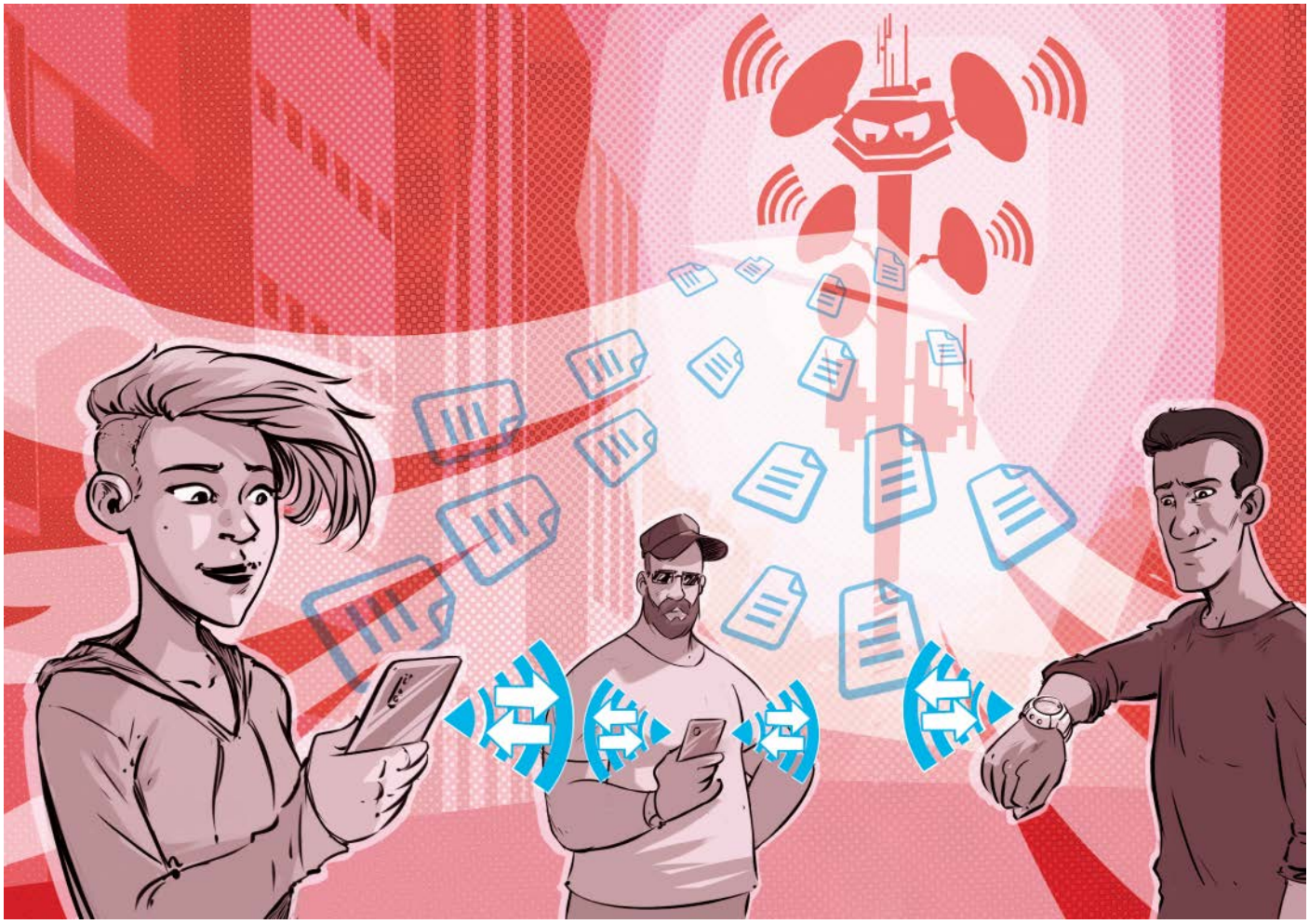

Bild: Albeet Hulm

Angst vorm Großen Bruder

Tracing-Apps zwischen Lebensretter und Überwachungswerkzeug

Die Diskussion um die zentrale oder dezentrale Auswertung der Kontaktdaten von Covid-19-Patienten hat das Vertrauen in Tracing-Apps ramponiert. Die Entwickler der Apps müssen aus den Fehlern lernen, wenn sie mehr Schutz als Unsicherheit verbreiten wollen.

