Jan-Philipp Stroscher, Sabrina Schomberg, Alexander Heinrich, Tim Grube

Datensicherheit von Corona-Apps nach der DSGVO

Der Beitrag analysiert die Protokolle der Konsortien DP-3T und PEPP-PT aus technischer Perspektive und grenzt diese voneinander ab. Zudem wird die technische Ausgestaltung der Entwicklerschnittstelle (API) von Google und Apple dargestellt. Aufbauend darauf erfolgt eine rechtliche Beurteilung der sich aus Art. 5 Abs. 1 lit. f, 25, 32 DSGVO ergebenden und die Datensicherheit betreffenden Kriterien und deren konkrete Umsetzung in den Protokollen.

Dr. Tim Grube

Wissenschaftlicher Koordinator GRK Privacy and Trust for Mobile Users am Fachbereich Informatik der Technischen Universität Darmstadt

E-Mail: grube@tk.tu-darmstadt.de

Alexander Heinrich, M.Sc. (IT-Sicherheit)

Wissenschaftlicher Mitarbeiter am Secure Mobile Networking Lab, Technische Universität Darmstadt

E-Mail:
aheinrich@seemoo.tu-darmstadt.de

Jan-Philipp Stroscher

Wissenschaftlicher Mitarbeiter am Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht im ITeG an der Universität Kassel; Projekt „emergenCITY – The Resilient Digital City“
E-Mail:
jan-philipp.stroscher@uni-kassel.de

Sabrina Schomberg

Wissenschaftliche Mitarbeiterin am Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht im ITeG an der Universität Kassel; Projekt Nudger.
E-Mail:
sabrina.schomberg@uni-kassel.de

Die Kontaktnachverfolgung per App bleibt weiterhin Gesprächsthema. Nachdem mittels strenger Kontaktbeschränkungen und weiteren, das öffentliche Leben beschränkenden Maßnahmen versucht wurde, die Verbreitung des Corona-Virus einzudämmen, werden diese Maßnahmen nun langsam gelockert. Um trotz der Lockerungen einen erneuten Anstieg der Infektionszahlen zu verhindern, soll eine App helfen, Kontakte mit mit COVID-19 infizierten Personen schnell und einfach nachzuverfolgen.

Es wurde viel darüber diskutiert, welcher der effektivste Ansatz zur Nachverfolgung ist und wie man die Privatsphäre der Bürgerinnen und Bürger am besten schützen kann. Nachdem ursprünglich funkzellenbasierte und GPS-basierte Ansätze zur Kontaktnachverfolgung diskutiert wurden, die zu Recht auf heftige Kritik gestoßen sind, erfolgt die Kontaktnachverfolgung nun mittels Bluetooth.

1 Die konkurrierenden Ansätze

Das PEPP-PT-Konsortium (Pan-European Privacy-Preserving Proximity Tracing) hat früh mit einer interdisziplinären Entwicklung einer Kontaktnachverfolgungs-App für ganz Europa begonnen. Das Konsortium verfolgte dabei vornehmlich einen zentralisierten Ansatz.

Das Konsortium DP-3T (Decentralized Privacy-Preserving Proximity Tracing), welchem sich nach einer Meinungsverschiedenheit über die technische Ausgestaltung auch verschiedene Wissenschaftler des PEPP-PT-Konsortiums angeschlossen haben, verfolgt hingegen zwei leicht unterschiedliche dezentrale Ansätze.

Außerdem arbeiten Apple und Google an einer API, welche direkt in die Betriebssysteme der Smartphones integriert werden soll, um eine umfangreiche Implementierung der Apps zur Kontaktnachverfolgung auf allen Geräten zu ermöglichen. Diese Schnittstelle macht jedoch auch gewisse Vorgaben für die daran anknüpfenden Apps. So sollen u. a. nur dezentrale Ansätze mit der Schnittstelle kompatibel sein.

