Update

Setzt die Corona-App aus der Schweiz europaweit Standards?

Die europäische Forschungsgemeinschaft für das Contact-Tracing droht komplett auseinanderzubrechen. In die Bresche könnte die Schweiz springen: Die Lösung von EPFL und ETH geht bald live. Die Armee testet bereits eine App auf dieser Basis.

Von Adrienne Fichter, 22.04.2020

Wie geeint sind die Länder Europas in der Krise? Nach dem Gezänk um die solidarische Haftung für die wirtschaftlichen Schäden mit sogenannten Corona-Bonds gibt es seit vergangenem Wochenende nun ein zweites europäisches Reizthema: das Contact-Tracing.

Zur Recherche

Hält die digitale Epidemiebekämpfung, was sie verspricht? Contact-Tracing-Apps sollen im Kampf gegen das Coronavirus eine wichtige Rolle spielen. Schweizer Anbieter haben bereits Lösungen entwickelt.

Dabei geht es darum, alle Personen ausfindig zu machen, die sich länger in der Nähe eines Infizierten aufgehalten haben, sie ebenfalls zu testen – und so die Übertragungsketten zu brechen. Das ist sehr personalintensiv. Darum hoffen Epidemiologinnen, dass Smartphone-Apps beim Rückverfolgen der Kontakte helfen könnten.

Dabei sah es bis vor kurzem nach einer Erfolg versprechenden Zusammenarbeit aus: Schweizer Forscher hätten gemeinsam mit Partnern aus Europa eine Proximity-Tracing-Lösung entwickeln sollen – also eine App, die Kontakte zwischen Smartphones registriert und bei Corona-Verdacht Alarm schlägt.

Doch am vergangenen Donnerstag kam es zum Eklat. Grund ist das Tracing-Protokoll DP3T, das Schweizer Forscherinnen wesentlich mitentwickelt haben.

Das Vorzeigemodell wurde stillschweigend von der Website des Konsortiums entfernt, das den europäischen Standard etablieren soll. Dem Konsortium hatten sich ursprünglich über 130 Wissenschaftlerinnen aus den Gebieten Epidemiologie, Datenschutz, Kryptografie, IT-Security und Ethik

sowie diverse Partnerunternehmen angeschlossen – mit dem Ziel, einen europäischen Standard für eine Contact-Tracing-App zu definieren.

Am Freitagmorgen gab EPFL-Epidemiologe Marcel Salathé seinen Austritt aus dem Konsortium bekannt. Und um Mitternacht reichte ETH-Professor Kenneth Paterson seinerseits das Austrittsschreiben der ETH ein.

Die Zusammenarbeit zwischen den Schweizer Hochschulen und dem besagten Konsortium – dem Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) – ist damit Geschichte. Und nicht nur das: Auch das deutsche Helmholtz Center for Information Security (Cispa), die belgische KU Leuven und die italienische ISI Foundation haben sich übers Wochenende aus dem Projekt verabschiedet.

Damit eskaliert ein Konflikt, den die Republik vergangene Woche bereits analysiert hat: der Konflikt zwischen einem zentralen und einem dezentralen Modell von Proximity-Tracing. Umstritten ist die Frage, wo die persönlichen Daten gesammelt, gespeichert, verschlüsselt und verarbeitet werden sollen: dezentral, also auf den Endgeräten der Nutzerinnen, oder eben zentral, auf einem Server.

Eine bizarre Pressekonferenz

Im innereuropäischen Drama um das Contact-Tracing stehen sich Deutschland und Frankreich momentan dem Rest von Europa gegenüber.

Unternehmen, Politiker, Beratungsfirmen und einige Forschungsinstitute der beiden verbündeten Staaten pochen dabei auf einen zentralen Ansatz. Eine besondere Rolle spielen dabei das deutsche Fraunhofer-Institut sowie der Kommunikationschef und De-facto-Kopf von PEPP-PT, Hans-Christian Boos. Er ist Gründer des KI-Unternehmens Arago, sitzt im Digitalrat der deutschen Bundesregierung und geniesst das Vertrauen hochrangiger CDU-Politiker. Die von ihm beauftragte PR-Agentur Hering Schuppener gilt ebenfalls als CDU-nah. Boos sagt offen, dass er sich für Deutschland eine Serverlösung vorstellt, die dem zentralen Modell entspricht.

Derweil vertreten die Urheber des DP3T-Protokolls, bei dessen Entwicklung die Schweizer Hochschulen führend sind, einen dezentralen Ansatz. Dieser sieht vor, dass Kontakte zwischen einzelnen Smartphones nur auf den jeweiligen Geräten, nicht auf einem zentralen Server gespeichert und verschlüsselt werden.

