MedWiss.Online

KIT-Experte zu aktuellem Thema: Datenschutz bei Corona-Tracing-Apps

Tracing-Apps sollen dabei helfen, die Ausbreitung des Coronavirus einzudämmen: Ist jemand erkrankt, lassen sich dank der Apps Kontaktpersonen nachvollziehen und warnen. In den vergangenen Tagen ist – mit Blick auf die Frage, wie sicher die Daten der Nutzerinnen und Nutzer sind – eine intensive Debatte zu möglichen zentralen oder dezentralen Lösungen für eine solche Anwendung entbrannt. Die deutsche Bundesregierung hat sich nun auf ein System verständigt, das Daten dezentral speichert – eine Entscheidung, die viele positiv sehen. Professor Thorsten Strufe, Leiter der Forschungsgruppe „Praktische IT-Sicherheit“ am Karlsruhe Institut für Technologie (KIT), und sein Team haben beide Ansätze einander gegenübergestellt und untersucht, wie datenschutzkonform sie wirklich sind.

„Der Unterschied der beiden Ansätze liegt lediglich darin, ob das Prüfen von Kontakten mit Erkrankten dezentral auf den Mobilgeräten oder zentral auf einem Server stattfindet“, erläutert Strufe. Befürworter der dezentralen Lösung argumentierten: Werde ein Nutzer, der nur eine andere Person getroffen hat, anschließend über eine potenzielle Infektion informiert, wisse er ohnehin, wer die infizierte Person sei. Ein zentraler Server hingegen, der die Kontakte zwischen allen positiv Getesteten und potenziell Infizierten berechnet, könne im Zweifel die Informationen aller Benutzer auswerten. **„Der Verlust der Privatheit aller Daten gegenüber einem zentralen Betreiber wird also als viel schwerwiegender eingeschätzt als der Verlust der Privatheit Einzelner gegenüber ihren Kontakten“**, so Strufe, der Professor für praktische IT-Sicherheit ist. **„Unsere Untersuchungen zeigen aber, dass keine der bislang insgesamt diskutierten Lösungen wirklich umfassend die Daten der Nutzerinnen und Nutzer schützt. Keiner der beiden Ansätze, zentral oder dezentral, ist dem anderen grundsätzlich überlegen – für beide kann es aber Lösungen geben, die vollkommen identische Schutzeigenschaften haben.“** Hier gelte es nun, intensiv an der Weiterentwicklung zu arbeiten.

Strufe und sein Team haben untersucht, wie datenschutzkonform verschiedene bisherige Vorschläge sind. Zwar erhoben viele den Anspruch, die Privatsphäre zu wahren, keinem sei dies bislang aber vollständig gelungen. **„Zwar schließen die meisten Vorschläge gewisse mögliche Datenlücken aus, lassen dabei allerdings andere außer Acht“**, so Strufe.

Die Wissenschaftlerinnen und Wissenschaftler haben zunächst den Begriff der Privatsphäre modelliert, um anhand dessen die verschiedenen App-Ansätze zu untersuchen. **„Eins ist klar: Gewisse Informationen muss die App sammeln – beispielsweise wer wann andere Personen für wie lange trifft“**, sagt Strufe. Dabei gelte es aber zu verhindern, dass Gesundheitszustände, Aufenthaltsorte, soziale Interaktionen oder Gewohnheiten der Personen an neugierige Benutzer, Dienstanbieter oder externe Dritte durchsickern.

Trotzdem sieht er die Tracing-App unter bestimmten Voraussetzungen als Option: **„Zum einen wäre ein System mit ‚Soft Privacy Technologies‘ denkbar, bei dem wir einer Instanz wie dem Robert Koch-Institut über verschlüsselte Kanäle die Daten spenden und darauf vertrauen, dass diese dort zu exakt dem Zweck des Contact-Tracings und zu nichts anderem genutzt werden.“** Dies setze natürlich eine Freiwilligkeit und eine klare, verständliche Einwilligung der Nutzerinnen und Nutzer voraus.

„Zum anderen müssten die App-Entwickler einen Schritt zurückgehen. Bisher hat man den Eindruck, dass es ein Wettlauf unterschiedlicher Initiativen war. Es wäre aber besser, zunächst die notwendige Funktion zu verstehen, die potenziellen Bedrohungen klar zu benennen und anschließend gemeinsam ein umfassend sicheres System zu entwickeln." Dabei gelte es darauf zu achten, dass keine großen Firmen als Treuhänder der Daten auftreten.

Formale Definitionen – wie sie Strufe und sein Team unter anderem für den Begriff „Privatsphäre" aufgestellt haben – erleichterten nicht nur eine systematische Sicherheitsanalyse, sondern machten es auch möglich, verschiedene App-Vorschläge im Hinblick auf den Schutz zu vergleichen, den sie bieten. Dies schaffe die Grundlage für den Entwurf datenschutzfreundlicherer Anwendungen.

Mehr Information:
https://arxiv.org/pdf/2004.07723.pdf