Corona-App

Wissenschaftler warnen vor "beispielloser Überwachung"

Corona lösen per App: Die Bundesregierung setzt dafür auf die Initiative PEPP-PT. Nun kritisieren 300 Forschende deren Ansatz – wegen Datenschutzmängeln.

Von Lisa Hegemann, ZEITONLINE, 20. April 2020

Es hatte alles so gut angefangen. Am 1. April stellten 130 Wissenschaftlerinnen und Unternehmer unter dem Namen PEPP-PT einen Ansatz vor, der das neue Coronavirus eindämmen helfen sollte: Mit ihrem Konzept sollten Länder europaweit datenschutzfreundliche Apps bauen können, die grenzübergreifend funktionieren.

Die Menschen müssten sich nur eine dieser Anwendungen auf ihr Smartphone herunterladen, Bluetooth anschalten und würden dann per Push-Nachricht informiert, sollten sie Kontakt mit einem Corona-Infizierten gehabt haben. Der Vorteil: Dadurch könnten sie sich früher in Quarantäne begeben und die Infektionsketten des Virus brechen. Und das, ohne persönliche Daten wie den Standort oder die Telefonnummer abzufragen.

Das Konzept stieß auf breite Zustimmung: Sicherheits- und IT-Experten lobten es, die Bundesregierung kündigte sogar an, eine vom Robert Koch-Institut geplante Contact-Tracing-App auf dem Grundgerüst von PEPP-PT aufzubauen. Es schien wie die richtige Idee zum richtigen Zeitpunkt. Ein Ansatz, an dem zwar mit großer Eile gearbeitet werden soll, ist er doch dazu gedacht, Wege aus dem Lockdown zu eröffnen. Und der sich doch Zeit zu nehmen schien, um Grundlagen zu schaffen, statt dass jedes Land in Europa an seiner eigenen App für das digitale Contact Tracing herumwerkelte.

Ein zentraler Streit

Doch jetzt regt sich Widerstand gegen PEPP-PT. Und zwar massiver. Denn von dem datenschutz- und privatsphärenfreundlichen Ansatz, den Initiator Hans-Christian Boos ursprünglich versprach, ist offenbar wenig übrig geblieben. So wenig, dass sich eine globale Allianz von mehr als 300 Wissenschaftlerinnen und Wissenschaftlern gebildet hat, die sich klar von dem von PEPP-PT eingeschlagenen Weg distanzieren – darunter mehr als 50 Forscherinnen und Forscher aus Deutschland. In einem offenen Brief, den sie jetzt veröffentlicht haben und der ZEIT ONLINE vorab vorliegt, warnen sie vor einer "beispiellosen Überwachung". Die Sorge: Eine App, mit der wir das Coronavirus eindämmen können sollen, könnte am Ende zum Spion auf unserem Smartphone werden.

Manche Beobachter halten derartige Debatten derzeit für zweitrangig oder angesichts der Bedrohungen durch die Corona-Pandemie für fehl am Platze: Ist es nicht wichtiger, eine App zu bekommen, die uns hilft, dass wir endlich wieder richtig raus dürfen, unsere Grundrechte weniger eingeschränkt werden? Doch das Problem bei allzu sorglos umgesetztem Contact-Tracing könnte im schlimmsten Falle sein, dass digitale Grundrechte nicht nur temporär eingeschränkt werden: Ist zurückrechenbar, welcher Erkrankte, welche Kontakte hinter all den

verschlüsselten und temporären Codes stehen, die die Apps hin- und her senden, und werden diese Daten eben nicht nur temporär aufbewahrt, so könnten solche Apps eine gigantische Datensammlung mit jeder Menge sehr privater Informationen bedeuten.

Im Kern geht es bei dem Streit um die Basis der Tracing-Apps, die in verschiedenen Ländern entstehen sollen. PEPP-PT baut selbst keine Anwendung, sondern will nur das Grundgerüst, auch Framework genannt, entwickeln: Die Initiatoren wollen sich um die Technologie kümmern, die den Austausch von Daten zwischen verschiedenen Apps ermöglichen soll – damit soll über Ländergrenzen hinweg verfolgbar werden, welche Menschen sich in der Nähe von anderen befunden und sie möglicherweise infiziert haben. Zum Grundgerüst soll aber auch zählen, die unterschiedlichen Signalstärken von Mobilfunkgeräten so zu testen, dass die Bluetooth-Messungen möglichst exakt funktionieren.

