Die Corona-Tracing Konzepte im Überblick

Wissenschaftler, Politik und Tech-Unternehmen diskutieren derzeit über unterschiedliche Konzepte zur Umsetzung von Corona Tracing-Apps. Anfang April hat Reporter ohne Grenzen bereits Mindestanforderungen an mögliche Apps formuliert, nun geben wir einen Überblick über die derzeit vorliegenden Ansätze und ihre Risiken. Den Kontext der Debatte erläutern wir hier.

Konzept von Apple und Google

Die Unternehmen Apple und Google haben ein vorläufiges Konzept vorgelegt, um technische Elemente einer Contact-Tracing-App in ihre Betriebssysteme zu integrieren. Diese sollen es Staaten zunächst leichter machen, eigene Contact-Tracing-Apps auf Basis von Bluetooth Low Energy Beacons[1] zu entwickeln, wie sie auch in Deutschland diskutiert werden. In einer ersten Phase planen die IT-Unternehmen Programmierschnittstellen (APIs) für Contact-Tracing in ihre iOS und Android Betriebssysteme zu integrieren. In einer zweiten Phase sollen von den Unternehmen entwickelte Contact-Tracing Tools direkt in die iOS und Android Betriebssysteme integriert werden.

Reporter ohne Grenzen (RSF) warnt, dass die Integration einer Tracing-Funktionalität in einen Großteil der Smartphone-Betriebssysteme weltweit ein erhebliches Missbrauchspotenzial durch autoritäre Staaten birgt. Das Konzept orientiert sich zwar derzeit an einem dezentralen Ansatz, der ohne zentrale Datenspeicherung auskommt. Ohne besondere Vorkehrungen ist ein Missbrauch zur Kontaktüberwachung der Bevölkerung allerdings nicht ausgeschlossen. RSF fordert von beiden Unternehmen geeignete Schutzmaßnahmen, um einen unbeabsichtigten Export von Überwachungstechnologie zu verhindern.

Die Integration als normale Funktion des Betriebssystems birgt zusätzlich die Gefahr einer Normalisierung von Contact-Tracing. Ungeachtet technischer und rechtlicher Datenschutzvorkehrungen sind Contact-Tracing-Apps eine Risikotechnologie und müssen für Nutzerinnen und Nutzer auch als solche erkennbar sein. RSF fordert von den Unternehmen deshalb auch technische Vorkehrungen um die Freiwilligkeit der Nutzung zu unterstützen.

Die Beteiligung von Apple und Google sind für den Erfolg von Contact-Tracing-Apps von zentraler Bedeutung. Durch die Hilfe der Betriebssystemhersteller lässt sich eine

[1] Als Bluetooth Low Energy Beacons wird eine stromsparende Funktechnik bezeichnet, mit der Geräte über die Bluetooth Funktechnik eine ID Nummer aussenden, die von anderen Smartphones in der näheren Umgebung empfangen werden kann.

praktische Limitierung von Contact-Tracing-Apps adressieren. Die App aus Singapur rät Nutzerinnen und Nutzern von iOS Geräten dazu, das Telefon entsperrt und die App im Vordergrund zu halten, da sie sonst weniger häufig nach benachbarten Telefonen sucht. Die Beteiligung von Apple verspricht, dieses Problem zu lösen. Sie dürfte sich auch positiv auf die Beteiligung der Nutzerinnen und Nutzer auswirken. Schätzungen zufolge müssten mindestens 60 Prozent der Bevölkerung eine Contact-Tracing-App installieren, um maßgeblich zur Eindämmung des Virus beizutragen. In Singapur nutzen die App Berichten zufolge nur 12 Prozent.

Der dezentrale Ansatz von Apple und Google

Das Konzept von Apple und Google lehnt sich an unterschiedliche, unabhängig von Expertinnen und Experten entworfene Konzepte wie TCN oder DP-3T an. Das letztere Projekt ist als Beitrag im Rahmen des PEPP-PT-Projektes entstanden, das zuletzt als wahrscheinlichster Standard für ein europäsches Contact-Tracing galt.

