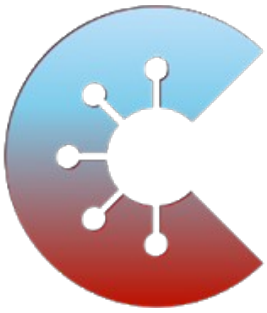

APPVISORY PrePentest

Corona-Warn-App (Android)

Durchschnitt CVSS 5.2 (medium)

Höchster CVSS 7.5 (high)

App-Informationen

• Hersteller	Robert Koch-Institut
• Name	Corona-Warn-App
• Betriebssystem	Android
• Version	1.3.0
• Erscheinungsdatum	02.09.2020
• BundleIdentifier	de.rki.coronawarnapp
• Benötigte OS-Version	Android 6.0 oder höher
• Store-Link	https://play.google.com/store/apps/details?id=de.rki.coronawarnapp&hl=de
• Store-Kategorie	Gesundheit und Fitness

Inhaltsverzeichnis

1 Testergebnis

Corona-Warn-App	Version 1.3.0	Android
Datenschutzverstöße • kein Verstoß festgestellt.	Einstufung	**unbedenklich**
Datensicherheitsverstöße • kein Verstoß festgestellt.	Einstufung	**unbedenklich**
AGB und Datenschutzerklärung • Keine Überprüfung der Datenschutzerklärung vorgenommen	Einstufung	**nicht verfügbar**
SSL/TLS Analyse • eine Man-In-The-Middle-Attacke war erfolgreich	Einstufung	**bedenklich**

1.1 Zusätzliche Funktionalitäten

Mobile Applikationen können über Drittanbieter erweiterte Funktionalitäten bieten. Dabei umfasst die Bandbreite neben In-App-Käufen zur Funktionserweiterung oder Entfernung von Werbung auch die externe Speicherung von Nutzerdaten in Cloud-Speicherdiensten, das Teilen von Meldungen über soziale Netzwerke oder die Registrierung eines Nutzer-Accounts über ein bereits bestehendes Profil eines sozialen Netzwerks.

1.1.1 In-App-Käufe

In der Applikation sind keine In-App-Käufe möglich.

1.1.2 Externe Cloud-Dienste

Die Applikation ermöglicht keine Sicherung von Daten über externe Cloud-Dienste.

Über Cloud-Dienste ist es theoretisch möglich, firmeninterne und möglicherweise geheime, sicherheitsrelevante oder anderweitig schützenswerte Daten manuell oder automatisch auf fremde, unbekannte Server eines Drittanbieters zu übertragen. Die Serverstandorte können im Ausland liegen. Es besteht die Möglichkeit eines unkontrollierten Datenabflusses.

1.1.3 Externe Login-Dienste

Die Applikation ermöglicht keinen verkürzten Registrierungs- und Loginprozess über externe Login-Dienste.

1.1.4 Social Network Sharing

Die App ermöglicht kein Sharing von Inhalten und Nutzerkommentaren über soziale Netzwerke.

1.1.5 Verwendung Webviews

Die Applikation verwendet keine Webviews.

2 Durchgeführte Analysevektoren

TLS analysierbar?	ja

Sniffing Item	Kategorie	Übertragung festgestellt	Verschlüsselung
ETag	Metadata	**ja**	**ja**
meta-cwa-hash	Metadata	**ja**	**ja**

Hinweis: Grundsätzlich wird empfohlen, die Kommunikation zwischen Applikation und Servern ausschließlich über verschlüsselte Verbindungen vorzunehmen.

3 Testergebnisse

In diesem Kapitel sind die Ergebnisse des Application Security Audits zusammengefasst. Das zugrunde liegende Testverfahren kann in der aktuell gültigen mediaTest digital Prüfspezifikation [separate Anlage] nachgelesen werden. Getestet wurde im Testlabor der mediaTest digital GmbH.

