AuraSec

ERFOLGSGESCHICHTEN

Corona-Datenspende-App (RKI)

www.aurasec.de

Daten. Sicher. Machen.

Informationssicherheit und Datenschutz für Apps und Infrastruktur

AuraSec testet die Sicherheit der Android- und iOS-App sowie des Backends

Welchen Zweck die Corona-Datenspende-App des Robert-Koch-Instituts verfolgt und wie sie zur Eindämmung der Pandemie beitragen kann

Mit der Corona-Datenspende stellen Bürgerinnen und Bürger dem Robert Koch-Institut Daten zur Verfügung, die dabei helfen können, die Ausbreitung des Coronavirus besser zu erfassen und zu verstehen. Dabei handelt es sich um Daten von Fitnessarmbändern und Smartwatches, auch Wearables genannt. Diese Daten werden mit Hilfe einer Smartphone-App zur Verfügung gestellt. Die Daten können Hinweise auf Symptome einer Infektion mit dem Coronavirus liefern. Die Datenfreigabe aus Fitnessarmbändern und Smartwatches soll zusammen mit Informationen aus anderen Datenquellen wie zum Beispiel den offiziellen Meldedaten dazu beitragen, dass die Wissenschaftler und Wissenschaftlerinnen ein genaueres Bild über die Verbreitung des Virus gewinnen.

Nutzerinnen und Nutzer senden über eine App verschiedene Daten an das Robert Koch-Institut. Dazu gehören Daten zur Aktivität und Herzfrequenz, die von Fitnessarmbändern und Smartwatches gesammelt werden. Ebenso wird nach der Postleitzahl der Nutzer und Nutzerinnen gefragt.

Neuartige Algorithmen können anhand dieser Daten verschiedene Symptome erkennen, die unter anderem mit einer Coronavirus-Infektion in Verbindung gebracht werden. Auf Basis wissenschaftlicher Methoden werden die Ergebnisse geografisch aufbereitet. Sie können den Wissenschaftlerinnen und Wissenschaftler des Robert Koch-Instituts zusätzliche Informationen zur Verbreitung des neuartigen Coronavirus liefern.

Die Corona-Datenspende-App kann kostenfrei im App Store von Apple und dem Google Play Store heruntergeladen werden.