Nachdem über Vor- und Nachteile eines dezentralen und eines zentralen Ansatzes der Kontaktnachverfolgung kontrovers diskutiert und die Kritik an einem zentralen Ansatz immer lauter wurde (u. a. vom Chaos Computer Club, CCC) hat die Bundesregierung eine Kehrtwende hin zu einem dezentralen Ansatz voll-

zogen. Es ist davon auszugehen, dass dies nicht zuletzt erfolgte, um mehr Akzeptanz für eine solche App in der Bevölkerung zu schaffen. Ein weiterer ausschlaggebender Punkt könnte gewesen sein, dass die von Apple und Google entworfene API ausschließlich einen dezentralen Ansatz unterstützt. Die Nutzung dieser Schnittstelle ist aber mitentscheidend für die Effektivität der Kontaktnachverfolgung, da beim Betriebssystem iOS von Apple eine Hintergrundnutzung von Bluetooth durch Apps auf Systemebene unterbunden wird und somit eine fortwährende Nachverfolgung der Kontakte nur durch Nutzung der API mit dem dahinterliegenden Bluetooth-Service gewährleistet werden kann.

Das Grundprinzip für eine Bluetooth basierte Kontaktnachverfolgung ist dabei in allen hier verglichenen Ansätzen gleich: Die Smartphones aller Nutzerinnen und Nutzer der App senden permanent Daten über BLE (Bluetooth Low Energy) an alle anderen sich in der Nähe befindenden Smartphones mit kompatiblen Apps. Diese Daten enthalten Identifikationsdaten (IDs), welche den installierten Apps zugeordnet werden können. Um eine Reidentifizierbarkeit und eine damit verbundene Profilbildung zu erschweren, werden diese IDs regelmäßig geändert. Mit Hilfe der IDs lässt sich die Kontakthistorie der Nutzerinnen und Nutzer nachvollziehen und eine entsprechende Kontaktbenachrichtigung erstellen.

2 Datenschutz und Datensicherheit

Über den Datenschutz der Apps zur Kontaktnachverfolgung, insbesondere über die Zulässigkeit der Datenverarbeitung, wurde bereits viel diskutiert.[1] Doch wie sieht es mit den technischen Komponenten des Datenschutzes und der Datensicherheit aus?

Die folgenden Überlegungen basieren, nach Betrachtung der bisherigen Protokolle der verschiedenen Ansätze sowie der aktuellen Debatte, auf der Annahme, dass die Apps nicht vollständig anonym funktionieren werden, sondern die Pseudonyme an verschiedenen Stellen ggf. einen Rückschluss auf Nutzerinnen und Nutzer der App zulassen und somit einen Personenbezug aufweisen könnten. Wenn dies der Fall ist, bedarf es für die Verarbeitung der Pseudonyme einer Rechtsgrundlage (Art. 6 Abs. 1 DSGVO). Als mögliche Rechtsgrundlage käme – solange weder auf europäischer noch auf nationaler Ebene entsprechende spezielle gesetzliche Regelungen bestehen – eine Einwilligung in Betracht.[2] Diese muss sich am Maßstab des Art. 7 und Art. 4 Nr. 11 DSGVO orientieren, ggf. in Verbindung mit Art. 9 Abs. 2 lit. a DSGVO, wenn Gegenstand der Verarbeitung die Bereitstellung der Information über ein positives COVID-19 Testergebnis mittels App ist. Die Einwilligung muss also nach Art. 4 Nr. 11 DSGVO zwingend freiwillig, für einen bestimmten Fall und in informierter Weise erfolgen, im Fall von Art. 9 Abs. 2 lit. a DSGVO zudem ausdrücklich.[3] Der Europäische Datenschutzausschuss betont daher auch in seinen Richtlinien für Kontaktnachverfolgungs-Apps vor allem das Erfordernis der Freiwilligkeit. Bürgerinnen und Bürgern dürfen keine Nachteile aus der Nichtnutzung der App erwachsen.[4] Neben diesen Anforderungen an die Einwilligung sind auch die allgemeinen Datenschutzgrundsätze aus Art. 5 DSGVO sowie die weiteren Anforderungen der DSGVO zu beachten.[5]