Das Testverfahren beinhaltet keine Aussagen über Funktionalität und Design sowie Performance und Stabilität der getesteten Applikation. Aussagen über Sicherheitslücken in angeschlossenen Backend-Systemen können lediglich in geringem Umfang getroffen werden.

Die vollständige technische Dokumentation kann im Kapitel 4 eingesehen werden. Dort finden sich ausführliche Informationen über Datenverbindungen und Datentransfer.

3.1 Test Setup

Der Testdurchlauf wurde im Testlabor der mediaTest digital GmbH durch einen Application Security Analyst durchgeführt. Getestet wurde auf einem physikalischen Testgerät. Grundsätzlich ist sowohl ein hoher Verbreitungsgrad des Testgerätes ebenso gegeben wie die Verwendung einer aktuellen Version des Betriebssystems.

- Testdatum 08. September 2020

.• Testgerät	Nexus 6P (Android 7.1.2)
• Testumgebung	mediaTest digital Testlabor
• Prüfspezifikation	mediaTest digital Prüfspezifikation rev. 2.0

3.2 Tracking-Dienste

Während des Testlaufs wurde die Applikation hinsichtlich eingebundener Module und Bibliotheken von Drittanbietern untersucht. Diese Module bieten erweiterte Funktionalitäten (z.B. durch die Bereitstellung von Kartenmaterial), erlauben die Auslieferung von Werbung oder erheben Nutzerstatistiken.

Die Untersuchung des von der Applikation erzeugten Datenverkehrs während des Testlaufs sowie einer statischen Analyse zeigt die Einbindung folgender externer Dienste.

Tracker	Beschreibung
• Keine Funde	

3.3 Virenanalyse

Während der Virenanalyse über die virustotal API durchläuft die Applikationsdatei über 50 Virenscanner. So kann eine, je nach Ergebnis gewichtete Aussage, über eine potenzielle Bedrohung durch Viren oder Trojaner getroffen werden.

• Dateiname	Corona Warn App_v1.3.0.apk
• SHA256 Hashwert	e1546369ac15644b92d200bdc31905052eeddbaf88e9ce28216c8fb1411277cc
• Virenscan-Ergebnis	**Funde: 0 von 63**

3.4 Berechtigungsanalyse

Die Berechtigungsanalyse basiert auf einer statischen Analyse während des Testlaufs. Aufgerufene Berechtigungen werden – soweit möglich – dynamisch durch einen Application Security Analyst verifiziert. Schlägt eine manuelle Verifizierung fehl, wird die Berechtigung als „potenziell genutzt“ eingestuft.

Berechtigungen werden in mehrere Schweregrade eingestuft, die sich am Zugriff der Applikation auf Nutzerdaten orientieren:

• system	Höchstes Risiko. Die Applikation muss mit dem identischen Zertifikat signiert sein wie die Applikationen auf Betriebssystemebene. Bei Aufruf der Berechtigung durch die Applikation wird der Nutzer **nicht** nach seiner Zustimmung gefragt.
• riskant	Hohes Risiko. Die Applikation erhält Zugriff auf Nutzerdaten oder weitreichende Funktionalitäten des Betriebssystems. Bei Aufruf der Berechtigung durch die Applikation wird der Nutzer nach seiner Zustimmung gefragt.
• normal	Niedriges Risiko. Die Applikation erhält isolierten Zugriff auf Applikationsebene und kann nicht auf Nutzerdaten oder weitreichende Funktionalitäten des Betriebssystems zugreifen. Bei Aufruf der Berechtigung durch die Applikation wird der Nutzer nach seiner Zustimmung gefragt.
• selbst erstellt	Durch den Entwickler selbst erstellte Berechtigung. Diese dient der Funktionalität der Applikation und erlaubt keinen Zugriff auf Nutzerdaten oder weitreichende Funktionalitäten des Betriebssystems.

Die Applikation fordert die folgenden Berechtigungen an.