Ein Teil der Initiative bevorzugt einen dezentralen Ansatz. Das heißt, die gespeicherten Daten würden nur lokal verwendet: Befinden sich zwei Smartphones in einem Abstand von wenigen Metern voneinander, tauschen sie zufällig generierte und ständig wechselnde Identifikationsnummern via Bluetooth aus und speichern sie auf dem Gerät. Wird einer der App-Nutzer positiv auf das neue Coronavirus getestet, schickt er alle seine jeweiligen Identifikationsnummern an alle Handys, deren Codes auf seinem Smartphone zu finden sind. Das bedeutet: Die Nutzerinnen der Handys werden gewarnt, dass sie mit einem Corona-Infizierten lange genug in Kontakt standen, um sich möglicherweise angesteckt zu haben. Sie wissen so aber weder, um welche Person es sich handelt, noch liegen diese Informationen in irgendeiner Datenbank. Einzig, um die Nachricht an seine Kontakte zu schicken, bräuchte er die Bestätigung einer Ärztin oder des Gesundheitsamts.Ein anderer Teil der Initiative präferiert einen zentralen Ansatz. Die genauen Details dazu wurden erst am Samstag vorgestellt. In den Dokumenten, die PEPP-PT auf der Entwicklerplattform Github veröffentlichte, heißt es: Lädt man die App herunter, wird sie einmal auf dem zentralen Server registriert und erhält eine dauerhafte Kennziffer. Auch die zufällig generierten und sich ständig ändernden Identifikationsnummern würden von einem zentralen Server stammen. Hat sich jemand infiziert, würde er seine Kontaktliste – also die zufällig generierten Identifikationsnummern der Smartphones, in deren Nähe man sich aufgehalten hat – zurück an den zentralen Server schicken, der diese Personen dann warnt. Auch die genaue Uhrzeit der Kontakte, Metadaten von Bluetooth wie etwa die Signalstärke und optional Daten über das WLAN könnten an den Server übermittelt werden, so das PEPP-PT.

"Extrem gefährlich“

Ein genereller Kritikpunkt an dem zentralen Ansatz: Werden Daten an einer Stelle gesammelt, könnten sie missbraucht werden. Lägen die Daten auf einem zentralen Server, ermögliche das "eine Form der Überwachung durch die Regierung oder den privaten Sektor", die das Vertrauen in eine App und ihre Akzeptanz in der Gesellschaft "katastrophal beeinträchtigen" würde, heißt es in dem offenen Brief der Wissenschaftler, den Forscher vieler wichtiger Universitäten unterschrieben haben – von Oxford bis Stanford, von der ETH Zürich bis zur Johns Hopkins-Universität, von der Ruhr-Universität Bochum bis zur Katholischen Universität Leuven. "Es ist von entscheidender Bedeutung, dass wir bei der Bewältigung der gegenwärtigen Krise kein Instrument schaffen, das eine groß angelegte Erhebung von Daten über die Bevölkerung ermöglicht, weder jetzt noch zu einem späteren Zeitpunkt." Lösungen, mit denen man per-

sönliche Daten von Millionen von Nutzern verfolgen könne, sollten "ohne Diskussion" abgelehnt werden. In dem Brief der Wissenschaftler wird PEPP-PT nicht namentlich angegriffen, aber dass auch deren Ansatz gemeint ist, wird in Gesprächen mit den Initiatoren deutlich.

Der zentrale und der dezentrale Ansatz unterschieden sich fundamental in der Art und Weise, wie man Privatsphäre garantieren wolle, sagt Kenneth Paterson, Professor für Computer Science an der ETH Zürich und einer der Initiatoren des offenen Briefs, im Gespräch mit ZEIT ONLINE. Wenn man Privatsphäre nicht von Anfang an mitdenke, könne man die Daten später für alles Mögliche verwenden. Die Macher von PEPP-PT hätten ohne Zweifel die besten Intentionen. Doch Privatsphäre zu vernachlässigen, sei "extrem gefährlich". Dass die Daten in der Hand deutscher Behörden liegen könnten, beruhigt ihn dabei nicht.

Eine Frage der Macht

Auch die Details des vorgestellten zentralen Ansatzes sehen Sicherheitsforscher kritisch. In einem Papier, das am Sonntagabend auf der Entwicklerplattform Github veröffentlicht wurde, heißt es: Egal ob die Nutzerin infiziert sei oder nicht, auf dem Server könne man jederzeit ihre permanente Identifikationsnummer mit den temporären abgleichen. Bedeutet: Man könnte Profile von Menschen anlegen – wo sie waren, mit wem sie in Kontakt standen. Und auch wenn diese auf dem Server pseudonymisiert, also nicht direkt einer Person zuzuschreiben wären: Es würde nach Ansicht der Verfasser reichen, die Kontaktinformationen von anderen Nutzern oder denen aus dem Bluetooth-Sensor mit anderen Daten wie einer Überwachungskamera zu kombinieren, und man könnte eine Person dadurch identifizieren. Wie genau das möglich wäre, schreiben die Forscher nicht. Hans-Christian Boos hatte in einem Interview mit ZEIT ONLINE gesagt, dass das System anonym sei.

Durch den zentralen Ansatz könne man die Beziehungen zwischen Nutzerinnen und Nutzern nachvollziehen, sagt Carmela Troncoso. Sie ist Assistenzprofessorin für Privatsphäre und Sicherheit an der Eidgenössischen Technischen Hochschule Lausanne (ETHL) und hat an der auf Github veröffentlichten Analyse des Server-Ansatzes mitgewirkt. Metadaten – also zum Beispiel die Information, wer mit wem in Kontakt stand – seien für Marketingfirmen und Geheimdienste sehr interessant. "Mit dem zentralisierten Ansatz haben sie Zugang zu einem detaillierten Protokoll der anonymisierten Interaktionen zwischen den Nutzern, was dazu führen kann, dass sie wissen, wer mit wem spricht."