Laden im App Store

JETZT BEI Google Play

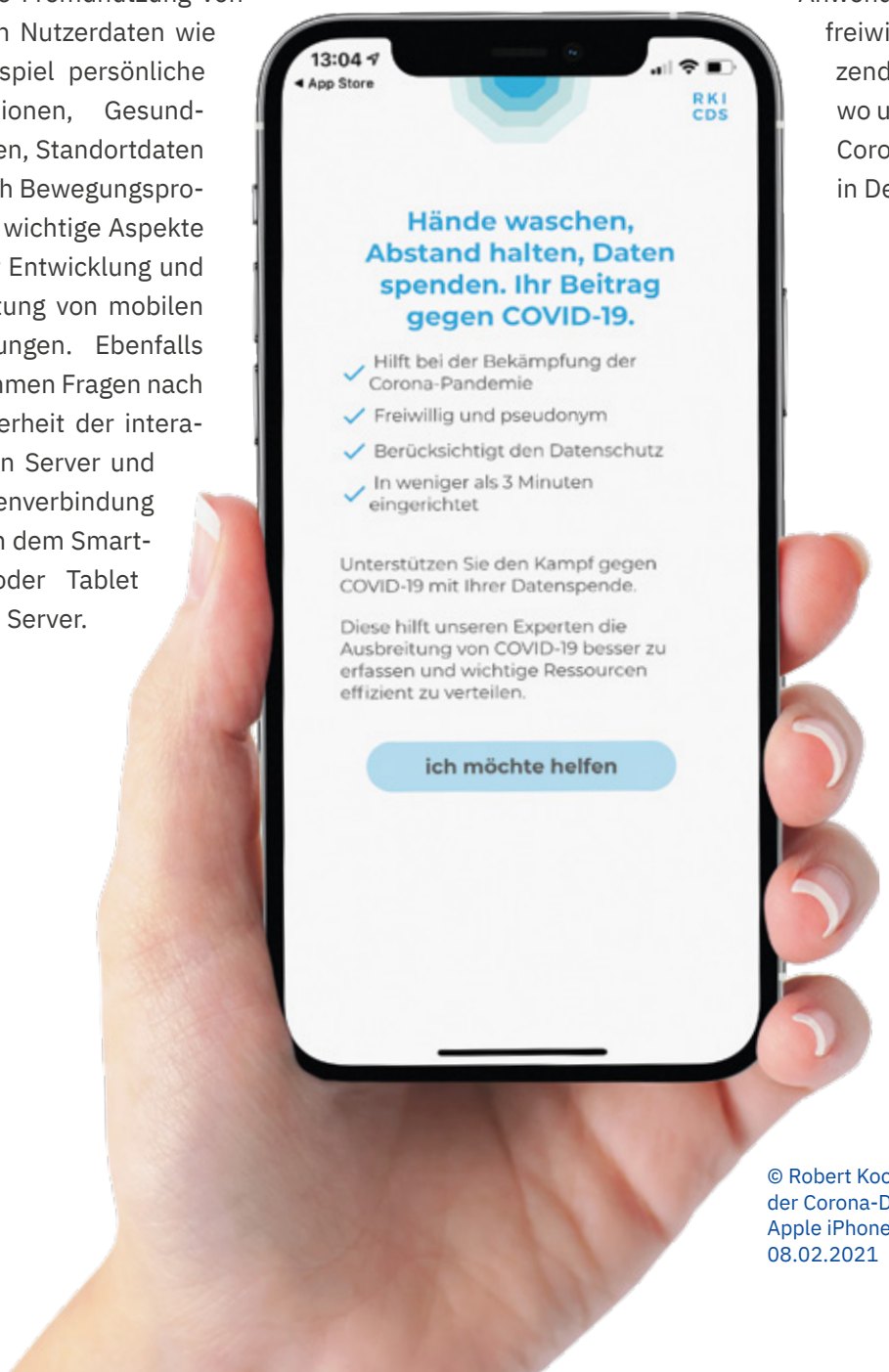
Sensible Gesundheitsdaten verdienen einen besonderen Schutz

Mobile Apps, die Gesundheitsdaten verarbeiten und zur Analyse weiterleiten unterliegen besonders hohen Anforderungen an den Schutzbedarf, da sie einen direkten Zugriff auf die hoch sensiblen Nutzerdaten der App-Anwender haben und falsche oder schlecht umgesetzten Sicherheitsvorkehrungen der App ein erhebliches Risiko darstellen.

Dies gilt für die App selbst, aber auch für die Backend-Infrastruktur, in welcher die eigentliche Datenverarbeitung erfolgt. Unberechtigte Zugriffe sowie eine unerwünschte Weitergabe beziehungsweise die Fremdnutzung von sensiblen Nutzerdaten wie zum Beispiel persönliche Informationen, Gesundheitsdaten, Standortdaten oder auch Bewegungsprofile, sind wichtige Aspekte bei einer Entwicklung und der Wartung von mobilen Anwendungen. Ebenfalls dazukommen Fragen nach der Sicherheit der interagierenden Server und der Datenverbindung zwischen dem Smartphone oder Tablet und dem Server.

Verständlicherweise rückte daher die von der Regierung und dem Robert Koch-Institut (RKI) beauftragte Corona-Datenspende-App des in Berlin niedergelassen Unternehmens mHealth Pioneers GmbH in den Fokus der Diskussion, welche zu Beginn der Corona-Pandemie in Deutschland veröffentlicht wurde.

Die App, welche zur Datenspende in Verbindung mit Fitness-Trackern genutzt wird, erreichte dabei direkt bei Ihrer Veröffentlichung den ersten Platz der meistgeladenen Apps im App Store. Die Anwendung, deren Nutzung freiwillig ist, liefert ergänzende Informationen dazu, wo und wie schnell sich das Coronavirus (SARS-CoV-2) in Deutschland ausbreitet.