Berechtigung	Beschreibung	Einstufung	Nutzung	Notwendig
Kamera	Erlaubt einer App den Zugriff auf die Kamera des Gerätes und die möglichkeit Fotos und Videos aufzunehmen	• riskant	Ja	ja
Bluetooth	Erlaubt einer App den Zugriff auf die Bluetoothfunktion des Gerätes	• riskant	Ja	ja
Mitteilungen	Erlaubt einer App den Zugriff auf die Push-Mitteilungs Funktion.	• normal	Ja	ja

Die Berechtigungsanalyse zeigt die Verwendung von **3** Berechtigungen, die zur Verwendung aller Funktionen der Applikation benötigt werden. Die Applikation ruft nur die Berechtigungen ab, die für den Funktionsumfang notwendig sind. Die Applikation wird nicht als überprivilegiert eingestuft.

3.5 Binärdatei-Analyse

Problematik	Schweregrad	Standards	Beschreibung
App uses SQLite Database and execute raw SQL query.	High	**CVSS V2:** 5.9 (medium) **CWE:** CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') **OWASP Top 10:** M7: Client Code Quality	Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.
Insecure Implementation of SSL.	High	**CVSS V2:** 7.4 (high) **CWE:** CWE-295 - Improper Certificate Validation **OWASP Top 10:** M3: Insecure Communication **OWASP MASVS:** MSTG-NETWORK-3	Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks
The App logs information.	Info	**CVSS V2:** 7.5 (high) **CWE:** CWE-532 - Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3	Sensitive information should never be logged.
This App uses Java Hash Code.	warning	**CVSS V2:** 2.3 (low) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP MASVS:** MSTG-CRYPTO-4	It's a weak hash function and should never be used in Secure Crypto Implementation.
This App uses SQL Cipher.	Info	**CVSS V2:** 0 (info) **OWASP MASVS:** MSTG-CRYPTO-1	SQLCipher provides 256-bit AES encryption to sqlite database files.

3.6 Risikobewertung

Anhand des aufgezeichneten Datenverkehrs während des Testlaufs sowie auf Basis einer statischen Analyse werden Sicherheitslücken und damit potentielle Risiken überprüft, die mit der Nutzung der Applikation einhergehen können.

Die Auswertung des Testlaufs erfolgt halb-automatisiert und wird durch einen Application Security Analyst vorgenommen. Im Zuge einer Kernfunktionalitäts- und Plausibilitätsprüfung wurde dabei besonderer Wert auf Datenübermittlungen und Berechtigungen gelegt, die zur Ausführung der primären Funktionen der Applikation nicht unbedingt notwendig sind oder für den Nutzer keinen Mehrwert bieten.

Weiterführende Details zu während des Testlaufs festgestellten Datenschutz- und Datensicherheitsverstößen werden im Kapitel 4 in der Datenübertragungsanalyse aufgelistet. Die Handlungsempfehlungen bieten für den Entwickler der Applikation eine erste Hilfestellung, identifizierte Probleme zu beheben.

3.6.1 Datenschutzverstöße

In diesem Unterkapitel werden die Datenschutzverstöße aufgelistet und eine Handlungsempfehlung abgegeben. Als Datenschutzverstoß wird die Übertragung eines personenbezogenen[1] oder anderweitig sensiblen Datums an Dritte definiert.

Keine Funde festgestellt	siehe **-** / **-**
Handlungsempfehlung:	

3.6.2 Datensicherheitsverstöße

In diesem Unterkapitel werden die Datensicherheitsverstöße aufgelistet und eine Handlungsempfehlung abgegeben. Als Datensicherheitsverstoß wird die Übertragung von Daten über eine unverschlüsselte Verbindung definiert.

