Dollar… laut Europol „eine der größten Polizeiaktionen jemals“. Von Australien bis Kanada, bis nach Großbritannien, Serbien, Spanien, Deutschland und Schweden.

...bis zu unserer Kommunikation

Warum dieser ganze Abriss über Repression gegen organisierte Kriminalität? Ich will mich hier keineswegs mit den teils betroffenen Kartellen solidarisieren, auch wenn ich niemandem Knaststrafen wünsche, aber die teils aufgedeckten Folterkammern zeigen eindrücklich, wie viel Blut an den ganzen scheiß Drogen klebt (und zudem wie viele Millionen die Cops und der Zoll durch den Scheiß mittels Bestechung verdienen). Aber darum soll es in diesem Text nicht gehen. Ich will viel eher die Frage aufwerfen, inwiefern es irgendwie möglich ist heutzutage

an sichere digitale Kommunikation zu glauben. Eine ältere Gefährtin meinte einmal zu mir, dass sie sich das Internet wie ein großes Amphitheater vorstellt: Egal ob man in einer Geheimsprache spricht oder nicht, das, was man ruft, gelangt an viele Ohren.

Ich weiß, dass es einen Unterschied zwischen zentraler und dezentraler Verschlüsselung gibt – EncroChat lief beispielsweise anscheinend maßgeblich über ein Serverzentrum in Frankreich und wurde dort angeknipst. Aber ist seit dem NSA-Skandal nicht klar, dass unsere ganze Kommunikation angeknipst wird? Den Bullen und den Tech-Firmen ist es möglich jeden Inhalt abzufangen oder zu beschlagnahmen. Und auch wenn alles x-mal verschlüsselt ist, wächst die Kapazität der Bullen zu entschlüsseln Jahr für Jahr… angesichts von Quantencomputern, Deutschen Behörden, die sich ausschließlich auf Entschlüsselung konzentrieren (ZITiS), plus Polizeiaufgabengesetzen, die pauschal den Einsatz von Staatstrojanern erlauben und Berichten, die

Zu den Spontis

Die Cops

Auf einer der letzten Spontis in der Stadt (und auch schon auf mindestens einer davor) waren Bullen vor uns am Startpunkt, ein Sammeln war nicht mehr möglich. Wir gehen davon aus, dass die „Signal-Struktur“ auf irgendeine Art und Weise infiltriert ist. Ob technisch oder personell, vermutlich werden wir es, wenn überhaupt, erst in ein paar Jahren durch irgendeinen Aktenvermerk wirklich nachvollziehen können.

Wir können noch verstehen, wenn Signal im Privaten genutzt wird. Darüber für Spontis zu mobilisieren halten wir für falsch und gefährlich. Ja, eine Spontandemonstration ist per se erstmal nicht verboten und mag als nicht so relevant gesehen werden. So wie wir die Spontis hier in der Stadt verfolgen – und wie wir sie uns auch wünschen – soll meist keine angemeldete Demo folgen, sondern ein empowernder Mob die vorhandenen Spielräume nutzen, um auch in

Es reicht EIN „unsicheres“ Smartphone in Euren Signal-Netzwerken und die Kommunikation liegt offen! Die gesamte Kommunikation. Alle beteiligten Nummern, alle versendeten Nachrichten. Denken wir zusätzlich an all die Hausdurchsuchungen der letzten Jahre und an all die dabei eingesackten Endgeräte. Noch eingeschaltete Smartphones wurden und werden sofort an Energiequellen angeschlossen, um sie später noch knacken bzw. einfach Kommunikation mitlesen zu können. Das Knacken eines Apple-Smartphones durch eine in München ansässige Firma kostet aktuell 1400 Euro. Ob nicht auch all die andern (Betriebssysteme auf) Smartphones bereits gehackt werden können und die Bullen auch diesen Service einkaufen, wissen wir nicht. Wir sollten aber zumindest von der Möglichkeit ausgehen.

von dem Einsatz der Smartphone-Spyware „Pegasus“ durch BKA, Verfassungsschutz und BND berichten, frage ich mich, wie sinnig es ist, in irgendeiner Art auf Verschlüsselungen zu vertrauen, so scheint es doch teils ein aussichtsloses Wettrennen zu sein. Sicher, besser verschlüsselt als gar nicht, man will es den Schweinen ja nicht zu einfach machen und zudem können sie unsere Verbindungen viel besser durchleuchten, wenn alles per Handy kommuniziert wird. Doch die oben aufgelisteten jüngsten Bullenoperationen sollten uns davor warnen, Sachen per Handy oder Internet zu planen, die dort nichts verloren haben. Nichtsdestotrotz stelle ich einen Trend fest, dass zunehmend gewissen Chat-Apps vertraut wird, die angeblich „ultra safe“ sind und alles über diese geregelt wird. Dies birgt die Gefahr repressiver Operationen, da diese entschlüsselt oder falsch genutzt werden oder es neue Gesetze gibt, wie der gerade vom BKA vorangebrachte Entwurf, dass zukünftig jede Chat-App das BKA informieren muss, wenn ein Inhalt potentiell

strafbar ist. Das heißt, dass eventuell bald ein Algorithmus Signal und Telegram durchleuchtet und alles nach Strafbarkeit filtert. Ja, sicher, anfangs wird dieser Algorithmus total scheiße sein…

...bis er es eben nicht mehr ist.