Von Hartmut Gieselmann

Mit ihrer überraschenden Abkehr von einem zentralen Ansatz zur Verarbeitung von Kontaktdaten, die Tracing-Apps über Covid-19-Patienten sammeln, hat die Bundesregierung Ende April einen mutigen Schritt unternommen. Dazu beigetragen hatten unter anderem lautstarke Interventionen von Datenschützern sowie interne Prüfberichte des Bundesamts für Sicherheit in der Informationstechnik (BSI), das laut Tagesspiegel 49 Sicherheitsprobleme in einer Vorabversion der App des Fraunhofer Heinrich-Hertz-Instituts festgestellt hatte.

Nicht zuletzt beharrte Apple darauf, dass seine neuen Programmierschnittstellen für iOS lediglich von staatlichen Apps mit dezentraler Kontaktauswertung genutzt werden dürfen. Ohne diese Schnittstellenfreigabe muss eine App auf einem ungesperrten iPhone immer im Vordergrund laufen. In der Praxis ist so etwas nicht nur unsicher, sondern verringert auch die Akkulaufzeit.

Mit dem Systemwechsel verzögert sich der Start einer offiziellen Corona-Tracing-App in Deutschland mindestens um ein bis zwei weitere Monate. Doch das muss kein Nachteil sein – im Gegenteil. Laut ZDF-Politbarometer waren Ende April nur noch 47 Prozent der Befragten bereit, freiwillig eine Tracing-App einzusetzen. Um die Ausbreitung des Virus kontrollieren zu können, müssten sie nach bisherigen Studien jedoch 60 bis 70 Prozent aller Bundesbürger nutzen.

Um das verlorene Vertrauen zurückzugewinnen, helfen die bisherigen Veröffentlichungen der Projekte. Viele geben ihre Konzepte und Quellcode auf GitHub frei. Die Analysen konzentrierten sich dabei vor allem auf die möglichst anonyme Benachrichtigung der Kontakte von Pati-

enten. Die Zuverlässigkeit solcher Tracing-Apps bei der Entfernungsmessung und die Vermeidung von falschen Warnungen wurde hingegen wenig diskutiert. Dabei sind sie entscheidend, ob ein Anwender einer App vertrauen kann und sie tatsächlich einsetzt.

Suspekter Ultraschall

In Staaten wie Österreich, wo das Rote Kreuz (ÖRK) bereits Ende März eine erste Tracing-App namens „Stopp Corona“ veröffentlichte, wandelte sich die anfängliche Euphorie bald in Misstrauen. Knapp einen Monat später hatten gerade einmal 400.000 von 8,9 Millionen Österreichern die App installiert. Die von Accenture entwickelte App bot anfangs nicht die Funktionen, die sich viele Anwender erhofft hatten. So konnte sie zunächst nur manuelle Handshakes speichern. Dazu wurden Kontakte über die Programmierschnittstelle Google Nearby ermittelt, die neben Bluetooth auch WLAN-Stationen auswertet und Töne im Ultraschallbereich zwischen 18,5 und 20 kHz aussendet. Diese sind zwar von den meisten Menschen nicht zu hören, wohl aber von Mikrofonen anderer Smartphones.

Ultraschallsignale erlauben laut Google einen Informationsaustausch im Umkreis von bis zu 1,5 Metern, wenn noch keine Bluetooth- oder WLAN-Verbindung besteht. Dazu dürfen aber nicht mehrere Smartphones gleichzeitig Signale absetzen und der Lautsprecher darf durch keine Hülle oder Tasche verdeckt sein, die die unhörbar hohen Töne zu stark dämpfen.

Bei der Installation fragte die ÖRK-App die Nutzer um Erlaubnis, auf das Mikrofon zugreifen zu dürfen und Standortdaten zu ermitteln – letztere sind unter Android fest mit der Freigabe von Bluetooth verbunden. Zahlreiche Anwender vermuteten jedoch eine versteckte Abhörfunktion, verweigerten die Freigabe und machten ihrem Unmut mittels 1-Stern-Bewertungen im Play Store Luft. Den Ärger hätten die Macher vermeiden können, wenn sie die Nutzer über die Hintergründe vorab besser aufgeklärt hätten.

Wenig später implementierte Accenture eine automatische Kontakterkennung in der ÖRK-App und nutzte dazu das p2pkit der Uepaa AG aus der Schweiz. Mithilfe von Bluetooth und WLAN-Signalen soll es die Entfernung zweier Smartphones ermitteln. Die App sollte alle Kontakte registrieren, die sich mindestens 15 Minuten in einem Abstand von bis zu zwei Metern aufhielten.