Das bisher von Apple und Google vorgesehene Konzept basiert auf einem dezentralen Ansatz, bei dem die Bestimmung von Kontaktpersonen lokal auf den Geräten von Nutzerinnen und Nutzern stattfindet. Die Firmen versprechen sich dadurch mehr Sicherheit und Datenschutz, da so auf eine zentrale Erfassung von Kontaktpersonen verzichtet werden kann. Kritikerinnen und Kritiker sehen darin zugleich eine verpasste Chance, Algorithmen aus den Daten lernen zu lassen und so beispielsweise die Abstandmessung und die damit einhergehende Risikoabschätzung zu verbessern. Zugleich böte eben diese zentrale Sammlung von Informationen über Nutzerinnen und Nutzer in Verbindung mit einer Übersicht über deren Kontaktpersonen erhebliches Missbrauchspotenzial. Zahlreiche Studien haben die Rückführbarkeit scheinbar anonymisierter bzw. pseudonymisierter Daten auf Einzelpersonen in Zeiten sozialer Netzwerke und digitaler Datenbanken aufgezeigt.

In der von Apple und Google favorisierten dezentralen Variante senden erkrankte Personen eine Liste ihrer eigenen, verschlüsselten IDs an einen Server. Die Apps der anderen Personen laden diese Liste regelmäßig herunter und überprüfen, ob eine der darin enthaltenen IDs in der Liste der eigenen Kontaktpersonen enthalten ist. Ist das der Fall, berechnet die App einen Risikowert und zeigt abhängig davon eine Warnung an. Die Überprüfung im vorletzten Schritt geschieht lokal auf den Telefonen, und die Liste der eigenen Kontaktpersonen bleibt geheim.

Der zentrale Ansatz von PEPP-PT

Bei den dezentralen Ansätzen findet der Abgleich gesammelter ID Nummern mit den ID-Nummern von Infizierten auf den Telefonen statt. Im zentralen Ansatz, den die deutsche Variante von PEPP-PT und die französische Variante ROBERT verfolgen, erfolgt die Überprüfung hingegen auf einem zentralen Server. Wie in der dezentralen Variante sammeln und senden Smartphones zunächst durchgehend temporäre IDs. Der erste Unterschied zur dezentralen Variante: Die Apps erstellen ihre temporären IDs nicht selbst, sondern bekommen sie von einem Server zugeteilt, der sicherstellt,

dass er diese IDs zu einem späteren Zeitpunkt wieder entschlüsseln und so einer Installation der App zuordnen kann.

Der zweite Unterschied betrifft den Upload von Daten einer erkrankten Person: Während die dezentrale Variante eine Liste der eigenen temporären IDs hochlädt, sendet die deutsche PEPP-PT-Variante eine Liste der gesammelten IDs. Anhand dieser IDs kann der Server nun jede Kontaktperson der erkrankten Person einzeln informieren.

Dieser Unterschied könnte sich als Schwachstelle der deutschen Variante herausstellen. Um alle Betroffenen informieren zu können, speichert der Server eine Liste von Zweier-Begegnungen ab: je die ID einer infizierten Person und ihrer Kontaktperson. Das Senden an den Server angestoßen hat aber nur die infizierte Person.

Im Alltag könnte das in etwa zu solchen Situationen führen: Eine Journalistin Alice trifft sich mit ihrer Quelle Bob in einem Cafe. In dem Cafe sitzt zwei Tische weiter ein junges Pärchen, sagen wir Charlie und Dave. Charlie erfährt zwei Tage später infiziert zu sein und lädt gemeinsam mit Dave gewissenhaft die Liste ihrer Kontaktpersonen hoch. Für den zentralen Server sehen diese Listen dann in etwa so aus:

Liste von Charlie: 397, 185, 920, 857

Liste von Dave: 830, 185, 920, 242

Die Zahlen 185 und 920 sind dabei die temporären IDs von Alice und Bob. Da die Apps zu jeder Kontaktperson auch den Zeitpunkt des Kontakts zum Server schicken, weiß dieser nun, dass das Treffen letzten Montag um 13:15 stattfand. Der Server kennt zwar nicht die Namen oder Telefonnummern von Alice und Bob. Er kann aber die Nummern 185 und 920, und jede andere Nummer die Alice und Bob in der Zukunft über ihre Telefone aussenden, in permanente ID Nummern entschlüsseln die er eindeutig Alice und Bob zuweisen kann.