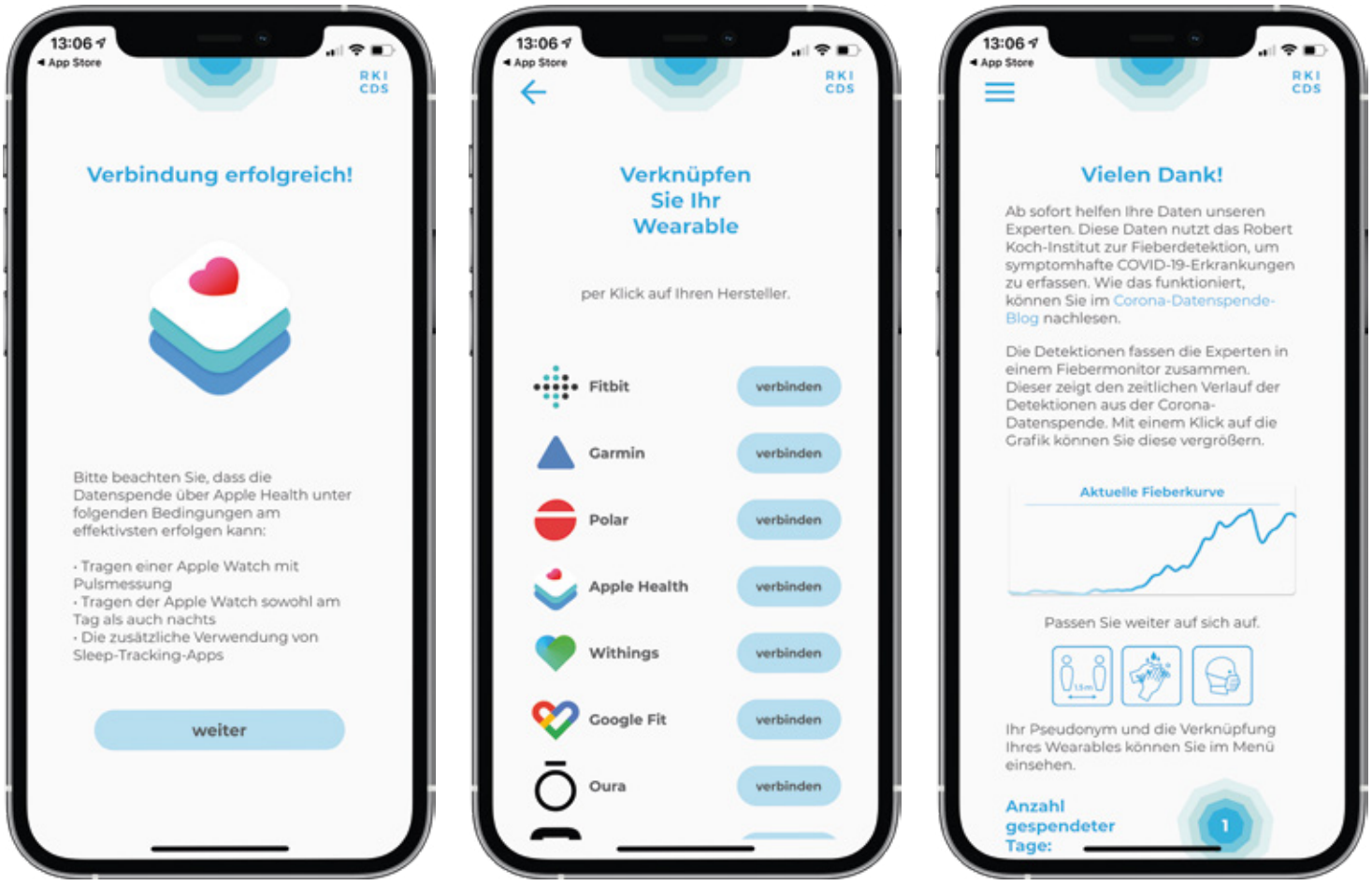
© Robert Koch-Institut. Startbildschirm der Corona-Datenspende-App auf einem Apple iPhone® 12 Pro. Abgerufen 08.02.2021

Funktionsweise der Corona-Datenspende-App in Kombination mit einem Fitnessarmband oder einer Smartwatch

Mit der Corona-Datenspende stellen die App Nutzer Gesundheits- bzw. Fitness-Daten wie zum Beispiel Alter, Größe, Gewicht, Geschlecht, Puls, Temperatur sowie Schlaf und Aktivitätsniveau zur Verfügung, die dabei helfen sollen, die Ausbreitung des Coronavirus in der Bevölkerung besser zu erfassen und zu verstehen.