Dieser Beitrag konzentriert sich auf die Datensicherheit nach der DSGVO. Diese ist vor allem im Grundsatz der Integrität und Vertraulichkeit aus Art. 5 Abs. 1 lit. f DSGVO normiert, welcher in Art. 32 DSGVO konkretisiert wird.[6] Die von Art. 25 DSGVO geforderten Maßnahmen des Datenschutzes durch Technikgestaltung gehen wiederum mit der Datensicherheit Hand in Hand und überschneiden sich teilweise.[7] Sowohl Art. 25 als auch Art. 32 DSGVO verlangen „geeignete technische und organisatorische Maßnahmen", wobei die Pseudonymisierung jeweils beispielhaft erwähnt wird (vgl. Art. 25 Abs. 1 DSGVO, Art. 32 Abs. 1 lit. a DSGVO). Der Regelungsgehalt der beiden Normen und folglich auch die Maßnahmen sind daher nicht immer trennscharf nur einer Norm zuzuordnen.[8] Art. 32 DSGVO, der die Sicherheit der Verarbeitung regelt, erzeugt eine Verbindung zwischen der klassischen IT-Sicherheit (vgl. hierzu auch § 2 Abs. 2 BSIG) und dem Datenschutz, indem die DSGVO auch die IT-Sicherheit – die DSGVO spricht von „geeignete technische und organisatorische Maßnahmen" – als notwendigen Bestandteil eines umfassend zu gewährleistenden Datenschutzes ansieht.

3 Vergleich der Ansätze

Für den Vergleich der Ansätze sollen zunächst ihre jeweiligen technischen Spezifikationen zur Kontaktnachverfolgung dargestellt werden. Hierbei gilt für alle Ansätze, dass die Daten, die über BLE gesendet werden, öffentlich einsehbar sind. Nur so kann sichergestellt werden, dass jedes Empfangsgerät die Daten auch verwerten kann, was aber auch eine Kenntniserlangung durch Dritte, nicht am Versendevorgang beteiligte Akteure ermöglicht.

3.1 DP-3T

Ansatz 1

Die Erzeugung der zu versendenden IDs findet auf dem Smartphone in drei Schritten statt: Zu Beginn wird auf dem Smartphone ein zufälliger Tagesschlüssel für den aktuellen Tag erzeugt (Schritt 1). Von diesem Schlüssel ausgehend werden nun mit Hilfe von kryptografischen Einweg-Funktionen mehrere IDs für den aktuellen Tag generiert. Diese werden über BLE versendet und ändern sich im Abstand von 10-20 min. Die Empfängerin oder der Empfänger einer solchen ID kann anhand dieser nicht den initialen Tagesschlüssel herausfinden, da die kryptografischen Einweg-Funktionen nicht zurückgerechnet werden können (Schritt 2). Zuletzt wird von dem ursprünglichen Tagesschlüssel der Tagesschlüssel für den Folgetag abgeleitet, von dem wiederum neue IDs erzeugt werden können (Schritt 3).

Der Ablauf für die Rückmeldung einer COVID-19-Erkrankung ist nach beiden Ansätzen des DP-3T-Konsortiums gleich. Eine Per-

1 Blasek, in: ZD-Aktuell 2020, 07120; Roßnagel, in: ZD-Aktuell 2020, 07117; zu verfassungsrechtlichen Grundlagen siehe auch Roßnagel, in: ZD-Aktuell 2020, 07118; zur Forderung nach einem eigenständigen Corona-App-Gesetz siehe Johannes, in: ZD-Aktuell 2020, 07114.

2 vgl. auch Leitlinien des Europäischen Datenschutzausschusses, 04/2020.

3 vgl. Klement, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7 DSGVO, Rn. 47 ff.; Petri, ebd., Art. 9 DSGVO, Rn. 33.

4 Leitlinien des Europäischen Datenschutzausschuss, 04/2020.

5 vgl. dazu ausführlich die Leitlinien des Europäischen Datenschutzausschusses, 03/2020; Rechtliche Analyse der "Contact-Tracing-App".

6 Richter, in: Jandt/Steidle (Hrsg.), Datenschutz im Internet, 2018, B. IV. Rn. 36.

7 Mantz, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 2018, Art. 25 Rn. 55.

8 vgl. Laue, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2019, § 7 Rn. 4.

