Kann eine Corona-App bei der Nachverfolgung helfen?

Eine ganze Reihe von Herausforderungen

Foto: alexandra, adobe stock

Ein kritischer Faktor bei der Verbreitung von Vireninfektionen ist die Inkubationszeit, in der es bereits zu Ansteckungen kommen kann. Die Nachverfolgung der Infektionswege steht daher unter einem besonderen Zeitdruck. Kann eine „Corona-App" dabei helfen?

Beim Ausbruch der Corona-Infektionen in Deutschland hat sich gezeigt, dass die Verfolgung der Infektionswege durch die Gesundheitsämter über eine Befragung Infizierter und telefonische Kontaktaufnahme mit möglichen Kontaktpersonen sehr schnell an personelle Grenzen stößt: Schon bei tausend Infektionen am Tag ist eine solche Nachverfolgung praktisch nicht mehr leistbar.

Daher liegt es nahe, über ein automatisierbares Verfahren zur Information möglicher Infizierter nachzudenken: eine App, die alle persönlichen Kontakte über einen gewissen Zeitraum protokolliert, bei denen es aufgrund der physischen Nähe zu einer Infektion gekommen sein könnte. Wird eine Person positiv auf die Viren getestet, könnten alle Kontaktpersonen automatisch und unverzüglich informiert werden.

So weit, so gut. Aber wie so oft liegen die Tücken im Detail. Die Lösungen, über die gerade diskutiert und an denen gearbeitet wird, haben dabei gleich mehrere Herausforderungen zu bewältigen.

Die Technik

Der ebenfalls nahe liegenden Idee, für die Positionsbestimmung die Daten der Mobilfunkanbieter auszuwerten, haben die Telekommunikationsunternehmen gleich eine Absage erteilt: Ganz unabhängig von rechtlichen Fragen ist die Information, mit welcher Basisstation ein Smartphone verbunden ist, viel zu ungenau, um entscheiden zu können, ob die „Infektionsdistanz" von 1,5 m zwischen zwei Menschen unterschritten wurde.

Selbst GPS-Daten sind – zumindest in Städten aufgrund der Reflektionen an Gebäuden und der geringen Anzahl „sichtbarer" Satelliten – viel zu ungenau, um einen 1,5-m-Abstand selbst mit einem 30-Prozent-Fehler (+/- 0,5 m) feststellen zu können.

Damit bleibt die Möglichkeit einer direkten Verbindung zwischen zwei Smartphones via Bluetooth. Tatsächlich kann man die Bluetooth-Signalstärke bestimmen und daraus – immer noch mit einer deutlichen Ungenauigkeit – auf den Abstand zwischen zwei Geräten zurückschließen. Aber auch dieser Wert ist fehlerbehaftet: Der Abstand der Geräte entspricht in der Praxis nicht dem Abstand zwischen zwei Menschen. Liegen die Smartphones zwischen den Personen auf dem Tisch, kann er erheblich geringer sein; steckt eins in einer Jackentasche, auch erheblich größer. Fehlalarme sind damit vorprogrammiert.

Das Persönlichkeitsrecht

Zumindest nach aktueller Rechtslage ist klar, dass eine allgemeine Verpflichtung zur Nutzung einer solchen App nicht zulässig wäre. Auch darf bezweifelt werden, dass eine gesetzliche Vorschrift oder Verordnung, die die Nutzung vorschreibt, verfassungskonform wäre. Damit folgt, dass man sich bei der Analyse der Infektionswege nicht allein auf eine solche App verlassen kann und darf.

Aber selbst wenn die Nutzung einer solchen App nicht vorgeschrieben werden kann, wäre es möglich, dass Einzelhändler, Gastwirte oder Veranstalter die Nutzung einer Corona-App zur Vorbedingung für den Zugang zu Geschäftsräumen oder Veranstaltungen machen. Auch das wäre eine deutliche Freiheitsbeschränkung der betroffenen Personen.

Noch schwerer wiegt, dass die Speicherung der Kontakte selbst bereits einen erheblichen Eingriff in das Persönlichkeitsrecht der Betroffenen darstellt. Schließlich lassen sich aus den Protokolleinträgen (Kontaktperson, Datum, Uhrzeit, Dauer) komplette Kontakthistorien über den Zeitraum der Speicherung (diskutiert werden zwei Wochen) ableiten.

Um eine zweckfremde Nutzung dieser Informationen auszuschließen, dürfen die Protokolldaten, darin sind sich Datenschützer einig, niemals zentral, sondern bestenfalls lokal auf dem Smartphone gespeichert werden. Auch darf die Kontaktperson nicht mit ihrem Namen, sondern höchstens unter einem Pseudonym im Protokoll des Gesprächspartners einge-

tragen werden. Dabei darf es einem Dritten nicht möglich sein, die verwendeten Pseudonyme der Identität einer Person zuzuordnen.
Da jeder, der mit einer Person in Kontakt stand, deren Pseudonym auflösen kann, muss das Pseudonym in kurzen Zeitabständen gewechselt werden. Umgekehrt muss es der Kontaktperson dennoch möglich sein, im Falle einer Infektionsmeldung diese Person mit dem Kontakteintrag in Verbindung zu bringen. Technisch möglich wäre das, indem z. B. täglich aktualisierte Listen mit allen Pseudonymen der positiv auf die Viren getesteten Personen veröffentlicht werden. Die App müsste lediglich prüfen, ob eines der Pseudonyme in ihren lokalen Kontakteinträgen auftaucht.

