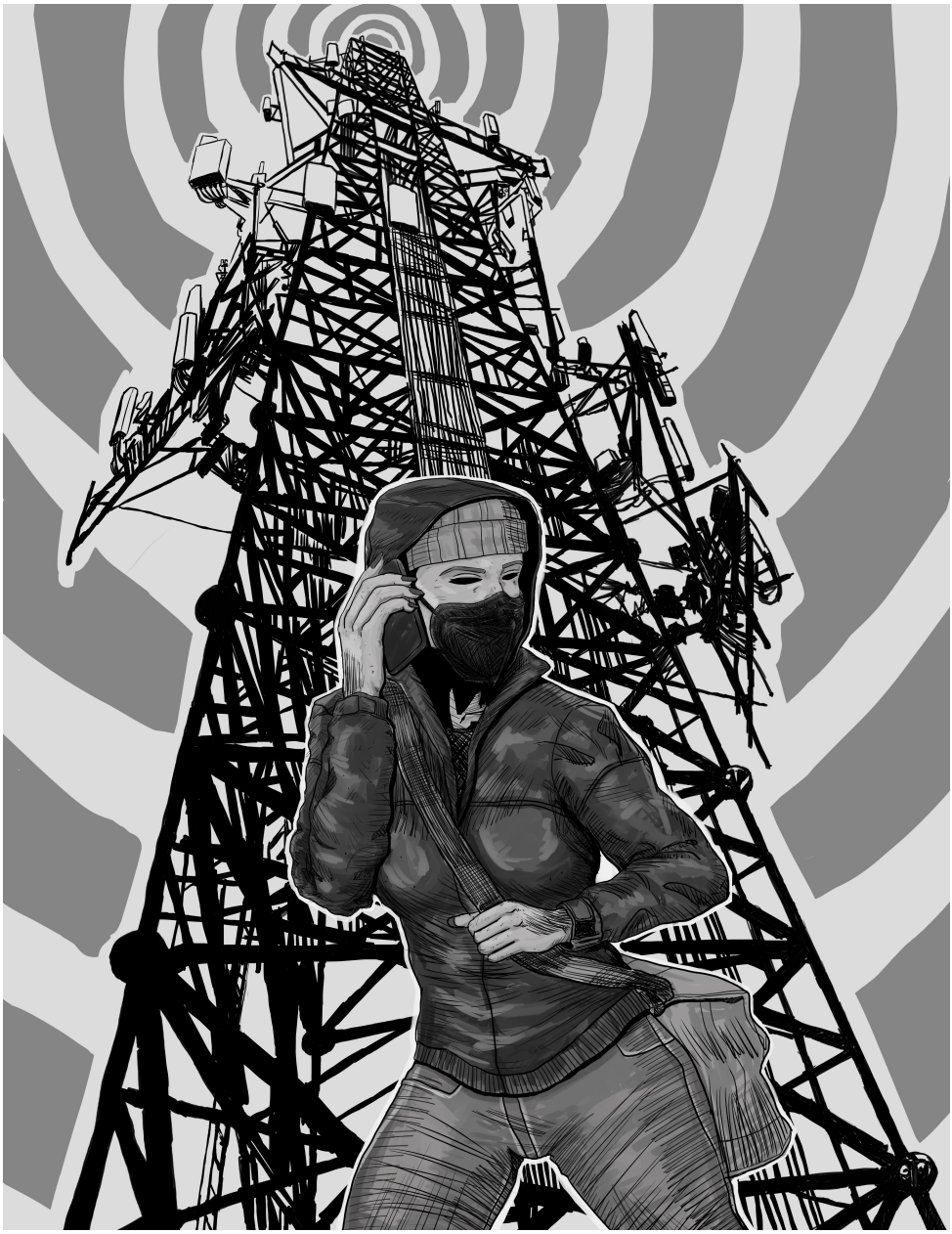
HANDY-SICHERHEIT

FÜR AKTIVIST:INNEN UND AGITATOR:INNEN



HÅKAN GEIJER

Anmerkung des Übersetzers

Übersetzungen sind nie exakt, und sie müssen lokalisiert werden. Es werden nicht nur die Wörter, sondern auch die Inhalte übersetzt, was zu Unterschieden zum Originaltext führt. Ich habe spezifisch Anmerkungen für die BRD hinzugefügt und für den englischen Sprachraum relevant Anmerkungen entfernt. Da in der deutschen Sprache viele Anglizismen verwendet werden, habe ich in diesen Fällen beide Begriffe mit aufgenommen.

Vorwärts!
— M.

Einführung

Einige der mächtigsten Werkzeuge, die uns zur Verfügung stehen, sind unsere mit dem Internet verbundenen Smartphones. Die sofortige Kommunikation und die Summe des gesamten menschlichen Wissens, das zum Greifen nah ist, erhöht unsere Fähigkeit, die Welt um uns herum enorm zu beeinflussen. Doch diese Konnektivität hat ihren Preis in der zunehmenden Überwachung durch staatliche Sicherheitsapparate und Privatpersonen. Diejenigen, die in radikalen/linken Bewegungen aktiv sind, sind sich—in unterschiedlichem Ausmaß—dieser Überwachung bewusst. Gemeinsam haben wir Praktiken der operativen Sicherheit (manchmal Betriebssicherheit, als OpSec abgekürzt) und eine interne Sicherheitskultur entwickelt, um Störungen unserer Bemühungen, uns zu organisieren, entgegenzuwirken.

Es existieren viele Mythen über die Nutzung von Handys. Sie beruhen auf Missverständnis über deren Technologien und über die Fähigkeiten, die Staat und privat Akteuren verfügen, um Privatpersonen zu überwachen. Bei der Erstellung von Bedrohungsmodellen geht es darum, Bedrohungen zu erkennen und spezifische und pragmatische Gegenmaßnahmen zu entwickel. Doch ohne genaue Modelle deiner Gegner:innen führen solche Modelle zu unwirksamen Gegenmaßnahmen. Maßnahmen, die auf der Grundlage von Fehlinformationen ergriffen werden, können zu einer leichten Verhaftung führen oder den Eindruck von allwissenden Gegner:innen erwecken, was wiederum Aktionen behindert. Diese Zine befasst sich mit den grundlegenden Technologien von Handys und geht auf verbreitete Mythen ein, damit du und deine Genoss:innen Störungen widerstehen und sich effektiv organisieren können.

So etwas wie perfekte Sicherheit gibt es nicht. Es handelt sich nicht um ein Binär, die entweder „an“ oder „aus“ ist, und auch nicht um ein Spektrum von „besserer Sicherheit“ oder „schlechterer Sicherheit“. Sicherheit wird am besten als „sicherer unter diesen Bedingungen gegen diese Bedrohungen“

diskutiert. Was vielleicht wirksam ist, um den Staat davon abzuhalten, deinen Standort über dein Handy zu verfolgen, kann nutzlos sein, um eine:n missbräuchliche:n Partner:in davon abzuhalten, deine Nachrichten zu lesen. Diese Zine soll dir helfen, die Risiken zu verstehen, denen du ausgesetzt bist, damit du fundierte Entscheidungen treffen kannst. Sicherheitskultur ist keine Garantie für Sicherheit, aber sie ist Schadensbegrenzung. Du kannst deine Inhaftierung verhindern oder dein Leben oder das Leben der Menschen in deinem Umfeld retten.

Diese Zine wurde Anfang 2022 von Anarchist:innen aus Europa und Nordamerika (und original auf Englisch) geschrieben, und daher wird dieses Wissen für diejenigen, die uns räumlich und zeitlich nahe stehen, am relevantesten sein. Wir lassen absichtlich (die meisten) rechtlichen Überlegungen weg. Nur weil deine Gegner:innen etwas nicht tun dürfen, heißt das nicht, dass sie es nicht trotzdem tun werden. Stattdessen konzentrieren wir uns darauf, was technisch möglich ist. Wir erkennen auch die Vorurteile an, über die wir nicht hinwegsehen können (sie finden sich immer noch in dieser Zine), und wir sind nicht in der Lage, die Zukunft vorherzusagen. Du musst das Wissen über deinen persönlichen und lokalen Kontext nutzen, um das hier Geschriebene an die spezifischen Bedrohungen anzupassen, denen du ausgesetzt bist.

Dein Handy und du

Dein Handy ist nicht nur ein wertvoller persönlicher Besitz. Es ist eine Erweiterung deiner Persönlichkeit. Es enthält deine Erinnerungen, dein Wissen, deine privaten und halbprivaten Gedanken. Es ermöglicht dir, schnell Informationen nachzuschlagen und sie mit anderen zu teilen. Diese Konnektivität und der Zugang zu Wissen machen uns bei der Verfolgung unserer Ziele effektiver. Handys sind—bis zu einem gewissen Grad—auch zu einer Voraussetzung für das Funktionieren in der modernen Gesellschaft geworden. Aus diesem Grund sind wir selten ohne sie unterwegs. Wenn der Akku leer ist oder wir ohne es das Haus verlassen, fühlen wir uns nackt, unfähig oder als würde ein Teil von uns fehlen.

Das Eindringen in ein Handy—entweder durch Beschlagnahmung oder durch Malware—durch eine:n Gegner:in kann verheerende Folgen haben. Alle deine Fotos, Textnachrichten, E-Mails und Notizen könnten Gegner:innen zugänglich gemacht werden. Sie könnten Zugriff auf alle derzeit angemeldeten Konten auf deinem Handy haben. Installierte Malware oder Stalking-Apps könnten das Mikrofon deines Handys oder die Echtzeit-Ortung aktivieren, nachdem es dir zurückgegeben wurde.

Abgesehen von diesen Arten der aktiven Überwachung bietet dein Handy privilegierten Parteien wie der Polizei, die Massen- oder Echtzeitzugriff auf Metadaten anfordern kann, die deinem Netzbetreiber oder Internetdienstanbieter zur Verfügung stehen, eine passive Überwachung.

Aufgrund dieser Überwachungsmöglichkeiten sagen Aktivist:innen zu Recht: „Your phone is a cop“ und „Your phone is a snitch.“[1] Sollten wir Handys aufgrund ihren Fähigkeiten weiter benutzen, weil sie uns die Möglichkeit dazu geben, oder sollten wir sie wegen der Gefahren, die sie darstellen, ausrangieren? Oder gibt es vielleicht eine Nuance in der Frage, wann und wie wir Handys benutzen können, die es uns erlaubt, viele ihrer Vorteile zu behalten und gleichzeitig viele ihrer Nachteile zu vermeiden?

Handy-Technik

Um zu verstehen, wie Handys kompromittiert und zur Überwachung genutzt werden können, müssen wir genau wissen, wie die verschiedenen in Handys verwendeten Technologien funktionieren, z. B. die Hardware, die Firmware und das Betriebssystem des Handys, die Mobilfunknetze und bis zu einem gewissen Grad auch das Internet insgesamt. Das wird dir helfen, ein Bedrohungsmodell zu erstellen, damit du fundierte Entscheidungen treffen kannst, was dem Auswendiglernen scheinbar willkürlicher Maßnahmen vorzuziehen ist.

Mobilfunknetze

Mobilfunknetze bestehen aus überlappenden Zellen, die von Transceiver-Sendemasten versorgt werden. In städtischen Gebieten ist die Netzabdeckung dichter, so dass ein einzelnes Handy mit mehr Sendemasten in Kontakt steht. In Vorstädten und ländlichen Gebieten gibt es weniger Überschneidungen, so dass ein Handy mit weniger Sendemasten in Kontakt steht.

Provider können Informationen über das Signal selbst verwenden, um den Standort des Handys zu bestimmen. Der grobe Standort kann anhand des Einfallswinkels am Sendemast oder anhand des Sektors[2], aus dem das Signal kommt, bestimmt werden. Wenn die Entfernung eines Handys von mehreren Masten gleichzeitig gemessen wird, kann der Provider den Standort des Handys sehr genau triangulieren.[3] LTE-Netze können die Position

[1] *Anm. d. Übersetzers*: Übersetzt als „Dein Handy ist ein Bulle“ und „Dein Handy ist ein:e Spitzel:in,“ aber solche Sprichwörter gibt's leider nicht auf Deutsch.

[2] Die kegelförmige Fläche, die von einer einzelnen Antenne abgedeckt wird.

[3] Das heißt „Aufwärtsstrecke-Multilateralisierung.“ Übrigens verwenden wir „Triangulation“ im Sinne von „Multilateralisierung,“ weil es sich in diesem Fall lohnt, technische Genauigkeit gegen Verständlichkeit einzutauschen.

eines Handys durchschnittlich 25 Meter genau bestimmen, und 5G-Netze können dies bis auf 5 Meter genau tun. Je mehr Sendemasten es gibt, desto genauer kann der Standort des Handys bestimmt werden. Daher ist die Triangulation auf dem Land im Allgemeinen weniger genau als in der Stadt.

Wenn Handys eine Verbindung zu einem Mobilfunknetz herstellen, senden sie eine eindeutige Geräte-ID (IMEI[4]) zusammen mit ihrer Teilnehmer-ID (IMSI[5]). Eine IMSI wird normalerweise auf einer physischen SIM-Karte[6] oder einer eSIM[7] gespeichert. Dies bedeutet, dass der Austausch mehrerer SIM-Karten zwischen einem Gerät oder einer SIM-Karte zwischen mehreren Geräten eine feste Verbindung zwischen diesen Identitäten herstellen kann. Eine gültige SIM-Karte oder IMSI ist nicht erforderlich, um einen Anruf zu tätigen. Sie dient lediglich der Authentifizierung des Geräts gegenüber dem Provider und bestimmt, ob das Gerät Anrufe tätigen oder mobile Daten nutzen darf. In den meisten (wenn auch nicht allen) Regionen können beispielsweise Notrufe auch ohne SIM-Karte getätigt werden. Das Entfernen einer SIM-Karte aus deinem Handy **verhindert nicht** die Ortung.