son erhält nach einer COVID-19-Diagnose einen Code (beispielsweise einen QR-Code) von einer autorisierten Stelle. Diesen gibt sie in der App ein, welche eine verschlüsselte TLS-Verbindung zum Server öffnet und den Autorisierungscode und die Tageschlüssel des relevanten Zeitraums an den Server sendet. Nach dem Upload auf den Server verifiziert dieser den Autorisierungscode und speichert die Tagesschlüssel. Dadurch wird sichergestellt, dass alle Tagesschlüssel auf dem Server von erkrankten Personen stammen. Es werden keine anderen Informationen im Zusammenhang mit dem Upload (wie IP-Adressen oder Uhrzeit) gespeichert. Die installierten Apps laden nur die Tagesschlüssel (nicht alle ausgetauschten IDs) des relevanten Zeitraums von allen infizierten Personen von einem entsprechenden (zentralen) Server herunter, um dann lokal auf dem Gerät einen Vergleich mit allen empfangenen IDs durchzuführen. Jeder Tageschlüssel ist fest mit einem Datum verknüpft. Dadurch wird verhindert, dass andere Personen getäuscht werden können, indem ein Schlüssel von einer infizierten Person verwendet wird, um neue IDs zu erzeugen und zu versenden.[9]

Ansatz 2
Die Erzeugung der IDs erfolgt bei diesem Ansatz komplett zufällig. Es gibt also keinen Tagesschlüssel, von welchem die IDs abgeleitet werden. Für jeden Zeitraum (10-20 min), in dem eine ID versendet wird, wird ein neuer zufälliger Wert generiert, von dem die ID abgeleitet wird. Außerdem wird nur ein wechselnder Teil dieser ID versendet. Diese einzelnen Teile der ID lassen sich nur zu einer vollständigen ID zusammenfügen, wenn zwei Nutzerinnen oder Nutzer sich für eine bestimmte Zeit (ca. 10-15 Minuten) in unmittelbarer Nähe aufgehalten haben (Abstand 1,5 bis 2 m), weil sich dann aus mehreren Übermittlungen eine vollständige ID ergibt. Dies hilft zugleich bei der Risiko-Bewertung, da somit auch die Dauer eines Kontakts abgeschätzt werden kann.

Der Ablauf für die Rückmeldung einer COVID-19-Erkrankung an die App erfolgt hingegen genau wie im ersten Ansatz (s. o.). Nachdem die (vollständigen) IDs der infizierten Personen auf den Server hochgeladen wurden, erzeugt dieser einen kryptografischen Filter, den alle Nutzerinnen und Nutzer erhalten, um lokal abgleichen zu können, welche IDs zu einer infizierten Person gehören. Dadurch besteht zwar weiterhin die Möglichkeit, herauszufinden, zu welcher Zeit man eine infizierte Person getroffen hat. Es ist aber nicht mehr möglich, neue IDs aus den initialen Werten zu generieren. Auch hier gilt, dass keine weiteren Nutzerdaten erhoben werden.

Überdies kann eine Person mit Zugriff auf den Server keine sozialen Graphen erstellen und somit nicht nachvollziehen, welche Personen miteinander in Kontakt standen. Da alle auf dem Server gespeicherten Informationen allen Nutzerinnen und Nutzern der App zugänglich sind, erhalten Angreiferinnen und Angreifer durch Zugriff auf den Server nicht mehr Informationen, als ohnehin bekannt sind. Somit können mit Hilfe der Serverdaten nur die IDs von Erkrankten mit eventuell vorher aufgenommenen IDs vergleichen werden.

3.2 PEPP-PT

Bei der zunächst geplanten zentralisierten Lösung des PEPP-PT-Konsortiums wäre eine begrenzte Anzahl von IDs zufällig auf einem zentralen Server erzeugt und sodann an die Smartphones mit der Kontaktnachverfolgungs-App übermittelt worden. Diese IDs können dann in einem bestimmten Zeitraum über BLE versendet werden. Sobald die übermittelten IDs verbraucht sind, werden vom Server neue IDs an die App übermittelt. Falls zu diesem Zeitpunkt keine Verbindung zum Server besteht, kann die Kontaktnachverfolgung mangels IDs nicht erfolgen. Das hat hingegen nicht zur Folge, dass eine dauerhafte Verbindung zum Server notwendig wäre. Dem zentralen Server wäre jede jemals versendete ID bekannt gewesen. Ohne weitere Sicherheitsmaßnahmen wäre es theoretisch möglich gewesen, auf dem Server soziale Graphen zu erstellen. Solch ein Graph könnte eine Deanonymisierung der Daten und damit auch eine Überwachung ermöglichen, was als einer der größten Kritikpunkte gegenüber einer zentralisierten Lösung formuliert wurde.