Zahlreichen Kommentaren der Anwender in den App Stores zu urteilen funktionierte das aber nicht zuverlässig. Ein Grund könnte sein, dass das p2pkit der Uepaa AG hoffnungslos veraltet ist. Laut Hersteller-Webseite stammt das letzte Update vom August 2017 und machte schon damals Probleme mit diversen iOS- und Android-Geräten.

Wie wichtig bei der Entfernungsmessung per Bluetooth aktuelle Kalibrierungsdaten von Smartphones sind, zeigten Untersuchungen der Bundeswehr Anfang April in Berlin. Dort wurden 48 Soldaten mit Android-Smartphones ausgerüstet und die Pegelmessungen der Telefone mit realen Abstandsmessungen in verschiedenen Situationen verglichen. Selbst unter diesen Laborbedingungen wurden nur zwei Drittel bis drei Viertel der Abstände richtig erkannt. Bis zu 18 Prozent der gemeldeten Kontakte waren falsch positiv – sie wären bei einer Erkrankung gewarnt worden, ohne in Gefahr gewesen zu sein. Der Einfluss von Fensterscheiben und Wänden wurde im Rahmen der Tests nicht untersucht.

Die inzwischen auf Eis gelegte PEPP-PT-App des Fraunhofer HHI sollte die Entfernung über den Empfangspegel (Received Signal Strength Indication, RSSI) und zusätzlich übertragener Angaben zur aktuellen Sendeleistung (Tx Power), der Empfangsempfindlichkeit (Rx Power) sowie weiterer dynamischer Korrekturparameter ermitteln, die etwa die Ausrichtung und den Bildschirmstatus des Smartphones berücksichtigen. Da sich diese von Gerät zu Gerät und dem aktuellen Akkusparmodus des Betriebssystems stark unterscheiden können, wären hierfür umfangreiche Kalibrierungen einer großen Zahl von Smartphones und Betriebssystemversionen nötig.

Apple könnte die Daten sicherlich für seine überschaubare Zahl an iPhone-Modellen ermitteln. Google will das Tracing rückwirkend bis zu Android 6 erlauben, das im Oktober 2015 auf den Markt kam. Die verschiedenen Hersteller von Android-Smartphones müssten also Updates und Kalibrierungsdaten für bis zu fünf Jahre alte Smartphones bereitstellen.

Warnungen ohne Test

Neben der unsicheren Abstandsmessung kann auch ein zu großer Zeitraum, in dem Kontakte gesammelt und bei einer Ansteckung übermittelt werden, die Zahl der fehlerhaften Warnungen erhöhen. Bislang übertragen die meisten Tracing-Apps bei einer Warnmeldung alle Kontakte der vergangenen zwei bis drei Wochen. Das bedeutet, dass mitunter auch Personen gewarnt werden, die den Patienten lange vor Beginn seiner ansteckenden Phase getroffen hatten. Diese reicht nämlich bis etwa drei Tage vor den ersten Symptomen zurück. Je nachdem, wie schnell sich ein Patient testen lassen konnte und sein Ergebnis erhielt, kann sich der relevante Ansteckungszeitraum von 21 auf bis zu 4 Tage vor der Warnungsversendung verkürzen.

Die Stopp-Corona-App in Österreich will die Zeitspanne genauer ermitteln. Dazu stellt sie den Nutzern drei Fragen zum Befinden und erlaubt ihnen, alle Kontakte der vergangenen 54 Stunden ohne offizielles Testergebnis zu warnen. Da die abgefragten Symptome (Haben Sie Husten, Fieber über 38 Grad?) aber auch auf andere Erkältungskrankheiten und Allergien zutreffen können, lassen sich hier viele voreilige Warnungen ungeprüft absetzen.

Um Missbrauch einzudämmen, müssen die Anwender dabei ihre Telefonnummer angeben. Diese werden auf Azure-Servern von Microsoft für mindestens 30 Tage gespeichert. Falls ein Missbrauch vermutet wird, können die persönlichen

Labortests der Bundeswehr zeigten, dass selbst ohne den Einfluss von Wänden und Scheiben eine korrekte Entfernungsmessung per Bluetooth in einem Viertel bis einem Drittel der Fälle scheitert.