Bauarten

Die meisten Menschen, die „Handy“ sagen, meinen ein „Smartphone“, d. h. ein Gerät mit einem Betriebssystem und Apps, die von den Benutzer:innen installiert werden können. Ein „klassisches“ Handy ist die am wenigsten ausgefeilte Art von Mobiltelefon, wie sie in den frühen Tagen der weit verbreiteten Nutzung von Mobiltelefonen üblich war und mit der mensch nur telefonieren und SMS-Nachrichten versenden konnte. Heutzutage sind Featurephones eher selten. Sie liegen irgendwo zwischen Smartphones und klassischen Handys. Sie können über herstellerspezifische Apps wie einen E-Mail-Client oder einen Webbrowser verfügen. Um Featurephones und klassisches Handys zusammen von Smartphones zu unterscheiden, wird der Begriff Tastenhandys[8] für die beiden erstgenannten Bauarten verwendet.

---

[4] Internationale Mobilfunk Ausstattungs-Identität (*International Mobile Equipment Identity*).

[5] Internationale Mobilfunk Teilnehmerkennung (*International Mobile Subscriber Identity*).

[6] Teilnehmer-Identitätsmodul (*Subscriber Identity Module*).

[7] Embedded-SIM, ein direkt in das Gerät integrierter Chip.

[8] *Anm. d. Übersetzers*: Die ursprünglichen Autor:innen verwendeten den Ausdruck *simple phones* („einfache Handys“), um Tastenhandys zu beschreiben. Im Deutschen beschreibt Tastenhandys die äußeren Merkmale und nicht die Funktionen, daher möchte ich hier klarstellen, dass die Verwendung des Begriffs Tastenhandy in diesem Zine „nicht-Smartphone“ bedeutet und nicht unbedingt, dass es Tasten hat.

Smartphones

Smartphones verfügen in der Regel über einen Ortungsdienst, mit dem das Handy hochpräzise Echtzeit-Standortdaten für Apps, insbesondere Karten, bereitstellen kann. Der Ortungsdienst nutzt die von GPS-[9] oder GLONASS-Satelliten[10] empfangenen Signale, um die Position des Handys zu triangulieren. Die meisten Handys verwenden A-GPS[11], das empfangene Sendemasten-Signale, WiFi-Signale und sogar über das Internet ausgetauschte Daten kombiniert, um die Position des Handys schneller und genauer zu berechnen.

Smartphones enthalten oft auch einen Kompass, einen Beschleunigungsmesser, ein Gyroskop und ein Barometer. Auch ohne GPS oder Multilateralisierung können die Messungen dieser Sensoren kombiniert werden, um den aktuellen Standort aus einer bekannten früheren Standort abzuleiten.

Das bedeutet, dass GPS-Signale zwar passiv von einem Gerät empfangen werden, die Verwendung von Ortungsdiensten jedoch den Standort des Handys übermitteln kann und dass das Deaktivieren von Ortungsdiensten möglicherweise nicht ausreicht, um zu verhindern, dass eine App oder Malware auf deinem Handy deinen Standort grob bestimmt.

Tastenhandys

Viele Aktivist:innen glauben, dass die Verwendung von Tastenhandys anstelle von Smartphones „sicherer“ ist. Da ein Handy ohne GPS oder Ortungsdienst immer noch geortet werden kann, bieten Tastenhandys keinen nennenswerten Schutz vor Standortverfolgung. Bei Featurephones gibt es in der Regel keine weit verbreiteten Text- oder Voice-Chat-Apps, und Tastenhandys verfügen definitionsgemäß nicht über solche Funktionen. Das bedeutet, dass nur unverschlüsselte SMS und Telefongespräche zur Verfügung stehen, die in höherem Maße abhörgefährdet sind, als wenn sie über eine Client-Server- oder End-zu-End-Verschlüsselung verfügen. Tastenhandys, die technologisch am wenigsten fortschrittlich zu sein scheinen, verfügen möglicherweise nur über 2G-Funktionen, was bedeutet, dass Anrufe und SMS mit Geräten im Wert von nur etwa 25 Euro abgehört werden können. Darüber hinaus können viele dieser Geräte über versteckte Internetfunktionen verfügen, die Telemetriedaten an die Hersteller zurücksenden, ohne dass die Nutzer:innen dies bemerken.

---

[9] Globales Positionsbestimmungssystem (*Global Positioning System*), von dem Verteidigungsministerium der Vereinigten Staaten betrieben.

[10] Globales Satellitennavigationssystem, eine von der russischen Roscosmos betriebene Alternativ zu GPS.

[11] Unterstütztes GPS (*Assisted GPS*).

Einfach ausgedrückt: Tastenhandys sind gegen die meisten Bedrohungen, denen die meisten Aktivist:innen ausgesetzt sind, **nicht sicherer als Smartphones.**

Malware

Malware (ein Schadprogramm) ist bösartiges (*malicious*) Software. Es handelt sich um ein Programm, das etwas tut, was du nicht willst, und versucht, seine Aktivitäten zu verbergen. Vom Staat geschaffene Malware[12] hat oft das Ziel, andere Handys oder sogar elektronische Geräte wie WiFi-Router zu überwachen und sich zu verbreiten.

Alte Internet-Sicherheitstrainings besagen, dass Malware durch den Besuch fragwürdiger Websites oder das Öffnen von E-Mail-Anhängen von unbekannten Empfängern installiert wird, und obwohl dies immer noch stimmt, ist die Angriffsfläche deines Handys viel größer. Die meisten, wenn nicht sogar alle, deiner Apps fragen nach Mitteillungen oder warten auf Mitteillungen von z. B. Google Play Services und stellen dann Anfragen an die Server der App. Einige Malware sind Zero-Click, d. h. sie erfordern keine Benutzerinteraktion. Die Spyware Pegasus der NSO Group beispielsweise nutzte einen Zero-Click-Exploit und zielte auf Aktivist:innen, Journalist:innen und Politiker:innen ab. Malware kann auf unsere Handys installiert wird, selbst wenn du nur vertrauenswürdige Apps verwenden und nur (wissentlich) Nachrichten von vertrauenswürdigen Kontakten akzeptierst.

Manche Malware verbleibt nur im Arbeitsspeicher eines Handys, solange das Handy eingeschaltet ist, und ist nicht in der Lage, über Neustarts hinweg zu bestehen. Aus diesem Grund missbraucht manche Malware die Abschaltroutine des Handys und führt eine falsche Abschaltung durch. Dennoch kann ein regelmäßiger Neustart des Handys Malware beseitigen.

Wenn du glaubst, dass dein Handy kompromittiert wurde, musst du Malware-Spezialist:innen aufsuchen, die dir bei die Feststellung helfen, und du musst dich möglicherweise ein neues Gerät zulegen. Malware kommt seltener vor, als du denkst, aber lass dich durch dieses Seltenheit nicht dazu verleiten, legitime Warnzeichen zu ignorieren. Sogenannte Staatstrojaner lassen sich nicht so leicht erkennen wie einfach Malware, so dass die üblichen Methoden möglicherweise nicht anwendbar sind. Du kannst sie leider nicht selbst erkennen.

[12] *Anm. d. Übersetzers*: Oft wird der Begriff „Staatstrojaner“ für alle vom Staat geschaffene Malware benutzt.

Betriebssysteme

Eine der häufigsten Fragen, die Aktivist:innen zu Smartphones stellen, lautet: „Was ist sicherer, iOS oder Android?“ Wie bei allen Sicherheitsfragen lautet die Antwort „Es kommt darauf an.“

Smartphone-Betriebssysteme (*Operating System*, OS) gibt es in zwei Varianten: iOS für Apple-Geräte und Android für alle anderen. iOS ist proprietär mit privatem Quellcode. Android ist ein Basisbetriebssystem mit öffentlichem Quellcode (*Open-Source*), den die Hersteller für ihre Geräte ändern können. Die Android-Betriebssysteme der Hersteller haben in der Regel einen privaten Quellcode. Darüber hinaus gibt es viele Vollversionen von Android, die von der Open-Source-Community entwickelt werden, insbesondere LineageOS,[13] GrapheneOS und CalyxOS sind Open-Source Android-Betriebssysteme, bei denen Datenschutz und Sicherheit im Vordergrund stehen.

Wenn ein Handy eingeschaltet wird, beginnt die Hardware mit dem Laden des Betriebssystems unter Verwendung eines Prozesses, bei dem jeder Schritt die Integrität der für den nächsten Schritt benötigten Software überprüft. Es gibt verschiedene Bezeichnungen dafür, z. B. *Secure Boot* (sicheres Boot[14]) oder *Verified Boot* (verifiziertes Boot). Um ein benutzerdefiniertes Betriebssystem zu installieren, muss dieser verifizierte Boot-Prozess deaktiviert werden, da sich die Hardware sonst weigern würde, das benutzerdefinierte Betriebssystem zu laden, da es nicht durch einen vertrauenswürdigen kryptografischen Schlüssel, der vom Originalhersteller mitgeliefert wurde, signiert ist. Dadurch besteht die Möglichkeit, dass anstelle des echten Betriebssystems ein bösartiges Betriebssystem installiert wird, das deine Daten lesen kann, entweder durch physischen Zugriff oder durch Malware. Das bedeutet jedoch nicht, dass Standard-Betriebssysteme mehr oder weniger sicherer sind als benutzerdefinierte Betriebssysteme. Es bedeutet, dass die Deaktivierung des verifizierten Boots und die Verwendung eines benutzerdefinierten Betriebssystems ein anderes Risikoprofil aufweisen.

Wenn Malware entwickelt wird, zielt sie auf einzelne Geräte oder ein einzelnes Betriebssystem ab. Die Entwicklung von Malware ist kostspielig und zeitaufwändig, und wenn die Malware erst einmal installiert ist, kann es durch Updates der App oder des Betriebssystems entdeckt und daran gehindert werden, neue Geräte zu infizieren.[15] Aus diesem Grund ist es wirtschaft-

[13] LineageOS ist der Nachfolger der beliebten, aber eingestellten CyanogenMod.

[14] *Anm. d. Übersetzers*: *Boot* ist die Abkürzung für *Bootstrap* (Stiefelriemen). Es ist ein Begriff für etwas, das von selbst beginnt (ungefähr).

[15] Darüber hinaus hat Malware die interessante Eigenschaft, dass sie, wenn sie eingesetzt wird, eingefangen und geklont werden kann, so dass andere sie wiederverwenden können.

licher, Malware zu schreiben, die viele Benutzer:innen angreifen kann. Für iOS gibt es eine begrenzte Anzahl von Versionen für eine begrenzte Anzahl von Geräten, während das Android-Ökosystem sehr viel vielfältiger ist. Das bedeutet, dass es für Gegener:inner weniger wirtschaftlich und schwieriger ist, Android-Nutzer ins Visier zu nehmen.

Unsere Empfehlungen lauten wie folgt:

- Für die meisten Personen, die versuchen, Massenüberwachung und weniger motivierte Hacker:innen zu vermeiden, sind iOS oder normales Android ausreichend, da sie am einfachsten zu benutzen sind.
- Personen, die sich stark in sozialen Bewegungen engagieren oder damit rechnen, dass sie individuell überwacht werden, empfehlen wir zum jetzigen Zeitpunkt für ihre organisatorische und politische Arbeit die Verwendung von GrapheneOS ohne Google Play Services, die Verwendung von f-droid als einziges App-Repository und die Installation nur der minimalen Anzahl von Apps, die für die Kommunikation erforderlich sind.
- Für Personen, die die Aufmerksamkeit von Geheimdiensten auf sich gezogen haben oder erwarten, dies zu tun, sollten Handys für alles, was mit Aktivismus zu tun hat, vermieden werden.

Geräteverschlüsslung

iOS und Android bieten die Möglichkeit, deine persönlichen Daten zu verschlüsseln. Dies geschieht unter verschiedenen Namen wie *Data Protection* (Daten-Verteidigung) oder *Device Encryption* (Geräteverschlüsselung). Bei Handys ist die Geräteverschlüsselung in der Regel **nicht** standardmäßig aktiviert. Diese Funktion **muss** vom Benutzer:innen entweder beim Einrichten des Handys oder später in den Einstellungen aktiviert werden. Ebenso muss der Schutz vor übermäßigen Anmeldeversuchen aktiviert werden.

Geräteverschlüsselungsimplementierungen verwenden in der Regel ein Hardware-Sicherheitsmodul (*Hardware Security Module*, HSM) oder einen Sicherheits-Coprozessor,[16] spezielle Chips im Handy, die die Ver- und Entschlüsselung sowie die für diese Vorgänge verwendeten kryptografischen Schlüssel verwalten. Diese Chips sind wichtig, weil sie die Schlüssel vor unbefugtem Zugriff und Manipulationen schützen. Diese Chips können den

Das wäre so, als ob jedes Mal, wenn eine Rakete auf feindlichem Gebiet landet, die Chance bestünde, dass sie sofort kopiert und unendlich vervielfältigt werden könnte, und außerdem wäre es sehr viel wahrscheinlicher, dass dieser bestimmte Raketentyp in Zukunft abgefangen wird. Die Militärs würden zögern, so viele Raketen abzufeuern, und müssten ihre Ziele viel strategischer wählen.

[16] Bei Apple-Geräten wird dieser Chip *Secure Enclave* (sichere Enklave) genannt.

Zugriff von Gegner:innen auf deine Daten verhindern, aber das ist keine Garantie. Das Tool GrayKey—neben anderen—ist in der Lage, Sicherheitslücken in HSMs auszunutzen, und in einigen Fällen kann es das Entsperrungspasswort schnell knacken und die Daten entschlüsseln. In HSMs, die heute vielleicht noch sicher sind, könnten nächsten Monat neue Lücken entdeckt werden, und die Strafverfolgungsbehörden könnten in fünf oder zehn Jahren neue Techniken zur Wiederherstellung von Daten entwickeln. Die Geräteverschlüsselung leistet gute Arbeit, wenn es darum geht, den Zugriff auf deine Daten zu verhindern, wenn ein Einbrecher Zugang zu deinem Handy erhält oder wenn Bullen es bei einer Durchsuchung mitnehmen. Es ist unwahrscheinlich, dass sie den konzertierten Bemühungen staatlicher Geheimdienste wie dem BND, dem MI5 oder dem FBI, auf deine Daten zuzugreifen, standhält.