Keine Funde festgestellt	siehe **-** / **-**
Handlungsempfehlung:	
HINWEIS:	
Handlungsempfehlung: Kein Handlungsbedarf	

4 Verbindungsanalyse

In diesem Kapitel werden ausführliche Informationen über die während des Testlaufs aufgezeichneten Datenübertragungen bereitgestellt.

[1]

4.1 Analyse Serververbindungen

In diesem Unterkapitel werden die Server aufgelistet, zu denen die Applikation während des Testlaufs Verbindungen aufgebaut hat.

Nr.	Servername	IP-Adresse	Port	Land	Betreiber
V1	https://svc90.main.px.t-online.de	87.140.208.122	443	DE	T-Online

4.1.1 Auszug Datenübertragungsprotokoll

4.1.1.1 Etag und meta-cwa-hash an t-online.de

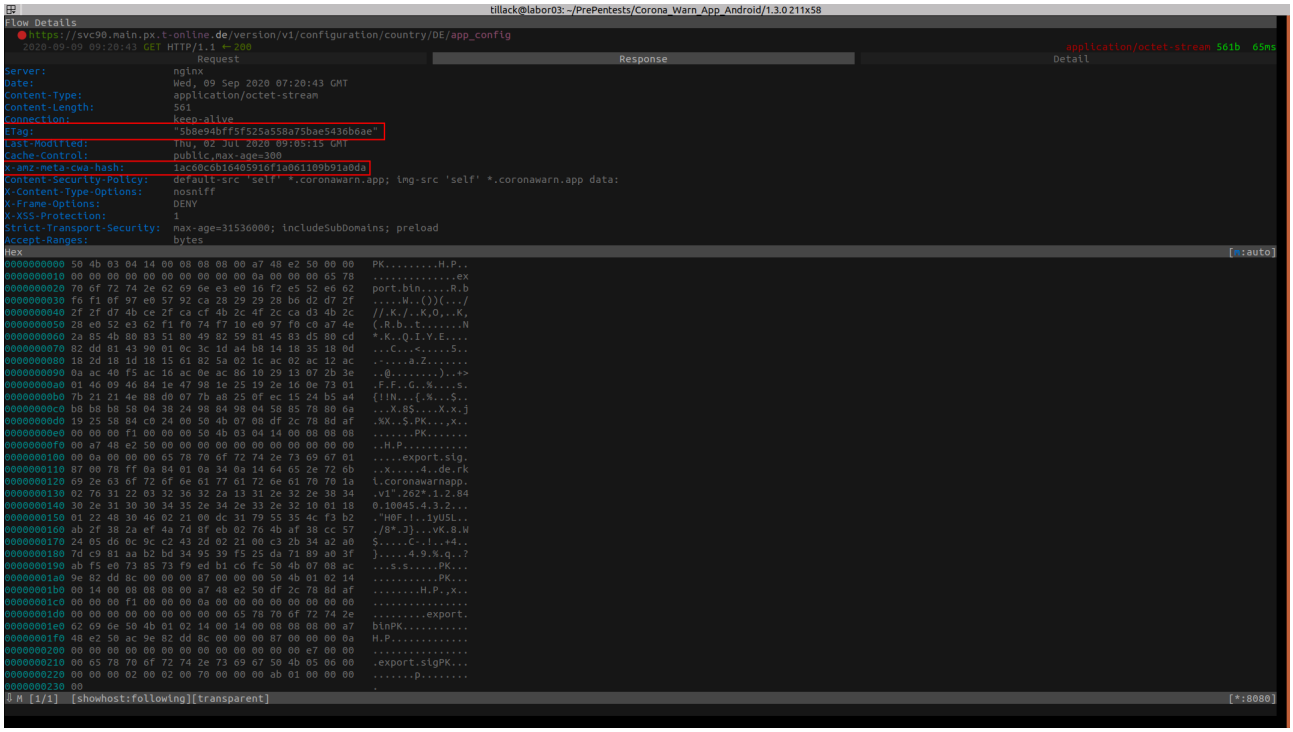

Abbildung 1.1 Etag und meta-cwa-hash werden an t-online.de übertragen

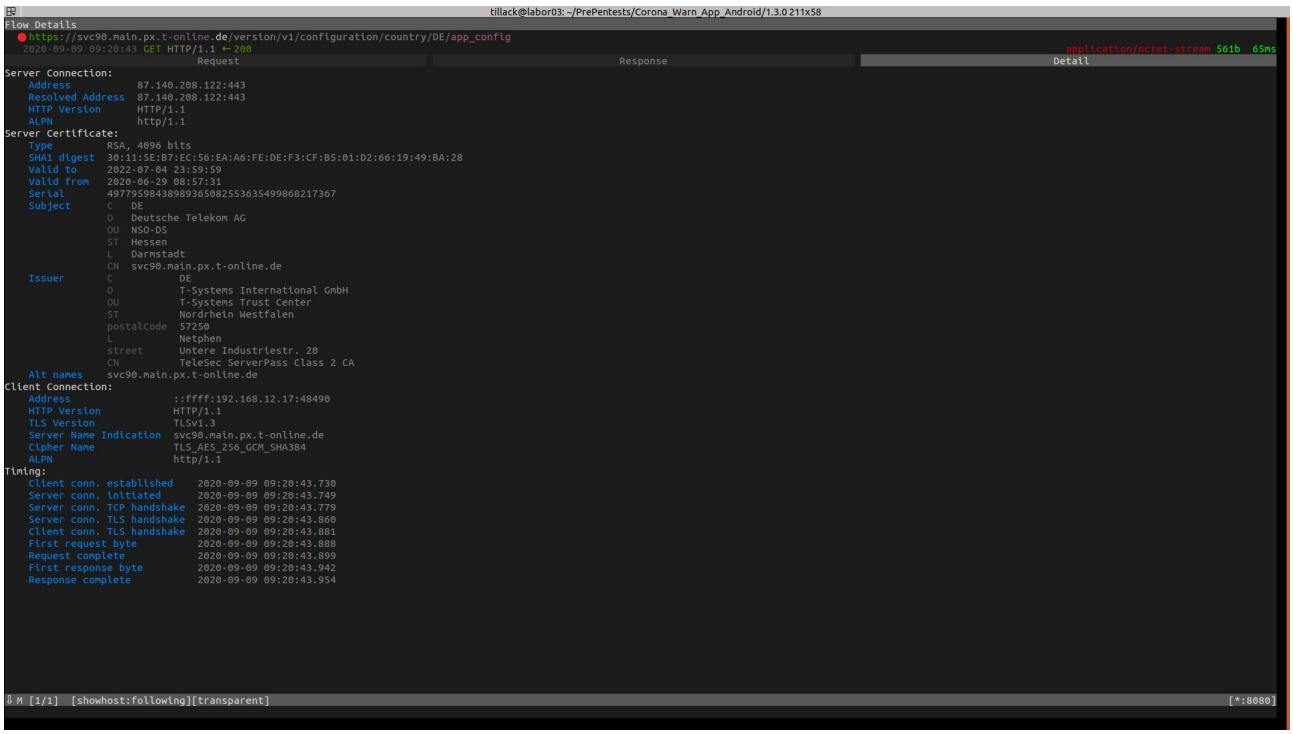

Abbildung 1.2 Server-Details t-online.de

5 Summary

Die Nutzung von Trackern oder Analyse-Tools konnte nicht festgestellt werden. Die Root-detection ist rudimentär implementiert. Gesammelte Daten werden möglicherweise nur lokal verarbeitet, da die volle Funktionsweise der Applikation uns während des Testlaufes nicht zur Verfügung stand (QR-Code). Es ist nicht absehbar was mit den gespeicherten Daten passiert, da die Kernfunktion der Applikation von dem jeweiligen Systemhersteller (Apple und Google) zur Verfügung gestellt wird.