MedWiss.Online

Corona-Warn-App: Einschätzungen von Experten des SICP – Software Innovation Campus Paderborn

Im Kampf gegen das Corona-Virus hat die Bundesregierung die Corona-Warn-App entwickelt. Sie soll dabei helfen, Menschen, die Begegnungen mit einer mit COVID-19 infizierten Person hatten, schnellstmöglich über die Begegnung zu informieren, Kontaktketten frühzeitig zu unterbrechen und somit weitere Infektionen zu verhindern. Die App zielt auf eine neue Technologie der Verbindung mit Bluetooth ab, bei der ein Austausch anonymer ID-Schlüssel zwischen den Mobiltelefonen stattfindet.

Die Corona-Warn-App wurde von der Deutschen Telekom und dem Software-Konzern SAP entwickelt. Die Unternehmen wurden dabei von der Fraunhofer-Gesellschaft und dem Helmholtz-Zentrum CISPA beraten. Die Warn-App beruht auf dem Konzept der dezentralen Datenverwaltung. Demnach werden Daten nicht auf einem zentralen Server zusammengeführt, sondern lokal auf den Smartphones der Nutzer gespeichert. „Zuvor hatte die Bundesregierung ein zentrales Design bevorzugt. Dieses hätte den Vorteil gehabt, dass dem Robert Koch-Institut die Auswertung anonymer Infektionsdaten erleichtert worden wäre“, erklärt Prof. Dr. Eric Bodden, Direktor des Kompetenzbereichs „Digital Security“ im SICP – Software Innovation Campus Paderborn und Leiter der Fachgruppe „Softwaretechnik” am Heinz Nixdorf Institut der Universität Paderborn. Bodden weiter: „Ebenso hätte man die Risikobewertung, die bestimmt, ob einzelne Personen sich wirklich in Quarantäne begeben sollen, einfacher aufgrund der Datenlage dynamisch anpassen können. Ein solch zentraler Ansatz birgt jedoch die theoretische Gefahr, dass das Robert Koch-Institut als Betreiber der App in Zusammenarbeit mit anderen Bundesbehörden die Daten de-anonymisieren und somit personalisierte Nutzerprofile erstellen könnte. Ob dies realistisch wäre oder nicht, darüber gab und gibt es in der Security-Community durchaus geteilte Meinungen. Aufgrund zahlreicher Proteste von Datenschützern hat man sich jedoch dazu entschieden, stattdessen den dezentralen Ansatz zu verfolgen.“

Damit die Corona-Warn-App auf Smartphones funktioniert, entwickelten die Unternehmen Google und Apple gemeinsam eine Technologie, mit der erkannt werden soll, auf welche Entfernung und über welchen Zeitraum hinweg sich Personen begegnet sind. Ein Austausch der anonymen ID-Schlüssel soll nur erfolgen, wenn sich zwei oder mehrere Personen so nahekommen, dass das Risiko einer Virusübertragung als sehr wahrscheinlich gilt. Hierbei kommen neu geschaffene Schnittstellen in Android und iOS zum Einsatz. Diese generieren speziell verschlüsselte und nur temporär gültige IDs, die auch nur im Infektionsfall entschlüsselt und somit für einen dezentralen Abgleich genutzt werden können. Dadurch scheint ein breit angelegtes Tracking nach aktuellem Stand der Technik realistischer Weise unmöglich.

Ob und inwieweit sich Personen nahegekommen sind, wird über die Signalstärke des Bluetooth-Signals ermittelt. Allerdings könnte die Signalstärke aufgrund verschiedener physischer Bedingungen in die Irre führen. So könnte sie z. B. hoch sein, weil zwei Personen nebeneinandersitzen, obwohl sie durch eine Scheibe voneinander getrennt sind. Ob die App falsche Warnungen in solchen Situationen verhindern kann, werden aktuelle Tests zeigen.

Wurde nun eine Infektion festgestellt, kann man dies auf freiwilliger Basis in der App melden. Um einen Missbrauch der App zu vermeiden, erfolgt die Meldung einer Infizierung nur mit einem

positiven Testergebnis, welches von einem Gesundheitsamt bestätigt wird. Die Nutzer der App müssen regelmäßig prüfen, ob sie in der Vergangenheit Kontakt zu einer infizierten Person hatten. Dazu müssen sie die Daten aktiv von dem Server abrufen, da der Abgleich ausschließlich auf den Smartphones der Nutzer erfolgt.

Da die Installation der App freiwillig ist, wäre man wohl auch eher moralisch als rechtlich verpflichtet, einer Warnung der App, sich in Quarantäne zu begeben, nachzukommen. Letztendlich wird es an jedem Einzelnen liegen, zu entscheiden, inwieweit sie oder er die weitere Eindämmung der Pandemie unterstützen und die vielleicht notwendige Wiedereinführung von Lock Down-Maßnahmen mit verhindern möchte.

Erfahrungen bezüglich der Effektivität von Corona-Tracing-Apps anderer Länder sind gemischt. Da Deutschland hier auf eine in weiten Teilen eigene Lösung setzt, sind in Bezug auf diese App noch keine Aussagen möglich.

Der Kompetenzbereich „Digital Security“ des SICP begrüßt, dass ein datensparsamer Ansatz nach dem Prinzip Privacy-by-Design gewählt wurde. „Gleich mehr zeigt sich, wie wichtig die Forschungsergebnisse des Kompetenzbereichs für die Praxis sind: Das Start-up CodeShield, an dem Prof. Dr. Eric Bodden beteiligt ist, hat mit seinen Analysewerkzeug eine Schwachstelle gefunden und direkt gemeldet. Diese Schwachstelle wurde umgehend geschlossen”, erläutert Dr. Simon Oberthür, Manager des Kompetenzbereichs. Der offengelegte Code ermöglicht auch präziser nach unterschiedlichen Seitenkanalangriffen zu suchen. Dies ist das Spezialgebiet von Prof. Dr. Juraj Somorovsky, seit Februar dieses Jahres Professor für Systemsicherheit an der Universität Paderborn, der in den letzten Jahren zahlreiche Lücken in weit eingesetzten kryptographischen Bibliotheken (wie OpenSSL) gemeldet hat.

Weitere Informationen www.sicp.de