Ein bekanntes Beispiel dafür ist, dass das FBI das Passwort des Handys des Täters etwa ein Jahr nach dem 2015 Amoklauf in San Bernardino, Kalifornien geknackt hat. Etwa fünf Jahre später wurde aufgedeckt, dass der Zugriff auf die Daten über eine Kette von Sicherheitslücken gegen die Software im HSM erfolgte.

Die Verwendung von Geräteverschlüsselung kann zum Schutz vor Datenerfassung beitragen, aber **der einzige Weg, um sicherzustellen, dass die Daten nicht in die Hände der Strafverfolgungsbehörden gelangen, ist, dass diese Daten gar nicht erst existieren.**

VPNs

Ein virtuelles privates Netzwerk (*Virtual Private Network*, VPN) bezeichnet in dem von den meisten Aktivist:innen verwendeten Kontext eine App, die den Internetverkehr eines Geräts an einen Dienst weiterleitet, dessen Zweck es ist, den Webverkehr und die IP-Adresse des Benutzers vor Netzwerkbeobachtern oder den Servern, mit denen eine Verbindung hergestellt wird, zu verschleiern. VPNs schützen deinen Datenverkehr vor dem Schnüffeln in öffentlichen WiFi-Netzwerken und verbergen deine IP-Adresse vor Servern, mit denen du dich verbindest. Du kannst Ermittlungen in die Irre führen und die passive Überwachung erschweren, aber VPN-Apps können Datenverkehr durchlassen, oder du vergisst, sie zu aktivieren. Der Verkehr zu und von deinem VPN-Anbieter kann von staatlichen Geheimdiensten, die den gesamten Internetverkehr einsehen können, korreliert werden, und dein VPN kann rechtlich dazu gezwungen werden, Protokolle zu sammeln oder an die Strafverfolgungsbehörden zu übergeben. VPNs sind billig und können die Sicherheit in gewisser Weise verbessern, aber mensch sollte sich nicht darauf verlassen, dass sie Anonymität gegenüber dem Staat bieten.

IMSI-Catcher

Ein IMSI-Catcher[17] (Fänger) ist ein Gerät, das einen legitimen Sendemast vortäuscht und Handys dazu bringt, sich mit ihm zu verbinden, um so das Abhören oder das Senden von SMS-Nachrichten oder Anrufen zu ermöglichen. Manchmal ist dieses Spoofing (Verschleierung/Vortäuschung) nachweisbar, aber darauf solltest du dich nicht verlassen. In einigen Regionen kann die Polizei ohne Durchsuchungsbefehl eingesetzt werden, insbesondere bei Demos. IMSI-Catcher funktionieren zum Teil durch Herabstufung des Protokolls auf ein unverschlüsseltes oder unverschlüsselbares Protokoll. Obwohl Smartphones Protokolle bevorzugen, die einen besseren Schutz gegen Abhören und Spoofing bieten, damit die Handys auch in Regionen mit nur 2G funktionieren, und weil dies Teil des GSM-Standards ist, können Smartphones von IMSI-Catchern dennoch auf unsichere Protokolle heruntergestuft werden. Von Smartphones gesendete und empfangene Anrufe und SMS-Nachrichten sind nicht gegen das Abfangen durch IMSI-Catcher geschützt.

Faraday-Taschen

Handys senden und empfangen Informationen per elektromagnetischer Strahlung. Diese Strahlung kann durch spezielle Materialien blockiert werden. Mythen und einige unterstützende Belege besagen, dass Signale blockiert werden können, indem mensch ein Handy in eine oder mehrere Kartoffelchips-Tüten mit Folienauskleidung steckt, aber darauf—wie auf viele andere Gegenmaßnahmen—sollte mensch sich nicht verlassen. Es kann eine speziell angefertigte Faraday-Tasche erworben werden, mit der sich Telefonsignale zuverlässig blockieren lassen.

Wenn du Handys transportierst und sicherstellen musst, dass sie keine Signale durchlassen, reicht es möglicherweise nicht aus, sie auszuschalten. Bei den wenigsten Smartphones können die Batterien entfernt werden. Wenn ein Gegenstand in der Tasche auf das Handy drückt, kann die Einschalttaste betätigt werden. Malware kann die Abschaltroutine manipulieren und verhindern, dass das Handy tatsächlich ausgeschaltet wird, wenn du versuchst, es auszuschalten. Wenn du ein ausgeschaltetes Handy in einen Faraday-Tasche steckst, kannst du verhindern, dass es Signale sendet, und die Wahrscheinlichkeit, dass sein Standort ermittelt werden kann, wird erheblich verringert.

[17] Im Englischen werden die IMSI-Catcher oft unter dem populären Markennamen *StingRay* geführt. *Anm. d. Übersetzers*: In der BRD werden sie in radikalen Kreisen kaum bzw. gar nicht diskutiert, also habe ich keine Ahnung wie/ob mensch sie nennt.

Sicherheitsgrundlagen

Es gibt einige Handypraktiken, die für die meisten Aktivist:innen ratsam sind. Einige davon werden hier beschrieben.

Softwareaktualisierungen

Zweifellos, das Beste, was du tun kannst, um zu verhindern, dass du von den Strafverfolgungsbehörden—oder zufälligen Hacker:innen—gehackt wirst, ist die unverzügliche Installation von Updates für das Betriebssystem deines Handys und allen Apps. Es mag lästig sein, aber viele Updates enthalten Sicherheits-Updates für kritische Schwachstellen. Dies kann zumindest verhindern, dass deine Bank-, Geldtransfer- oder Zahlungskonten geleert werden.

Passwort-Managers

Die zweite nützliche und allgemein anwendbare Sicherheitspraxis ist die Verwendung eines Passwort-Managers (Passwortverwaltungs) für alle deine Konten, einschließlich der auf deinem Handy verwendeten. Es gibt kostenpflichtige Varianten, die die automatische Synchronisierung von Passwörtern zwischen Geräten und die automatische Anmeldung bei Webseiten ermöglichen. Diese erfordern jedoch ein bisschen Vertrauen in das Unternehmen, das das Produkt anbietet. Es gibt kostenlose Alternativen wie KeePassX, die jedoch nicht besonders benutzerfreundlich sind wie die kostenpflichtigen Produkte. Wenn du einen Passwort-Manager verwendest, sollten alle deine Konten sichere, eindeutige und zufällige Passwörter haben. Diese werden in der Regel automatisch von dem Manager generiert. Das Passwort zum Entsperren des Managers sollte eine lange, zufällige Phrase sein.

Menschen sind notorisch schlecht darin, die für Passwörter benötigte Zufälligkeit zu erzeugen, und die Anfangszeile deines Lieblingsgedichts oder einige ausgeklügelte Substitutionsregeln, um `antifaschismus` in `an7if4sc1hsmu5` zu ändern, können von Computern ziemlich leicht geknackt werden. Diceware ist eine Methode zur Erstellung von Passwörtern durch Würfeln und die Auswahl von Wörtern aus einer vordefinierten Liste. Fünf Wörter sind das absolute Minimum, sechs sind besser, aber alles über acht ist übermäßig. Auf diese Weise erhält mensch eine unberechenbare Zufälligkeit, die mensch nicht selbst erzeugen kann, und die mensch sich zudem leicht merken kann. Eine benutzerfreundliche Wortliste in englischer Sprache wird von der EFF bereitgestellt. Die gebräuchlichste deutschsprachige Wortliste von A. G. Reinhold ist eher umständlich, und

stattdessen wird die Liste von dys2p empfohlen.[18,19] Eine Beispielphrase ist `EbensoBatzenTackerBrandSeegang` (bitte **nicht** tatsächlich *diese* Phrase verwenden; mach dir eine eigenen).

Tabelle 1: Auszug aus den Wortlisten

Zahl	**EFF**	**dys2p**
24311	drowsily	erdreich
24312	drudge	erdrosselt
24313	drum	erdrutsch
24314	dry	erdteil
24315	dubbed	erdtrabanten
24316	dubiously	erdulden
24321	duchess	erdumlaufbahn
24322	duckbill	erdwall

Sperren des Handys

Je nach Bedrohungsmodell solltest du die Entsperrung deines Handys erschweren oder nahezu unmöglich machen. Dies ist besonders wichtig, da die Entsperrmethode auch die Entschlüsselungsmethode ist. Eine starke Entsperrmethode schützt also vor unerwünschtem Zugriff auf deine Daten, wenn dein Handy gekapert wird. Im Allgemeinen solltest du Passwörter den PINs oder Mustern vorziehen, da erstere für Maschinen schwieriger zu knacken sind. Du solltest auf jeden Fall die Entsperrfunktion für das Gesicht deaktivieren und eventuell auch die Entsperrung per Fingerabdruck ausschalten. In einigen Regionen sind Passwörter rechtlich geschützt, nicht aber Fingerabdrücke oder andere biometrische Merkmale.

Einige Handys bieten die Möglichkeit, alle Daten zu löschen, wenn es zu viele falsche Entsperrungversuche gibt. Du solltest diese Funktion aktivieren (und das Handy dann von neugierigen Kleinkindern und Haustieren fernhalten).

Deaktiviere Mitteillungen auf dem Sperrbildschirm oder zumindest sie von Apps, die sensible Informationen enthalten könnten. Deaktiviere den Zugriff auf Apps von deinem Sperrbildschirm.

[18] https://github.com/dys2p/wordlists-de

[19] *Anm. d. Übersetzers*: Ich habe diesen Satz im Rahmen der Lokalisierung des Textes in den Absatz eingefügt. Im Original kam er natürlich nicht vor.

Wenn du die Geräteverschlüsselung auf deinem Handy aktiviert hast, sind deine Daten am stärksten geschützt, wenn dein Handy ausgeschaltet ist (oder eingeschaltet wurde, aber dein Entsperrungspasswort noch nicht eingegeben wurde). Nachdem du dein Handy einmal entsperrt haben, sind deine Daten weniger geschützt.

Viele Aktivist:innen lassen die Fingerabdruck-Entsperrung aktiviert, weil sie im Vergleich zur eines Passwort mit 30 oder mehr Zeichen 100 mal Eingeben pro Tag enorm bequem ist. Da das Bedürfnis nach Bequemlichkeit oft über das Bedürfnis nach besserer Sicherheit siegt, ist dies ein weiterer Grund, keine sensiblen Informationen auf deinem Handy zu speichern. Wenn du die Fingerabdrucksperre aktiviert hast, kannst du sie vorübergehend deaktivieren, indem du die Einschalttaste gedrückt hältst. Du kannst dies tun, bevor du mit Strafverfolgungsbehörden interagieren, ins Bett gehen oder dein Handy unbeaufsichtigt lassen.

Drahtlose Funktionen

Du solltest WiFi und Bluetooth deaktivieren, wenn du sie nicht verwendest. Beide können für das *Fingerprinting* (Fingerabdrucken) und die Identifizierung deines Handys verwendet werden. Außerdem vergrößern sie die Angriffsfläche für Hacker:innen, die versuchen, in dein Handy einzudringen. Auch wenn die Risiken, die mit der ständigen Aktivierung dieser Funktionen verbunden sind, minimal sind, können diese Praktiken deine Sicherheit geringfügig verbessern, und wenn du sie nicht brauchst, warum solltest du es nicht tun?

Datensicherung

Smartphones verfügen oft über eine Funktion für automatische Backups in einem mit dem Handy verbundenen Cloud-Konto (bei Apple für iOS und bei Google für Android). Apple hat seine Pläne für verschlüsselte Backups in der iCloud auf Druck des FBI gestoppt, und seine Backups sind unverschlüsselt. Google bietet Ende-zu-Ende-verschlüsselte Backups an, die nach externen Überprüfungen starke Datenschutzgarantien von Google selbst oder den Strafverfolgungsbehörden bieten. Darüber hinaus können einige Apps ihre eigenen Backupdienste anbieten. WhatsApp zum Beispiel kann deine Unterhaltungen auf seinen Servern sichern.

Wir empfehlen, Backups bei Apple zu vermeiden, aber Backups bei Google sind sicher genug, da du ohnehin keine belastenden Beweise auf deinem Handy haben solltest. Data, die an Dritte gesendet werden, können jederzeit verloren gehen oder zerstört werden. Um die Daten zu sichern solltest du darüber nachdenken, sei auf einer verschlüsselten externen Festplatte zu

speichern und diese zu Hause oder an einem sicheren Ort aufbewahren. Damit die Polizei die Daten nicht wiederherstellen kann, sollte die Festplatte verschlüsselt werden.

Chat-Apps

Text- und Sprachnachrichten-Apps bieten sicherere Alternativen zu Telefonanrufen und SMS-Nachrichten.

Verschlüsselung

Chat-Apps bieten eine von zwei Arten der Verschlüsselung.

Bei der **Client-Server-Verschlüsselung** wird der Kanal zwischen einem Client (z. B. deinem Handy) und dem Server verschlüsselt und vor Abhören oder Manipulationen geschützt. Die Nachricht wird entschlüsselt und auf dem Server gespeichert. Wenn die Nachricht von einem anderen Client (z. B. dem Handy einer befreundete Person) angefordert wird, wird sie für die Übertragung erneut verschlüsselt und gesendet.

Bei der **Ende-zu-Ende-Verschlüsselung (E2EE)** erzeugen die Clients kryptografische Schlüssel und tauschen ihre öffentlichen Teile untereinander aus. Die Nachrichten werden mit dem öffentlichen Schlüssel des anderen Clients verschlüsselt und über den Server gesendet, wobei der Server nur als unwissendes Relais fungiert, da die Nachrichten nur von dem anderen Client entschlüsselt werden können.