Bemüht um Schlichtung, hielt PEPP-PT auf der Videokonferenzplattform Zoom am Freitagnachmittag eine Pressekonferenz ab. PEPP-PT-Chef Hans-Christian Boos sagte, er wolle Marcel Salathé unbedingt wieder zurück an Bord gewinnen. Er betonte immer wieder, dass man bei PEPP-PT offen sei für beide Ansätze, zentrale und dezentrale. Man sei schon mit sieben Regierungen im Gespräch, die eine PEPP-PT-App installieren würden. Vierzig weitere Interessierte würden dazukommen. Die Republik fragte bei Boos nach, um welche Staaten es sich handle. Boos' Sprecherin sagt dazu: «Das werden wir in Kürze veröffentlichen.»

Am Freitagabend veröffentlichte das PEPP-PT-Konsortium zudem ein Dokument zu den Leitlinien der Umsetzung. Doch fünf Minuten nach Veröffentlichung wurde dieses wieder entfernt, was für zahlreiche Diskussionen im Netz sorgte. Der Kryptologe Nadim Kobeissi hat das PDF heruntergeladen und auf seinem Blog publiziert. Die DP3T-Autorengruppe analysiert das Dokument und nannte es «function creep». Was damit gemeint ist: Beim Systemvorschlag von PEPP-PT sind schleichende nachträgliche Ver-

änderungen auf Serverseite und gezielter Überwachungsausbau der Nutzerin ohne weiteres möglich, ohne dass dafür Änderungen in der App nötig sind.

Ein neues, zentrales Modell

Am Sonntag veröffentlichte das Konsortium ein weiteres Tracing-Protokoll. Es trägt den Namen Robert («ROBust and privacy-presERving proximity Tracing protocol»). Die Prämisse des Protokolls lautet: Wir – Gesundheitsbehörde und App-Betreiber – schützen dich und deine Identität besser vor externen Angriffen als dein Endgerät. Das Protokoll scheint sich als Gegenentwurf zu DP3T zu verstehen.

Die Beschreibung nimmt explizit auf die in der Analyse des Lausanner Kryptologen Serge Vaudenay identifizierten Schwachstellen Bezug, die wir auch letzte Woche diskutiert haben: Dezentrales Proximity-Tracing ist hackeranfällig, weil die wichtigsten Prozesse auf Endgeräten laufen und man dieses mit falschen Identitäten austricksen kann. Die Autoren von Robert schreiben dazu: Ein «komplett dezentralisierter» Ansatz sei deswegen nicht realistisch.

Kryptografen bemängeln jedoch, bei Robert würden zu viele unnötige Daten hochgeladen, die später auswertbar wären. ETH-Professor Kenneth Paterson nennt das Protokoll einen Albtraum hinsichtlich Privatsphäre und Sicherheit: «Es ist ein hoch zentralisiertes System, bei dem man sich allein auf den Server verlassen muss.» Und weiter: «Vor Machtmissbrauch ist man nicht gewappnet. Der Server kann sehr einfach jedes Pseudonym mit den realen Identitäten verknüpfen.»

Es sei ein erster kleiner Schritt in Richtung Massenüberwachung.

Ich will es genauer wissen: Robert

Das Robert-Protokoll wurde vom französischen Inria entwickelt, dem Institut national de recherche en sciences et technologies du numérique in Paris, einem der letzten verbleibenden Forschungsinstitute bei PEPP-PT.

Bei Robert kennt der Server-Betreiber die IP-Adresse der Nutzerin (also die Netzwerkadresse ihres Gerätes). Theoretisch ist diese Adresse «zufällig», doch praktisch werden sich die wichtigsten Prozesse (wie Upload und Download der Begegnungspaare) wohl im hauseigenen WLAN oder Arbeits-WLAN abspielen. Zusammen mit dem Zeitstempel (dem Zeitpunkt der Begegnung) wird damit nicht nur eine Deanonymisierung der infizierten App-Nutzerin, sondern die Rekonstruktion ihres gesamten Begegnungsnetzwerks möglich.

Ob sich Robert durchsetzt, ist offen. Interessant dürfte die Debatte in Deutschland sein. Denn bestimmte Netzpolitik-Gruppen wie das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung halten bereits die zufällig generierten Identitäten für personenbezogene Daten – also für Daten, die unter speziellem Schutz stünden und deshalb unter die europäische Datenschutzverordnung DSGVO fallen würden. Wenn dem so wäre, würde das eine Reihe rechtlicher Fragen mit sich bringen. Etwa ob man ein Recht auf Auskunftsbegehren hätte.

Forscher appellieren an die Politik

In der Zwischenzeit distanzieren sich immer mehr beteiligte Forscher von PEPP-PT. Der Jurist Michael Veale nennt dessen Lösung ein «trojanisches Pferd». Ein wichtiger Grund für den Forscher-Exodus: Es ist nicht klar, wie stark das Agieren von PEPP-PT von Unternehmensinteressen bestimmt ist.

Auf der PEPP-PT-Website sind auch einige Firmennamen aufgeführt. Zu ihnen gehört etwa die Telekomanbieterin Vodafone. Oder auch das Zürcher Unternehmen AGT, das 2013 in Wikileaks-Dokumenten auftauchte und von ehemaligen Geheimdienstmitarbeitern gegründet worden sei, wie die «Aargauer Zeitung» berichtete.

Unklar ist auch, ob PEPP-PT den Quellcode von Robert und weiteren Optionen veröffentlichen wird. Die Dokumentation dazu lässt Fragen offen, weil sie lediglich die Wichtigkeit «externer» Prüfer betont. Eine solche nicht öffentliche Prüfung widerspricht diametral dem Ethos vieler Forscherinnen. ETH-Professor Paterson sagt dazu: «Wir wollen offenen Quellcode und Dokumente: Jeder soll seine eigene App basierend auf dem DP3T-Protokoll programmieren können.»

Paterson und andere Forscherinnen haben deswegen einen offenen Brief unterzeichnet, der am Montagnachmittag veröffentlicht wurde. Die Forschungsgemeinschaft bittet die Regierungen, ein dezentrales Protokoll wie DP3T, PACT und TCN Coalition umzusetzen. Auffällig ist die grosse Zahl von deutschen Wissenschaftlern, die den Appell mitunterzeichnet haben.

Ohne den Rückhalt der europäischen Forschergemeinschaft wird es für Boos und das Fraunhofer-Institut zunehmend ungemütlich. Selbst das Europäische Parlament hat letzten Freitag eine Resolution verabschiedet, in der nun ein dezentraler Ansatz gewünscht ist. Google und Apple werden in den nächsten Tagen bekannt geben, ob sie Contact-Tracing-Apps mit zentralisiertem Modell überhaupt in ihren Betriebssystemen zulassen.

Es fragt sich also, welche Trümpfe PEPP-PT-Chef Boos noch in der Hand hat. Wird er zum Beispiel gegen die Tech-Konzerne rechtlich vorgehen, wenn diese nicht mitspielen? Seine Sprecherin widerspricht auf Anfrage der Republik und betont, dass der Austausch mit den Tech-Konzernen sehr konstruktiv verlaufe.

Schweiz probt den Alleingang

Offizielle Linie der Schweiz war bislang, beim Proximity-Tracing eng mit den anderen europäischen Staaten zusammenzuarbeiten. Katrin Holenstein, die Mediensprecherin des Bundesamts für Gesundheit, sagt dazu: «Wir stehen in Kontakt mit den europäischen Gesundheitsbehörden und tauschen uns auch intensiv mit ihnen aus.»

Ungeachtet des europäischen Zwists arbeitet das BAG aber am Prototyp von DP3T weiter. «Diese Kontroversen haben keine Auswirkungen auf die Vorbereitungsarbeiten des BAG.» Seit Freitag testen Schweizer Rekruten die App im Feldeinsatz in Lausanne. Der Eidgenössische Datenschutzbeauftragte hat für das DP3T-Konzept bereits grünes Licht gegeben. Und am Dienstag gab BAG-Chef Pascal Strupler bekannt, dass bis zum 11. Mai gemeinsam mit der ETH und der EPFL eine App fertiggestellt werde.

Verläuft alles nach Plan, gehört die Schweiz zu den Pionierländern und würde die erste dezentrale Contact-Tracing-App lancieren.

Möglich ist, dass sich bald ein neues, europäisches Forschungsprojekt rund um die Lösung der ETH und der EPFL bilden wird. Es gebe viele Länder, die mit dem hiesigen Protokoll arbeiten möchten, sagt der Jurist und DP3T-Mitautor Michael Veale. Interessenten gäbe es zum Beispiel aus den Niederlanden. Epidemiologe Marcel Salathé fände dies interessant: «Ein internationales dezentrales Konsortium würde ich begrüssen», sagt er auf Anfrage der Republik.

Das Drama rund um das europäische Contact-Tracing wird wohl bald in den nächsten Akt gehen.