Doch darüberhinaus etablieren diese verschlüsselten (und oft trotzdem auf zentralen Servern gespeicherten) Apps, dass auch eigentlich sich als technologiekritisch verstehende Menschen mehr und mehr im Netz verfangen und alles über Smartphones kommunizieren, die ganze Zeit chatten und ihr scheiß Phone immer dabei haben. Kein Wunder – sie sind ja auch auf dieses angewiesen, da alles mit und durch und dank diesem organisiert wird. So werden wir meiner Meinung nach bestimmter essenzieller menschlicher und organisatorischer Fähigkeiten enteignet, wenn wir im Hinblick auf „Praktikabilität“ und „Schnelligkeit“ und „Reichweite“ alles über Chats kommunizieren. Der Fähigkeit etwas durch zu diskutieren und zu reflektieren, anstatt nur hin und

muss aber trotzdem gemacht werden. Die Antirepressionsarbeit danach – wenn die Bullen erstmal mitlesen – ist um ein Vielfaches größer. Bullen und Schlapphüte haben Spezialist_innen, die für sie Trojaner, Onlinedurchsuchungen, Telekommunikationsüberwachung, Hacking, Metadatenauswertung und all die ganzen Sachen machen. Wir sind nicht schlauer als diese!

Die technische und auch die menschliche Sicherheit eines Smartphones sind also nicht gegeben. Es gibt genug Einfallstore ein Smartphone mitzulesen, abzuhören etc.. Die Zugänglichkeit erleichtert sich mit der Nutzung von Google-Konten, keiner oder nur schlechter Verschlüsselung, Sim-Karten und IMEI-Nummern (Hardwarenummer des Mobiltelefons, die stets mitgesendet wird), die auf existierende Personen laufen, usw.. Die Liste an Problemen ist lang, sehr lang! Und selbst wenn das individuell beachtet wird, all die Sicherheitsstandards eingehalten und Vorsichtsmaßnahmen getroffen sind, kann sich nicht in Sicherheit gewogen werden.

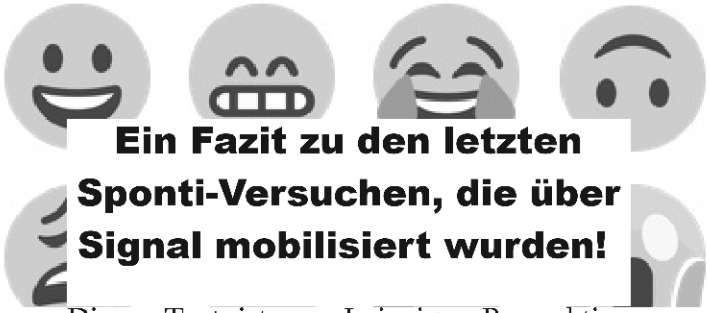
die Unsicherheit herausstellte? Können wir wirklich einfach zum nächsten „sicheren“ Messenger wechseln und darauf warten, in welchem kommenden Verfahren uns oder anderen auch dieser um die Ohren fliegen wird?

Noch entscheidender als die (Un-)Sicherheit des Messengers an sich ist die dauerhaft richtige Anwendung der Smartphones mit dem die meisten Nutzer_innen Signal nutzen. Erst dann kann die technische Sicherheit überhaupt greifen. Ständige Updates, Verschlüsselung, Trennung von Politisch und Privat, das Smartphone jeden Abend ausschalten, nicht mit sich herumtragen… Verhalten sich viele Leute so? Keineswegs. Abgesehen davon, dass all dies Vielen nicht alltagstauglich erscheint, wird die Thematisierung von Sicherheit und Antirepressionsmaßnahmen präventiver Art sich zu oft gespart. Der Aufwand dafür ist groß, auch wenn eine_n die meist männlichen Techno-Spezialisten stets versichern, „dass das alles ganz einfach“ sei. Einfach ist das nicht,

her zu chatten. Sich auch ohne Handy zu connecten, zu wissen wo man die Leute treffen kann oder wo sie wohnen. Sich zu treffen und füreinander Zeit zu haben – konzentriert im hier und jetzt zu sein – anstatt die ganze Zeit nervös auf Chatprotokolle zu starren. Die Praxis auch einfach mal so aufzutauchen und zu klingeln, ohne dass dies komisch ist. Abmachungen und Verabredungen zu treffen, die sicher stattfinden, ohne dass dies noch einmal digital bestätigt werden muss. Letztendlich geht es generell um die Konsistenz unserer Beziehungen und Freundschaften und die Qualität, welche diese verlieren, wenn alles nur per Bildschirm geregelt und vermittelt wird.

Während der Revolte in Kasachstan im Januar schaltete der Staat das Internet aus… ich hoffe ein solcher Zustand würde unsere Ausgangsbasis nicht verschlechtern. Im Gegenteil. Denn wenn alle auf die Straße kommen und kein Handy mehr funktioniert, hat unsere Kommunikation ganz andere Potentiale sich frei zu entwickeln und auf Worte Taten folgen zu lassen. Auf dass der digitale Käfig uns nicht zum Verhängnis wird, sondern wir ihm!

Entnommen:
IN DER TAT - Anarchistische Zeitschrift
Nr. 14
Frühling 2022



Ein Fazit zu den letzten Sponti-Versuchen, die über Signal mobilisiert wurden!

Dieser Text ist aus Leipziger Perspektive geschrieben, bezieht sich auf vergangene Spontis in der Stadt und die Einladungspolitik zu diesen per Smartphone-Messengerdienst Signal. Vieles lässt sich auch auf andere Städte übertragen und darf dort auch gerne verbreitet werden!

Smartphones und Messengerdienste/ Signal

Wird Signal komplett richtig gebraucht, ist die technische Sicherheit des Messengers aktuell vielleicht gegeben. Wir wissen es nicht und vermutlich wissen es die meisten Nutzer_innen auch nicht. Wer von uns versteht schon diese Quellcodesachen bzw. den Stand der Gegenseite? War nicht Telegram auch lange en vogue bis sich im Nachhinein