Verantwortungsvoller Umgang mit der Smartphones - Ein Diskussionspapier der Roten Hilfe Nürnberg

Am 11. Oktober 2023 kam es zu mehreren Hausdurchsuchungen in Nürnberg. Grund dafür sind Ermittlungen nach §129 StGB„Bildung einer kriminellen Vereinigung“ gegen 6 Personen aus Nürnberg. Das besondere an dem §129, sind die umfangreichen Maßnahmen der Polizei die Beschuldigten als auch deren Umfeld auszuforschen.
Wir als Rote Hilfe Nürnberg wollen die §129 Ermittlungen als Aufhänger nehmen, um eine Diskussion über eine verantwortungsvolleren Umgang mit Smartphones anzustoßen.
Eine Vorbemerkung unsrerseits: Eine vollumfängliche Sicherheit gibt es nicht. Das sollte aber noch lange kein Grund sein, es Ermittlungsbehörden leicht zu machen und sich zu diesem Thema keine Gedanken zu machen. Die Anforderung sollte sein den Aufwand nach oben zu treiben, damit Überwachung möglichst wenig Informationen preisgibt und im besten Fall ins Leere läuft.

1. Kommunikationsdaten

Im Rahmen des §129-Verfahren in Nürnberg wurden über mehrere Monate ein- und ausgehende Anrufe und SMS der Beschuldigten überwacht. Von einer solchen Überwachungsmaßnahme sind alle mitbetroffen, die in dem Zeitraum mit den Beschuldigten per SMS oder Telefonanruf kommuniziert haben. Ziel der Behörden ist es hier Kommunikationsstrukturen auszuforschen, um sich ein umfassendes Bild von sozialen und politischen Beziehungen zu machen.
In den letzten zehn Jahren ist der Umfang an versendeten SMS deutlich zurückgegangen. Die SMS spielt in unserm Alltag nur noch eine untergeordnete Rolle. Der Großteil der Nachrichten wird heute per Messanger verschickt. Das ist kein Wunder, so bieten Messanger wie WhatsApp, Signal, Telegram oder Threema mehr Funktionen als die Standard-SMS. Wir wollen hier gleich darauf hinweisen, dass zumindest Telegram und Whatsapp, das zum Facebook-Mutterkonzern Meta gehört, nicht zur sicheren Kommunikation geeignet sind.
Wir empfehlen aufgrund der weiten Verbreitung die App Signal. Bei Signal ist die Kommunikation zwischen zwei Menschen standardmäßig verschlüsselt. Auch die Kommunikation von Gruppen ist verschlüsselt. Ohne physischen Zugriff auf eines der Geräte oder dass das Smartphone selbst kompromittiert wurde, sind uns keine Fälle bekannt bei dem die Signal-Verschlüsselung versagte. Was bei Nachrichten gut funktioniert, spielt bei Telefonanrufen faktisch keine Rolle. Wir wollen hier den Appell an alle starten: Nutzt auch für das Telefonieren bevorzugt Signal!

2. Aktualität von Systemen

Apple-Nutzer:innen haben es einfach, sie werden sehr lange, auch bei älteren Geräten mit Updates versorgt. Bei Android sieht das anders aus, hier gibt es viele Einschränkungen bei Updates. Nur wenige Hersteller wie z.B. Google und Nokia versorgen ihre Geräte langfristig mit Updates. Bei vielen anderen Herstellern bekommen nur die teuersten Geräte ein paar Aktualisierungen. Das Problem hierbei ist: Keine Software ist sicher, jede Software hat Sicherheitslücken. Werden diese bekannt und sind schwerwiegend, dann werden sie auch ausgenutzt. Über diese Sicherheitslücken kann, z.B. wenn eine manipulierte Website aufgerufen wird/wurde, das Smartphone mit Überwachungssoftware infiziert werden. Viele weitere Szenarien sind hier denkbar.
Für uns als Nutzer:innen muss das Smartphone funktionieren und sollte am besten nicht so viel kosten. Nutzer:innen wollen sich nicht mit technischen Details aufhalten oder mit der Frage wie das Gerät funktioniert . Teilweise werden uralte Smartphone mit völlig unsicheren Systemen immer noch verwendet. Hiermit gefährdet man nicht nur sich selbst, sondern auch jede andere Person mit der man kommuniziert. Für uns als politische Aktivist:innen sollte daher ein aktuelles System der Standard sein.
Beim Verwenden von alternativen Systemen, die auf Android basieren ist Vorsicht geboten. Von der Benutzung des verbreiteten Systems LineageOS raten wir ab, da hier zwar der Datenschutz erhöht