Die französische Variante, ROBERT, führt noch weitere Elemente auf, die gespeichert werden sollen. Zum Beispiel wie häufig eine Person Kontakt mit anderen Infizierten Personen hatte, und wann sich eine Person zum letzten Mal beim Server gemeldet hat. Ob die deutsche PEPP-PT diese Daten ebenfalls speichert, ist aus den bisher veröffentlichen Dokumenten nicht zu entnehmen.

Zentrales wie dezentrales Contact-Tracing birgt Gefahren

Während der dezentrale Ansatz zwar ohne eine zentrale datensammelnde Instanz auskommt, birgt er doch Gefahren. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF) und der Leiter des Labors für IT-Sicherheit und Kryptographie an der Schweizer École polytechnique fédérale de Lausann (EPFL), Serge Vaudenay, weisen auf Sicherheitslücken hin. Das FIfF verweist im selben Dokument auch auf Datenschutzbedenken in zentralisierten Ansätzen.

Das FIfF macht zum Beispiel darauf aufmerksam (Angriff A3), dass auch eine dezentrale Variante das Problem hat, dass sich bei der Verknüpfung mit IP-Adressen oder anderen Daten infizierte Individuen de-anonymisieren lassen, und falls diese eine Kontaktperson angesteckt haben, diese ebenfalls. Damit ließe sich ein Treffen zwischen zwei Personen nachweisen, zum Beispiel das einer Journalistin und ihrer Quelle. Im Vergleich zur zentralen Variante aber nur dann, wenn beide krank werden und die Liste ihrer temporären IDs mit dem Server teilen.

Serge Vaudenay zeigt ebenfalls mehrere Sicherheitslücken im dezentralen Ansatz auf. Darunter ist ein Szenario, in dem eine Gruppe von Personen gezielt andere Personen de-anonymisieren können (Abschnitt 5.2), sollten diese sich infizieren. Ebenso skizziert er Szenarien (Abschnitt 4.4), in denen Personen ein Kontakt mit einer infizierten Person "untergejubelt" wird, mit dem Ziel, diese mit falschen Nachrichten zu belästigen oder dem damit verbundenen sozialen Stigma auszusetzen. Ein ähnlicher Angriff funktioniert auch in der zentralen Variante von PEPP-PT (S. 21, F-REQ-7). Die Risikobewertung von PEPP-PT argumentiert mit einer erhöhten Infektionsgefahr für angreifende Personen - was diese abschrecken soll. Sie müssten sich eine längere Zeit in der Gegenwart infizierter Personen aufhalten. Warum diese Aufgabe nicht durch ein umprogrammiertes und liegengelassenes Telefons erfolgen kann, erklärt die PEPP-PT Risikobewerung jedoch nicht.

Das Dokument zu PEPP-PT dokumentiert weitere offene Risiken, die aber kategorisch ausgeschlossen werden. So könnten die Betreiber des Servers nach belieben temporäre IDs in permanente umrechnen, und dadurch die Anonymität von Nutzerinnen und Nutzern gefährden. Laut dem PEPP-PT-Konzept werden sie dies jedoch nicht tun, da dies unter anderem illegal wäre und gegen Verträge verstoßen würde. Wie ein solcher Angriff auf die Anonymität erkennbar wäre, erwähnt die Risikobewertung nicht.

Ähnlich wird das Risiko behandelt, dass Staaten jederzeit die Anonymität einzelner Nutzerinnen und Nutzer aufheben können. Laut dem Konzept würde so etwas voraussetzen, dass soziale und rechtliche Normen soweit abgeschafft würden, dass ein Staat nicht mehr auf PEPP-PT zurück greifen müsste, um die erwünschten Daten zu erlangen.

Reporter ohne Grenzen weist darauf hin, dass die Schaffung einer Datenbank schnell weitere Begehrlichkeiten wecken kann. So ist es vorstellbar, dass in Zukunft Personen, die nicht auf eine Benachrichtigung reagieren, identifiziert und zur Rechenschaft gezogen werden könnten. Im *Heute Journal* hat Bundesgesundheitsminister Jens Spahn bereits die Entwicklung einer App angekündigt, mit der Quarantänemaßnahmen überwacht und kontrolliert werden sollen.