4 API von Apple & Google

Die von Apple und Google mit dem jeweiligen Betriebssystemupdate bereitgestellte API wird auch von der von SAP und der Telekom entwickelten deutschen Corona-Warn-App verwendet. Die API und das dahinterliegende Framework setzen das Protokoll um, welches sich im Wesentlichen an den Spezifikationen des Ansatzes 1 von DP-3T orientiert, und stellt eine möglichst hohe Kompatibilität sicher.

Die Tagesschlüssel werden dabei auch verwendet, um weitere Metadaten, gegenwärtig nur die Signalstärke und die Protokollversion, verschlüsselt mit den per BLE versendeten Nachrichten zu verbinden. Durch die Aufzeichnung der Signalstärke wird eine Schätzung des Abstands zwischen den Smartphones ermöglicht. Die Tagesschlüssel bleiben dabei maximal 14 Tage auf dem eigenen Smartphone gespeichert. Wird eine Nutzerin oder ein Nutzer positiv auf COVID-19 getestet, dann werden diese Schlüssel an den Server übertragen. Die Corona-Warn-App rekonstruiert aus den Tagesschlüsseln IDs und vergleicht diese. Soweit Kontakt zu einer erkrankten Person bestanden hat, können auch die Metadaten entschlüsselt werden. Dadurch kann beispielsweise ermittelt werden, wie viel Abstand die Personen zueinander hatten und über welchen Zeitraum der Kontakt bestand.

Demzufolge ermöglicht die API die Kommunikation zwischen den Apps auf den Smartphones und nimmt die erforderliche Risikoberechnung vor. Die Privatsphäre der Nutzer wird durch das komplexe kryptografische System geschützt. Da jedoch lediglich die Spezifikationen der API und nicht der Quellcode als Open Source veröffentlicht wurde, kann an dieser Stelle keine weitergehende Analyse der ermöglichten Verarbeitungsvorgänge erfolgen.

5 Erfüllen diese Ansätze die Anforderungen von Art. 25, 32 DSGVO?

5.1 Art. 25 DSGVO – Datenschutz durch Technikgestaltung

Der Regelungsgehalt von Art. 25 Abs. 1 DSGVO (Datenschutz durch Technikgestaltung) beinhaltet, dass der Datenschutz gerade mit Hilfe der Technik erreicht werden soll. Dem Verantwortlichen wird damit per Gesetz auferlegt, technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu er-

9 vgl. zum Ablauf: Overview of Data Protection and Security, DP-3T https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf

greifen. Die Technikgestaltung setzt also bereits vor der Verarbeitung von personenbezogenen Daten an.[10] Damit geht der Regelungsgehalt des Art. 25 DSGVO über rein datensicherheitsrechtliche Aspekte hinaus, wobei wir uns hier jedoch auf diese Aspekte konzentrieren.

Die Protokolle des DP-3T-Konsortiums und die API von Apple und Google sehen als technische und organisatorische Maßnahme i. S. d. Art. 25 DSGVO u. a. eine Pseudonymisierung vor. Eine echte und vollständige Anonymisierung ist hingegen in keinem Ansatz vorgesehen. Allerdings dürfte diese sich auch funktional nicht mit dem Zweck der App vertragen, sodass sie rechtlich nicht gefordert ist. Immerhin beabsichtigt keiner der Ansätze Klarnamen oder Handynummern zu nutzen, da alle Ansätze mindestens eine Pseudonymisierung vorsehen. Ansatz 1 des DP-3T-Konsortiums sieht vor, einen zufälligen Tagesschlüssel auf dem Smartphone zu erzeugen, welcher dann mit Hilfe kryptografischer Einweg-Funktionen IDs erzeugt. Ansatz 2 geht darüber sogar noch hinaus, indem nur ein wechselnder Teil der zufällig erzeugten IDs versendet wird und sich erst nach einiger Zeit aus diesen Teilen die vollständige ID zusammensetzen lässt. Die Verbesserung der Datensicherheit erfolgt in diesem Ansatz durch das Aufbrechen der ID: Bewegt sich eine Nutzerin oder ein Nutzer, während die IDs von Geräten zur stillen Beobachtung empfangen werden, so werden wahrscheinlich nicht alle notwendigen Teile der ID empfangen und die Wahrscheinlichkeit der Zuordnung einer ID zu einer Nutzerin oder einem Nutzer sinkt.