E2EE bedeutet lediglich, dass ein Server oder eine andere Person, die sich zwischen deinem Handy und dem Handy deines Gesprächspartners befindet, eine Nachricht nicht lesen oder verfälschen kann. Ein:e Gegner:in kann aus den Metadaten Informationen über die Größe der Nachricht, den Zeitpunkt des Versands, den Absender und den Empfänger ableiten.

Einige Chat-Apps bieten nur optionale E2EE an, wie z. B. Telegram mit ihren geheimen Chats, aber diese Funktion ist nicht für Gruppen verfügbar. Bei anderen Apps wie Signal oder Wire ist E2EE obligatorisch, ebenso wie bei iMessage (Apple) und WhatsApp.[20] Bei einigen Apps wie Element ist E2EE standardmäßig aktiviert, kann aber aus Kompatibilitätsgründen mit älteren Clients deaktiviert werden.

Die Sicherheit von E2EE hängt von der Verifizierung der ausgetauschten Schlüssel ab, die häufig durch das Scannen von QR-Codes erfolgt, die einen

[20] Es gibt interessantere *Peer-to-Peer-* (Rechner-Rechner-Verbindung-) Chat-Apps wie Briar und Cwtch, die Metadaten verheimlichen und andere interessante Sicherheitseigenschaften aufweisen, aber sie haben keine große Verbreitung. Sie sind auch nicht für iOS verfügbar, was die meisten Besatzungen daran hindert, sie für sichere Kommunikation zu nutzen.

Fingerabdruck enthalten, der (statistisch) eindeutig dem generierten Schlüssel zugeordnet ist. Bei einigen Apps musst du nur einen Fingerabdruck für alle Geräte verifizieren, bei anderen musst du einen Fingerabdruck für jedes Gerät verifizieren. Einige Apps senden Mitteillungen in der Konversation, wenn sich der Fingerabdruck deines Kontakts ändert, was möglicherweise auf etwas Schändliches hindeutet. Einige Apps tun dies leider nicht. Du **musst** alle Fingerabdrücke für alle Geräte verifizieren, und wenn sich ein Fingerabdruck ändert, **musst du ihn erneut verifizieren**, da sonst deine gesamte Sicherheit zunichte gemacht werden könnte. Außerdem geben einige Chat-Apps die von deinen verifizierten Geräte nicht für andere Geräte frei, und aufgrund dieser schlechten Benutzerfreundlichkeit musst du die Geräte aller deiner Kontakte von jedem deiner eigenen Geräte aus verifizieren.

2B **C6** DE **D5** 12
CF **B0** 69 **10** 56
8C **FB** 1D **8F** 60
B5 **03** 1D **60** B5

Abbildung 1: QR Code und Fingerabdruck

Nutzung

Das Mantra „Benutzt einfach Signal“ wird von Aktivist:innen oft wiederholt, aber es geht fälschlicherweise davon aus, dass alle Menschen identische Bedrohungsmodelle haben. In einigen Regionen kann die Nutzung von Signal durch nationale Firewalls blockiert sein, oder die Nutzung ist so selten, dass sie einen Nutzer als verdächtig einstufen könnte. In Nordamerika und Europa gibt es diese Nachteile im Allgemeinen nicht. Es gibt jedoch allgemeine Beschwerden gegen Signal, z. B. dass eine Telefonnummer für die Registrierung erforderlich ist und dass Kontaktlisten nur auf halbwegs sichere Weise mit dem Server geteilt werden, um die Kontaktsuche und den anfänglichen Schlüsselaustausch zu ermöglichen.

Bei den meisten Chat-Apps werden die Nachrichten beim Empfang entschlüsselt und im Klartext auf dem Gerät gespeichert. Bei einigen Chat-Apps wie Signal kannst du ein Passwort festlegen, um den Zugriff auf die Nachricht zu verhindern, während eine andere Person deiner Handy benutzt, aber dies verschlüsselt sie in keiner Weise erneut. Wenn die Geräteverschlüsselung auf deinem Gerät aktiviert ist, erhältst du einen gewissen Schutz

für diese Nachrichten, wie im Abschnitt über die Geräteverschlüsselung beschrieben.

Da Nachrichten im Klartext gespeichert werden und selbst bei Geräteverschlüsselung wiederhergestellt werden können, solltest du die Funktion zum Verschwindenlassen von Nachrichten aktivieren. Bei einigen Chat-Apps kann ein:e Teilnehmer:in die Funktion „Nachrichten verschwinden lassen“ für alle Teilnehmer:innen des Chats aktivieren. Bei anderen Chat-Apps muss jede:r Teilnehmer:in die Option zum Verschwindenlassen von Nachrichten aktivieren, um sicherzustellen, dass alle Nachrichten schließlich verschwinden. Es kann unpraktisch sein, verschwindende Nachrichten zu haben, da die Suche nach einem Bild, einer Datei oder einer Entscheidung nur bis zu einer Woche oder einem Monat zurück möglich ist. Dies ist vielleicht besser als ein mehrere Jahre langes Protokoll von allem, was mensch gesagt oder gedacht hat, und vor allem von allen Orten, an denen mensch angeblich gewesen ist.

Das bedeutet, dass du Chat-Apps mit obligatorischem E2EE bevorzugen solltest, es sei denn, es gibt einen zwingenden Sicherheitsgrund, der dagegen spricht.

Nicht „einfach Signal benutzen“

Verschiedene Datenschutz-Organisationen und besorgte Aktivist:innen haben hervorragende Arbeit geleistet, um die Akzeptanz von Signal in der breiten Öffentlichkeit und insbesondere bei Aktivist:innen zu fördern. Möglicherweise haben sie das *zu* gut gemacht, denn viele Menschen haben das so verstanden, dass „wenn mensch Signal benutzt, dann ist sie:er total sicher.“ Das hat dazu geführt, dass einige Leute Dinge besprechen, die sie auf keinen Fall über elektronische Medien besprechen sollten, und dann davon ausgehen, dass es in Ordnung ist, weil sie Signal benutzen. Jede Sicherheitsmaßnahme geht von einer Reihe von Annahmen aus, und davon ausgehend kann es akzeptierte Risiken oder Dinge geben, die außerhalb des Anwendungsbereichs liegen. Signal ist sehr gut darin, einen staatlichen Akteur daran zu hindern, eine Massenüberwachung zu nutzen, um den Inhalt von Textnachrichten zu lesen. Es verbirgt sogar einige—aber nicht alle—Metadaten. Andere Chat-Apps haben ein ähnliches Bedrohungsmodell. Wenn dein Handy jedoch durch Malware kompromittiert wird, weil du die Aufmerksamkeit auf sich gezogen hast oder einfach nur Pech hattest, wird Signal nicht verhindern, dass deine Nachrichten gelesen werden.[21]

[21] Darüber hinaus gibt es grausame Sicherheitspraktiken, wie z. B. die Teilnahme an vielen großen Signal-Gruppenchats und die Diskussion ihrer Aktionen, ohne zu überprüfen, wer sonst noch in der Gruppe ist. Es spielt keine Rolle, wie gut die Verschlüsselung

Abbildung 2: Eingabemethode und Pinyin Optionen

Bei einigen Sprachen, insbesondere bei Sprachen, die auf Zeichen statt auf Buchstaben basieren, wird ein Eingabemethoden-Editor (*Input Method Editor*, IME) verwendet, um Sequenzen von lateinischen Buchstaben in die Zeichen der Zielsprache zu konvertieren. Dabei handelt es sich häufig um installierte Apps von Drittanbietern. Signal warnt Nutzer, die IMEs verwenden, nicht ausreichend vor der Möglichkeit, dass ihre Chats von der Software gelesen und an den Staat gemeldet werden könnten, bevor die Nachrichten verschlüsselt werden.

Signal ist keine Garantie für Sicherheit. Das Gleiche gilt für jede andere E2EE-Chat-Apps. Behandel sie nicht als eine.

Auch wenn wir hier starke Kritik an Signal üben, ist diese Kritik auf die Popularität von Signal und die falschen Vorstellungen zurückzuführen. Zum Zeitpunkt des Verfassens dieses Artikels ist Signal immer noch eine der wenigen verschlüsselten Chat-Apps, auf das mensch sich für die Sicherheit verlassen kann.

Anm. d. Übersetzers: Da dieser Text für das Vereinigte Königreich und die USA geschrieben wurde, wäre es nachlässig, wenn ich hier keine speziellen Bemerkungen zur BRD hinzufügen würde. In der BRD (zu oft) stößt Signal auf merkwürdigen Widerstand von Aktivist:innen. Chat-Apps mit schwächeren Sicherheitseigenschaften wie Telegram oder XMPP werden oft bevorzugt, und früher erfreute sich Threema einer gewissen Beliebtheit. Ein Teil davon scheint aus einem grundsätzlichen Misstrauen gegenüber den USA, den Amis und ihrer Technik zu kommen. Kettennachrichten mit dubiosen Behauptungen, wie Signal sei gehackt oder kaputt, machen oft die Runde, und es wird wenig bis gar nicht nachgefasst oder korrigiert. Wenn du glaubst, dass Telegram oder ein selbst-konfiguriertes XMPP-System sicherer ist als die meisten der Bedrohungen, denen wir hier ausgesetzt sind, dann hast du dich gewaltig verrechnet. Überdenk es noch einmal.

---

ist, wenn eines der Gruppenmitglieder ein:e Infiltrator:in oder Spitzel:in ist.

E-Mail

Es gibt Möglichkeiten, die E-Mail-Kommunikation sicherer zu machen, aber E-Mail als Protokoll und Kommunikationsmedium ist generell nicht sicher für private Kommunikation. Boutique- und aktivistenfreundliche E-Mail-Anbieter (d. h. Nicht-Gmail/Nicht-Microsoft/etc.) bieten keine signifikanten Sicherheitsvorteile gegen das Abfangen durch Strafverfolgungsbehörden oder Hacker:innen. Beim Versenden von E-Mails verwenden einige Leute PGP oder S/MIME, aber diese sind schwierig zu benutzen und bieten insgesamt eine schlechte Benutzererfahrung. Zwei Personen, die diese Verschlüsselungsmethoden verwenden, können einen recht guten Schutz gegen das Mitlesen ihrer E-Mails haben, aber ein einziger falscher Klick kann den gesamten Verlauf einer Konversation im Klartext senden, so dass er für die Strafverfolgungsbehörden einsehbar wird. ProtonMail hat kühne Behauptungen über die Verschlüsselung ihrer E-Mails und Clients aufgestellt, und viele Aktivist:innen haben diese Halbwahrheiten dahingehend interpretiert, dass die Nutzung eines ProtonMail-Kontos bedeutet, dass *alle* ihrer E-Mails verschlüsselt sind, was jedoch nicht der Fall ist. E-Mail sollte generell für die Planung und insbesondere für die sichere Kommunikation vermieden werden.

Dennoch ist die E-Mail nach wie vor beliebt, weil jedes Gerät E-Mails senden und empfangen kann und manche Leute „keine Chat-Apps“ nutzen. Für die Koordinierung einer örtlichen Mietervereinigung oder die Einrichtung von Schichten im örtlichen Infoshop ist E-Mail vielleicht ganz gut geeignet. Wenn du sich für die Verwendung von E-Mail entscheidest, geh davon aus, dass die Strafverfolgungsbehörden alle Nachrichten lesen, und beschränke die Konversation auf ein Minimum. Besprich keine illegalen Aktivitäten. Besprich keine Drama der Szene, die vom Staat ausgenutzt werden können.

Schließlich gibt es legitime Anwendungsfälle, in denen E-Mail und PGP ein letzter Ausweg sein können, z. B. ein einmalig verwendbarer verschlüsselter Kanal für jemanden, der auf der Flucht ist, damit er einen zweiten, sichereren Kanal einrichten kann. In solchen Fällen sollten Handys immer noch vermieden werden, da sie sich leicht aufspüren lassen.

Mehrere Identitäten, Mehrere Handys

Je nach deinem Bedrohungsmodell kannst du dich dafür entscheiden, mehrere Handys zu unterhalten, die mit deinen verschiedenen Identitäten mit verschiedenen Decknamen verbunden sind. Du kannst zum Beispiel ein Handy haben, das mit deinem öffentlichen Leben verbunden ist, mit Konten in den sozialen Medien, die du nutzt, um mit deiner Familie in Kontakt zu

treten, und ein zweites Handy mit einer separaten SIM-Karte und separaten Konten, die mit deinem Leben als Aktivist:in verbunden ist. Diese Trennung der Konten ist Teil eines Prozesses, der Kompartmentalisierung genannt wird.

Der erste Vorteil besteht darin, dass die Verwendung unterschiedlicher Geräte für jedes deiner Identitäten verhindert, dass Programmier- oder Benutzerfehler diene privaten Informationen preisgeben. Apps auf deinem Handy können ein unerwartetes Verhalten zeigen, z. B. indem sie deiner gesamten Kontaktliste eine Verbindungsanfrage senden, wenn du dich bei einer neuen Chat-App anmeldeset. Du kannst einen Fehler machen und auf einen Post in sozialen Medien vom falschen Konto aus antworten. Wenn du auf eine E-Mail-Adresse klickst, um einen deiner Identitäten zu verwenden, beginnt das Betriebssystem deines Handys möglicherweise, eine E-Mail mit einem Standard-E-Mail-Client zu verfassen, der mit einem anderen Identität verbunden ist.

Der zweite Vorteil ist, dass dein aktivistisches Gerät auf ein Minimum reduziert werden kann und nur für sichere Kommunikation verwendet wird. Jede App, die du installierst, ist ein möglicher Weg für Malware, auf dein Handy zu gelangen. Wenn dein Handy also nur ein einfaches Betriebssystem und zwei Chat-Apps hat, ist es schwieriger zu kompromittieren.