Diese Daten werden durch Fitnessarmbänder und Smartwatches, auf iOS oder Android-Basis auch Wearables genannt, erfasst und über die Corona-Datenspende-App dem RKI in pseudonomisierter Form zur Analyse und Auswertung zur Verfügung gestellt.

Die gesammelten Informationen sollen Hinweise auf Symptome einer möglichen Infektion mit dem Coronavirus liefern. Zusammen mit anderen Datenquellen, zum Beispiel den offiziellen Meldedaten sollen die Daten der Datenspender dem RKI helfen die Ausbreitung des Corona Virus besser voraussagen zu können. Mitbegründer von mhealth Pioneers, Friedlich Lämmel erklärt: „Die Corona-Datenspende-App dient in diesen Krisenzeiten als eine Art medizinisches Thermometer“. Mehr als 500.000 Menschen in Deutschland haben die App bereits heruntergeladen (Stand: 24.04.2020).



© Robert Koch-Institut. Verknüpfung der Corona-Datenspende-App mit einer Smartwatch (am Beispiel mit Apple Health in Kombination mit einer Apple Watch®) auf einem Apple iPhone® 12 Pro. Abgerufen 08.02.2021

mHealth Pioneers GmbH (Thryve) – Spezialisiert auf Digital Health

mHealth Pioneers hatte bereits Anfang 2020 das Grundkonzept für die dann später genannte Corona-Datenspende-App entwickelt – in Form eines Algorithmus zur Erkennung grippeähnlicher Symptome. Noch bevor die Corona-Pandemie Deutschland erreichte, untersuchten Lämmel und sein Team im Februar, wie ihre Technologie zur Bekämpfung der Pandemie beitragen kann.

„Wir haben festgestellt, dass wir mit einigen Anpassungen unseres bestehenden Algorithmus auch COVID-19-Symptome erkennen können." mHealth Pioneers wandte sich proaktiv an das RKI und schlug vor, eine App zu entwickeln. Innerhalb von nur vier Wochen wurde in enger Zusammenarbeit mit dem RKI die Corona-Datenspende-App entwickelt. mHelath Pioneers lieferte die technische Grundlage für die Analyse und Auswertung der Daten, das Design und die Benutzeroberfläche wurden in Zusammenarbeit mit dem RKI erstellt.

Die breite und weitgehend positive Berichterstattung in den Medien – wie die New York Times und die Washington Post berichteten – ist eine Premiere für das noch junge Unternehmen mHealth Pioneers.

Obwohl DSGVO-konform und nach dem Stand der neusten Technik entwickelt, äußerten einige Datenschützer und Sicherheitsexperten Kritik an der App.

Um noch mehr Vertrauen für die App zu schaffen, beauftragte das Berliner mHealth Pioneers GmbH die AuraSec GmbH mit der Durchführung eines App-Security Tests sowie einer Prüfung des Backends.

Ziel dabei war die Identifizierung potentieller Schwachstellen, die es Angreifern erlauben könnten, die Applikation zu kompromittieren, missbräuchlich zu nutzen, in ihrer Verfügbarkeit einzuschränken oder vertrauliche Daten auszuspähen.

„Der Start der App war weitaus erfolgreicher, als wir es uns jemals hätten vorstellen können. Dank unserer agilen internen Strukturen waren wir flexibel genug, um schnell auf die ankommende Spitzenlast zu reagieren – obwohl wir nur ein Team von zwölf Personen sind. Das Projekt zeigt eindrucksvoll welch wertvolle Informationen, vom Smartphone und Fitnesstracker gesammelte, Gesundheitsdaten liefern."