Das PEPP-PT-Protokoll sieht hingegen vor, dass die IDs zufällig auf dem Server erzeugt werden, weswegen diesem Server alle IDs bekannt wären. Im Gegenzug müssten die IDs der Infizierten jedoch nicht an alle Nutzerinnen und Nutzer versendet werden.

5.2 Art. 32 DSGVO – Datensicherheit

Art. 32 DSGVO behandelt die Datensicherheit, also die Gesamtheit aller technischen und organisatorischen Maßnahmen, die einen unzulässigen Umgang mit personenbezogenen Daten verhindert. Im Gegensatz zu Art. 25 DSGVO, welcher auf alle Datenschutzgrundsätze verweist, setzt Art. 32 DSGVO vornehmlich am Datenschutzgrundsatz der Integrität und Vertraulichkeit aus Art. 5 Abs. 1 lit. f DSGVO an.[11] Da die Maßnahmen zur Pseudonymisierung bereits im Rahmen des Art. 25 DSGVO aufgeführt wurden, konzentrieren sich die Ausführungen im Folgenden auf die Punkte der Verfügbarkeit, Vertraulichkeit und Integrität.

Verfügbarkeit
Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen, IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.[12] Dies gilt auch für den Fall eines Hackerangriffes oder einer Naturkatastrophe. Verfügbarkeit kann z. B. dadurch erreicht werden, dass eine Lösung ohne die regelmäßige Verbindung zu einem Server auskommt oder durch die Verwendung resilienter Server-basierter Lösungen, die im Falle eines Angriffs automatisch ein zweites System starten.

Die Ansätze von DP-3T haben den Vorteil, dass die auf dem Protokoll aufbauenden Apps auch bei einem längeren Serverausfall weiterhin IDs versenden und empfangen können. Lediglich positiv Getestete können in diesem Zeitraum keine IDs mehr hochladen und auch andere Nutzerinnen und Nutzer können diese IDs nicht herunterladen. Somit kann zeitweise niemand mehr gewarnt werden, was im Falle eines Serverausfalls auch für den PEPP-PT-Ansatz gilt. Die Kontaktnachverfolgung der App bleibt jedoch nach den Protokollen des DP-3T-Konsortiums und bei der Lösung von Apple und Google auch bei einem Serverausfall verfügbar. Bei der Lösung von PEPP-PT funktioniert die App nur so lange autonom weiter, bis alle zuvor vom Server übermittelten IDs verbraucht wurden. Da bei einem Serverausfall keine IDs mehr übermittelt werden können, ist eine Kontaktnachverfolgung zu dieser Zeit nicht möglich und kann auch nicht nachgeholt werden.

Ein Nachteil, zumindest im Hinblick auf die Verfügbarkeit, ist der Umstand, dass die Lösung von Apple und Google in das Betriebssystem eingepflegt wird und damit jederzeit auf Grundlage einer eigenen Bewertung von den Herstellern deaktiviert werden kann. Daher bleibt es Apple und Google vorbehalten, über das Fortbestehen der Notwendigkeit zu entscheiden, was Apple und Google auch bereits angekündigt haben zu tun. Ein datenschutzrechtlicher Vorteil ist demgegenüber zweifelsfrei die Förderung des Grundsatzes der Datenminimierung und die Einhaltung der Zweckbindung. Soweit der Zweck erfüllt ist, dürfen auch keine weiteren personenbezogenen Daten verarbeitet werden. Kehrseite dieses Vorteils ist wiederum, dass man theoretisch der Bewertung der Zweckerreichung von Apple und Google „ausgeliefert" ist. Hierbei bleibt zu hoffen, dass eine Deaktivierung in Absprache mit den jeweiligen Länderregierungen erfolgt.