Die Verwendung mehrerer Handys allein hindert die Strafverfolgungsbehörden nicht daran, deine Identitäten miteinander zu verknüpfen. Wenn du die Handys zur gleichen Zeit bei sich tragen oder an den gleichen Orten benutzen, können sie miteinander verbunden werden.

Als Alternative zu mehreren Handys kannst du das Risiko von Datenverlusten durch Fehler oder unerwartetes Verhalten verringern, indem du mehrere Profile auf deinem Android-Gerät erstellst. Dies schützt dich zwar nicht vor Malware, aber es bietet einen gewissen Schutz.

Einer der häufigsten Anwendungsfälle für mehrere Handys ist das Organisieren einer Gewerkschaft. Einige Unternehmen verlangen die Installation von Apps für die Fernverwaltung, um das geistige Eigentum des Unternehmens zu schützen oder um Sicherheitsverletzungen zu verhindern. Dabei handelt es sich um Spyware-Apps, die dein Handy vollständig kontrollieren können. Abgesehen davon verlangen viele Unternehmen eine Chat-App für die Kommunikation. Du solltest es vermeiden, sich auf Geräten des Unternehmens oder auf Geräten mit installierter Spyware zu organisieren, und du solltest den Unternehmens-Chat nicht für gewerkschaftliche Organisierungsbemühungen nutzen.

Wegwerf-, Demo-, und Einweghandys

Die meisten Menschen sind sich der Bedeutung ihrer Handys bewusst und wissen, dass sie von ihnen geortet werden können oder dass ihr Verlust verheerend sein kann. Eine Reihe von Ansätzen wird von Aktivist:innen—und anderen—verwendet, um ihr Risiko zu verringern, auch wenn sie ihr Risiko oder die Gründe für ihre Gegenmaßnahmen nicht vollständig artikulieren können.

Manche Menschen haben Demohandys oder Wegwerfhandys, die sie zu Aktionen mitnehmen oder beim Grenzübertritt benutzen. Auf diesen Geräten befinden sich nur wenige private Daten, und sie gelten als nicht vertrauenswürdig—wegen der möglichen Installation von Malware—wenn sie von Strafverfolgungsbehörden behandelt werden. Diese Handys werden nicht zur Anonymität verwendet. Sie können eine SIM-Karte mit dem normalen Handy ihres:r Benutzer:in teilen und so verwendet werden, dass die Ortung sie mit dem Wohnort ihres:r Benutzer:in in Verbindung bringt. Demohandys stellen der Polizei weniger Daten und Konten zur Verfügung, wenn sie beschlagnahmt werden. Ein Demo- oder Wegwerfhandy muss nicht unbedingt ein Tastenhandy sein. In vielen Fällen handelt es sich um Smartphones, weil sie ihrem:r Benutzer:in Karten und E2EE-Kommunikation ermöglichen.

Aktivist:innen verwenden fälschlicherweise den Begriff „Einweghandy“ (*burner phone*) für Demohandys, Wegwerfhandys oder Tastenhandys.[22] Ein Einweghandy verdankt seinen Namen der Tatsache, dass es nur zum einmaligen Gebrauch bestimmt ist und danach zerstört wird. Sie werden erworben, wenn der:die Benutzer:in während einer Aktion, die zu einem massiven und konzertierten staatlichen Einsatz führen wird, eine mobile Kommunikation benötigt.

Damit ein Handy als Einweghandy gilt, muss es die folgenden Kriterien erfüllen:

1. Das Handy muss mit Bargeld gekauft werden.[23]
2. Die SIM-Karte, die für das Handy verwendet wird, muss mit Bargeld gekauft werden.

[22] Die Leute scheinen den Begriff „Einweghandy“ zu verwenden, weil er mega-illegal und super-kriminell klingt, und nicht, weil sie tatsächlich die Eigenschaften eines Einweghandys beschreiben.

[23] Der Klau von Handys mit aktivierter SIM-Karte ist im Allgemeinen nicht zu empfehlen, da bei jedem Klau ein zusätzlicher Standortdatenpunkt erzeugt wird, der mit der Aktion in Verbindung gebracht werden kann, die Handys möglicherweise nicht entsperrt werden können und der:die Besitzer:in die Geräte möglicherweise in die von den Provider geführten Sperrlisten aufnehmen lassen, so dass sie nicht zum Telefonieren oder zur Datennutzung verwendet werden können.

3. Das Handy und die SIM-Karte müssen von einem:r Nutzer:in erworben werden, der zu diesem Zeitpunkt keine anderen Handys oder verfolgbaren Geräte bei sich trägt.
4. Das Handy und die SIM-Karte dürfen nur gemeinsam benutzt werden.
5. Das Handy darf niemals an Orte mitgenommen werden, die mit dem:der Benutzer:in verbunden sind, es sei denn, es ist ausgeschaltet und befindet sich in einer Faraday-Tasche.
6. Das Handy darf niemals in der Nähe von nicht Einweghandys oder anderen Geräten benutzt werden, die auf den:die Benutzer:in oder seine:ihre Freund:innen zurückgeführt werden können.
7. Alle Konten auf dem Handy müssen anonym erstellt, nur mit diesem Handy verwendet und dann nie wieder benutzt werden.
8. Das Handy muss für genau eine Aktion verwendet werden.
9. Das Handy darf nur mit anderen Einweghandys oder unbeteiligten Parteien Kontakt aufnehmen (z. B. mit einem Büro oder einem:r Gegner:in, der:die das Ziel der Aktion ist).
10. Das Handy und die SIM-Karte müssen nach der Aktion ausgeschaltet und sofort vernichtet werden.

Erschwerend kommt hinzu, dass manche Handys oder SIM-Karten eine Aktivierung erfordern, entweder durch einen Anruf bei einer Nummer oder durch den Besuch der Website des Providers. Manchmal blockieren diese Websites Verbindungen aus dem Tor-Netzwerk. Die Verwendung eines nicht Einweghandys, um die SIM-Karte zu aktivieren, ist eine offensichtliche Verletzung der erforderlichen Sicherheitseigenschaften. Du musst vielleicht ein Münztelefon finden oder eine fremde Person an einem Bahnhof dazu bringen, dir ihr Handy für ein paar Minuten zu leihen.

Wenn wir sagen, dass ein Einweghandy für eine Aktion verwendet werden kann, meinen wir „eine zeitlich begrenzte Abfolge von Aktivitäten.“ Damit kann eine direkte Aktion gemeint sein, die in nur zwei Stunden durchgeführt wird. Es kann auch die Planung und Koordination im Monat vor einer Aktion sowie die Aktion selbst bedeuten.

Bei besonders vorsichtiger Verwendung kann eine einzelne geschlossene Bezugsgruppe ihren Satz von Einweghandys für wiederkehrende Aktionen wiederverwenden. Wenn dies der Fall ist, müssen die Handys all gleichzeitig verwendet werden, damit sich die verschiedenen geschlossenen Kreisen von Einweghandys nicht überschneiden.

Eine nicht obligatorische, aber dringend empfohlene Eigenschaft ist, dass Einweghandys nicht unmittelbar vor einer Aktion gekauft werden sollten. Dies schafft die zusätzliche Möglichkeit, dass das gespeicherte Sicherheitsmaterial des Kaufs noch zugänglich sein könnte.

Der Versuch, die Existenz des geschlossenen Kreisen zwischen den Handys zu verschleiern, kann dazu beitragen, die Entdeckung der Bezugsgruppe zu verhindern. Ein Schritt besteht darin, sie nicht alle innerhalb eines kurzen Zeitraums zu aktivieren. Eine schrittweise Aktivierung ist bei der Analyse der Daten durch den Staat weniger auffällig. Tätige einige Telefonanrufe von zufälligen Standorten aus an Nummern, die jemand plausibelerweise anrufen würde, aber **sprich nicht**, wenn jemand abhebt. Rufe Nummern an, bei denen lange Wartezeiten zu erwarten sind, z. B. Banken oder Versicherungsfirmen. Rufe einige lokale Geschäfte an, bevor sie öffnen oder nachdem sie schließen. Die gefälschten Anrufe sind möglicherweise unnötig, da viele Nutzer in bestimmten Regionen nie telefonieren und einfach ihren Datentarif für alles nutzen.

Aufgrund der Sorgfalt, mit der ein Einweghandy erworben und verwendet werden muss, ist es höchst unwahrscheinlich, dass es die Mühe wert ist. Wenn du glaubst, dass deine Aktion ein Wegwerfhandy erfordert, solltest du auf jeden Fall versuchen, einen Weg zu finden, die Aktion ganz ohne Handys durchzuführen. Um anderen zu verdeutlichen, dass ein Einweghandys diese Eigenschaften haben muss, solltest du den Begriff „Einweghandy“ vermeiden und stattdessen „Demohandy“ oder „Wegwerfhandy“ verwenden.[24]

Kontrollierter Abstieg

In dieser Zine geht es hauptsächlich um ideale Eigenschaften für die sichere Nutzung von Handys, aber oft sind diese Ideale nicht erreichbar. Ein Beispiel dafür ist, wenn mensch mit Leuten organisiert, die sich keine Smartphones leisten können. Die Beschaffung von billigen, Tastenhandys für die Organisation einer Aktion oder sogar für die Koordinierung regelmäßiger Treffen kann einfacher und finanziell überschaubarer sein als das Gleiche mit Smartphones zu tun. Leider bedeutet das Fehlen von verschlüsselten Sprach- und Chat-Apps eine verstärkte Überwachung deiner Nachrichten.

Um zu verhindern, dass der Staat zu viele Informationen über ihre Aktionen erhält, musst du dich auf menschliche Lösungen statt auf technische Lösungen verlassen. Eine Vereinbarung, dass du Zeiten und Orte von Treffen immer nur mit einem Minimum an Informationen besprichst, kann die gesammelten Informationen auf ein absolutes Minimum reduzieren. Ein einfaches Codebuch, in dem gängige Phrasen, die bei der Organisation verwendet werden, durch zufällige, unverfängliche Codephrasen ersetzt werden, kann bei Nachforschungen in die Irre führen, und die Verwendung von Codephra-

[24] *Anm. d. Übersetzers*: Die Begriffe Wegwerfhandy und Einweghandy sind im Deutschen sehr ähnlich, so dass es wahrscheinlich am besten ist, Demohandy in allen Fällen zu verwenden, in denen man weder sein Alltags-Handy noch ein Einweghandy benötigt.

sen kann verhindern, dass automatische Systeme die Behörden alarmieren.

Maßnahmen wie diesem ermöglicht es dir, von einer höheren Sicherheit zu einer geringeren Sicherheit überzugehen, ohne sich vollständig der Überwachung und staatlichen Repression auszusetzen. Diese Methoden erfordern größere Sorgfalt, sind aber machbar.

Einen Plan erstellen

Wir können nicht so tun, als ob wir dein Bedrohungsmodell kennen würden, und wir können nicht auf jede Nuance in jeder Region und Situation eingehen. Was wir tun können, ist, einige Leitlinien aufzulisten, die allgemein anwendbar sind. Wenn du sie liest, musst du für dich überlegen, was praktisch ist. Was kannst du tatsächlich tun? Und was werden die Menschen in deinem sozialen Umfeld tun? Dein neuer Plan muss nicht perfekt sein. Er muss nur besser sein als das, was du jetzt tust. Wenn dies bedeutet, dass du Kompromisse bei der Sicherheit eingehen musst, damit du weiter organisieren kannst, dann kannst du das tun. Aber lass dich auch nicht durch die schlechte Sicherheit anderer gefährden. Finde einen Ausgleich.

Dies ist keineswegs eine vollständige Liste, aber es sind einige Möglichkeiten zur Entwicklung einer persönlichen OpSec und Sicherheitskultur:

- Verwende ein Smartphone, da es gegen die meisten Bedrohungen, denen Aktivisten ausgesetzt sind, sicherer ist als ein Tastenhandy.
- Nimm dein Handy nicht zu Aktivitäten mit, die die Polizei interessieren könnten, und insbesondere nicht zu Demos, bei denen es zu Ausschreitungen kommen könnte.
- Bevorzuge verschlüsselte E2EE-Chat-Apps für die Kommunikation, aktiviere das Verschwindenlassen von Nachrichten und vermeide E-Mails.
- Verwende ein Passwort, um dein Handy zu entsperren, und aktiviere die Geräteverschlüsselung.
- Deaktiviere die Fingerabdruck-Entsperrung deines Handys, bevor du ins Bett gehen oder es unbeaufsichtigt lasst.
- Erstelle regelmäßig Backups von Fotos und anderen Daten auf einer verschlüsselten Festplatte oder USB-Stick und lösche diese von deinem Handy.
- Lösche alte Daten: Direktnachrichten (DMs), Gruppenchats, E-Mails, Kalendereinträge, usw.
- Verlasse Gruppenchats, in denen du nicht anwesend sein musst, und entferne inaktive Teilnehmer:innen aus Gruppenchats.

- Übe, dein Handy zu Hause zu lassen oder es auszuschalten, wenn du Besorgungen machst oder kleine Aktionen durchführst, um dich an die Abwesenheit des Smartphones zu gewöhnen.
- Kläre zu Beginn jedes Plenums, ob elektronische Geräte erlaubt sind oder nicht. Wenn nicht, schaltet sie aus, sammelt sie ein und bringt sie aus dem Gesprächsbereich.

Und vor allem:

Sende keine Nachrichten oder führe keine Telefonate über hochsensible heikle Angelegenheiten. Fotografiere und filme keine belastenden Dinge. Erstelle keine Beweise, die gegen dich oder andere verwendet werden können.