Bild: Torsten Kraatz / Bundeswehr

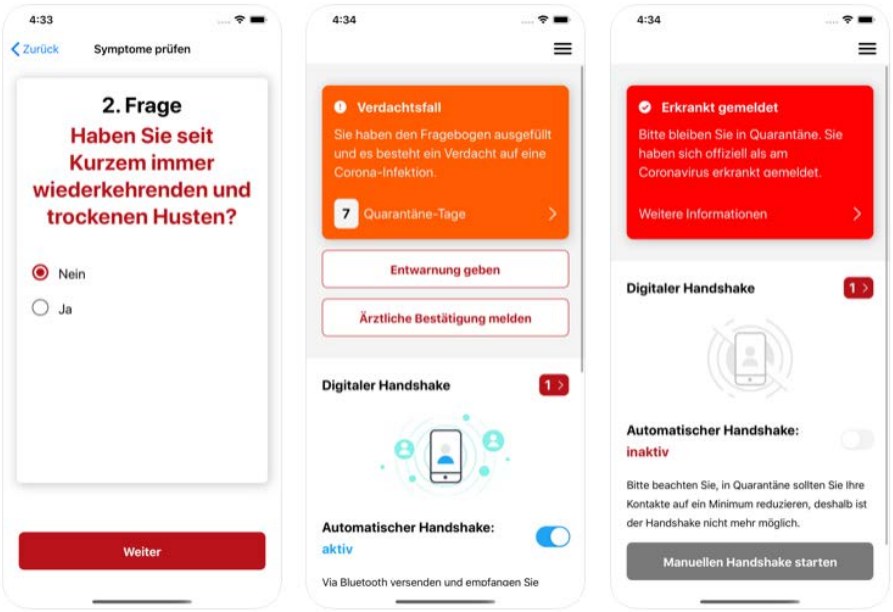

Bild: ÖRK

Die Stopp-Corona-App des Roten Kreuz aus Österreich erlaubt das Verschicken von Warnungen ohne Corona-Test, was zu vielen Falschmeldungen führen kann.

Informationen laut Datenschutzerklärung aber auch bis zu drei Jahre gespeichert bleiben. Unklar ist, ob und in welcher Form Zugriffe auf die Datenbank protokolliert und Nutzer darüber informiert werden.

Umstellung auf DP-3T

Bei ihrer Analyse der Stopp-Corona-App stießen die Prüfer von Epicenter.Works, Noyb und SBA Research auf weitere Probleme. So wechselte die App nicht die ausgesendeten Bluetooth-Kennungen zur Kontaktermittlung. Wer die Kennungen aufzeichnet, könnte Bewegungsprofile der Nutzer erstellen.

Das ÖRK reagierte auf die Kritik und kündigte an, die App auf das schweizerische System von DP-3T umzustellen, sobald dies verfügbar sei. Bei DP-3T wie auch bei dem von Apple und Google vorgestellten System werden die per Bluetooth gesendeten Kennungen nach einiger Zeit ausgetauscht. Hierzu kommt ein komplexes System aus wechselnden Schlüsseln zum Einsatz, die eine Zuordnung der Patienten möglichst gut verschleiern sollen.

Nach den bisher bekannten Entwürfen sollen die Empfänger der Warnungen den Zeitpunkt des Kontakts nicht erfahren, weil sich darüber rückschließen ließe, bei wem sie sich eventuell angesteckt haben. Und wenn Patienten befürchten müssen, dass Fremde sie erkennen und womöglich bedrohen – wie in manchen Ländern geschehen – dann werden sie ihre Kontaktdaten womöglich nicht mehr so freigiebig teilen.

Durch eine starke Anonymisierung wird es für die Empfänger der Kontaktwarnungen jedoch schwieriger, ihre Richtigkeit zu überprüfen. Denn aktuell können sie weder sicher sein, dass die Entfernung per Bluetooth korrekt gemessen wurde, noch, dass der Versender beim Kontakt tatsächlich infektiös war.

Nach den Plänen von PEPP-PT sollte der zentrale Server anhand der Kontaktdaten für jeden Nutzer einen Risikowert berechnen. Erst wenn dieser einen bestimmten Grenzwert überschreitet, sollte er Warnungen verschicken, ohne jedoch den Risikowert mitzuteilen. Über den Algorithmus, der darüber entscheidet, ob sich eine Person in Quarantäne begeben soll, wurde nichts bekannt. Derart essenzielle Informationen fanden wir bislang in keiner Tracing-App.

Eingegrenzter Zeitraum

Um die Quote der falsch positiven Warnungen zu verringern, müsste eine Tracing-App einerseits sicherstellen, dass Warnungen nur nach einer offiziell festgestellten Infektion versendet werden – beispielsweise über die Eingabe einer TAN, die zusammen mit dem Testergebnis verteilt wird. Damit die App dann den Zeitraum der infektiösen Phase berechnen kann, müsste der Patient das Datum eintragen, wann seine Symptome begannen.