Weiterhin ist das Kriterium der Belastbarkeit als Unterpunkt der Verfügbarkeit auf dessen Erfüllung hin zu untersuchen. Dieses Kriterium beschreibt die Fähigkeit einer Organisation, einer Beeinträchtigung durch Störung zu widerstehen und eine rasche Wiederherstellung der Verfügbarkeit von bzw. dem Zugang auf personenbezogene Daten bei einem physischen oder technischen Zwischenfall zu gewährleisten.[13]

Die dezentralen Systeme haben in diesem Fall den Vorteil, dass das System selbst bei Verlust aller Daten durch Nutzung eines neuen Servers wieder starten kann. Auf dem Server liegen nur Daten, mit denen die IDs von infizierten Personen berechnet werden können. Da die Apps sich automatisch aktualisieren, ist es wahrscheinlich, dass viele bereits die aktuellen Datensätze lokal gespeichert haben. Nach einem Neustart können sich die Apps wieder mit dem neuen Server verbinden und lokal die Möglichkeit eines Kontakts zu infizierten Personen prüfen. Ein Verlust dieser Daten wäre also weniger dramatisch als bei einem zentralen System, da bei diesem alle versendeten IDs aller Nutzer und Nutzerinnen verloren gehen würden und eine Identifizierung im Nachhinein nicht mehr möglich wäre. Wie die Belastbarkeit letztendlich zu bewerten ist, hängt von der konkreten Umsetzung dieser Systeme ab, die gegenwärtig noch nicht zur Verfügung steht.

Vertraulichkeit
Die Vertraulichkeit bezeichnet die Eigenschaft eines Systems, berechtigte Zugriffe festzulegen und das System vor unberechtigten

10 vgl. dazu Barlag, in: Roßnagel (Hrsg.), Europäische Datenschutz-Grundverordnung, 2017, S. 172 f.

11 Hansen, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 32 DSGVO, Rn.1.

12 BSI, IT-Grundschutz-Kompendium, Verfügbarkeit, Glossar, 2020.

13 Witt, in: Koreng/Lachenmann (Hrsg.), Formularhandbuch Datenschutzrecht, 2018, C, V, Rn. 1,2.

Zugriffen zu schützen.[14] Bei der Vertraulichkeit der Daten kommt es darauf an, dass Dritte keinen einfachen Zugriff auf die Daten erhalten. Somit muss sichergestellt werden, dass sowohl die Daten auf dem Server als auch auf dem Gerät ausreichend geschützt sind. Hinzu kommt, dass die Daten auch während der Kommunikation zum Server oder vom Server nicht ausgelesen werden können.

Auch hier bietet ein dezentrales System einige Vorteile. Alle IDs (oder, je nach Ansatz, Tagesschlüssel) von Erkrankten, die an den Server gesendet werden, sind öffentlich verfügbar, damit alle Nutzerinnen und Nutzer von Kontaktnachverfolgungs-Apps diese mit ihren empfangenen IDs abgleichen können. Da die IDs pseudonym sind, ist ein Schutz vor Angreifern nicht nötig. Auf dem Gerät sollten alle empfangenen IDs geschützt werden, was jedoch eine Frage der Implementierung der App ist. Diese Frage ist nicht Gegenstand dieses Beitrags. Eine entsprechende Verschlüsselung der Daten auf dem Smartphone ist jedoch ohne weiteres möglich.

Da auch vom PEPP-PT-Konsortium keine fertige Lösung vorgestellt wurde, kann auch hier die Einhaltung dieses Kriteriums nicht bewerten werden. Wichtiger ist es ohnehin, einen entsprechenden Schutz der Server zu gewährleisten, auf denen sämtliche von den Nutzerinnen und Nutzern geteilten IDs gesammelt vorliegen. Dazu zählt auch die Geheimhaltung der Zuordnungsregeln, da andernfalls die Pseudonyme aufgelöst und Personen identifiziert werden könnten.

Letztlich muss auch der schreibende Zugriff auf den Server geschützt werden. Die App wird die Möglichkeit haben, nach einem positiven COVID-19-Test IDs an den Server zu senden. Daher muss sichergestellt werden, dass es für Angreifer keine Möglichkeit gibt, sich dieser Schnittstelle zu bedienen, um falsche IDs an den Server zu senden, da dies zu falschen Benachrichtigungen führen würde.

Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten (dass die Daten vollständig und unverändert sind) und der korrekten Funktionsweise von Systemen.[15]

Dieses Kriterium gilt für jeden Ansatz und kann nicht ohne eine veröffentlichte Softwarelösung validiert werden. Mit Hilfe von verbreiteten kryptografischen Funktionen ist es jedoch möglich, die Einhaltung dieses Kriteriums zu gewährleisten. Ansatz 2 des DP-3T-Konsortiums sieht beispielsweise vor, nicht die initiale, zufällige ID einer infizierten Person mit allen Nutzerinnen und Nutzern der App zu teilen, sondern diese in einen kryptografischen Filter zu integrieren. Durch diesen Filter ist es nicht mehr möglich, neue IDs aus den initialen Werten zu generieren und somit andere Menschen fälschlicherweise zu benachrichtigen.

