MedWiss.Online

Datenschutzfreundliche Corona-Tracing-App

Das Ermitteln von Kontaktpersonen ist eine der wichtigsten Maßnahmen, um die Ausbreitung des Coronavirus einzudämmen. Tracing-Apps sollen dabei helfen: Mit ihr können diejenigen benachrichtigt werden, die sich in einem definierten Zeitraum in der Nähe der infizierten Person aufgehalten haben. Doch die technische Umsetzung birgt Missbrauchsgefahr und die bisherigen Ansätze schützen nicht in vollem Umfang die Privatsphäre. Wissenschaftler des Karlsruher Instituts für Technologie (KIT) und des FZI Forschungszentrums Informatik, eines Innovationspartners des KIT, haben jetzt einen Vorschlag für eine App gemacht, welche die Vorteile von zentralem und dezentralem Ansatz kombiniert und so höheren Datenschutz bietet. Die Ergebnisse haben sie in einem Technical Report veröffentlicht.

In den vergangenen Wochen ist eine intensive Diskussion um mögliche zentrale oder dezentrale Lösungen für Tracing-Apps und ihre Datensicherheit entbrannt. Dabei geht es vor allem auch um die Frage, ob diese Ansätze die Privatsphäre der Nutzerinnen und Nutzer ausreichend schützen. Einen dualen Ansatz, der einen stärkeren Datenschutz auch gegenüber aktiven Angreifern garantiert, haben deshalb jetzt Wissenschaftler des Kompetenzzentrums KASTEL am KIT und des Kompetenzzentrums IT-Sicherheit am FZI erarbeitet.

Kombination von zentraler und dezentraler Lösung

„Um die Risiken für die Privatsphäre am Coronavirus erkrankter Personen möglichst auszuschließen, sollte es zum einen kein zentrales Register von allen Infizierten geben, zum anderen sollten Nutzerinnen und Nutzer des Systems bei einer Warnung keine Rückschlüsse darauf ziehen können, wer tatsächlich krank ist“, sagt Professor Thorsten Strufe, Leiter der Forschungsgruppe „Praktische IT-Sicherheit“ am KIT. „Dies erreichen wir, indem wir die Tracking-Informationen aufteilen: zum einen in die, die für die Warnung der Nutzerinnen und Nutzer verwendet werden, zum anderen in die, die für das Tracking selbst benötigt werden.“ Außerdem sollten die Daten auf mehrere unabhängige Server verteilt werden, die jeweils nur eine geringe Menge an sensiblen Informationen erhielten.

Die Wissenschaftler wollen die Daten, wie bei den bisherigen dezentralen Ansätzen, lokal auf den Mobiltelefonen speichern und sie dann nur im Fall der positiven Diagnose auf zentrale Server laden. „Auf den Servern findet dann auch der Abgleich der Kontaktpersonen statt. So können wir verschleiern, wer infiziert ist. Dies ist bei einem rein dezentralen Konzept nicht möglich“, so Jörn Müller-Quade, Professor für Kryptographie und Sicherheit am KIT und Direktor am FZI. „Gleichzeitig haben wir den Server aufgeteilt, sodass keine einzelne Partei allein irgendwelche sensitiven Informationen abgreifen kann. Dabei könnte beispielsweise ein Server vom Robert Koch-Institut und andere von großen Firmen betrieben werden.“ Selbst wenn alle diese Server kompromittiert seien, erreiche das Verfahren immer noch die gleichen Sicherheitseigenschaften wie die bisherigen Ansätze – solange sie nicht böswillig miteinander kooperieren.

Schutz gegen unnötige und gefälschte Warnmeldungen

Der Vorschlag der Wissenschaftler beinhaltet außerdem, dass der Anwender beispielsweise gegenüber medizinischen Fachleuten sicher beweisen kann, dass er Kontakt mit einer erkrankten

Person hatte, um sich auf COVID-19 testen zu lassen. Ohne diese Funktion könnte jeder einen Test fordern, indem er einen Screenshot einer Warnung von einem fremden Smartphone zeigt. Um unnötige und potenziell panikauslösende Warnungen vor Kontakten zu vermeiden, wird die Information über ein Infektionsrisiko erst nach einem bestimmten Zeitraum ausgegeben. So wollen die Wissenschaftler verhindern, dass jemand gewarnt wird, wenn er beispielsweise an einem Auto vorbeigegangen ist, in dem eine infizierte Person saß.

„Unser Ansatz ist praktikabel, skaliert und bietet zusätzliche Sicherheitseigenschaften, die in keinem bisherigen Verfahren realisiert werden konnten“, sagt Müller-Quade. „Einen optimalen Kompromiss zwischen Nutzen, Privatsphäre, Robustheit und Leistung für Anwendungen zu finden, ist allerdings eine heikle Angelegenheit, die weitere Arbeiten zum Datenschutz und zur Sicherheitstechnik sowie eine sorgfältige Prüfung nicht nur durch Wissenschaftler, sondern auch durch die Gesellschaft als Ganzes erfordert.“

Das FZI Forschungszentrum Informatik mit Hauptsitz in Karls-ruhe und Außenstelle in Berlin ist eine gemeinnützige Einrichtung für Informatik-Anwendungsforschung und Technologietransfer. Es bringt die neuesten wissenschaftlichen Erkenntnisse der Informationstechnologie in Unternehmen und öffentliche Einrichtungen und qualifiziert junge Menschen für eine akademische und wirtschaftliche Karriere oder den Sprung in die Selbstständigkeit. Das FZI ist Innovationspartner des Karlsruher Instituts für Technologie (KIT).

Als „Die Forschungsuniversität in der Helmholtz-Gemeinschaft“ schafft und vermittelt das KIT Wissen für Gesellschaft und Umwelt. Ziel ist es, zu den globalen Herausforderungen maßgebliche Beiträge in den Feldern Energie, Mobilität und Information zu leisten. Dazu arbeiten rund 9 300 Mitarbeiterinnen und Mitarbeiter auf einer breiten disziplinären Basis in Natur-, Ingenieur-, Wirtschafts- sowie Geistes- und Sozialwissenschaften zusammen. Seine 25 100 Studierenden bereitet das KIT durch ein forschungsorientiertes universitäres Studium auf verantwortungsvolle Aufgaben in Gesellschaft, Wirtschaft und Wissenschaft vor. Die Innovationstätigkeit am KIT schlägt die Brücke zwischen Erkenntnis und Anwendung zum gesellschaftlichen Nutzen, wirtschaftlichen Wohlstand und Erhalt unserer natürlichen Lebensgrundlagen. Das KIT ist eine der deutschen Exzellenzuniversitäten.