Ungültig, wo verboten

Was hier geschrieben wurde, und auch der Rest dieser Zine, sind Leitlinien. Sie treffen vielleicht nicht auf dich zu.[25] Vor allem die digitale Sicherheit kann besonders auffällige Spuren hinterlassen. Wenn Signal in deiner Region sehr ungebräuchlich ist, könnte seine Verwendung dich zu einer Zielscheibe machen. VPNs können kriminalisiert werden. Die Verwendung von der Tor-Netzwerk kann dir einen Besuch der Polizei einbringen. Das Vorhandensein von Apps für sichere Kommunikation auf deinem Handy könnte deine Verhaftung in ein Verschwinden verwandeln. Bevor du etwas herunterlädst, recherchiere über die Repression in deiner Region, um festzustellen, ob die von uns bereitgestellten Leitlinien dich sicherer machen oder ob sie dich gefährden.

Alternativen

Es ist immer einfacher zu sagen „Mach mal das stattdessen“ als „Tu das nicht,“ und wenn mensch versucht, ein Verhalten oder eine Praxis zu ändern, erhöht das Anbieten von Alternativen die Chancen, dass jemand das alte, unsichere Verhalten aufgibt. Es gibt legitime Gründe, Handys zu haben, und Alternativen können eine geringere Belastung bedeuten, wenn wir unsere Handys aufgeben oder unsere Gewohnheiten ändern.

[25] *Anm. d. Übersetzers*: Da du dies auf Deutsch liest, trifft der Absatz wahrscheinlich nicht auf dich zu, wenn du in der BRD, Österreich oder der Schweiz wohnst. Er kann jedoch zutreffen, wenn du dies in deiner Muttersprache lesen und in einer anderen Region wohnst. Ich sage das, weil ich befürchte, dass bei dem derzeitigen Stand der Sicherheitskultur hier und der extremen Paranoia jemand, der diesen Absatz liest, zu dem Schluss kommen könnte, dass diese ganze Zine nicht für sie:ihn und ihre:seine Genoss:innen gilt.

Ein Hindernis für die Vermeidung von Handys ist, dass die Menschen Informationen haben, Informationen sammeln und Kontaktdaten austauschen wollen. Mit einem Stift und einem Notizblock kannst du die Protokolle deiner Gruppe auf analoge Weise schreiben und später verteilen. Wenn du geschickt bist, kannst du eine Kopie des kryptografischen Fingerabdrucks (Sicherheitsnummer, *Safety Number*) deines Geräts mit dir führen, um eine sichere Verbindung herzustellen, auch wenn du und dein:e Gesprächspartner:in ihre Handys nicht dabei haben. Mit einem Papierkalender kannst du Termine planen. Das Ausdrucken von Papierkarten des Einsatzgebietes einer Aktion kann dir die Orientierung erleichtern. Wenn du Kopien von Informationen auf Papier erstellst, sorge dafür, dass diese umgehend und sicher entsorgt werden, um zu vermeiden, dass eine buchstäbliche Papierspur deiner Aktivitäten entsteht.

Handylose Kontingente

Dein Plan könnte zwar heute funktionieren, aber er muss auch zukunftsorientiert sein. Du kannst dich bei der Organisation stark auf dein Handy verlassen und dabei die Sicherheitsrisiken in Kauf nehmen, aber es könnte eine Zeit kommen, in der Repressionen oder Katastrophen deine Handys oder das Internet lahm legen. Bei verstärkter Repression ist es üblich, dass der Staat den Mobilfunk- oder Internetzugang für ganze Regionen unterbricht. Wenn deine Fähigkeit, dich zu organisieren, und deine Sicherheit davon abhängen, dass fast alle Menschen über Handy und ein funktionierendes Internet verfügen, bist du auf bestimmte Arten des Scheiterns gefasst. Mund-zu-Mund-Propaganda und das sogenannte Turnschuhnetzwerk (*Sneakernet*) sind Ausweichmöglichkeiten, und deine Planung muss die Möglichkeit einbeziehen, dass dies die einzige Möglichkeit ist, Informationen verbreiten.

Fallstudien

Um die vorangegangenen Diskussionen zu konkretisieren, stellen wir eine Reihe von Fallstudien aus unseren Erfahrungen zur Verfügung. Einige dieser Fälle zeigen Personen, die bereits über genauere Bedrohungsmodelle verfügen, und andere, die dies nicht tun. Einige beruhen auf Mythen, andere eher auf überprüfbaren Fakten oder sehr wahrscheinlichen Vermutungen. Wo es Fehler gibt, werden sie diskutiert.

Fall 1: Plena für eine halb-öffentliche Aktion

Szenario

Ein Kollektiv plant eine Besetzung, die bis zu ihrem Beginn geheim gehalten und dann über die sozialen Medien bekannt gemacht wird. Die Planung erfolgt in erster Linie bei Plena in einem örtlichen Kulturzentrum.

Annahmen

Das Kollektiv geht davon aus, dass die Polizei daran interessiert ist, Besetzungen zu verhindern, und die Aktivist:innen möglicherweise überwacht werden. Diese Überwachung umfasst unter anderem Staatstrojaner, die sich auf den Handys der Personen befinden könnte.

Gegenmaßnahmen

Um zu verhindern, dass der Staat die Mikrofone der Handys benutzt, um die Plena aufzuzeichnen, werden die Handys eingesammelt und in einer versiegelten Plastikbox in einem Nebenraum untergebracht.

Analyse

Es ist richtig, dass die Handys durch Malware kompromittiert worden sein könnten, und es kann richtig sein, dass die Verlegung der Handys in einen anderen Raum die Mikrofone bei der Aufzeichnung der Gespräche behindert. Dies könnte überprüft werden, indem mensch eine Aufnahme startet, das Handy in die Box legt und dann ein lautes Gespräch führt, um zu sehen, wie viel mensch versteht. Wenn die Stimmen auch nur annähernd erkennbar sind, könnte mensch mit einer Software zur Audiobearbeitung Ausschnitte davon wiederherstellen.

Wenn das Kulturzentrum nicht regelmäßig nach Mikrofonen oder anderen Abhörwanzen abgesucht wird, können die Gespräche trotzdem aufgezeichnet werden. Wenn das Kollektiv oder andere Kollektive, die das Kulturzentrum besuchen, stark überwacht werden, könnten in nahe gelegenen Gebäuden platzierte Lasermikrofone die Gespräche aufzeichnen.

Wenn Einzelpersonen passiv überwacht werden, könnte die Tatsache, dass ein Treffen stattgefunden hat und wer daran teilgenommen hat, durch die wiederholte Anwesenheit derselben Gruppe von Handy an einem festen Ort mittwochs von 19 bis 21h über viele aufeinanderfolgende Wochen hinweg aufgedeckt werden.

Empfehlungen

Wenn Handys eingesammelt werden, um eine Überwachung zu verhindern, sollten sie auch ausgeschaltet werden. An den Orten, an denen die Han-

dys platziert werden, sollten laute Umgebungsgeräusche herrschen, um die Wahrscheinlichkeit zu minimieren, dass die Handys den Ton der Gespräche auffangen können.

Wenn das Kollektiv glaubt, dass sie wegen Aufruf zu einer Straftat belangt werden könnte, sollte sie die Handys zu Hause lassen oder ausschalten, bevor sie zu den Plena reist. Dies kann noch weiter minimiert werden, indem mensch nicht dieselben Handy zu der Aktion selbst mitbringt.

Wenn ein hohes Maß an Sicherheit erwünscht ist, kann das Abhören des Raums oder die Aufzeichnung durch staatliche Akteure weiter reduziert werden, indem mensch sich an Orten trifft, die nicht mit Aktivismus verbunden sind. Wenn sich das Kollektiv der Einfachheit an einem zentralen bekannten Ort treffen will, sollte zu Beginn des Plenums festgelegt werden, dass nur die aktuelle Aktion (und nichts Illegales) besprochen werden soll.

Fall 2: zufällig mitgehörtes Geschwätz

Szenario

Einige Mitglieder einer Bezugsgruppe treffen sich in einem Park, um Kontakte zu knüpfen, nicht um eine Aktion zu planen. Ihre Handys sind dabei und eingeschaltet, aber ihre Sicherheitskultur beinhaltet, dass sie nicht über vergangene Aktionen sprechen oder Kampfsgeschichten austauschen, da diese belastende Informationen enthalten können.

Annahmen

Die Gruppe geht davon aus, dass die Polizei ihre Gespräche nur abhören will, wenn es um vergangene oder zukünftige illegale Aktivitäten geht. Sie gehen davon aus, dass ihre Alltagsgespräche uninteressant und uninformative sind.

Gegenmaßnahmen

Die Gruppe hat gar keine Gegenmaßnahmen ergriffen, um zu verhindern, dass ihre Gespräche abgehört werden.

Analyse

Wenn die Gruppe bewusst nicht über Pläne oder vergangene Aktionen spricht, dann kann natürlich kein Mikrofon mithören, was nicht laut gesagt wird. Geplante und durchgeführte Aktionen sind jedoch nicht das einzige, was den Staat interessiert. Auch Klatsch und Tratsch, Liebesbeziehungen, soziale Bindungen und sogar die Einstellung von Personen und Organisationen innerhalb eines Milieus zueinander sind wertvolle Informationen. Dadurch kann der Staat genauere soziale Karten erstellen. Wenn der Staat vermutet, dass eine Person in etwas verwickelt war, das er untersucht, und

er weiß, dass diese Person Kompliz:innen hatte, kann die Verwendung von sozialen Karten, die aus zufälligen Gesprächen erstellt wurden, dabei helfen, die Liste der Verdächtig:innen einzugrenzen oder die Mitglieder einer Bezugsgruppe zu ermitteln. Solche belauschten Gespräche können dem Staat Aufschluss darüber geben, wer sich ausgegrenzt fühlt und Ressentiments hegt, so dass diese Personen gezielt als Spitzel:innen angesprochen werden können. Kleine Konflikte können ausgenutzt und aufgeheizte Emotionen zu heftigen Auseinandersetzungen angefacht werden.

Empfehlungen

Unter den Aktivist:innen gibt es einen Generationsunterschied zwischen denjenigen, die sich vor der weit verbreiteten Nutzung von Handys organisiert haben, und denjenigen, die erst nach der Verbreitung von Handys mit der Organisation begonnen haben. Es gibt auch eine weitere Spaltung zwischen denjenigen, die sich mit Tastenhandys vor der Popularität von Smartphones organisiert haben, und denjenigen, die sich immer in einer Welt organisiert haben, in der fast alle ihre Kontakte Smartphones haben. Diese Diskrepanz zeigt sich in der Fähigkeit, Pläne in der Annahme zu machen, dass die anderen Personen keine Handys haben, wie z. B. die Festlegung von Orten und Zeiten mit weniger spontanen Änderungen. Darüber hinaus haben diejenigen, die vor der Einführung von Handys organisiert haben, ein besseres Gespür dafür, wie es war, wenn das Organisieren zunehmend dort stattfand, wo jeder tatsächlich keine Mikrofone dabei hatte.

Wie bereits in dieser Zine erwähnt, ermöglichen uns Smartphones die sofortige Kommunikation und die ständige Verfügbarkeit unbegrenzter Informationen. Dies hat jedoch den Preis, dass es neue Möglichkeiten der Überwachung gibt. Aktivist:innen sollten sich darüber im Klaren sein, dass Handys, die sich in Wohnungen, Autos und sozialen Einrichtungen befinden, möglicherweise weiche Informationen über soziale Gruppen sammeln. Wenn wir empfehlen würden, die Handys häufiger auszuschalten, würden wir vielleicht als Verschwörungstheoretiker:innen oder als unpraktisch belächelt werden. Die sogenannte liberale Demokratie vermittelt die Illusion, dass wir nicht in einem repressiven Polizeistaat leben, aber es gibt viele Fälle, in denen harmlose soziale Kreise und Aktivistengruppen gehackt und überwacht werden, ganz zu schweigen von den radikaleren und engagierten Gruppen.

Wir schlagen nicht vor, dass wir niemals Handys bei uns tragen sollten, aber wir möchten anregen, dass sich jeder bewusster wird, welchen Aufwand der Staat betreibt, um uns zu überwachen, und wie nützlich die Informationen sind, die wir aus zufälligen Gesprächen gewinnen. Es könnte eine

Zeit kommen, in der die Repression zunimmt und wir ihre Präsenz stärker spüren. Um uns auf solche Zeiten vorzubereiten und uns Gewohnheiten anzueignen, die uns in die Lage versetzen, einer solchen Repression zu widerstehen, ist unser Vorschlag eher moderat. Übe dich ab jetzt in erhöhter Sicherheit. Versuche telefonlose Veranstaltungen zu organisieren. Wenn ihr zusammen ausgeht oder wandert, auch wenn ihr sich in einer Kneipe trifft, versucht alle dazu zu bringen, eure Handys zu Hause zu lassen. Gewöhne dich an ihre Abwesenheit. Spüre die Freiheit zu wissen, dass du keine Standortdaten an den Staat weitergibst und dass niemand außer den Anwesenden deine Gespräche hören kann.

Fall 3: Besetzen und Tastenhandys

Szenario

Ein Kollektiv will ein leerstehendes Gebäude besetzen, um die Aufmerksamkeit auf spekulative Immobilieninvestitionen zu lenken und, wenn die Besetzung erfolgreich ist, das Gebäude in eine kostenlose Unterkunft für die Nachbar:innen umzuwandeln, die kürzlich zwangsgeräumt wurden. Ein Team wird im Gebäude sein und die Besetzung durchführen, während andere Teams vor Ort mit dem Staat verhandeln und in den sozialen Medien posten werden.

Annahmen

Die Besetzer:innen sind der Meinung, dass die Polizei ihre Identitäten herausfinden könnte, indem sie sieht, welche Handys innerhalb des Gebäudes kommunizieren, und selbst wenn sie für diese Aktion nicht verhaftet oder strafrechtlich verfolgt werden, könnte dieses Wissen in Zukunft gegen sie verwendet werden.