6 Zusammenfassung und Ausblick

Die Bundesregierung hat die Unternehmen SAP und Telekom mit der Entwicklung der Corona-Warn-App beauftragt, die auf einer dezentralen Lösung basiert. Dabei werden sie von der Fraunhofer-Gesellschaft und dem Helmholtz-Zentrum für Informationssicherheit CISPA beratend unterstützt. Die Dokumente und der Code der App sind über die Open-Source-Plattform Github einsehbar.[16] Die App startete erfolgreich und hat schon innerhalb der ersten Woche rund 10 Millionen Downloads erreicht.

Die Maßnahmen zum Zweck der Datensicherheit des Ansatzes 2 des DP-3T-Konsortiums gehen noch über die im Ansatz 1 vorgesehenen Maßnahmen hinaus. Aus Sicht der Datensicherheit wäre daher eine Umsetzung der App nach dem Protokoll des Ansatzes 2 des DP-3T-Konsortiums wünschenswert gewesen. Ansatz 1 ist jedoch im Zusammenspiel mit der Schnittstelle von Apple und Google leichter umzusetzen und daher praktikabler. Auch Ansatz 1 des DP-3T Protokolls erfüllt die Anforderungen der Datensicherheit aus der DSGVO. Eine Veröffentlichung des Quellcode der API wäre jedoch wünschenswert, um eine umfassende technische und rechtliche Analyse zu ermöglichen.

Literatur

[1] Blasek, K., *Covid-19-Contact-Tracing-Apps – Leitlinien des EDSA*, ZD-Aktuell 2020, 07120.

[2] BSI, *IT-Grundschutz-Kompendium*, Glossar, 2020, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html (Stand: 01.06.2020).

[3] Bundesregierung, *Infektionsketten unterbrechen, So hilft die Corona-Warn-App*, Beitrag vom 29.05.2020, https://www.bundesregierung.de/breg-de/aktuelles/corona-warn-app-1747738 (Stand: 01.06.2020).

[4] Europäischer Datenschutzausschuss (EDSA), *Leitlinien 3/2020 für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem Covid-19-Ausbruch*, angenommen am 21.04.2020.

[5] Europäischer Datenschutzausschuss (EDSA), *Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von Covid-19*, angenommen am 21.04.2020.

[6] Jandt, S./Steidle, R. (Hrsg.), *Datenschutz im Internet*, Rechtshandbuch zu DSGVO und BDSG, Baden-Baden 2018

[7] Johannes, P., *Bedarf an und Inhalt eines Gesetzes für Corona-Tracing-Apps*, ZD-Aktuell 2020, 07114.

[8] Koreng, A/Lachenmann, M. (Hrsg), *Formularhandbuch Datenschutzrecht*, München, 2. Auflage 2018

[9] Laue, P./Kremer, S., *Das neue Datenschutzrecht in der betrieblichen Praxis*, Baden-Baden, 2. Auflage 2019

[10] Simitis, S./Hornung, G./Spiecker gen. Döhmann, I. (Hrsg.), *Datenschutzrecht, DSGVO mit BDSG*, Baden-Baden 2019.

[11] Sydow, G. (Hrsg.), *Europäische Datenschutzgrundverordnung*, Handkommentar, Baden-Baden, 2. Auflage 2018

[12] Roßnagel, A. (Hrsg.), *Europäische Datenschutz-Grundverordnung, Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts*, Baden-Baden 2017

[13] Roßnagel, A., *Streit über Datenschutz bei Tracing-Apps*, ZD-Aktuell 2020, 07117.

[14] Roßnagel, A., *Tracing-App: Verfassungsrechtliche Grundlagen und Kriterien für ihren Einsatz*, ZD-Aktuell 2020, 07118.

14 Hansen, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 32 Rn. 39.

15 BSI, IT-Grundschutz-Kompendium, Integrität, Glossar, 2020; Hansen, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 32 Rn. 40.

16 Bundesregierung, So hilft die Corona-Warn-App, Internetquelle.