Berlin, den 28. April 2020

Impulse für eine Corona-App in Deutschland: Anonymität und Quellenschutz gewährleisten

Reporter ohne Grenzen (RSF) begrüßt die Initiative des Bundesgesundheitsministeriums zur Entwicklung einer Bluetooth-basierten Open-Source-App, die datensparsam, anonym und unter der freiwilligen Beteiligung der Nutzerinnen und Nutzer zur Eindämmung des Virus beitragen soll. Zugleich birgt jegliche digitale Lösung Sicherheitsrisiken, die umfänglich geprüft und denen entsprechende technische Vorkehrungen entgegengesetzt werden müssen.

Basierend auf den bisher öffentlich zugänglichen Informationen hat RSF eine erste Einschätzung der derzeitigen Vorschläge vorgenommen und benennt potenzielle Risiken und die Mindestanforderungen an eine solche Lösung, um den journalistischen Quellenschutz im digitalen Raum nicht auszuhöhlen. Anonymität und Schutz vor Überwachung sind nicht nur, aber besonders für Journalistinnen und Journalisten essenziell, die auch in der Corona-Krise in der Lage sein müssen, Missstände und Fehlentwicklungen aufzudecken und dabei ihre Quellen zu schützen.

Mindestanforderungen an eine Corona-Tracing-App

- Eine Corona-App sollte so wenige Daten wie möglich und nur so viele wie unbedingt nötig speichern. Ihre Nutzung muss auf dem Prinzip der Freiwilligkeit beruhen und darf nicht mit wirtschaftlichen oder sonstigen Anreizen verbunden werden.

- Jede Corona-App muss von Anfang an als Open-Source-Software veröffentlicht werden. Dasselbe gilt für Änderungen an der App durch Software-Updates. Nur so können unabhängigen Expertinnen und Experten die Software bewerten und überprüfen, ob sie Anonymität und journalistischen Quellenschutz gewährleistet.

- Alle durch die App gesammelten Daten müssen strikt vor jeder anderen Nutzung durch Geheimdienste, sonstige Behörden oder Unternehmen geschützt werden. Klar benannte Löschfristen müssen essenzieller Bestandteil der Lösung sein; ihre Einhaltung ist von einer unabhängigen Stelle zu prüfen.

- Der Aufbau privater Datenbanken mit temporären Identifikationsnummern (IDs) oder anderen pseudonymen Identifikatoren einer Corona-Tracing-App muss unbedingt verhindert werden.

- Nachträgliche Erweiterungen des Zwecks einer solchen App zum Beispiel zur Kontrolle oder Überprüfung von Ausgangs- und Kontaktbeschränkungen müssen kategorisch ausgeschlossen sein.

- Die von Mobiltelefonen ausgestrahlten Bluetooth Low Energy Beacons dürfen ausschließlich zur Bekämpfung von Infektionsketten genutzt werden. Jede andere Nutzung auch zu kommerziellen Zwecken, der ein Nutzer nicht explizit zugestimmt hat, muss verboten werden.

- Sobald sich die konkreten Sicherheitsrisiken einer Bluetooth-basierten Lösung beurteilen lassen, muss eine sorgfältige und transparente Abwägung der zu erwartende digitalen Sicherheitsrisiken gegen den voraussichtlichen Nutzen der Lösung stattfinden.

Schutzmaßnahmen, um einen Missbrauch als Überwachungstechnologie zu verhindern:

- Maßnahmen, um Missbrauch bei internationalem Einsatz in autoritären Staaten weitestgehend auszuschließen oder zu minimieren.

- Schutz gegen das Auslesen pseudonymer IDs oder anderer Identifikatoren der Tracing-Apps von Telefonen.

- Transparente, zeitliche Beschränkung der Integration der Software-Komponenten zu Contact-Tracing in Betriebssystemen.

Schutzmaßnahmen, um die Freiwilligkeit technisch und rechtlich zu unterstützen und einer Normalisierung entgegenzuwirken:

- Die Zustimmung der Nutzerinnen und Nutzer sollte in Abständen erneut abgefragt werden. Eine Beendigung der Nutzung und Löschung der Daten muss jederzeit möglich sein.

- Keine Verwendung von manipulativen Techniken ("dark patterns") in Benutzeroberflächen der Contact-Tracing-Komponenten.

- Eine Gestaltung von Benutzeroberflächen von Tracing-Apps und Tracing-Optionen in Betriebssystemen, die die Freiwilligkeit der Nutzung dieser Komponenten unterstützt.

- Eine prominent in die Benutzeroberfläche integrierte Aufklärung über Risiken der Technologie.

Mindestanforderungen im Detail

Wie auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Ulrich Kelber unterstreicht Reporter ohne Grenzen die Bedeutung einer auf Freiwilligkeit basierenden Lösung für öffentliches Vertrauen und damit für die Akzeptanz und Wirksamkeit einer Corona-App. Selbst die freiwillige Zustimmung zur Nutzung einer solchen App unterliegt in Krisenzeiten erheblichem sozialen Druck und sollte die gesellschaftliche Verantwortung für die Wahrung von Privatsphäre und den Schutz persönlichster Daten nicht auf einzelne Bürgerinnen und Bürger abwälzen.

Der Wahrung der Anonymität der Nutzerinnen und Nutzer ist höchste Priorität einzuräumen. Sicherheitsfragen ergeben sich vor allem aus der Übertragung und Speicherung temporärer IDs, ob auf einem zentralen Server oder dezentral auf den Telefonen der Nutzenden sowie aus der Infrastruktur zur Meldung bestätigter Corona-Fälle. Insbesondere für Medienschaffende und ihre Quellen ist auch in Zeiten der Corona-Krise von zentraler Bedeutung, dass ein mögliches mobiles Tracing keine Rückschlüsse auf Kontakte oder etwaigen Missbrauch sensibler Daten ermöglicht.

Bei Entwicklung unter Zeitdruck sind Sicherheitslücken oft vorprogrammiert. Aktuell wird dies an der Corona-App der deutschen Telekom deutlich, die es Hackern trotz Verschlüsselung erlaubt, die von einer Ärztin oder einem Arzt übermittelten Corona-Testergebnisse

mitzulesen oder gar zu verfälschen. Umso wichtiger ist es, dass so wenige Daten wie möglich und nur so viele wie unbedingt nötig gespeichert werden.

Um eine unabhängige Prüfung zu ermöglichen und das notwendige öffentliche Vertrauen zu stärken, muss die Implementierung von Beginn an als Open-Source-Software veröffentlicht werden. Dies trifft genauso auf Änderungen an der App durch Software-Updates zu. Nur so lässt sich eine Bewertung und Diskussion durch unabhängige Expertinnen und Experten gewährleisten.

Ebenso müssen die gesammelten Daten strikt vor jeder anderen Nutzung durch Geheimdienste, andere Behörden oder Unternehmen geschützt werden. Klar benannte Löschfristen müssen essenzieller Bestandteil der Lösung sein. Die Einhaltung der festzulegenden Löschfristen und die tatsächliche Löschung der Daten sollten durch eine unabhängige Stelle wie den Bundesdatenschutzbeauftragten überwacht werden.

Des Weiteren fordert Reporter ohne Grenzen ein Verbot der Nutzung der durch Corona-Apps ausgestrahlten IDs zu anderen Zwecken als zur Aufklärung von Infektionsketten. Anbieter mit kommerziellen Interessen verwenden schon heute Tracking-Geräte um anhand von Bluetooth und/oder WLAN-Signalen die Bewegungen von Kundinnen und Kunden in Geschäften und in der Öffentlichkeit zu verfolgen. Der Aufbau von privaten Datenbanken mit temporären IDs ist ein Sicherheitsrisiko und muss in jedem Fall verhindert werden.

Auch denkbare Erweiterungen einer App, zum Beispiel zur Kontrolle oder Überprüfung von Ausgangs- und Kontaktbeschränkungen, müssen kategorisch ausgeschlossen sein.

Zahlreiche politische Vorstöße der letzten Wochen sehen deutlich weitergehende Eingriff in den Datenschutz und Grundrechte vor. Ein klares Bekenntnis aller beteiligten Akteure zu einer auf Freiwilligkeit und Transparenz aufbauenden Lösung ist nun dringend erforderlich.

Kontakt
Lisa Dittmer, Referentin für Internetfreiheit, Reporter ohne Grenzen
Mail: ld@reporter-ohne-grenzen.de
Telefon: +49 30 60 98 95 33 40