werden kann, aber bei der Installation das verifizierte Booten des Systems ausgehebelt wird und dadurch ein neuer Angriffsfaktor entsteht.
Für eine erhöhte Sicherheit empfehlen wir das auf Datenschutz und Sicherheit ausgelegte, auf Android basierende Betriebssystem GrapheneOS.

3. Bildschirmsperre und Verschlüsselung

Die gängigen Androidsysteme sind heute alle mit einer Speicherverschlüsselung ausgestattet. Das gleiche gilt für Apple iOS. Wenn man ein nicht mehr mit Updates versorgtes Betriebssystem verwendet, kann die Verschlüsselung von Fehlern betroffen sein, die es den Repressionsorganen leichter macht, die Verschlüsselung zu brechen.
Bei Apple Geräten muss man aufpassen, dass das Backup für die Entschlüsselung nicht in der Cloud liegt. Zudem muss man Apple als Unternehmen vertrauen, da der Quellcode von iOS nicht öffentlich zugänglich ist.
Ein weitere Angriffsvektor ist die Methode zum Entsperren des Gerätes. Viele nutzen einen vierstelligen Pin, der beim Starten eingegeben werden muss. Wenn das Gerät läuft wird entweder über Fingerabdruck oder diesen Pin das Gerät entsperrt. Hier nutzt die ganze Verschlüsselung nichts, da der vierstellige Pin nur 10.000 verschiedene Möglichkeiten zulässt. Der Fingerabdruck wurde in der Vergangenheit per Gerichtsbeschluss unter Zwang genommen, damit die Polizei auf das Handy zugreifen konnte. Folglich bieten alle biometrischen Entsperrmethoden, wie z.b: Gesichtserkennung, keine Sicherheit. Eine Wischgeste ist ebenfalls wegen der geringen Komplexität als sichere Authentifizierung abzulehnen.
Es ist sinnvoll ein tatsächliches Passwort, das nicht nur ein paar Zeichen hat, zur Entsperrung des Gerätes zu verwenden. Das klingt ziemlich unattraktiv und aufwendig, vielleicht sogar für Manchen als nicht nutzbar. Wir versichern euch, ihr werdet euch daran gewöhnen. Regeln, was sichere Passwörter sind, findet Ihr hier: https://www.privacy-handbuch.de/handbuch_35a.htm

4. Zusammenfassung

Es ist zwingend notwendig, dass wir uns als politische Aktivist:innen dem Thema Technik-Sicherheit annehmen. Es gehört genauso zu unserem grundlegenden Handwerkzeug wie Texte schreiben oder das Organisieren von Veranstaltungen. Jede:r von uns, jede politische Struktur ist aufgerufen sich mit diesem Thema auseinanderzusetzen, um sich selbst zu schützen.
Wir als Rote Hilfe Ortsgruppe sind gerne ansprechbar, wenn ihr Diskussionsbedarf zu diesem Thema habt.

1. Nutzt Signal zum Telefonieren
2. Benutzt ein aktuelles Betriebssystem auf dem Smartphone
3. Benutzt keinen Fingerabdruck zum Entsperren des Gerätes
4. Benutzt ein echtes Passwort zum Entsperren des Gerätes
5. Nutzt ein starkes Passwort, dass Ihr nirgendwo anders auch verwendet