Bisher veröffentlichte Entwürfe berücksichtigen eine solche individuelle Berechnung des relevanten Kontaktzeitraums jedoch nicht. Im Gegenteil schlugen manche Entwickler wie etwa die von ROBERT (ROBust and privacy-presERving proximity Tracing) vor, echte Mitteilungen mit weiteren zufälligen Warnmeldungen von Nicht-Infizierten zu kombinieren, um die Identität der Patienten besser zu schützen. Dadurch würde sich die Zahl der falsch positiven Warnungen weiter erhöhen.

Unseriöse Schnellschüsse

Auch wenn zentrale Lösungen wie etwa „Trace Together“ in Singapur oder „COVIDSafe“ in Australien Datenschutzbedenken auslösen, so haben diese Länder verstanden, dass rein automatisierte Benachrichtigungen durch eine App derzeit noch zu fehleranfällig sind. Singapur und Australien nutzten die Kontaktdaten deshalb nur als zusätzliche Informationsquelle für Interviews, bei denen Mitarbeiter der Gesundheitsbehörden die Infizierten zu ihren Kontakten persönlich befragen. Im Gespräch lassen sich offensichtliche Fehler der Apps korrigieren.

Aufgrund der exakten Zeitangabe des Kontakts in der App Corona Go von Wegzwei aus Aachen besteht für infizierte Personen die Gefahr, dass sie identifiziert werden.

Bild: Wegzwei GmbH

Wie das Beispiel Österreich und anderer Länder zeigt, ist die Entwicklung einer zuverlässigen und datenschutzkonformen Tracing-App alles andere als trivial. Da die Daten selbst bei dezentralen Lösungen nicht allein in den Apps verbleiben, genügt die bloße Veröffentlichung des Quellcodes nicht. Darüber hinaus müssen auch alle Datenübertragungen für den Nutzer transparent aufgelistet und die Algorithmen offengelegt werden, die über die Warnungen entscheiden. Unabhängige Experten müssten die Server-Architektur regelmäßig prüfen.

Vorsicht ist deshalb bei Start-ups geboten, die nun wie Pilze aus dem Boden schießen und tagtäglich neue alternative Corona-Apps anpreisen. Sie nutzen die Sehnsucht nach einer wundersamen IT-Lösung für Covid-19 aus, die auf die Schnelle jedoch nicht zu erfüllen ist. Dazu gehört beispielsweise die „geoHealthApp“ der gleichnamigen gGmbH aus Hannover, die Nutzer per GPS überwacht. Derartige Ansätze, die beispielsweise auch in Norwegen zum Einsatz kommen, fallen nicht nur in puncto Datenschutz durch. Sie können Nutzer auch nicht seriös warnen, da GPS-Messungen viel zu ungenau sind. Solche Apps schüren mehr Misstrauen, als dass sie die Gesundheit schützen könnten, und sind deshalb zu Recht mit den Leitlinien der EU zu Tracing-Apps nicht vereinbar. Nicht zuletzt verbietet die Konvention 108+ des Europarats, dass sich Bürger rein automatisierten Entscheidungen unterwerfen müssen.

Keep it simple, stupid!

Weil Fehler zwangsläufig auftreten werden, sollten Telekom und SAP, die die neue offizielle App in Deutschland entwickeln, genügend Zeit für eine Beta-Phase einplanen. Eine zuverlässige Tracing-App braucht die Unterstützung von Apple und Google, damit sie problemlos im Hintergrund läuft und Entfernungen mit einer möglichst kleinen Fehlerquote einschätzt. Zudem muss sie eng mit den Gesundheitsämtern abgestimmt werden, die sicherstellen, dass gewarnte Nutzer telefonisch beraten werden und im Falle eines Fehlalarms schnell eine Entwarnung bekommen. Dazu braucht es genügend Testkapazitäten.

Die Zeit sollte zudem genutzt werden, um juristische Fragen zu klären. Etwa, ob bei einer freiwilligen Nutzung den Anweisungen einer App Folge zu leisten ist, oder ob es rechtliche Konsequenzen hat, wenn man diese ignoriert.

Bis eine offizielle App von Telekom und SAP bereitsteht, lassen sich Kontakte natürlich auch manuell protokollieren. Nach dem KISS-Prinzip (keep it simple, stupid) würde bereits ein Tagebuch helfen, in dem jeder täglich einträgt, wen er in engem Kontakt getroffen hat. Bei einer späteren Infektion kann er die Kontakte den Interviewern vom Gesundheitsamt dann leichter nennen. Dazu braucht es nur einen Bleistift und ein Blatt Papier. *(hag@ct.de)* c't

Studien und White-Paper: ***ct.de/y5uz***