Eine PEPP-PT-App könnte nämlich auch ein hilfreiches Werkzeug beim Aufspüren und Verfolgen terroristischer und extremistischer Gruppen, der Verfolgung schwerer Straftaten oder dem Drogenhandel sein. Die zentrale Contact-Tracing-Technologie birgt also ein großes Missbrauchspotenzial, und in der Corona-Krise ist es in Deutschland bereits zu rechtswidrigen Datenweitergaben von Gesundheitsdaten durch Gesundheitsämter an die Polizei gekommen.

Die Diskussion zu Missbrauchsmöglichkeiten und der offene Brief von 300 renommierten Wissenschaftlerinnen und Wissenschaftlern im Bereich der Kryptographie und IT-Sicherheit säen Zweifel daran, ob es sich bei der Frage nach zentral oder dezentral wirklich nur um eine rein philosophische Frage handelt. Als solche hatte sie zum Beispiel der Leiter des Forschungsbereiches „Eingebettete Intelligenz“ am Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) Paul Lukowicz bezeichnet.

Missbrauch durch autoritäre Staaten

Auch ohne Einbindung eines zentralen Servers, wie im Konzept von Apple und Google vorgesehen, besteht die Gefahr, dass die Contact-Tracing-Technologie von autoritären Staaten missbraucht werden kann. Der technischen Dokumentation von Apple zufolge verwendet das Konzept drei unterschiedliche Arten von ID-Nummern: sogenannte Tracing-Keys, Daily Tracing-Keys, und Rolling Proximity ID. Die erste Nummer, der Tracing-Key, wird beim Start von Contact-Tracing generiert und ändert sich danach nicht mehr. Die nachfolgenden Nummern werden aus der vorherigen berechnet, und die Rolling Proximity ID wird schließlich an benachbarte Telefone gesendet.

Ist der Tracing-Key nicht gegen unbefugtes Auslesen geschützt, so lassen sich damit alle ID-Nummern einer Person aus der Vergangenheit und der Zukunft berechnen. Das kann zum Beispiel bei einer Polizeikontrolle passieren. Damit ist die Anonymität der gespeicherten Daten nicht mehr gewährleistet. Ebenso ist nicht ausgeschlossen, dass autoritäre Staaten die von den Firmen erstellte API für selbst entwickelte Überwachungswerkzeuge missbrauchen.

Reporter ohne Grenzen fordert daher geeignete Maßnahmen, um diesen Risiken zu begegnen. Dies kann zum Beispiel durch die Speicherung von IDs in sicheren Koprozessoren, durch eine Option, die Tracing-ID neu zu generieren oder eine Option für die Verwendung von komplett zufälligen Rolling Proximity IDs ohne Bezug zur Tracing-ID geschehen. Eine geeignete Maßnahme kalkuliert auch das Risiko von Sicherheitslücken in Geräten mit ein. Die an zahlreiche Strafverfolgungsbehörden weltweit verkauften Produkte der Firma Cellebrite nutzen zum Beispiel solche Sicherheitslücken, um das Auslesen geschützter Informationen aus Telefonen zu ermöglichen. Die Regierung in Myanmar nutzte ein solches Produkt, um die späteren Pulitzer-Preisträger Wa Lone und Kyaw Soe Oo für ihre Recherchen zu der Massenermordung von Rhoyinga durch das Militär in Myanmar zu verurteilen.

Ebenso muss die Integration der Software-Komponenten zeitlich beschränkt und später wieder aus dem Betriebssystem entfernt werden. Plausibel kann dies zum Beispiel durch die Verwendung kurzlebiger Software-Signaturen geschehen, die von den Firmen regelmäßig aktualisiert werden müssen. Contact-Tracing darf nicht zu einer Standardfunktion moderner Mobiltelefone werden.

Risiken durch Normalisierung von Contact-Tracing

Jede Form des Contact-Tracing, unabhängig davon wie datenschutzfreundlich sie umgesetzt wird, stellt einen tiefen Eingriff in Freiheitsrechte und die Privatsphäre dar. Das Etikett "datenschutzfreundlich" darf darüber nicht hinwegtäuschen und zu einer Normalisierung von Contact-Tracing beitragen.