Es sei daher keine rein technische Frage, ob man sich für Zentralität oder Dezentralität entscheide, sondern dahinter stehe eine sehr viel größere: "Es geht um Macht." Nämlich ganz konkret um die Frage: Was passiert mit unseren Daten, wenn die Corona-Krise einmal vorbei ist? Offiziell heißt es, die Informationen sollten nach 21 Tagen wieder gelöscht werden. Doch ob das wirklich passiert, ist auch eine Frage des Vertrauens – zum einen in den Staat, zum anderen in die Unternehmen, die an der Verarbeitung der Daten beteiligt sind.

In dem offenen Brief, den auch Troncoso unterschrieben hat, heißt es: Es gebe zahlreiche Vorschläge für Methoden, mit denen man Kontaktpersonen ermitteln könne und die Privatsphäre der Nutzerinnen und Nutzer respektieren könne. "Wir fordern alle Länder nachdrücklich auf, sich nur auf Systeme zu verlassen, die der öffentlichen Kontrolle unterliegen und die die Privatsphäre von vornherein schützen", schreiben die Forscherinnen und Forscher. Dafür definieren sie vier zentrale Prinzipien: Die Apps dürften nur für Maßnahmen der öffentlichen

Gesundheit verwendet werden. Alle Informationen zu Ansätzen müssten öffentlich einsehbar sein und transparent diskutiert werden. Es sollte immer die privatsphärenfreundlichste Variante gewählt werden. Und der Einsatz müsse freiwillig erfolgen und alle Daten nach Ende der Corona-Krise gelöscht werden.

Versehen oder Vorentscheidung?

Ein weiterer Kritikpunkt an PEPP-PT ist die mangelnde Transparenz über die Linie, die das Projekt verfolgt: Zunächst verfolgte PEPP-PT den dezentralen wie den zentralen Ansatz – und die Länder sollten entscheiden, welchen sie präferierten. Als die Bundesregierung am Mittwoch verkündete, dass sie auf den zentralen Ansatz von PEPP-PT setzen wolle, verschwand abends plötzlich der Hinweis auf den dezentralen Ansatz DP-3T von der Website. Initiator Boos beteuerte am Freitag auf einer Pressekonferenz, dass dies aufgrund eines Versehens geschehen sei. Mitinitiator Thomas Wiegand vom Fraunhofer Heinrich Hertz-Institut bezeichnete die Diskussionen, ob man nun den zentralen oder dezentralen Ansatz verfolge, gar als "side show", also einen Nebenschauplatz.

Doch einige Beobachter werteten den verschwundenen Hinweis auf DP-3T auf der Website als Vorentscheidung für einen zentralen Ansatz. Am Freitag distanzierte sich ein erster Mitstreiter von dem Projekt: Auch wenn er noch an die Kernidee einer internationalen und datenschutzfreundlichen App glaube, so wisse er nicht mehr, wofür PEPP-PT genau stehe, schrieb der Epidemiologe Marcel Salathé auf Twitter. "Für mich ist die Diskussion um Dezentralität oder Zentralität zentral", sagte er ZEIT ONLINE. Am Wochenende kündigten weitere Institute an, PEPP-PT nicht länger zu unterstützen – darunter die ETH Zürich, die ETHL, das Helmholtz-Institut für Informationssicherheit (CISPA) und die Katholische Universität Leuven.

Was auch nicht für Vertrauen in PEPP-PT sorgte: Am Karfreitag hatten auch Google und Apple in einer mehr als ungewöhnlichen Kooperation einen Ansatz vorgestellt, der dezentral funktioniert. Ihre Betriebssysteme würden dabei langfristig sogar ohne Apps das Contact-Tracing ermöglichen. Ein Weg, der natürlich kritisiert wurde, weil er von den Zentralisierungskönigen Apple und Google kam, dessen dezentrale Idee aber auch Lob aus der Crypto-Community erhielt. Und ein Weg, der Boos offenbar nicht gefällt. Auf der Pressekonferenz am Freitag soll er gesagt haben: Erziele man keine Einigung mit den Unternehmen über einen zentralen Bluetooth-Ansatz, würden Minister aus Regierungen das ihnen um die Ohren fliegen lassen.

Für ihn sei das keine religiöse Frage, ob man nun einen zentralen Ansatz wähle oder einen dezentralen, sagt Epidemiologe Salathé. Er fordert vielmehr, diese Debatte müsse mit voller Transparenz geführt werden. Aber wenn man einen zentralen Ansatz vorschlage, brauche er als Wissenschaftler alle Informationen und müsse dann auch offen Kritik äußern dürfen. Ganz vom PEPP-PT-Projekt verabschiedet scheint Salathé sich nicht zu haben: Er sei grundsätzlich weiter diskussionsbereit. "Letztlich geht es darum, dass sich möglichst viele Menschen eine App herunterladen. Dafür müssen sie dem Grundkonstrukt vertrauen können."