Gegenmaßnahmen

Um die Wahrscheinlichkeit zu verringern, dass ihre Identitäten in Erfahrung gebracht wird, falls sie während der Aktion nicht verhaftet werden, hat das Besetzungsteam beschlossen, ihre persönlichen Handys nicht mitzunehmen. Sie werden nur ein „Einweghandy“ mitbringen, um mit dem Verhandlungsteam zu kommunizieren, damit sie an den Entscheidungen beteiligt werden können, um Beiträge an das Sozialmedien-Team zu senden und um ein Gefühl der Sicherheit zu haben, anstatt bis zum Ende der Aktion isoliert zu sein. Sie werden ein Handy mit einer SIM-Karte benutzen, die auf keinen ihrer Namen registriert ist, um anonym zu bleiben.

Analyse

Es ist richtig, dass das Kollektiv keine persönlichen Handys in das Gebäude mitnimmt, in dem sie sich aufhält, da sie damit identifiziert werden könnten. Die Polizei könnte dies tun, indem sie nachschaut, welche Handys sich im Gebäude befinden und auf wen sie registriert sind oder wo sie die meiste Zeit verbringen (z. B. wenn der:die Benutzer:in zu Hause schläft). Das Kollektiv bezeichnet das Handy fälschlicherweise als Einweghandy, da seine wiederholte Nutzung dazu verwendet werden kann, es mit dem Kollektiv und Personen in Verbindung zu bringen. Dieses Handy ist eher als Demohandy zu bezeichnen. Da ein Teil des Kollektivs ohne Masken außerhalb des Gebäudes bleibt, ist die Identität des Kollektivs bekannt, auch wenn nicht alle Identitäten des Besetzungsteams bekannt sind. Wenn es sich um ein privates „Einweghandy“ handelt, das eine:r Aktivist:in gehört, und dieses Handy in der Wohnung des:der Aktivist:in eingeschaltet wurde, könnte dies als Beweis dafür dienen, dass der:die Aktivist:in im Gebäude war oder daran beteiligt war.

Das Kollektiv hat die Sicherheitsaspekte bei der Verwendung des Tastenhandys für die Kommunikation mit dem Verhandlungsteam nicht bedacht. Die Polizei könnte einen IMSI-Catcher einsetzen,[26] um die SMS-Nachrichten zu lesen, die zwischen dem Besetzungsteam und dem Verhandlungsteam hin und her geschickt werden. Dies kann der Polizei einen Vorsprung bei den Verhandlungen verschaffen oder ihr die Möglichkeit geben, Uneinigkeit innerhalb des Kollektivs auszunutzen, um eine Räumung leichter zu erzwingen.

Wenn die Polizei jedoch einen derartigen Aufwand betreibt, um die Personen anhand der bei der Besetzung vorhandenen Handys ausfindig zu machen, ist der Drang nach „Recht und Ordnung“ wahrscheinlich so groß, dass die Besetzung selbst nicht einmal mehr eine praktikable Aktion wäre.

Empfehlungen

Die Gründe, warum das Besetzungsteam ein einziges Handy mit in das Gebäude bringen wollte, waren legitim, aber sie hätten ein Demohandy mit einem Wegwerfkonto verwenden sollen, das sie in einer E2EE-Chat-App erstellt haben. Dieses Konto sollte nur mit einem anonymen Konto kommunizieren, das zu den Teams außerhalb des Gebäudes gehört, um zu verhindern, dass das soziale Netzwerk des Kollektivs durchsickert, wenn das Handy beschlagnahmt wird oder die App-Entwickler:innen Daten für diese Konten

[26] *Anm. d. Übersetzers*: IMSI-Catcher werden in der BRD selten eingesetzt. Im Jahr 2017 gab es „nur“ 67 Einsätze, laut Netzpolitik. Gegenwärtig sind sie von geringer Bedeutung als in andere Länder. https://netzpolitik.org/2018/bundesbehoerden-spaehen-immer-oefter-mobiltelefone-aus/

hätten, die später vor Gericht vorgeladen werden.

Fall 4: Tastenhandy + Signal-Desktop

Szenario

Ruben ist ein Aktivist, der sich einem Kollektiv anschließt, von dem er glaubt, dass es wegen seiner regierungsfeindlichen Haltung aktiv überwacht wird. Um zu verhindern, dass Geheimdienste und die örtliche Polizei ihn verfolgen können, benutzt er ein Tastenhandy mit einer SIM-Karte, wenn er unterwegs ist. Da einige Gespräche mit seinem Kollektiv sensibler sind, benötigen sie einen verschlüsselten Chat-App und haben sich für Signal entschieden. Signal erfordert eine Registrierung mit einer Telefonnummer und generiert die ersten kryptographischen Schlüsseln nur bei den iOS- und Android-Apps. Damit die Signal-Desktop-App auf seinem Laptop funktioniert, hat er die SIM-Karte seines Tastenhandy in das Smartphone seiner Freundin eingesetzt, um ein erstes Schlüsselpaar einzurichten, das er mit seiner Desktop-App verknüpfen konnte. Anschließend meldet sich Ruben von seinem Konto in der Signal-App auf dem Telefon seiner Freundin ab.

Annahmen

Rubens Entscheidung, kein Smartphone mit sich zu führen, beruht auf der Überzeugung, dass Smartphones besser auffindbar sind als Tastenhandys. Ruben geht auch davon aus, dass Signal sicherer ist als Telefonanrufe oder SMS, daher nutzt er Signal für einen Teil seiner Kommunikation.

Gegenmaßnahmen

Rubens Entscheidung, ein einfaches Telefon zu verwenden, soll die Standortverfolgung über sein Smartphone minimieren. Seine Entscheidung für Signal-Desktop soll verhindern, dass seine sensiblen Nachrichten an Genoss:innen abgefangen werden.

Analyse

Rubens Standort ist mit einem Tastenhandy in etwa genauso gut zu orten wie mit einem Smartphone. Seine Kommunikation ist unsicherer, weil er nicht die Möglichkeit hat, „Notfall“-Nachrichten an Mitglieder seines Kollektivs zu senden oder von ihnen zu empfangen, wenn er sein Tastenhandy benutzt, und wenn er dies tut, werden sie vom Staat abgefangen und gespeichert. Seine Gegenmaßnahmen gegen die Überwachung haben sowohl für ihn selbst als auch für sein Kollektiv eine Belastung dargestellt, und sie haben ihn nicht wirklich sicherer gegen die Bedrohungen gemacht, denen er ausgesetzt ist.

Empfehlungen

Ruben sollte sein eigenes Smartphone für die allgemeine Kommunikation verwenden. Wenn es Zeiten gibt, in denen er seinen Standort verbergen muss oder seine Gespräche nicht abgehört werden sollen, sollte er sein Handy zu Hause lassen.

Fall 5: Handylose Planung

Szenario

Die Mitglieder einer Bezugsgruppe sind schon so lange in den aktivistisch Bewegungen aktiv, dass sie dem Staat bekannt sind. Sie planen gerade *etwas Großes*. Sie haben ein Verbot, darüber auf elektronischem Methode zu diskutieren, und besprechen es nur persönlich.

Annahmen

Sie gehen davon aus, dass der Staat große Anstrengungen unternehmen würde, um ihre Aktion zu verhindern, und noch größere Anstrengungen unternehmen würde, um sie zu untersuchen, nachdem sie stattgefunden hat. Sie gehen davon aus, dass es möglich ist, dass ihre Elektronik durch staatliche Malware kompromittiert wurde. Sie gehen davon aus, dass sie selbst bei fehlenden Beweisen auf der Liste der Hauptverdächtigen für die Aktion stehen werden, so dass ihr OpSec für die Aktion hieb- und stichfest sein muss.

Gegenmaßnahmen

Wegen der Möglichkeit von Malware behandeln sie ihre elektronischen Geräte als nicht besonders vertrauenswürdig. Wegen der Möglichkeit gezielter Ermittlungen besprechen sie ihre Aktion nicht in ihren Wohnungen, ihren Fahrzeugen oder bekannten Projekte und Räumen, die mit aktivistischen Gruppen verbunden sind. Um Metadaten, die sie miteinander in Verbindung bringen, zu reduzieren, schalten sie ihre Handys aus, bevor sie an ihren Treffpunkten ankommen, und schalten sie erst wieder ein, wenn sie diese verlassen haben.

Analyse

Die Bezugsgruppe hat Recht, wenn sie davon ausgeht, dass sie gezielt überwacht wird, und sie hat Recht, wenn sie ihre Handys wie Spitzel behandelt. Wenn sie ihre Handys ausschalten, verringert sich die Möglichkeit, dass Malware Mikrofone benutzt, um sie auszuspionieren, und es schafft eine gewisse Bestreitbarkeit bezüglich ihrer Standorte während der Plena. Das Fehlen von Informationen kann jedoch im Vergleich zur normalen Handynutzung

ungewöhnlich sein, und wenn alle Handy ungefähr zur gleichen Zeit an einem Ort verschwinden, könnte dies ein Hinweis für den Staat sein, dass während dieser Lücken etwas Bemerkenswertes passiert. Dies könnte ein Anreiz für zusätzliche Überwachungsmaßnahmen sein, wie z. B. das Abhören des Ortes—wenn sie denselben Ort wiederholt benutzen—oder das Entsenden eines Spions in Zivil, der ein Mikrofon trägt und ihnen in das Café oder die Bar folgt, in dem sie sich treffen. Wenn ein Mitglied der Bezugsgruppe gefasst wird, aber bei der Vernehmung nichts sagt, könnte die Polizei außerdem die Telefondaten auf Auffälligkeiten überprüfen. Die Polizei könnte die Daten abfragen, indem sie die entsprechenden Fragen stellt: Welche anderen Handys gingen zu den Zeiten, als dieses Handy ausging, in seiner Nähe aus? Und was taten die Handys unserer anderen Verdächtigen zu dieser Zeit? Dies könnte die übrigen Mitglieder der Bezugsgruppe aufdecken oder Beweise dafür liefern, dass die Mitglieder der Bezugsgruppe die Kompliz:innen der Person waren. Es ist möglich, dass die Polizei nicht daran denkt, diese Fragen zu stellen, oder dass dies nicht zu den Standardmaßnahmen gehört, aber es ist besser, keine Spuren zu hinterlassen.

Empfehlungen

Da sie mit gezielter Überwachung und Ressourcen zur Untersuchung ihrer Aktivitäten rechnen müssen, sollten sie alle elektronischen Geräte zu Hause lassen und für ihre Plena zufällige Orte wählen, die entweder sehr laut oder sehr abgelegen sind.

Fall 6: Handys bei Massenaktionen

Szenario

Isa ist eine Aktivistin, die vor allem an größeren Demos teilnimmt. Obwohl sie selbst nicht radikal ist, hat sie einige Freund:innen, die es sind, und sie weiß im Allgemeinen, was sie tun. Die Faschos haben einen Aufmarsch geplant, und Isa und Freund:innen wollen sich der Menschenmenge anschließen, die ihre geplante Route blockieren will. Um mit ihren Freund:innen in Kontakt zu bleiben und aktuelle Informationen über die Blockaden oder die Änderung der Route zu erhalten, nimmt Isa ihr Alltagshandy mit (das einzige, das sie hat).

Annahmen

Isa hat keine Angst vor einer Verhaftung, denn bei ähnlichen Aktionen in der Vergangenheit, bei denen eine große Menschenmenge, die nicht der klassischen Antifa zuzuordnen ist, die Straßen blockierte, wurden sie von der Polizei lediglich gekesselt oder aus dem Weg geschleppt, bevor sie die Fa-

schos umleiteten. Sie glaubt nicht, dass mensch im Falle ihrer Verhaftung ihr Handy durchsuchen würde, weder legal noch illegal. Sie macht sich auch keine Sorgen um die Standortdaten ihres Handys.

Gegenmaßnahmen

Isa hat keine Gegenmaßnahmen gegen die Erfassung ihrer Standortdaten oder die Beschlagnahmung ihres Handys ergriffen.

Analyse

Bei Massenaktionen kann die Polizei mit Hilfe von IMSI-Catchern feststellen,[27] wer an diesen Demos teilgenommen hat, um Profile zu erstellen. Diese Standortdaten können verwendet werden, um Menschen wegen Ausschreitungen anzuklagen, selbst wenn die Anklagen nicht zu einer Verurteilung führen.

Wenn Isa verhaftet wird, was immer noch passieren kann, wenn die Blockaden zu klein sind oder sie zu den Pechvögeln gehört, die auf der Straße erwischt werden, kann ihr Handy durchsucht werden. Dadurch erfährt die Polizei möglicherweise von ihrem sozialen Netzwerk oder den Aktivitäten ihrer engeren Freund:innen. Dies kann ihre Freund:innen mehr gefährden als sie selbst.

Empfehlungen

Auch wenn Isa nicht mit einer Verhaftung rechnet, sollte sie vorsichtiger mit ihrem Handy umgehen. Sie könnte vereinbaren, sich mit Freunde:innen an einem festen Ort und zu einer festen Zeit vor der Demo zu treffen, so dass sie ihre Handys gar nicht erst mitnehmen müssen, oder wenn sie wirklich Informationen in Echtzeit haben wollen, sollte nur eine Person in ihrer Gruppe ein Handy mitbringen. Ein vorsichtiger Umgang mit ihrem Handy kann ihre radikalen Freund:innen schützen, die sich möglicherweise militanter gegen die Faschos setzen.

Die Wahrscheinlichkeit, dass eines dieser Ereignisse eintritt, ist jedoch gering, und der wahrgenommene Nutzen der Mitnahme eines Handys ist hoch. Das macht diesen Fall zu einem, in dem es für Isa „in Ordnung“ ist, ihr Handy mitzunehmen… bis es plötzlich nicht mehr sicher ist.

---

[27] *Anm. d. Übersetzers*: Immer noch muss ich sagen, dass IMSI-Catcher sind (derzeit) nur selten in der BRD benutzt.