- Friedlich Lämmel, CEO & CoFounder mHealth Pioneers

Vorgehen zur Überprüfung der iOS und Android-App sowie der Backend-Infrastruktur auf Sicherheitsmängel

Prüfung der Konzepte und der Architektur der Systeme

Überprüfen und validieren der benötigten und angeforderten Berechtigungen

Sicherstellen der ordnungsgemäßen lokalen Speicherung sensibler Daten

Kontrolle der Kommunikationswege zur sicheren und datenschutzkonformen Datenübermittlung an das Robert Koch-Institut (RKI)

Überprüfen der iOS- sowie Android-App auf Plattform-spezifische Sicherheitslücken

Sicherheitsanalyse des Backends und der API

Abschlussbericht und Präsentation der Ergebnisse, ggf. Retest

Anfang April 2020 erfolgte die Überprüfung auf Sicherheitsmängel für iOS (Version 1.0.2) und Android (Version 1.0.1) durch die Sicherheitsexperten der AuraSec GmbH. Nach dem ersten Penetrationstest gaben die Experten unterschiedliche Hinweise, welche unmittelbar durch den Auftraggeber umgesetzt wurden. In einem erneuten Penetrationstest wurde dann überprüft, ob die verschiedenen Hinweise korrekt implementiert wurden. Diese Überprüfung ergab, dass die relevanten Sicherheitslücken korrekt geschlossen wurden und somit über diese keine Angriffe mehr auf das System ausgeführt werden können.

Durch die umfassende Sicherheitsüberprüfung der Corona-Datenspende-App und den zugehörigen Systemen, ist nun sichergestellt, dass die App auf dem neuesten Stand der Technik ist und eine Gefahr vor missbräuchlichen Zugriffen somit weitestgehend ausgeschlossen werden kann.

„Die Verschlüsselungsmechanismen sind ordnungsgemäß integriert und es werden keine sensiblen Daten unverschlüsselt und außerhalb von Deutschland übertragen.“

– Daniel Janshoff, Consultant Informationssicherheit und Datenschutz AuraSec

Überprüfung des Backends zur Identifizierung potentieller Schwachstellen

Bei der Überprüfung des Backends wurden die Dienste des genutzten Servers, die Domain datenspende.und-gesund.de und die zur Verfügung gestellten APIs untersucht. Es wurden keine wesentlichen Sicherheitslücken festgestellt.

Eine durch den Chaos-Computer-Club (CCC) durchgeführte Analyse des Gesamtsystems deckte weitere Angriffsszenarien auf. Auf Grundlage dieses Berichtes führte mHealth Pioneers weitere Verbesserungen am System durch, welche die allgemeine Sicherheit verbessern sollten.

Im Rahmen weiterer Prüfungshandlungen wurden die vom CCC gegebenen Hinweise mit dem überarbeiteten Stand des Gesamtsystems verglichen, um zu überprüfen, ob die Angriffsvektoren erfolgreich geschlossen wurden. Schwachstellen, welche nicht geschlossen wurden bzw. geschlossen werden konnten, wurden seitens AuraSec einer Risikoanalyse unterzogen, damit deren Kritikalität korrekt bewertet werden konnte. Hierbei wurden ausschließlich die technischen Aspekte der Umsetzung betrachtet.

„Für uns war das ein spannendes Projekt eine so stark in der öffentlichen Wahrnehmung diskutierte App zu prüfen. Für alle im Team war diese Sicherheitsanalyse ein enormer Motivationsschub. Im Hinblick auf die bei Penetrationstests limitierte Zeit war es eine Herausforderung die relevanten Sicherheitslücken zu identifizieren. Wir sind stolz mit unserem Engagement einen positiven Beitrag zur Bekämpfung der Covid19-Pandemie zu leisten. Nur wenn die Menschen Vertrauen in die App haben, kann diese erfolgreich sein.“

- Jan C. Arfwedson, Geschäftsführer AuraSec

AuraSec

05/2021 KS

KONTAKT

AuraSec GmbH
Unter den Linden 16
10117 Berlin

Telefon: +49 (0)30-408173352
E-Mail: info@aurasec.de
Web: www.aurasec.de

UNSERE BRANCHEN

- Gesetzliche Krankenversicherungen
- Private Krankenversicherungen
- Kliniken und Krankenhäuser
- Pharmaunternehmen
- Rechenzentren
- Softwarehersteller
- Kritische Infrastrukturen

UNSERE LEISTUNGEN

- IT- und Informationssicherheitsmanagement
- Business Contiuity-Management
- Datenschutzmanagement
- Risikomanagement
- Kritis-Nachweisverfahren nach § 8a BSIG
- Weiterbildung
- Prüfgemeinschaft zur gemeinschaftlichen Durchführung von Lieferantenprüfungen
- Datenschutzmanagement-Tool ADAMA