Eine Normalisierung verstärkt soziale und ökonomische Zwänge, sich an Contact-Tracing zu beteiligen. Vor diesen Zwängen hat jüngst das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF) in seiner Datenschutz-Folgenabschätzung gewarnt. Zum Beispiel könnte die Verwendung der App an die Wahrnehmung anderer Freiheitsrechte, wie der Teilnahme am öffentlichen Leben oder dem Besuch des Arbeitsplatzes, gekoppelt werden. Vorstellbar wäre auch, dass die Akkreditierung von Journalistinnen und Journalisten an die Teilnahme am Contact-Tracing gekoppelt werden könnte.

Freiwilligkeit muss technisch und rechtlich unterstützt werden

Um dem entgegenzuwirken, sollte die Freiwilligkeit nebst rechtsstaatlichen Vorkehrungen durch technische Maßnahmen unterstützt werden. Ein wichtiger Aspekt hierbei ist die Gestaltung der Benutzeroberflächen und des Zustimmungsmechanismus. So ist es bei den Mobiltelefon der Firmen Apple und Google zum Beispiel sehr umständlich, Bluetooth zu deaktivieren. Die leicht zugänglichen Einstellungen deaktivieren Bluetooth nicht vollständig (Android), oder aktivieren es nach einem Tag wieder (iOS).

Beide Firmen standen in der Vergangenheit auch in der Kritik so genannte Dark Patterns in ihren Produkten zu verwenden. Dark Patterns sind Elemente von Benutzeroberflächen, die Nutzerinnen und Nutzer durch psychologische Tricks dazu verleiten sollen, eine Wahl zu treffen, die sie eigentlich nicht treffen wollten. Ein bekanntes Beispiel ist die Akzeptanz von Cookie-Richtlinien auf Webseiten, bei der die Ablehnung von Cookies mehr Aufwand erfordert als die Akzeptanz.

Apple, Google und andere Entwickler von Contact-Tracing-Apps sind daher dringend dazu aufgerufen, auf die Verwendung sogenannter Dark Patterns bei der Gestaltung ihrer Contact-Tracing-Apps und -Einstellungen vollständig zu verzichten. Die Gestaltung von Interaktionen und Benutzeroberflächen müssen stattdessen die Freiwilligkeit der Verwendung von Contact-Tracing unterstützen**.** Dies kann zum Beispiel dadurch geschehen, dass Nutzerinnen und Nutzer in regelmäßigen Abständen, etwa jede Woche, ihre Zustimmung erneuern müssen. Zudem muss es jederzeit möglich sein, die Zustimmung zu entziehen und sämtliche Daten auf dem Telefon zu löschen und zwar ohne negative Konsequenzen befürchten zu müssen.

Ebenso sollten die Benutzeroberflächen leicht zugängliche und verständliche Aufklärungen über die bisher bekannten Risiken, sowohl bei der Nutzung als auch der Entscheidung Kontaktdaten zu übermitteln, enthalten. Auf Transparenz hat bereits Scott Leibrand, der mit dem CoEpi ein eigenes Contact-Tracing Projekt leitet, hingewiesen. Es muss sichergestellt werden, dass Nutzerinnen und Nutzer wie auch

Journalistinnen und Journalisten diese Risiken verstehen, um für sich selbst im Einzelfall eine informierte Entscheidung treffen zu können.

Zusammenfassend lässt sich sagen, dass es sich bei Contact-Tracing trotz aller bisherigen Bemühungen um eine Risikotechnologie mit hohem Missbrauchspotenzial handelt. Sowohl die bisher diskutierten dezentralen Varianten wie sie Apple und Google vorschweben, wie auch die zentrale Variante von PEPP-PT enthalten Sicherheitsrisiken, die noch nicht vollständig gelöst sind. Wie freiwillig die Nutzung in der Praxis wirklich sein wird, hängt von vielen Entwicklungen ab, die sich noch nicht absehen lassen. Reporter ohne Grenzen wird die Debatte der Expertinnen und Experten weiter kritisch verfolgen.