Fall 7: Allgemeine Planung und Kommunikation

Szenario

Ein Kollektiv organisiert legale Demos und verteilt Flyers, in denen für grüne und ökologische Alternativen zum derzeitigen Status quo geworben wird, wie z. B. die Umstellung auf vegane Ernährung, eine bessere Finanzierung der Fahrradinfrastruktur und eine geringere Abhängigkeit von Privatfahrzeugen. Sie verwenden eine E-Mail-Liste, die auf einem Server gehostet wird, der von einigen lokalen Tech-Aktivist:innen bereitgestellt wird.

Annahmen

Das Kollektiv geht davon aus, dass die Polizei generell an Aktivist:innen interessiert ist, dass aber das Kollektiv selbst nicht speziell ins Visier genommen wird. Sie wissen, dass die lokalen Trolle gerne die „Hippie-Kommunisten“ belästigen. Sie wissen auch, dass es andere, militantere grüne Kollektive in ihrer Region gibt und dass Mitglieder ihres Kollektivs in allen möglichen anderen Gruppen sein können.

Gegenmaßnahmen

Das Kollektiv möchte Belästigungen vermeiden, daher halten sie ihre E-Mail-Liste privat und laden nur ein. Sie wollen die Verfolgung durch große E-Mail-Anbieter vermeiden und hosten daher ihre E-Mails selbst.

Analyse

E-Mail-Listen sind sehr beliebt, weil jede:r Zugang zu E-Mail hat, aber es gibt viele verschiedene Chat-Apps, und nicht jeder verwendet die gleichen, so dass Kollektive dazu neigen, weiterhin E-Mail-Listen zu verwenden. Oft geben die Leute an, dass sie nicht genug Speicherplatz auf ihren Handys für weitere Apps haben. Einige Mitglieder von Kollektiven verfügen über geringe technische Kenntnisse und wollen keine anderen Apps erlernen, so dass E-Mail manchmal unvermeidbar ist.

Ökoaktivist:innen weltweit, auch in den sogenannten westlichen Demokratien, werden gezielt überwacht, auch wenn sie nicht an direkten Aktionen teilnehmen. Die E-Mail-Liste selbst zu hosten, mag die Überwachung durch Unternehmen verringern, aber es gibt immer eine Schwachstelle, wenn Daten angefordert werden. Ein großer Provider könnte der Aufforderung nachkommen, ohne das Kollektiv zu benachrichtigen, und während die Techniker:innen, die den Server für das Kollektiv betreiben, sie wahrscheinlich ruhig informieren würden, selbst wenn sie eine Nachrichtensperre hätten, könnte die Polizei diese umgehen, indem sie sich direkt an die Hosting-Firma des

Servers wendet und sie vorlädt. Außerdem haben die Techniker:innen vielleicht nicht die technische Kompetenz eines großen E-Mail-Anbieters, um den Server sicher zu halten oder überhaupt zu bemerken, wenn er von Trollen oder dem Staat gehackt wird.

Empfehlungen

Wenn der Platz auf dem Handy ein Problem ist, sollten die Aktivist:innen ein Backup von ihren Fotos und Videos machen dann sie löschen, um Platz zu schaffen. Dies ist generell eine gute Praxis, um Daten zu sichern, falls das Handy verloren geht oder kaputt geht.

Das Kollektiv sollte idealerweise auf eine verschlüsselte Chat-App umsteigen, aber wenn sie weiterhin E-Mails verwenden, dann nur für die grundlegendsten Details wie Zeiten und Orte ihrer Aktivitäten. Planungen, interne Debatten und wichtige Diskussionen sollten nicht per E-Mail ausgetauscht werden, da diese Informationen dem Staat große Einblicke in das Kollektiv geben können, die zur Störung genutzt werden können.

Fall 8: Underground Raves

Szenario

Ein Kollektiv plant underground Raves im Freien während der Coronavirus-Pandemie. Sie bitten die Leute, Masken zu tragen, und halten dies für ausreichend sicher, was die Verbreitung des Virus angeht. Die Polizei hat ein generelles Verbot von Massenversammlungen verhängt (außer bei der Arbeit und anderen Dingen, die die Kapitalmaschine am Laufen halten).

Annahmen

Der Staat hat aktive Anstrengungen unternommen, um Massenversammlungen aufzulösen (natürlich nur der Arbeiterklasse und den Marginalisierte), aber er wird wahrscheinlich nicht rückwirkend nach Beweisen für diese Versammlungen suchen. Die Polizei ist in der Lage, Telefonortungsdaten in Echtzeit zu sammeln, mit denen sie mehrere hundert Personen an einem abgelegenen Ort aufspüren kann. Die Polizei hat Spitzel:innen, die auf solche Dinge achten, und manche Leute verpfeifen andere gerne, wenn sie von etwas hören, das ihnen nicht gefällt.

Gegenmaßnahmen

Der Rave wird nicht in den sozialen Medien gepostet, und es wird darum gebeten, die Informationen nur auf sicherem Kanäle an weitere Kontakte weiterzuleiten. In der Info werden die Leute gebeten, ihre Handys in den Flugmodus zu schalten, wenn sie sich dem Veranstaltungsort nähern.

Analyse

Die Veranstaltung nicht zu veröffentlichen, ist ein offensichtlich richtiger Schritt, um zu verhindern, dass die Polizei von sich aus davon erfährt. Die Aufforderung, die Informationen nur an vertrauenswürdige Kontakte auf sichere Kanäle weiterzugeben, ist ebenfalls ein guter Weg, um das Risiko zu verringern, aber es genügt eine Person, die eine verkürzte Nachricht mit nur dem Ort und der Uhrzeit weiterleitet, damit die Warnung verloren geht. Selbst wenn das Kollektiv dies weiß, ist es ein Risiko, das es eingehen muss.

Empfehlungen

Es gibt wenig, was das Kollektiv tun kann, um zu verhindern, dass Leute mit eingeschalteten Handys ankommen, und es gibt wenig, was sie tun können, um sicherzustellen, dass die Nachricht nur in den vertrauenswürdigen und sicherheitsbewussten Teilen des sozialen Netzes bleibt. Dies ist ein schwieriges Problem in der Sicherheitskultur, da das Fehlen von OpSec bei einem Bruchteil der Teilnehmer:innen immer noch die ganze Gruppe zu Fall bringen kann, zumal der individuelle Nutzen eines eingeschalteten Handys hoch, das Risiko für den Einzelnen aber gering ist. Die Organisator:innen, die den Rave organisieren und die Ausrüstung mitgebracht haben, müssen am ehesten mit Konsequenzen rechnen. Wenn sich die Menge während einer Razzia zerstreut, werden sie wahrscheinlich keine Konsequenzen zu befürchten haben. Das Beste, was das Kollektiv tun kann, ist zu versuchen, die Leute vor und während der Veranstaltung mit Schamgefühlen davon zu überzeugen, dass ihre Handlungen den Rave für alle ruinieren könnten.

Fall 9: Umgang mit einem schwachen Glied

Szenario

Eine Bezugsgruppe hat es auf Nazis abgesehen, die Menschen in ihrer Community belästigen. Sie haben sich darauf geeinigt, zu ihren nächtlichen Aktionen keine Handys mitzubringen. Felix, eines ihrer aktivsten Mitglieder, hält dies für übertrieben paranoid und weigert sich, sein Handy zu Hause zu lassen.

Annahmen

Die Bezugsgruppe geht davon aus, dass der Staat die Standortdaten des Handys nutzen könnte, um ihre Aktivitäten zu untersuchen. Sie gehen auch davon aus, dass Felix, der sein Handy mitbringt, sie alle in Gefahr bringt.

Gegenmaßnahmen

Um zu verhindern, dass Felix sie gefährdet, haben sie ihre Aktivitäten gestoppt, bis sie eine Einigung mit Felix erzielen können.

Analyse

Felixs Handlungen gefährden die Gruppe, und sie hat Recht, dass sie ihn nicht an ihren Aktionen teilnehmen lassen sollte. Wenn die Gruppe ihre Aktionen vollständig einstellt, könnte ihrer Community noch mehr Schaden zugefügt werden, und das Risiko einer Verhaftung wegen der Handys könnte recht gering sein, je nachdem, wie die Polizei in der Region der Bezugsgruppe ermittelt.

Empfehlungen

Die Bezugsgruppe könnte eine Untergruppe von Mitgliedern bilden, die sich darauf einigen, keine Handys zu Aktionen mitzubringen und ihre Arbeit fortzusetzen. Parallel dazu könnten sie mit Felix arbeiten, um ihm klar zu machen, wie und warum das Mitbringen seines Handys ein unnötiges Risiko darstellt. Sie könnten mit ihm besprechen, dass sein Verhalten ihnen Unbehagen bereitet und dass sein Verhalten nicht nur ihn selbst betrifft. Die Gruppe könnte in der Lage sein, Genoss:innen mit ihm zu bleiben, aber sie müssen ihn vielleicht von geheimen Aktionen ausschließen, wenn er sich weigert, sein Handy zu Hause zu lassen.

Schlussbemerkungen

Technik ist weder gut noch schlecht—zumindest die meisten nicht. Sie ist nicht von Natur aus befreiend oder unterdrückend. Neue Technologien schaffen neue Gelegenheiten, während sie andere ausschließen. Bei Handys ist das nicht anders. Der Zugang zu sofortiger Kommunikation und umfangreichem Wissen in unserer Hosentasche ist unermesslich leistungsfähig, hat aber auch den Preis einer verstärkten Überwachung.

Du denkst vielleicht, dass der Staat dich nicht überwacht, aber wenn du in einer aktivistischen Bewegung aktiv bist—und sei es auch nur in geringem Umfang—dann ist er es mit Sicherheit. Wenn du dich selbst schützt, kannst du deine Freund:innen, Familie oder Genoss:innen schützen, die in die Bewegung involviert sind. Du denkst vielleicht, dass der Staat dein Handy hackt, um die wöchentlichen Plena deines Hausprojekts abzuhören, aber das ist sicherlich nicht der Fall. Maximale Sicherheit zu jeder Zeit ist unerreichbar, und sie anzustreben ist anstrengend.

Nachdem du diese Zine gelesen hast, bist du vielleicht versucht zu sagen: „Aber sie werden mich auf jeden Fall aufspüren.“ Die Überzeugung, dass ein

gewisses Maß an Sicherheit vor äußeren Bedrohungen unmöglich ist, wird als Sicherheitsnihilismus bezeichnet. Menschen, die so denken, schlagen oft einen von zwei Wegen ein. Sie können glauben, dass keine Gegenmaßnahmen funktionieren, also handeln sie weiter und treffen keine Vorsichtsmaßnahmen, was zu einer sich selbst erfüllenden Prophezeiung führt, die mit ihrer Verhaftung endet. Oder sie glauben an die Vormachtstellung des Staates und werden durch Untätigkeit gelähmt. Repression funktioniert nicht nur wegen der Peitsche, die uns trifft, oder des Gefängnisses, in das wir eingesperrt werden, sondern auch wegen der Angst vor diesen Strafen und unserer daraus resultierenden selbst auferlegten Untätigkeit.

Jede Maßnahme, die du ergreifst, kann dich schützen, und viele von ihnen sind so einfach, dass du sie sofort anwenden kannst. Im einfachsten Fall kannst du eine Rasterfahndung vermeiden, indem du einfache verschlüsselte Chat-Apps verwendest und dein Handy bei Demos oder direkten Aktionen zu Hause lasst. Jeder Schritt, den du darüber hinaus gehst, erfordert von deinen Gegner:innen mehr konzertierte Anstrengungen, wenn sie dich überwachen oder stören wollen. Zeit und Ressourcen sind begrenzt, selbst bei den großen Geheimdiensten. Menschen machen Fehler, und Computer gehen kaputt. Deine Gegner:innen sind fehlbar, und du kannst die Menge der Daten, die sie erfassen können, und die Art der Erkenntnisse, die sie daraus gewinnen können, erheblich verringern.

Außerdem setzt der Staat nicht immer die theoretisch maximal möglichen Überwachungsmethoden ein. Nur weil es dem Staat möglich ist, dein Handy zu hacken oder zu verfolgen, macht er das sicher nicht, um dich dabei zu erwischen, wie du nach der Sperrstunde durch die Parks läufst. Selbst in Fällen, in denen der Staat ein Maximum an Überwachung anstrebt, kann es sein, dass er dies auf ungeschickte Weise tut. Dein Bedrohungsmodell sollte die realistisch zu erwartende Reaktion deiner Gegner:innen berücksichtigen, da diese über deine Aktionen Bescheid wissen.

Informiere dich über die Arbeitsweise von Polizei, Faschos und anderen Gegner:innen in deinem Gebiet und entwickle ein Bedrohungsmodell für dich und deine Bezugsgruppe. Diskutiere es ausführlich mit deinen Genoss:innen. Beginne mit ein paar OpSec-Tips und verwandle sie in eine Sicherheitskultur. Fördere ein gemeinsames Verständnis und Praktiken, die zu mehr Sicherheit gegen die Bedrohungen führen, mit denen du wahrscheinlich konfrontiert wirst. Ergreife konkrete Maßnahmen, aber gehe pragmatisch vor. Beginne langsam mit ein paar neuen Dingen, bis sie zur Normalität geworden sind, und baue dann von dort aus auf. Ein Plan ist nur dann gut, wenn mensch ihn auch durchführt, und der Versuch, einer Gruppe viele große Veränderungen auf einmal aufzudrängen, ist in der Regel überwältigend und frustrierend.

Die meisten erfolgreichen Pläne werden schrittweise umgesetzt.

Hüte dich vor Mythen. Aktivistische Räume sind voll davon, und bei der Sicherheit gibt es keine Ausnahme. Frag mal „wie?“ und „warum?“, wenn jemand Behauptungen über Überwachung oder Gegenmaßnahmen aufstellt. Stütze dein Bedrohungsmodell und deinen Sicherheitsplan auf überprüfbare Fakten—oder zumindest auf sehr wahrscheinliche Vermutungen mit entsprechenden Beweisen.

Nutze dieses Wissen, um dich zu schützen, während du die Welt umgestaltest.