Schutz vor Missbrauch

Da die ausgetauschten Pseudonyme nicht auf Korrektheit geprüft werden können (denn dafür wäre ja eine Identifikation der Kontaktpersonen erforderlich), besteht weiter die Gefahr, dass „Fake-Apps" falsche Pseudonyme verwenden – möglicherweise die von Personen, die bereits positiv getestet wurden. Damit könnten Personen gezielt einem Infektionsverdacht ausgesetzt werden – mit ggf. erheblichen persönlichen Konsequenzen (Quarantäne).

Einheitliche Lösung

Da fast alle derzeit diskutierten und entwickelten Corona-Apps unterschiedliche Strategien und technische Konzepte verfolgen, die untereinander überwiegend inkompatibel sind, wird auch dies dazu beitragen, dass der praktische Nutzen einer solchen App weiter sinkt – denn noch seltener werden zwei Personen, die auf Infektionsnähe miteinander in Kontakt kommen, dieselbe (oder eine kompatible) App verwenden.
Von einer – wie auch immer technisch ausgestalteten – Corona-App sollten wir uns also für die Eindämmung der Pandemie nicht zu viel erwarten.

Dirk Fox, Secorvo Security Consulting GmbH

Homeoffice? – Aber sicher!
Tipps für sicheres mobiles Arbeiten

Eine empfohlene Maßnahme im Kontext der Corona-Prävention ist die intensivere Nutzung von Homeoffice und mobilem Arbeiten. Dafür gilt es, pragmatische Lösungen zu finden, die einerseits die Arbeitsfähigkeit einer Organisation erhalten, gleichzeitig jedoch Vertraulichkeit, Verfügbarkeit und Integrität gewährleisten.
Trotz der gegebenen herausfordernden Situation sollte auch bei der Einrichtung von Homeoffice-Arbeitsplätzen die IT-Sicherheit angemessen berücksichtigt werden. Bei spontanen Lösungen für mobiles Arbeiten können in der Regel nicht alle Anforderungen für IT-Sicherheit vollständig umgesetzt werden. Schnellere und stabile Netzanschlüsse, der Aufbau von VPN-Lösungen (Virtual Private Networks) sowie die Anschaffung geeigneter Hardware können nur in Ausnahmefällen ad hoc aufgebaut oder bewerkstelligt werden.

TOP 5 für Ihre IT-Sicherheit

1 Klar geregelt:
Treffen Sie deutliche, unmissverständliche und verbindliche Regelungen zur IT-Sicherheit und zur Sicherheit Ihrer Daten in Papierform. Kommunizieren Sie diese schriftlich an alle Beteiligten.

2 Hier gibt es nichts zu sehen:
Ergreifen Sie an ihrem Heimarbeitsplatz Maßnahmen, mit denen sich ein Sicherheitsniveau erreichen lässt, das mit einem Büroraum vergleichbar ist. Verschließen Sie Türen, wenn Sie den Arbeitsplatz verlassen, geben Sie Dritten keine Chancen durch einsehbare oder gar geöffnete Fenster.

3 Eindeutige Verifizierung:
Sorgen Sie für eindeutige Kontaktstellen und Kommunikationswege, die von den Beschäftigten verifiziert werden können.

4 Vorsicht Phishing:
Es können vermehrt Phishing E-Mails auftreten, die die aktuelle Situation ausnutzen und versuchen werden, Ihre sensiblen Daten mit Hinweis auf Remote-Zugänge, das Zurücksetzen von Passwörtern etc. abzugreifen.

5 VPN:
Idealerweise greifen Sie über einen sicheren Kommunikationskanal (z. B. kryptografisch abgesicherte VPN auf interne Ressourcen der Institution zu. Sofern Sie bisher keine sichere und skalierbare VPN-Infrastruktur haben, informieren Sie sich über mögliche Lösungen.
Die aufgeführten Hinweise tragen der kurzfristigen Entwicklung um das Corona-Virus Rechnung und sollten mittelfristig stetig weiterentwickelt und verbessert werden. Empfehlungen und Maßnahmen zur langfristigen Etablierung von sicheren Telearbeitsplätzen sowie tiefergehende Ausführungen zu den hier genannten Tipps hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) in den entsprechenden Bausteinen des IT-Grundschutzes zusammengetragen.

Quelle: BSI

INFO Diese und weitere Maßnahmen mit vertiefenden Details als PDF auf der Webseite des BSI unter: