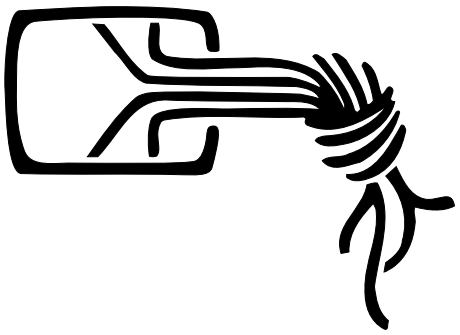

Blackbox-Sicherheitsbetrachtung Corona-Datenspende-App des RKI

Selektive Analyse und Empfehlung für Verantwortliche

Martin Tschirsich, Patrick Jäger, André Zilch

Chaos Computer Club

Version 1.0, 19. April 2020

KURZFASSUNG

Am 7. April 2020 veröffentlichte das Robert-Koch-Institut (RKI) eine Corona-Datenspende-App zur Weitergabe von Fitnesstracker-Daten. Ein erfolgreicher Angriff auf die Informationssicherheit dieser „Corona-App“ hat das Potenzial, die Akzeptanz von und das Vertrauen in App-gestützte Maßnahmen zur Eindämmung der SARS-CoV-2-Pandemie zu schwächen.

Hieraus entspringt ein gesamtgesellschaftliches Risiko. Die vorliegende Sicherheitsbetrachtung bietet Anstoß und Hilfestellung zu dessen Eingrenzung und ist aus dem Wunsch heraus entstanden, das RKI und weitere Betreiber von Corona-Apps zu einer proaktiven, transparenten und chancengetriebenen Betrachtung der Informationssicherheit zu ermutigen.

Folgende Sicherheitsmängel der Corona-Datenspende-App wurden identifiziert und mit entsprechenden Empfehlungen dokumentiert:

- Fitnessdaten werden regelmäßig nicht vom Smartphone des Datenspenders aus an das RKI übermittelt, sondern vom RKI direkt beim Anbieter des Fitnesstrackers oder Google Fit abgefragt und erst anschließend pseudonymisiert. Hierzu speichert das RKI Zugangsdaten, mit denen u. a. auf die vollständige Fitnesshistorie und die Namen der Datenspender zugegriffen werden kann. Die Möglichkeit, Datenspender unter Missbrauch dieser Zugangsdaten direkt zu identifizieren, hebelt den Zweck der Pseudonymisierung aus.
- Es ist beabsichtigt, aus den Analyseergebnissen der Fitnessdaten lokale Maßnahmen zur Eindämmung der SARS-CoV-2-Pandemie abzuleiten. Das einfache Einbringen falscher Fitnessdaten erlaubt jedoch eine gezielte Beeinflussung dieser Maßnahmen.
- Bei Verknüpfung der App mit einem Fitnesstracker müssen dessen Zugangsdaten eingegeben werden. In der Mehrzahl der Fälle können diese durch Man-in-the-Middle-Angreifer mitgelesen werden. Zugangsdaten können zudem bei Verlust oder Diebstahl des Smartphones durch Dritte gestohlen werden.
- Der Server des RKI exponiert zusätzliche Funktionalität wie ein Management- und Admin-Interface sowie eine SOAP-API über das Internet. Die Angriffsoberfläche dieses sicherheitskritischen Servers wird damit unnötig vergrößert.
- Kenntnis des Pseudonyms eines Datenspenders erlaubt Dritten, dessen Verknüpfung mit einem Fitnesstracker einzusehen und zu manipulieren. Zudem besteht die Gefahr, dass Dritte darüber Ansprüche inkl. Recht auf Einsicht gemäß DSGVO erheben.
- Zudem sind die Anforderungen an eine wirksame Einwilligung zur Verarbeitung von Gesundheitsdaten nach DSGVO nicht erfüllt.

Viele der identifizierten Risiken lassen sich bereits mit Anwendung der vom Chaos Computer Club veröffentlichten 10 Prüfsteine für die Beurteilung von „Contact Tracing“-Apps eliminieren. Die Autoren empfehlen eine zeitnahe Umsetzung der gegebenen Empfehlungen.

INHALT

1 HINTERGRUND

Am 7. April 2020 veröffentlichte das Robert Koch-Institut (RKI) eine Corona-Datenspende-App für Android und iOS zur freiwilligen Weitergabe von Fitnesstracker-Daten an das RKI.

Zweck dieser von der Bundesregierung[1] beworbenen und vom Bundesgesundheitsministerium unterstützten App ist „eine bessere Vorhersage des bundesweiten Erkrankungsverlaufs mit Covid-19 und damit eine verbesserte Steuerung von Eindämmungsmaßnahmen gegen die Corona-Pandemie".

Bis zum 14. April 2020 wurde diese im Auftrag des RKI von der mHealth Pioneers GmbH entwickelte und betriebene App von bereits mehr als 400.000 Freiwilligen heruntergeladen und mit einem Fitnesstracker verknüpft[2].

Ein erfolgreicher Angriff auf die Informationssicherheit dieser prominenten und Pars pro Toto als „Corona-App" betitelten App hätte das Potenzial, die Akzeptanz von und das Vertrauen in diese und künftige App-gestützte Maßnahmen zur Eindämmung der SARS-CoV-2-Pandemie zu schwächen. Akzeptanz und Vertrauen aber bilden die Grundlage für eine großflächige freiwillige Nutzung und somit auch die Grundlage für einen möglichen epidemiologischen Nutzen. Ohne diese Grundlage ergeben sich vermeidbare gesamtgesellschaftliche Risiken.

Die Autoren sind daher der Überzeugung, dass die Informationssicherheit der App des RKI von gesamtgesellschaftlicher Bedeutung und von öffentlichem Interesse ist.

Dieser Bedeutung gegenüber steht bislang eine selbst durch die Fachöffentlichkeit nicht nachprüfbare Eigenerklärung des RKI. Ein zeitweilig vorgezeigtes Datenschutz-Gütesiegel „ePrivacyseal DE"[3] ist nach Auffassung der Autoren kein belastbarer Nachweis für die Angemessenheit der umgesetzten technischen und organisatorischen Sicherheitsmaßnahmen des RKI.

Mit der Veröffentlichung der vorliegenden und aus dem Eindruck dieses wahrgenommenen Defizits heraus unabhängig entstandenen und somit allenfalls punktuellen Sicherheitsbetrachtung verbinden die Autoren die Zuversicht, sowohl das RKI als auch Hersteller und Entwickler künftiger „Corona-Apps" zu einer proaktiven, transparenten und chancengetriebenen Betrachtung der Informationssicherheit ermutigen zu können. Der vorliegende Bericht bietet hierzu Anstoß und Hilfestellung.

[1] https://www.bundesregierung.de/breg-de/themen/coronavirus/datenspende-app-1739928, abgerufen am 13. April 2020.

[2] https://netzpolitik.org/2020/ein-fieberthermometer-fuer-deutschland/, abgerufen am 17. April 2020.

[3] https://web.archive.org/20200411203728/https://play.google.com/store/apps/details?id=de.rki.coronadatenspende, abgerufen am 13. April 2020.

2 SCHADPOTENZIALE

Die dem Nutzen einer App gegenüberstehenden Risiken entspringen Bedrohungen durch Angreifer, die unter Ausnutzung von Schwachstellen die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen aufbrechen und damit Schäden verursachen können.

Voraussetzung einer zielgerichteten Schwachstellenanalyse ist das vorherige Verständnis der Schadpotenziale und daraus abgeleiteter Schutzbedarfe.

2.1 Verarbeitete Daten und Betroffene

Schutzobjekte sind insbesondere die von den Benutzern der App (Datenspendern) bereitgestellten und vom RKI verarbeiteten Daten. Laut Datenschutzerklärung[4] verarbeitet das RKI folgende Daten, welche hauptsächlich aus mit dem Smartphone des Datenspenders verbundenen Fitnesstrackern entspringen:

- Soziodemographische Daten: Alter gerundet auf 5 Jahre. Größe gerundet auf 5 cm, Geschlecht. Gewicht gerundet auf 5 kg
- Aktivitätsdaten: Sport (bspw. Fahrradfahren, Laufen), Schlafen und Schlafphasen, Aktivsein (bspw. Gehen, Aktivität), Ruhezeiten
- Vitaldaten: Puls, Herzratenvariabilität, Stress, Temperatur, Gewicht
- Postleitzahl

Gesundheitsdaten sind nach Art. 9 DSGVO besonders sensible personenbezogene Daten. Alle Daten werden mit einem Pseudonym des Datenspenders verknüpft an das RKI übertragen.

Von der Verarbeitung der Daten und daraus abgeleiteten Maßnahmen Betroffene sind neben den Datenspendern insbesondere die Bürger und Unternehmen sowie das RKI selbst.

2.2 Schädigung der Datenspender

Eine Verletzung vor allem der Vertraulichkeit von Gesundheitsdaten kann negative Auswirkungen auf einen Datenspender haben. Der Schutz der Vertraulichkeit dieser Informationen ist daher von sehr hoher Bedeutung. Es ist davon auszugehen, dass pseudonyme Gesundheitsdaten umso eher einen Rückschluss auf die Identität des betroffenen Datenspenders zulassen, desto länger der Erhebungszeitraum ist.

[4] https://corona-datenspende.de/datenschutz-app/, abgerufen am 17. April 2020.

2.3 Schädigung der Bürger und Unternehmen

Zweck der App ist laut RKI „eine verbesserte Steuerung von Eindämmungsmaßnahmen gegen die Corona-Pandemie zu ermöglichen“. Die aus den Fitnessdaten gewonnenen wissenschaftlichen Ergebnisse sollen laut Bundesgesundheitsminister Spahn mit zur Beantwortung der politischen Frage herangezogen werden, „ob und welche Maßnahmen notwendig sind“.

Durch eine Verletzung der Integrität oder Authentizität der Fitnessdaten kann eine Einflussnahme auf diese Entscheidungsfindung versucht werden mit dem Ziel, die Eindämmung der SARS-CoV-2-Pandemie zu behindern oder unnötige volkswirtschaftliche Schäden zu verursachen.

Zudem wird bei einer Verletzung insbesondere der Vertraulichkeit der Gesundheitsdaten die Akzeptanz von und das Vertrauen in weitere App-gestützte Maßnahmen zur Eindämmung der SARS-CoV-2-Pandemie beschädigt. Eine daraus resultierende geringere Beteiligung an derartigen Maßnahmen kann sich ebenfalls negativ auf die Eindämmung der SARS-CoV-2-Pandemie auswirken.

2.4 Schädigung des Robert Koch-Institutes

Als Namensgeber für die App tritt das RKI sowohl gegenüber Datenspendern als auch gegenüber Wissenschaftlern und der Öffentlichkeit auf.

Damit wirken sich Mängel beim Schutz der erhobenen Daten ebenso wie fehlerhafte Prognosen und Maßnahmensteuerung direkt auf die Wahrnehmung des RKI in der Öffentlichkeit aus. Eine auf diese Weise beschädigte Reputation wird sich jedoch nicht nur auf das RKI, sondern auch auf zukünftige eHealth-Vorhaben direkt oder indirekt auswirken und den Grundtenor für die Wahrnehmung in der Öffentlichkeit setzen.

3 SCHWACHSTELLEN

Die nachfolgend gelisteten Schwachstellen wurden durch eine zeitlich begrenzte nicht-intrusive Analyse des Systems von außen identifiziert.

Betrachtet wurden zum einen die online exponierten Schnittstellen auf dem Server des RKI sowie die auf dem Smartphone des Datenspenders installierte Android- sowie iOS-App in Version 1.0.1. Alle Befunde konnten erneut in der aktuellen Android-App in Version 1.0.6 nachvollzogen werden.

Darüber hinaus wurden Schwachstellen in der Organisation und den Abläufen betrachtet.

3.1 Zentrale Speicherung von Zugangsdaten und Re-Identifikation

Die zentrale Funktionalität der Smartphone-App ist das Herstellen einer Verbindung zwischen dem Fitnesstracker des Datenspenders und dem Server des RKI sowie anschließend die kontinuierliche Weitergabe der Fitnessdaten über diese Verbindung. Die App leitet Fitnessdaten je nach Datenquelle auf unterschiedlichen Wegen an den Server des RKI:

1. Bei Wahl von Apple Health unter iOS werden Fitnessdaten vom Smartphone zunächst an die Smartphone-App und von der Smartphone-App an den Server des RKI übermittelt.
2. Bei Wahl einer der anderen Datenquellen wie Fitbit, Garmin, Polar, Withings oder Google Fit dagegen werden die Fitnessdaten sowohl unter iOS als auch Android direkt vom Server des Fitnesstracker-Anbieters oder von Google Fit an den Server des RKI übermittelt, ohne den Weg über die Smartphone-App zu gehen. Die Daten werden dabei laut RKI „im Hintergrund von den Servern der Hersteller Ihres Fitnessarmbands oder Ihrer Smartwatch automatisch abgefragt“[5]. Der Smartphone-App selbst kommt dabei keine aktive Rolle zu: „Die Anwendung kann geschlossen werden“[6].

Im Test wurde der zweite und erwartungsgemäß meistgenutzte Übertragungsweg exemplarisch anhand der Verknüpfung mit Google Fit nachvollzogen. Der Server des RKI fragt dabei Zugangsdaten u. a. für den Zugriff auf den vollständigen Namen des Datenspenders mit dem Parameter „response_type=code“ an:

```
https://accounts.google.com/o/oauth2/v2/auth?
access_type=offline&scope=https://www.googleapis.com/auth/fitness.activity.read+https:
//www.googleapis.com/auth/fitness.body.read+https://www.googleapis.com/auth/fitness.bo
dy_temperature.read+https://www.googleapis.com/auth/userinfo.profile&response_type=cod
e&redirect_uri=https://corona-
datenspende.de/gf_redirect/8wAHEjL2n9HXgBNzHVs5sW7JadFQfV2C/gf_redirect.php&state=••••
••••••••••••••••••••••_12_2_&prompt=consent&client_id=840426162873-
3sc1gus7f55c1atnavkoehfknfm6c01n.apps.googleusercontent.com&lang=de
```

[5] https://corona-datenspende.de/faq/, abgerufen am 13. April 2020

[6] https://corona-datenspende.de/faq/, abgerufen am 13. April 2020

Auch die Verknüpfung mit Fitnesstrackern von Withings, Fitbit sowie Polar erfolgt identisch zu Google Fit mit dem Parameter „response_type=code“. Damit wird der sog. „Authorization Code Flow“ nach OAuth2 initiiert.[7] Dabei erlangt der Server des RKI dauerhaft gültige Zugangsdaten in Form sog. Refresh-Token.

Bei Google Fit wird hierzu zusätzlich noch die oben gezeigte Angabe von „access_type=offline“ verlangt: „This value instructs the Google authorization server to return a refresh token and an access token the first time that your application exchanges an authorization code for tokens.“[8]

Das Refresh-Token erlaubt dem Server des RKI die Abfrage von Fitnessdaten und weiterer Daten des Datenspenders solange bis der Datenspender die erteilte Freigabe wieder entzieht. Google weist auf den damit einhergehenden hohen Schutzbedarf hin: „Important: Your application should store both tokens in a secure, long-lived location.“[9]

Aus dieser direkten Datenübertragung von Server zu Server folgt:

1. Der Server des RKI erhält direkten Zugang zu auf den Servern der Fitnesstracker-Anbieter oder bei Google Fit gespeicherten Daten. Hierzu speichert das RKI eine große Anzahl von Zugangsdaten mit hohem Schutzbedarf. Diese Zugangsdaten erlauben den Zugriff auf nicht pseudonymisierte und historische Fitnessdaten und bei den Anbietern Fitbit, Garmin, Polar und bei Google Fit den Zugriff auf die vollständigen Namen der Datenspender.
2. Der Server des RKI hat nicht nur Zugriff auf, sondern empfängt auch vollständige, d. h. nicht-pseudonymisierte Daten teils mitsamt vollständiger Namen der Datenspender. Eine Pseudonymisierung ist erst anschließend nach Empfang der vollständigen Daten auf Seiten des RKI möglich.
3. Eine Kontrolle des Datenflusses an das RKI und der anschließend vorgenommenen Pseudonymisierung durch das RKI ist dem Datenspender nicht möglich.
4. Der direkte Zugang des RKI zu den Fitnessdaten wird bei Deinstallation der Smartphone-App nicht automatisch beendet.

Die direkte Übertragung von Server zu Server ohne Umweg über das Smartphone des Datenspenders steht im Widerspruch zu Aussagen der Datenschutzerklärung der App:[10]

1. „Erfasste Daten werden von meinem Smartphone verschlüsselt zu den von uns ausschließlich in Deutschland betriebenen Servern übertragen, dort verarbeitet und gespeichert.“

[7] https://tools.ietf.org/html/rfc6749#section-4.1, abgerufen am 13. April 2020.
[8] https://developers.google.com/identity/protocols/oauth2/web-server, abgerufen am 13. April 2020.
[9] https://developers.google.com/identity/protocols/oauth2/web-server#offline, abgerufen am 13. April 2020.
[10] https://corona-datenspende.de/datenschutz-app/, abgerufen am 13. April 2020.

2. „Die App hat zu keinem Zeitpunkt Zugriff auf unmittelbar identifizierende Informationen wie Namen oder Adresse.“
3. Die Aussage „Ihre Daten werden komplett verschlüsselt und pseudonym übertragen“ ist mit einer Pseudonymisierung erst nach Erhalt der Daten beim Empfänger nicht vereinbar.
4. Die Speicherung des Refresh-Tokens ist nicht Bestandteil der Datenschutzerklärung.

Daher muss im Fall einer Kompromittierung durch externe oder interne Angreifer auf Seiten des RKI oder des Betreibers davon ausgegangen werden, dass die unter einem Pseudonym gespeicherten Gesundheitsdaten inklusive daraus gewonnener Analyseergebnisse durch den Angreifer unter Zuhilfenahme des Refresh-Tokens mit Identitätsattributen des Betroffenen wie dem vollständigen Namen zusammengeführt werden können.

Neben dem direkten Zugriff auf die unter dem Pseudonym gespeicherten Gesundheitsdaten und der Möglichkeit der unmittelbaren Identifikation des Datenspenders ist davon auszugehen, dass ein Angreifer über das Refresh-Token an den vollständigen Verlauf auch historischer Gesundheitsdaten des Datenspenders gelangt.

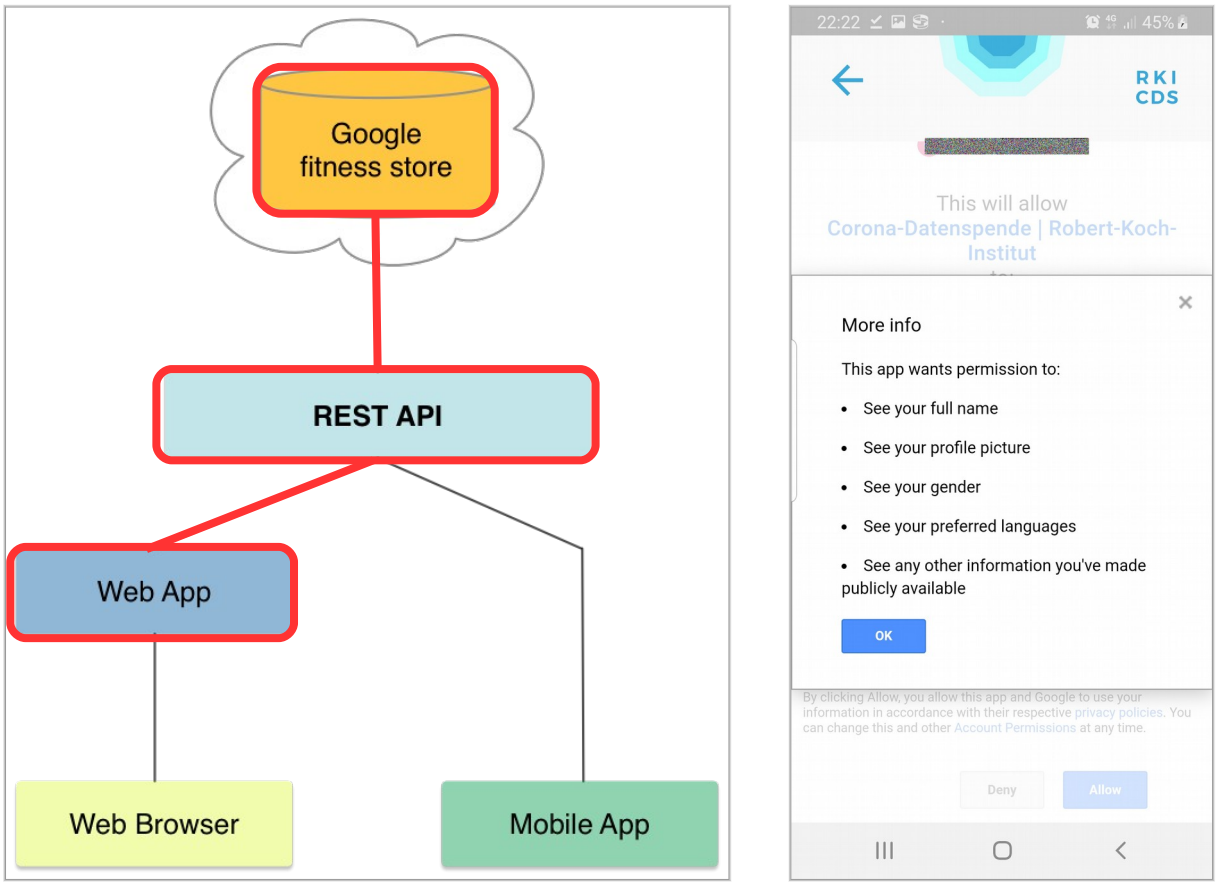

Abbildung 1: Nach Verknüpfung mit Google Fit speichert der Server des RKI („Web App“) zentral Zugangsdaten, welche Zugriff auf die in Google Fit („Google fitness store“) hinterlegten Identitätsattribute des Datenspenders ermöglichen.

3.1.1 Empfehlung

Das hohe, aus der zentralen Speicherung der Refresh-Token auf Seiten des RKI erwachsende Missbrauchspotenzial und die damit einhergehenden Risiken lassen sich vermeiden, indem lediglich der erstgenannte Übertragungsweg gewählt wird. Bei diesem werden alle Daten stets vom Smartphone des Datenspenders aus an den Server des RKI übertragen. Hierbei speichert die App dann Zugangsdaten zu den Fitnessdaten des Datenspenders lokal auf dessen Smartphone. Damit kann sowohl die Abfrage als auch die Pseudonymisierung der Fitnessdaten bereits auf dem Smartphone des Datenspenders stattfinden.

Das RKI wird durch diese dezentrale Speicherung der Zugangsdaten von der hohen Verantwortung befreit, eine dauerhaft sichere Speicherung zu gewährleisten.

Solange Zugangsdaten jedoch zentral gespeichert werden, müssen unbedingt alle notwendigen Schutzmaßnahmen[11] umgesetzt und deren Umsetzung unabhängig überprüft werden.

Durch die Pseudonymisierung der Fitnessdaten bereits auf dem Smartphone des Datenspenders in Kombination mit einer quelloffenen Smartphone-App ist eine deutlich bessere Nachvollziehbarkeit und Kontrollmöglichkeit für die Datenspender gegeben.

3.2 Fehlende Authentizität und Integrität der Fitnessdaten

Es ist beabsichtigt, aus den Analyseergebnissen der Fitnessdaten lokal begrenzte Maßnahmen zur Eindämmung der SARS-CoV-2-Pandemie abzuleiten. Kann die Herkunft der Fitnessdaten (Authentizität) oder deren Korrektheit und Unversehrtheit (Integrität) angegriffen bzw. manipuliert werden, dann können auch die veranlassten Maßnahmen manipuliert bzw. gezielt herbeigeführt werden. Die Motivation für derartige Angriffe ist vielfältig, denkbar ist beispielsweise die gezielte Behinderung eines produzierenden Gewerbes durch Veranlassen strenger Eindämmungsmaßnahmen in einem bestimmten Postleitzahlbereich mittels einer hohen Anzahl vorgetäuschter Infektionen. Ein Angriffsweg ist das wiederholte, zeitversetzte und plausibel variierte Einspielen von Fitnessdaten eines infizierten Datenspenders.

3.2.1 Neue Pseudonyme anlegen

Der Server des RKI bietet eine einfache Möglichkeit zum Erstellen eines neuen Pseudonyms mit frei wählbarer Postleitzahl (siehe 3.6) mit sehr geringem Ressourcen-Einsatz (einfacher HTTP-POST-Request). Laut Datenschutzerklärung der App werden zudem serverseitig keine personenbeziehbaren IP-Adressen zur Missbrauchserkennung gespeichert.

[11] Eine erste Übersicht siehe https://api.slack.com/authentication/best-practices, abgerufen am 13. April 2020.

3.2.2 Neue Daten bestehenden Pseudonymen zuordnen

Unter Kenntnis des Pseudonyms eines Datenspenders (siehe 3.6) können Dritte dessen Authentication-Token vom Server des RKI abfragen und damit weitere Daten unter dem Pseudonym des Datenspenders an das RKI senden, darunter z. B. die Anzahl gelaufener Schritte:

```
PUT /restjson/v5/dynamicEpochValues HTTP/1.1
Host: datenspende.und-gesund.de
Content-Type: application/json
Authorization: Basic ••••••••••••••••••••••••••••••••••
AppAuthorization: Basic ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
authenticationToken: ••••••••••••••••••••••••••••••
…

{
  "dataSource": 5,
  "data": [
    {
      "value": 3.0,
      "dynamicValueType": 1000,
      "endTimestamp": "2020-04-13T10:03:54+02:00",
      "startTimestamp": "2020-04-13T10:03:51+02:00"
     },
     …
```

Dritte können ebenfalls einen eigenen Fitnesstracker und somit dessen Gesundheitsdaten mit dem Pseudonym des Datenspenders verbinden:

```
POST /restjson/v4/dataSourceURL HTTP/1.1
Host: datenspende.und-gesund.de
Content-Type: application/x-www-form-urlencoded
Authorization: Basic ••••••••••••••••••••••••••••••••••
AppAuthorization: Basic ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
…

authenticationToken=••••••••••••••••••••••••••••••
```

Der Server des RKI antwortet mit einer URL, unter welcher die aktuelle Verbindung des Datenspenders mit einem Fitnesstracker eingesehen, aufgehoben oder geändert werden kann (siehe auch 3.3.3):

```
https://datenspende.und-gesund.de/dataSourceSelection.html?
token=••••••••••••••••••••••••••
```

3.2.3 Empfehlung

Die gezeigten Angriffe lassen sich allein durch serverseitige Plausibilitätsprüfung oder statistische Verfahren nicht effektiv unterbinden. Daher müssen zwingend weitere Maßnahmen in Betracht gezogen werden, welche den Ressourcenbedarf (insbesondere Kosten und Zeit) eines Manipulationsversuches erhöhen und das Skalieren eines derartigen Angriffs erschweren. Ggf. ist eine datenschutzkonforme Bindung an Smartphone-Hardware oder SIM-Karten (Global Plattform)

möglich. Datenschutzkonforme Authentizität auf hohem Vertrauensniveau lässt sich ggf. auch mit Umsetzung der Maßnahmen aus 3.8 herstellen.

3.3 Unsichere Verknüpfung mit Fitnesstrackern

Bei der Verknüpfung mit einem Fitnesstracker von Withings, Garmin, Fitbit, Polar bzw. Google Fit leitet die Smartphone-App den Datenspender auf eine Webseite des Fitnesstracker-Anbieters oder von Google weiter. Dort wird der Datenspender nach Anmeldung im Regelfall mit Benutzername und Passwort zur Freigabe des Zugriffs aufgefordert.

3.3.1 Verknüpfung über corona-datenspende.de

Im Test wurde der Datenspender nach Verknüpfung mit Google Fit nicht direkt zurück zum Server des RKI, sondern zunächst von accounts.google.com an corona-datenspende.de weitergeleitet.

Erst der Webserver corona-datenspende.de leitet den Datenspender dann zurück zum Server des RKI:

```
HTTP/1.1 303 See Other
Server: Apache/2.4.41 (Unix)
X-Powered-By: PHP/7.2.15
…
Location: https://datenspende.und-gesund.de/dataSourcesSwitch.html?
state=••••••••••••••••••••••••••_12_0_&code=••••••••••••••••••••••••••••••••••••
••••••••••••••••••••••••••••••••••••••••••••••&scope=…
```

Auf dem Webserver corona-datenspende.de wird eine Wordpress-Instanz betrieben. Die angegeben Versionen von Apache und PHP sind veraltetet und bekannte Schwachstellen in diesen Versionen möglicherweise ungepatcht. Bei einer Kompromittierung von corona-datenspende.de wird auf diesem Umweg der OAuth2-Authorization-Code sowie der vertrauliche State-Parameter exponiert (siehe 3.3.3). Zudem gestattet eine Kompromittierung von corona-datenspende.de einem Angreifer direkte Einflussnahme auf die innerhalb des Webviews in der Smartphone-App angezeigten Inhalte und somit Potenzial für Phishing-Angriffe. Insgesamt stellt dieser Umweg eine deutliche Vergrößerung der Angriffsoberfläche dar (siehe 3.4).

3.3.2 Verknüpfung innerhalb Webview

Die Verknüpfung mit einem Fitnesstracker erfolgt innerhalb eines in die Smartphone-App eingebetteten Browsers (Webview). Daraus folgt:

- Die verschlüsselte Kommunikation aus dem Webview heraus mit der Webseite des Fitnesstracker-Anbieters oder Google Fit ist nicht gegen Man-in-the-Middle-Angriffe gesichert. Insbesondere kann ein Angreifer in Besitz eines von einer der im Smartphone verankerten Certificate-Authorities signierten Zertifikats für den Server des RKI die Kommunikation zwischen Server und Smartphone-App mitlesen und übertragene Zugangsdaten stehlen.

- Zudem speichert der Webview standardmäßig vom Fitnesstracker-Anbieter oder Google Fit ausgestellte Session-Cookies im Cache der Smartphone-App, ohne diese auf Anwendungsebene zu verschlüsseln (siehe 3.5).
- Eine kompromittierte Smartphone-App kann die in einem Webview auf der Webseite des Fitnesstracker-Anbieters oder Google Fit eingegebenen Zugangsdaten mitlesen und an Dritte weiterleiten.

Die Verwendung eines Webviews zur Verknüpfung mit Google Fit verstößt daher auch gegen die Sicherheitsanforderungen von Google.[12]

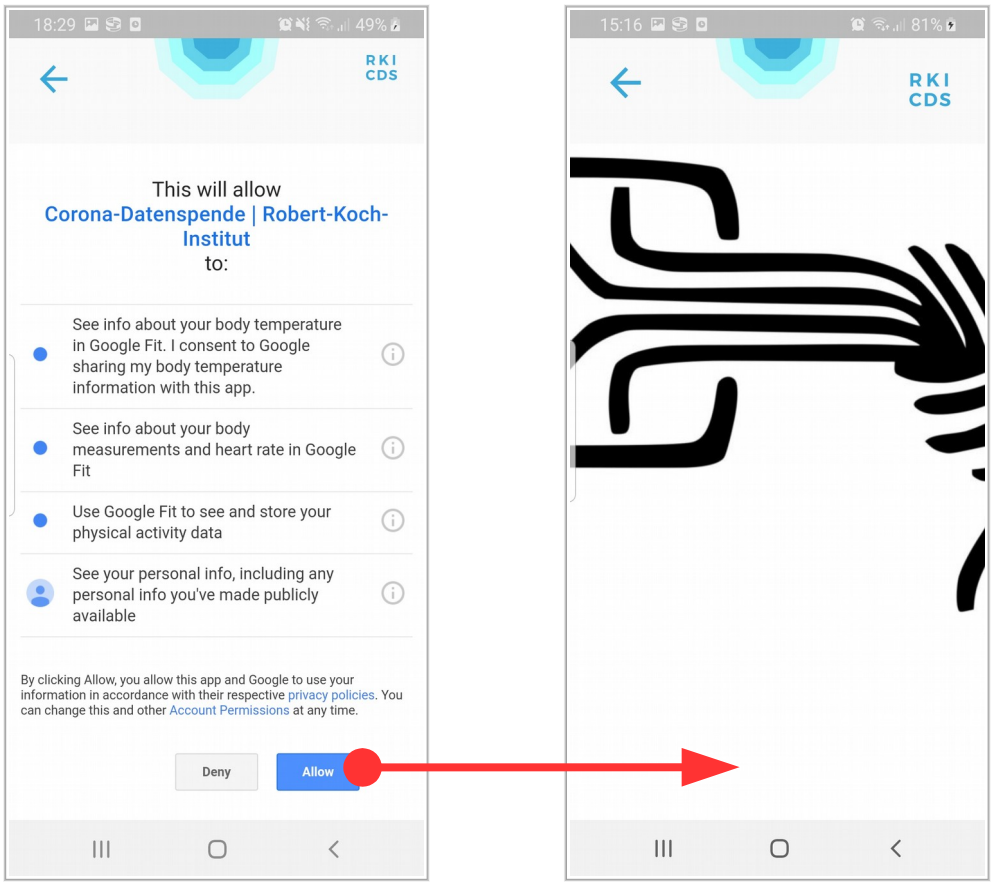

Abbildung 2: Ein Man-in-the-Middle-Angriff auf datenspende.und-gesund.de nach erfolgreicher Verknüpfung mit Google Fit wurde wegen fehlendem Certificate-Pinning im Webview der Smartphone-App nicht erkannt. Ein Angreifer kann wie abgebildet eigene Inhalte einbinden und Zugangsdaten stehlen.

3.3.3 State-Parameter ist Zugangstoken

Nach erfolgreicher Freigabe des Zugriffs wird der Datenspender von der Webseite des Fitnesstracker-Anbieters oder von Google Fit zurück auf den Server des RKI geleitet. Dabei wird zur Verhinderung von sog. Cross-Site-Request-Forgery-Angriffen ein „state“-Parameter, unten

[12] https://developers.googleblog.com/2016/08/modernizing-oauth-interactions-in-native-apps.html, abgerufen am 13. April 2020.

„token“ genannt, übertragen. Laut RFC6819 „OAuth 2.0 Threat Model and Security Considerations“ gilt:[13]

> *„This parameter should bind to the authenticated state in a user agent and, as per the core OAuth spec, the user agent must be capable of keeping it in a location accessible only by the client and user agent, i.e., protected by same-origin policy.“*

Im Test wurde der „state“-Parameter jedoch entgegen der Schutzanforderung per HTTP-Referer-Header an Google weitergegeben.

```
GET /css?family=Roboto:100,400 HTTP/1.1
Host: fonts.googleapis.com
Connection: close
User-Agent: FlutterUserAgent
Sec-Fetch-Dest: style
Accept: text/css,*/*;q=0.1
X-Requested-With: de.rki.coronadatenspende
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Referer: https://datenspende.und-gesund.de/dataSourceDirectConnectionResult.html?
token=••••••••••••••••••••••••••••&dataSource=12&connected=true
Accept-Encoding: gzip, deflate
Accept-Language: de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7
```

Dies ist insbesondere deshalb problematisch, weil der hier verwendete „state“-Parameter entgegen der abschließend zu verstehenden RFC-Anforderung hinaus vom Server des RKI zudem als Zugangstoken verstanden wird. Eine Kenntnis dieses Parameters erlaubt Dritten Einsichtnahme und Manipulation in die Verknüpfung mit Fitnesstrackern des betroffenen Datenspenders.

Zudem wird der „state“-Parameter unnötig exponiert (siehe 3.3.1).

[13] https://tools.ietf.org/html/rfc6819#section-3.6, abgerufen am 13. April 2020.

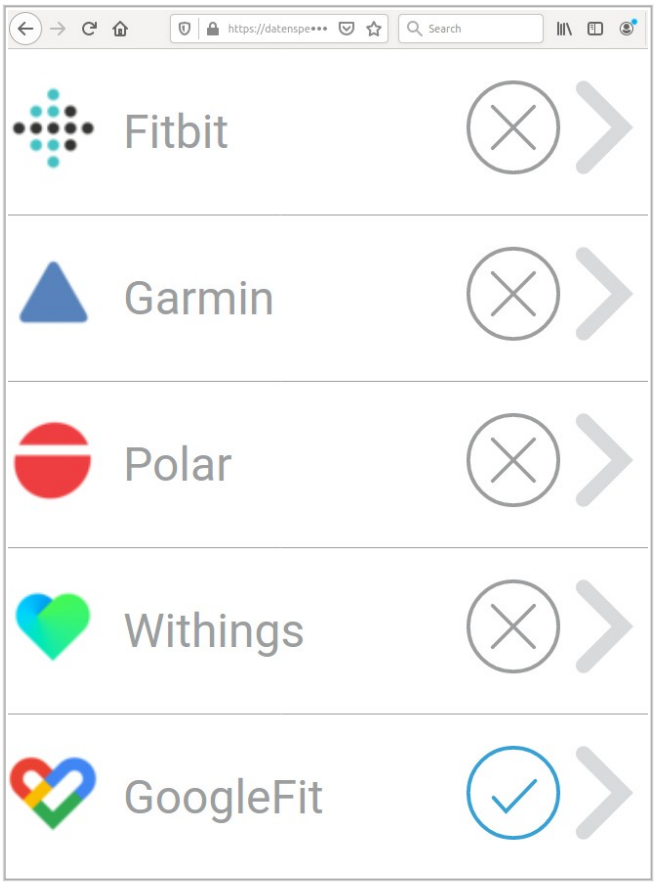

Abbildung 3: Ein Dritter in Kenntnis des „state"-Parameters kann aufgrund dessen Doppelfunktion als Zugangsdatum die Verknüpfung mit Fitnesstrackern des betroffenen Datenspenders einsehen, lösen oder überschreiben.

3.3.4 Empfehlung

Die Verknüpfung der Smartphone-App mit dem Fitnesstracker sollte über den sicheren Standard-Browser und nicht über einen in die Smartphone-App eingebetteten Webview geschehen. Dies ist unbedingt mit einem Certificate-Transparency-Monitoring zu verbinden, da vorbeugende Maßnahmen gegen Man-in-the-Middle-Angriffe wie striktes Certificate-Pinning im Standard-Browser nicht umgesetzt werden können. Letzteres gilt auch für die Zertifikate des Servers des RKI, dessen Authentizität für die Smartphone-App nicht nur während der Verknüpfung mit Fitnesstrackern von übergeordneter Bedeutung ist (siehe 3.7).

In jedem Fall ist die Kommunikation auch aus einem Webview heraus gegen Man-in-the-Middle-Angreifer mittels Certificate-Pinning abzusichern. Dies ist auf Android-Smartphones mittels Network Security Configuration[14] umsetzbar. Die Überprüfung der Certificate-Transparency dagegen wird im Webview unter Android nicht unterstützt.

[14] https://developer.android.com/training/articles/security-config, abgerufen am 19. April 2020.

Der für den Verknüpfungsvorgang erzeugte „state“-Parameter darf keine weitere sicherheitskritische Funktion tragen. Während der Verknüpfung dürfen zudem keine externen Ressourcen wie Schriftarten oder Bilder eingebunden werden, um eine Weitergabe vertraulicher Parameter über den Referer-Header zu unterbinden.

Zur Reduktion der Angriffsoberfläche sollte die Verknüpfung mit Google Fit zudem direkt zwischen Server des RKI und Google ohne Umweg über einen weiteren Webhost erfolgen (siehe auch 3.4).

3.4 Vergrößerte Angriffsoberfläche auf dem Server

Der Server des RKI nimmt die Fitnessdaten der Datenspender sowie langlebige Zugangsdaten mit Möglichkeit der Re-Identifikation (siehe 3.1) zur weiteren Verarbeitung und dauerhaften Speicherung entgegen und somit ist der Server des RKI zentrales Schutzobjekt mit hohem Schutzbedarf.

Dessen durch einen Angreifer sichtbare und gegenüber dem Internet exponierte Angriffsoberfläche ist dabei sehr umfangreich, darunter u. a.:

- Ein Management-Interface „Manage your App“, welches die öffentlichen und in der Smartphone-App hinterlegten Zugangsdaten „AppID“ und „AppSecret“ zur Anmeldung abfragt.
- Eine Admin-Interface, welches über eine HTTP-Basic-Authentication einen Benutzername und ein Passwort abfragt.
- Eine Status-Anzeige, welche Informationen über den Systemzustand wie die aktuelle Zahl an Datenspendern, die Zahl verknüpfter Fitnesstracker usw. ausgibt.
- Ein Web-Interface für Datenspender, welches Zugriff auf erweiterte Funktionen im gleichen Umfang wie die angebotene SOAP-API ermöglicht.
- Eine SOAP-API mit hohem Funktionsumfang, darunter das Versenden von Freundschaftsanfragen, Teilen von Gesundheitsdaten mit Freunden, Ändern von Passwörtern usw.
- Eine JSONXML-API mit ähnlichem Funktionsumfang wie die von der Smartphone-App angesprochene JSONREST-API v5.
- Eine JSONREST-API in Version v4 und v5, wobei nur ein geringer Teil der API-Endpunkte von der Smartphone-App angesprochen wird.

Weitere Beobachtungen deuten auf die Risiken hin, die sich aus einer gegenüber der Kernfunktionalität der App vergrößerten Angriffsoberfläche ergeben:

- Der Server des RKI ordnet jedem Datenspender eine User-ID bzw. E-Mail-Adresse zu, welche sich aus dem Pseudonym und dem Suffix „@datenspendeausweis.com“

zusammensetzt. Sowohl das Web-Interface als auch die SOAP-API bieten neben der Authentisierung mittels Authentication-Tokens einen Login mit User-ID und Passwort an. Im Fall eines Passwort-Reset über das Web-Interface oder die SOAP-API ist zu vermuten, dass der Server des RKI eine E-Mail mit einem Passwort-Reset-Token an die Domain datenspendeausweis.com adressiert, womit diese Domain ebenfalls zur Angriffsoberfläche zu zählen ist.

- Über einen API-Endpunkt der JSONREST-API v4 auf den Server des RKI gesendete Angaben zu Alter, Größe und Geburtsdatum des Datenspenders wurden unter Kenntnis des Pseudonyms über einen von der Smartphone-App angesprochenen API-Endpunkt der JSONREST-API v5 offenbart.

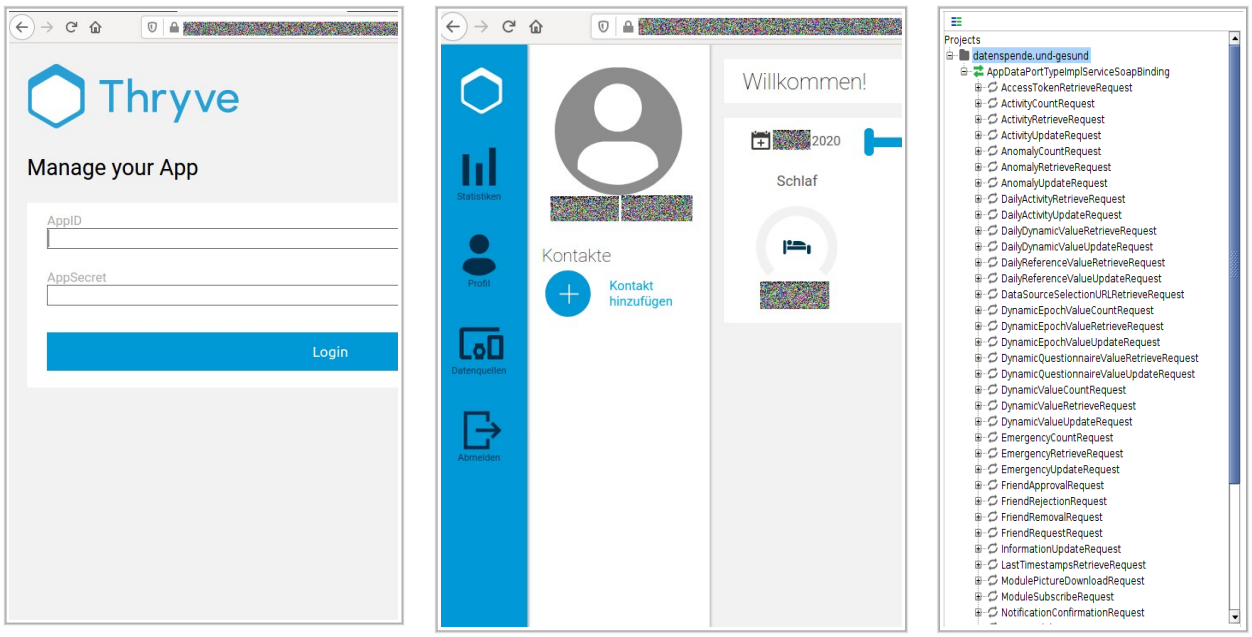

Abbildung 4: Web- und Management-Oberfläche sowie SOAP-API auf dem Server des RKI.

3.4.1 Empfehlung

Insbesondere die zum öffentlichen Internet hin exponierte Angriffsoberfläche ist auf ein notwendiges Minimum zu reduzieren. Ein API-Server darf keine weitere Funktionalität exponieren. Segmentierung, Isolierung und Reduktion der Komplexität sind wesentliche Prinzipien der Informationssicherheit.

Siehe CWE-1125: Excessive Attack Surface

3.5 Unverschlüsselte Speicherung auf dem Smartphone

Die Android-App speichert vertrauliche Daten im internen Speicher des Gerätes, ohne diese auf Anwendungsebene zu verschlüsseln.

Zwar können Android-Smartphones diese Anwendungsdaten bis Android 9 mittels Full-Disk-Encryption (FDE) und ab Android 9 mittels File-Based-Encryption (FBE) schützen. Dieser Schutz geht jedoch mit der erstmaligen Entsperrung des Smartphones nach dem Einschalten verloren. Solange das Smartphone nicht vollständig ausgeschaltet wird, können die Daten insbesondere bei Verlust oder Diebstahl des Smartphones durch Dritte ausgelesen werden.[15]

3.5.1 Vertrauliche Daten in Datenbank

Die Android-App speichert das Pseudonym sowie das Authentication-Token des Datenspenders unverschlüsselt im internen Speicher des Smartphones.

Im Test wurden das Authentication-Token „9e2••••••••••••••••••••••••••••••357“ und das Pseudonym „de12345••••••••••••••••••••••••“ aus der SQLite-Datenbank „/data/user/0/de.rki.coronadatenspende/databases/daten_spende_ausweis“ ausgelesen:

```
de.rki.coronadatenspende on (samsung: 9) [usb] # file cat daten_spende_ausweis
…
9e2••••••••••••••••••••••••••••••357de12345••••••••••••••••
...
```

Pseudonym und Authentication-Token sind jedoch zu schützende Zugangsdaten (siehe 3.6).

3.5.2 Vertrauliche Daten im Cache

Die Android-App speichert bei der Kopplung mit einem Fitnesstracker anfallende vertrauliche Informationen im internen Speicher des Smartphones.

Im Test wurden OAuth-State-Parameter und OAuth-Authorization-Code aus dem Cache unter „/data/user/0/de.rki.coronadatenspende/cache/WebView/Default/HTTP Cache/a04b6d53739158e0_0“ ausgelesen:

```
de.rki.coronadatenspende on (samsung: 9) [usb] # file cat a04b6d53739158e0_0
…
https://corona-
datenspende.de/gf_redirect/8wAHEjL2n9HXgBNzHVs5sW7JadFQfV2C/gf_redirect.php?
state=••••••••••••••••••••••••••_12_0_&code=••••••••••••••••••••••••••••••••••••••••
••••••••••••••••••••••••••••••••••••••••••••••••
…
```

Der OAuth-State-Parameter ist dabei sicherheitskritisch und verliert auch längerfristig nicht seine Gültigkeit (siehe 3.3.3).

Im Test wurden nach Verknüpfung mit Google Fit vertrauliche Session-Cookies aus dem Cache unter „/data/user/0/de.rki.coronadatenspende/app_webview/Default/Cookies“ ausgelesen:

```
de.rki.coronadatenspende on (samsung: 9) [usb] # file cat Cookies
…
```

[15] Dies gilt explizit auch für FBE: „If the user enables the lock screen after unlocking the device, this doesn't lock credential encrypted storage.“

```
Secure-SSID••••••••••••••••
…
Secure-HSID••••••••••••••••
…
SID••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
…
```

Ein Angreifer mit direktem Zugang zum Smartphone des Datenspenders – beispielsweise nach einem Diebstahl oder Verlust – kann mit diesen Session-Cookie auf das Google-Konto des Anwenders zugreifen – und zwar dauerhaft, da bei Login die Option „Angemeldet bleiben“ vorausgewählt ist.

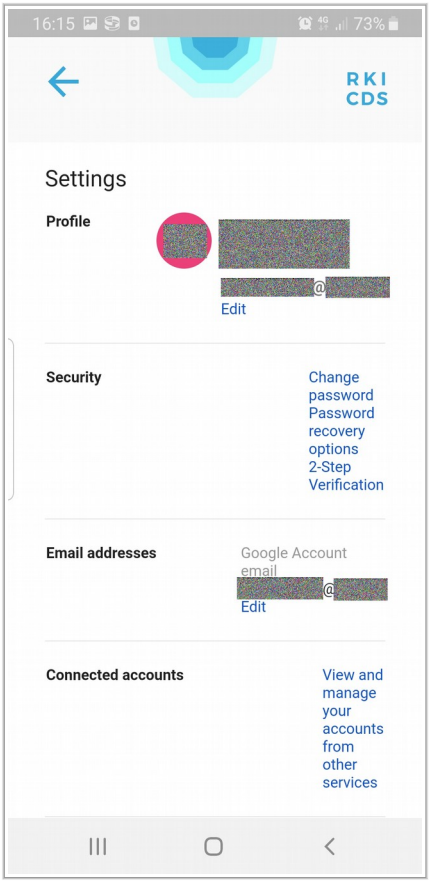

Abbildung 5: Mit den unsicher gespeicherten Session-Cookies des Webviews war im Test der Zugriff auf das Google-Konto des Datenspenders möglich.

3.5.3 Unauthentisierter Zugriff auf Schlüsselmaterial

Die Smartphone-App speichert das Authentication-Token des Datenspenders zusätzlich verschlüsselt (im Vgl. zu 3.5.1) auf dem Smartphone.

Im Test unter Android wurden das verschlüsselte Authentication-Token neben einer „appId“ und einem „appSecret“ aus dem Shared-Preferences-Verzeichnis unter „/data/user/0/de.rki.coronadatenspende/data/user/0/de.rki.coronadatenspende“ ausgelesen.

Die Entschlüsselung erfolgt mit einem im Android Keystore hinterlegten Schlüssel. Zugriff auf diesen Schlüssel ist jedoch ohne vorherige Authentisierung des Datenspenders möglich:

```
[Samsung SM-G950F::Gadget]-> AliasInfo("9cDkJ25WUqEYq7Mc")
[Keystore.load(LoadStoreParameter)]: keystoreType: AndroidKeyStore, param: null
[Keystore.getKey()]: alias: 9cDkJ25WUqEYq7Mc, password: '(null)'
{
     "isInsideSecureHardware": true,
     "isInvalidatedByBiometricEnrollment": false,
     "isTrustedUserPresenceRequired": false,
     "isUserAuthenticationRequired": false,
     "isUserAuthenticationRequirementEnforcedBySecureHardware": false,
     "isUserAuthenticationValidWhileOnBody": false,
     …
     "userAuthenticationValidityDurationSeconds": -1
}
```

Auch unter iOS ist ein Zugriff möglich, da der Zugang zum enstprechenden Keychain-Item mit dem Zugangsattribut „kSecAttrAccessibleAfterFirstUnlock“[16] ebenfalls ungenügend gesichert ist.

Ein Angreifer mit direktem Zugang zum Smartphone des Datenspenders – beispielsweise nach einem Diebstahl oder Verlust – kann auch im gesperrten Zustand auf diesen Schlüssel zugreifen, ohne dass der Datenspender sein Smartphone dazu vorher entsperren müsste.

3.5.4 Empfehlung

Schützenswerte Daten sollten wenn möglich gar nicht auf dem Smartphone gespeichert werden. Bei Verwendung eines eingebetteten Webviews kann dies beispielsweise durch Abschalten des Cachings erreicht werden. Wird anstelle eines Webviews der Standard-Browser verwendet, dann werden schützenswerte Cookies zudem automatisch verschlüsselt (siehe auch 3.3.4).

Ist eine Speicherung notwendig, sollten die Daten durch die Anwendung nur verschlüsselt abgelegt werden. Hierzu gibt Google entsprechende Empfehlungen.[17]

Bei verschlüsselter Speicherung sollte der Schlüssel mit dem Attribut „UserAuthenticationRequired” im sicheren Hardwarespeicher erzeugt werden.

Siehe CWE-312: Cleartext Storage of Sensitive Information

3.6 Unsichere Handhabung des vertraulichen Pseudonyms

Bei erstmaligem Starten der Smartphone-App wird aus dem Ländercode „de“, der abgefragten Postleitzahl sowie einer auf dem Smartphone erzeugten 16-stelligen hexadezimalen Zufallszahl ein Pseudonym bzw. eine „partnerUserID“ erzeugt.

[16] https://mezdanak.de/2019/04/03/ios-keychain_dumper-extension/, abgerufen am 13. April 2020.
[17] https://developer.android.com/topic/security/data, abgerufen am 13. April 2020.

Dieses Pseudonym wird dem Datenspender in der Smartphone-App daraufhin gut lesbar unverschlüsselt in Base-64-Codierung angezeigt. Dem Datenspender wird zudem die Möglichkeit geboten, das Pseudonym direkt in die Zwischenablage auf dem Smartphone zu kopieren.

Sobald ein Pseudonym existiert, fragt die Smartphone-App vom Server des RKI ein statisches Authentication-Token ab:

```
POST /restjson/v5/accessToken HTTP/1.1
Host: datenspende.und-gesund.de
Content-Type: application/x-www-form-urlencoded
Authorization: Basic ••••••••••••••••••••••••••••••••••=
AppAuthorization: Basic ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
…

partnerUserID=de12345••••••••••••••••&language=de
```

Der Server des RKI antwortet mit einem 32-stelligen hexadezimalen Authentication-Token. Mit diesem Token können anschließend einige mit dem Pseudonym verknüpfte Informationen abgefragt werden. Im Test wurde dazu folgender HTTP-Request an den Server des RKI gesendet:

```
POST /restjson/v5/userInformation HTTP/1.1
Host: datenspende.und-gesund.de
Content-Type: application/x-www-form-urlencoded
Authorization: Basic ••••••••••••••••••••••••••••••••••=
AppAuthorization: Basic ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
…

authenticationToken=••••••••••••••••••••••••••••••••
```

Der Server des RKI antwortete u. a. mit dem Pseudonym des Datenspenders bzw. der „partnerUserID“ und Informationen zu den verbundenen Fitnesstrackern:

```
[{"authenticationToken":"••••••••••••••••••••••••••••••••","partnerUserID":"de12345•••
••••••••••••","connectedSources":[{"dataSource":5,"connectedAt":"2020-04-
09T02:42:31Z"}]}]
```

Ein Angreifer in Kenntnis des Pseudonyms gelangt darüber auch stets in den Besitz des Authentication-Tokens und kann damit neben der Abfrage der oben dargestellten Informationen auch Fitnessdaten an den Server des RKI senden sowie die Verknüpfung mit einem Fitnesstracker einsehen, aufheben oder ändern (siehe 3.2). Zudem kann der Angreifer das Pseudonym und die damit verbundenen Daten vom Server des RKI löschen und ggf. ein Recht auf Löschung, Korrektur und Auskunft nach DSGVO kompromittieren (siehe 3.8).

Im Widerspruch zu diesem Angriffspotenzial wird das Pseudonym innerhalb der Smartphone-App sowie durch das RKI wie ein öffentliches Datum behandelt.

- Es wird prominent nach Erzeugung sowie anschließend im Menü der Smartphone-App angezeigt. Auch in Werbematerial des RKI sowie in der Medienberichterstattung wird das Pseudonym demonstrativ öffentlich abgebildet.

- Die Smartphone-App bietet eine Funktion an, das Pseudonym in die Zwischenablage zu kopieren. Dort ist das Pseudonym für weitere auf dem Smartphone installierte und möglicherweise nicht vertrauenswürdige Apps zugänglich.
- Das Smartphone erzeugt und zeigt beim Wechseln zwischen verschiedenen Apps eine Vorschau der Smartphone-App mitsamt darin sichtbarem Pseudonym. Unter Android ist das FLAG_SECURE nicht gesetzt.

In Folge dessen haben bereits einige Datenspender Bildschirmfotos oder Videos der Smartphone-App mit sichtbarem Pseudonym im Internet und insbesondere in sozialen Netzwerken veröffentlicht.

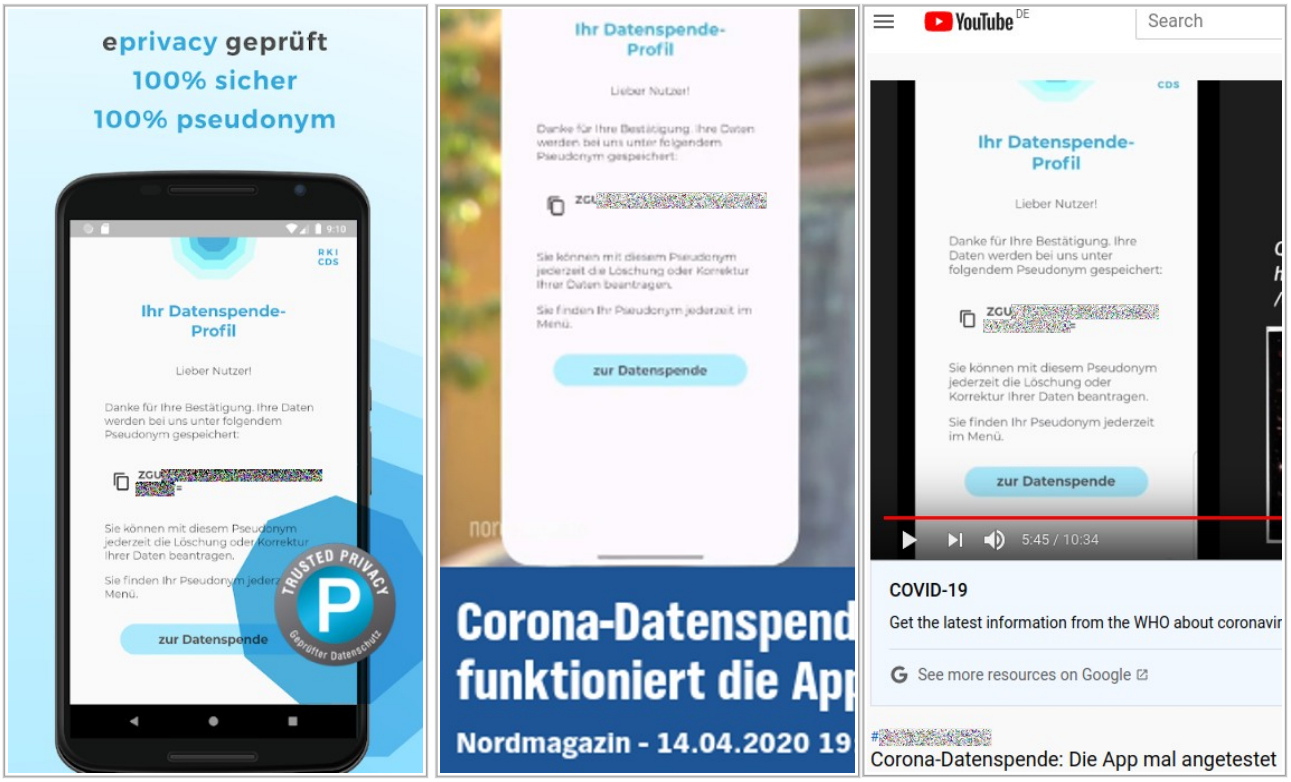

Abbildung 6: Das Pseudonym wird sowohl in Werbematerial des RKI als auch in Medienberichten u. a. des NDR unverdeckt dargestellt. Der Datenspender wird dadurch gegenüber dessen Bedeutung als geheimes und geheimzuhaltendes Zugangsdatum in die Irre geführt.

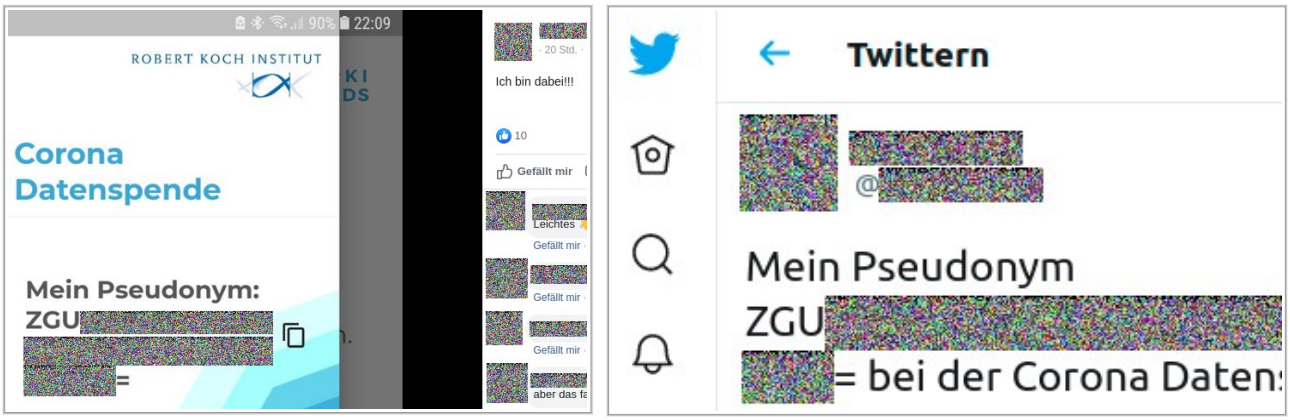

Abbildung 7: In sozialen Medien wie Facebook, Twitter und LinkedIn teilen Datenspender unbedarft Bildschirmfotos ihrer Pseudonyme.

3.6.1 Empfehlung

Das Pseudonym dient dem Server des RKI als Ordnungskriterium bzw. Datenbankschlüssel und ist in der weiteren Verarbeitung der Fitnessdaten potentiell einem großen Personenkreis zugänglich. Das Pseudonym darf schon alleine daher nicht die Funktion eines Zugangsdatums bzw. eines Authentisierungsfaktors vom Typ „Wissen“ ähnlich einem Passwort übernehmen.

Tatsächlich suggeriert schon der Name „Pseudonym“ gegenüber dem Datenspender, dass es keinen besonderen Geheimhaltungsbedarf hat, sondern im Gegenteil gerade dem Schutz der Identität dient und gefahrlos als „gleichsam alternativer Name“ verwendet werden kann.

Die Funktion des Zugangsdatums muss folglich vom Pseudonym abgetrennt durch ein eigenständiges Authentisierungsmittel umgesetzt werden.

3.7 Schwache Authentisierung des Servers

Die Smartphone-App überträgt Zugangs- und Fitnessdaten mit hohem Schutzbedarf an den Server des RKI, welcher sich zur Absicherung gegen Angriffe auf dem Transportweg der Daten gegenüber der Smartphone-App eindeutig authentisiert. Hierbei kommen Zertifikate zum Einsatz.

Gelingt es einem Angreifer, sich gegenüber der Smartphone-App als Server des RKI auszugeben, können die anschließend verschlüsselt übertragenen Daten mitgelesen werden.

3.7.1 Wildcard-Zertifikat mit gemeinsam genutztem Schlüssel

Im Test hat sich gezeigt, dass es sich bei dem vom Server des RKI vorgezeigten und auf den Betreiber ausgestellten Zertifikat um ein sog. Wildcard-Zertifikat handelt. Dieses kommt noch auf mindestens einem anderen Host des Betreibers zur Absicherung der dort angeboten Schnittstellen zum Einsatz. Der zugehörige private Schlüssel ist somit auf mindestens zwei unterschiedlichen Webhosts im Einsatz. Dies erhöht das Risiko für die Kompromittierung des privaten Schlüssels.

Laut Betreiber ist die App zudem „von anderen kommerziellen Anwendungen des Thryve-SDK komplett getrennt“ und läuft „als eigene Instanz“.[18] Diese Trennung wird durch Verwendung eines Wildcard-Zertifikates unterlaufen. Die Smartphone-App kann nicht erkennen, ob sie Daten an den Server des RKI oder an eine andere kommerzielle Anwendung des Betreibers sendet.

3.7.2 Empfehlung

Mit Verzicht auf Wildcard-Zertifikate und einen gemeinsam genutzten Schlüssel kann die behauptete Identität des Servers des RKI durch die Smartphone-App sicher überprüft werden. Zusammen mit wichtigen weiteren Maßnahmen (siehe 3.3.4) sichert dies die Kommunikation zwischen Smartphone-App und Server des RKI gegen Man-in-the-Middle-Angreifer ab.

3.8 Unwirksame Einwilligung und unklare Betroffenenrechte

Das Robert Koch-Institut ist das nationale Public-Health-Institut für Deutschland und somit eine selbstständige deutsche Bundesoberbehörde.

Demzufolge unterliegt das RKI neben den Regelungen der DSGVO auch weiteren Regelungen wie beispielsweise der BSI TR-03107 vollumfänglich.

Gemäß DSGVO sind Gesundheitsdaten definiert als „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.“ Der Schutzbedarf für Gesundheitsdaten ist „hoch“.

Die Verarbeitung ist gemäß DSGVO (wie auch bereits unter dem BDSG) nur aufgrund einer Einwilligung der betroffenen Person oder eines der abschließend aufgezählten Erlaubnistatbestände des Art. 9 Abs. 2 lit. a. DSGVO zulässig. Hierauf bezieht sich auch das RKI in seinen Datenschutzhinweisen.[19]

Die datenschutzrechtliche Einwilligung der Betroffenen im Umgang mit Gesundheitsdaten ist von herausragender Bedeutung für die Verarbeitung. Neben einer Freiwilligkeit und Informiertheit muss eine Einwilligung „wirksam“ erfolgen. So führt beispielsweise die Bayerische Landesdatenschutzbehörde dazu aus, dass „ausdrücklich in die Verarbeitung der sensiblen Daten

[18] https://www.computerwoche.de/a/alles-zur-corona-datenspende-app,3548822, abgerufen am 13. April 2020.

[19] Datenschutzhinweise 2. Einwilligung in die Datenverarbeitung

eingewilligt werden muss. Eine Einwilligungserklärung durch schlüssiges Handeln ist hier somit ausgeschlossen.“[20]

3.8.1 Anforderungen an eine wirksame Einwilligung nicht erfüllt

Im Falle der hier untersuchten App wird die Einwilligung durch ein Opt-in realisiert. Die Einwilligung (eine Willenserklärung) soll somit elektronisch, mittels nicht-signaturbasierter Verfahren realisiert werden. Die Bedingungen zur wirksamen Abgabe elektronischer, nicht-signaturbasierter Willenserklärungen sind in der BSI TR-03107-1 definiert. Das im Falle der App eingesetzte Verfahren steht im Widerspruch zu den Anforderungen des BSI.[21]

Dort heißt es, dass eine wirksame Abgabe einer Willenserklärung auf Vertrauensniveau „hoch“ für nicht-signaturbasierte Verfahren entweder mittels der eID-Funktion des Personalausweises oder De-Mail erfolgen kann.[22]

Darüber hinaus ist für das RKI zum Zeitpunkt der Einwilligung auch nicht erkennbar, wer diese Einwilligung erteilt. Wirksame elektronische Willenserklärungen setzen aber einerseits einen Identitätsnachweis als auch ein technisches Verfahren zur Durchführung der Willenserklärung auf dem Vertrauensniveau voraus, für das die Willenserklärung abgegeben werden soll. Dies ist bei der hier untersuchten App nicht der Fall.

Als öffentliche Stelle stützt sich das RKI auf eine Einwilligung der Betroffenen. Somit muss das RKI auch nachweisen können, dass die betroffenen Personen in die Verarbeitung der personenbezogenen Daten eingewilligt haben. Vor diesem Hintergrund schlägt die Bayerische Landesdatenschutzbehörde alternativ zur Abgabe einer elektronischen Willenserklärung vor, dass die DSGVO zwar keine Schriftform explizit fordert, aber insbesondere im Hinblick auf die Nachweispflicht die Schriftform der Einwilligungserklärung zu empfehlen ist.

In Summe lässt sich feststellen, dass weder die Anforderungen der BSI TR-03107-1 zur wirksamen Abgabe einer elektronischen Willenserklärung (Einwilligung) noch die Empfehlung der Bayerischen Landesdatenschutzbehörde zur Erfüllung der Nachweispflicht einer wirksamen Einwilligungserklärung zur Verarbeitung von Gesundheitsdaten erfüllt werden.

3.8.2 Unstimmigkeiten bei Wahrnehmung der Betroffenenrechte

Aufgrund der ungenügenden Verfahren zur Abgabe einer Willenserklärung, die auch darin begründet sind, dass das RKI zu keinem Zeitpunkt die Identität des Betroffenen tatsächlich kennt, werden die Grundlagen für weitere Schwachstellen aus Sicht des Datenschutzes geschaffen.

[20] Bayerische Landesdatenschutzbehörde, Die Einwilligung nach der DSGVO, Mai 2018: https://www.datenschutzbayern.de/datenschutzreform2018/einwilligung.pdf

[21] BSI TR-03107-1 vom 7.5.2019

[22] BSI TR-03107-1 vom 7.5.2019 S. 37 Tabelle 9

Das RKI ist daher nicht in der Lage zu verhindern, dass Angreifer massenweise Fake-Identitäten erzeugen und so grundlegend die Aussagekraft der Auswertungen des RKI kompromittieren (siehe 3.2.1).

Auch heißt es unter Punkt 6 der Datenschutzhinweise, dass personenbezogene Daten streng vertraulich behandelt und nicht an Dritte weitergegeben werden.

Die Datenschutzerklärung der App räumt dem Betroffenen nach Art. 15-20 und 77 Abs. 1 DSGVO folgende Rechte ein:[23]

> *„Das Recht, Auskunft zu verlangen, welche Daten über mich gespeichert wurden, und diese bei Unrichtigkeit berichtigen bzw. vervollständigen zu lassen, das Recht, die mich betreffenden personenbezogenen Daten, löschen oder für die Verarbeitung beschränken zu lassen sowie das Recht, die von mir bereitgestellten Daten in einem strukturierten, gängigen maschinenlesbaren Format zu erhalten.*
>
> *Diese Rechte kann ich solange geltend machen, wie die Daten meiner Person zugeordnet werden können.“*

Mangels wirksamer Willenserklärung, insbesondere der fehlenden sicheren Identitätsfeststellung des Betroffenen, kann entweder das Recht, Auskunft zu verlangen, welche Daten gespeichert wurden, nicht eingeräumt werden („Rechte kann ich solange geltend machen, wie die Daten meiner Person zugeordnet werden können“), oder es besteht die Gefahr, dass das Recht, Auskunft zu verlangen, einer Person eingeräumt wird, von der nicht sichergestellt ist, dass es sich um die betroffene Person handelt.

Die Nennung eines durch die App erzeugten Pseudonyms bei Anfragen zu Auskünften nach DSGVO erfüllt die Anforderung an den Nachweis der Identität nicht, zumal dieses Pseudonym im Laufe der Verarbeitung weiteren Personen zugänglich gemacht wird (siehe 3.6):

- Im Registrierungsprozess wird die wahre Identität des Betroffenen nicht festgestellt
- Das Pseudonym stellt kein Geheimnis dar
- Das Pseudonym ist nicht kopiergeschützt

Im Ergebnis führt dies dazu, dass entweder irreführende Aussagen in den Datenschutzhinweisen gegeben werden, da Ansprüche gemäß DSGVO nicht realisiert werden können, oder die Gefahr der Auskunft an unbefugte Dritte besteht, da nicht sichergestellt werden kann, dass Datenspender und Auskunft ersuchende Person identisch sind.

[23] https://corona-datenspende.de/datenschutz-app/, abgerufen am 13. April 2020.

3.8.3 Empfehlung

In einem ersten Schritt sollte der Registrierungs- und Einwilligungsprozess den Anforderungen der DSGVO und der BSI TR-03107-1 angepasst werden. Ein Pseudonym kann erst nach wirksamer Einwilligung erzeugt werden.

Weiterhin sollte eine Anpassung der Informationen über die Betroffenenrechte an die tatsächlichen Gegebenheiten erfolgen.

Zur Wahrung der Betroffenenrechte können kryptographische Nachweise der Zugehörigkeit eines Pseudonyms zu einer Person bzw. einem Gerät in Besitz der Person dienen.

Die Nutzung der App mittels Pseudonymen könnte auch ein Einsatzgebiet für elektronische Gesundheitskarten sein, da diese bereits über Pseudonyme (AUTN) verfügen. Aktuell scheitert die Nutzung der elektronischen Gesundheitskarten für diesen Einsatzzweck jedoch bereits daran, dass die Gesundheitskarten nicht über die entsprechenden technischen (NFC)-Schnittstellen verfügen und andererseits aufgrund des fehlenden Identitätsnachweises bei Beantragung und der unsicheren Übermittlung der Karten an Versicherte nicht genutzt werden dürfen.

4 Fazit

Das RKI hat vor dem Hintergrund der gebotenen Eile im Umgang mit der SARS-CoV-2-Pandemie in sehr kurzer Zeit eine „Corona-App“ herausgegeben. Angesichts des hohen Schadpotenzials auch in Hinblick auf weitere App-gestützte Maßnahmen zur Eindämmung der SARS-CoV-2-Pandemie sind die identifizierten Schwachstellen und daraus resultierenden Risiken auf Dauer nicht tragbar. Die Autoren empfehlen daher eine zeitnahe nachträgliche Umsetzung der gegebenen Empfehlungen.

Für künftige Vorhaben nicht nur unter dem Oberbegriff „Corona-App“ empfehlen die Autoren dagegen proaktives Handeln: Viele der identifizierten Risiken lassen sich bereits im Vorfeld unter Berücksichtigung der vom Chaos Computer Club veröffentlichten 10 Prüfsteine für die Beurteilung von „Contact Tracing“-Apps[24] eliminieren. Die darin vom Chaos Computer Club geforderte Transparenz fördert zudem eine aktive und konstruktive Einbindung der Fachöffentlichkeit und hat damit das Potenzial, künftige App-gestützte Maßnahmen noch zielgerichteter zur Reife zu bringen.

[24] https://www.ccc.de/de/updates/2020/contact-tracing-requirements, abgerufen am 13. April 2020.

5 Dank

Mit besonderem Dank an Sven Fassbender für Beiträge zur iOS-App, Thomas Maus für fachliche Kritik und Kommentare und Christian Brodowski für die wertvolle Unterstützung.