ePrivacyseal GmbH

Kriterienkatalog (inklusive High Security)

„ePrivacyApp“

Technische Begutachtung

September 2021

Das Gütesiegel „ePrivacyApp“ für Datensicherheit der ePrivacyseal GmbH zertifiziert dem jeweiligen Antragsteller, dass sein Angebot mit den im nachfolgenden Kriterienkatalog näher spezifizierten Kriterien im Einklang steht, die sich an den Anforderungen an Datensicherheit auf der Basis des deutschen Datenschutzrechtes, an der zukünftigen Datenschutz-grundverordnung und dem aktuellen Stand der Technik orientieren.

Die Prüfung bezieht sich dabei allein auf die nachfolgend beschriebenen sicherheits-technischen Fragestellungen. Eine juristische Bewertung ist damit **nicht** verbunden.

Im Einzelnen wird damit die Einhaltung folgender Anforderungen bestätigt:

I. Formale Anforderungen

Die Überprüfung der App erfolgt zunächst dahingehend, ob die formalen Voraussetzungen der ordnungsgemäßen Begründung und Abwicklung eines Vertragsverhältnisses zur Installation auf dem Endgerät des Users erfüllt sind. Am Anfang des Evaluierungsprozesses wird der „Ist-Zustand" der zu prüfenden App und die Voraussetzungen für die Prüfung selbst festgehalten. Hierfür werden zunächst die folgenden allgemeine Informationen der zu prüfenden App ermittelt und festgehalten:

1. Allgemeines

- In welche Kategorie, Funktionsweise und Beschreibung ist die App eingeordnet?
- Wie wird die App exakt bezeichnet?
- Liegt eine exakte Versionierung der App vor? (Dies beinhaltet Versionsnummer und Versionsdatum)
- Wer ist Anbieter der App und wer gegebenenfalls Entwickler?
- Erfolgt die Installation der App ohne Fehler oder treten eventuell Probleme auf?
- Werden bei der Installation noch andere Apps oder sonstige Software installiert mit oder auch ohne ersichtliche Einwilligung des Nutzers?
- Existiert eine Altersempfehlung für den App Store und scheint diese zutreffend zu sein?
- Gibt es eine Datenschutzerklärung innerhalb der App oder gibt es einer Verlinkung zu dieser? (keine juristische Bewertung)

2. Anmeldeoptionen

- Ist eine Nutzung der App ohne Anmeldung möglich?
- Ist die Nutzung der App ohne Nennung von personenbezogenen Daten möglich?
- Ist die Funktionalität ohne Anmeldung eingeschränkt?
- Wie weit gehen die Einschränkungen, wenn keine Anmeldung erfolgt?
- Mit welchen anderen Apps kann sich der Nutzer anmelden / sich die App synchronisieren (z.B. Facebook Login)?
    - Welche Daten werden durch solche SDKs an Dritte weitergeleitet?
    - Ab welchem Zeitpunkt geschieht eine Datenübermittlung an solche Dritte?
    - Werden auch nach Ablehnung Daten gesendet?
- Kann sich der Nutzer mit einer E-Mail-Adresse anmelden?
- Kann der Nutzer seine Daten verändern?
- Kann der Nutzer seine Daten löschen?
- Erhält der Nutzer eine Bestätigung über die Löschung der Daten?
- Wie lange dauert eine Löschung der Daten (Gibt es eine Angabe dazu)?

II. <u>Datensicherheit – Grundlegende Anforderungen</u>

Der App-Anbieter muss darlegen, dass in seiner App hinreichende technische und organisatorische Sicherheitsmaßnahmen zum Schutz personenbezogener Daten implementiert worden sind. Die App sollte den aktuell geltenden Sicherheitsstandards entsprechen. Insofern sind folgende Fragen von Relevanz:

1. Datenverkehr

- Wird von der App Datenverkehr generiert?
- Welche Arten von Datenverkehr werden generiert?

- Funktionale Daten (ein- sowie ausgehend) zur Gewährleistung der Funktionalität der App
- Statistische Daten über die Benutzung der App
- Personenbezogene Daten, beispielsweise zur Generierung von Nutzerprofilen

- Woher kommt und wohin geht der Datenverkehr?
  - Daten werden „nativ“ im Rahmen der zugrunde legenden App generiert / erhoben / erhalten
  - Daten werden im Rahmen von Code eines Drittanbieters generiert / erhoben / erhalten

2. Eingehende und ausgehende Daten

- Werden eingehende Daten verschlüsselt?
- Werden ausgehende Daten verschlüsselt?
- Werden vertrauliche Datensätze (z.B. Nutzername, Passwort, E-Mail) zusätzlich verschlüsselt?
- Entspricht die Verschlüsselung dem aktuellen Stand der Technik?
- Mit welcher Schlüssellänge werden vertrauliche Datensätze kodiert?
- Können verschlüsselte / verhashte vertrauliche Daten mit einem verhältnismäßig geringem Aufwand dekodiert werden?
  - Wird für das Verhashen ein Salt verwendet?
  - Wird ein potenziell unsicheres Hashverfahren genutzt?
- Kann ein Man-in-the-Middle Angriff durchgeführt werden, um den Datenverkehr auszulesen?
- Erhält der Nutzer eine Warnung über eine potentiell unsichere Verbindung?
- Kann der Datenverkehr manipuliert werden?

    - Ist es möglich dadurch Schaden an Daten Dritter anzurichten?
    - Können dadurch Sicherheitsmaßnahmen umgangen werden?
- Können Informationen unbeteiligter Dritter über die App erhoben werden?
- Findet eine Authentizitätsprüfung über die Validität des SSL Zertifikates statt?
- Können potenziell jugendgefährdende Inhalte über die App aufgerufen werden?
- Wurden Sicherheitsmaßnahmen implementiert, die im Falle der Erkennung einer Kompromittierung der App greifen?

3. Einsatz von Tracking-Cookies und Ad-ID‘s

- Werden Tracking-Cookies, im Falle einer Web-App eingesetzt?
- Enthalten die Cookies personenbezogene Daten (z.B. IP-Adresse, Handynummer, Ad-ID)?
- Enthalten die Cookies einen Timestamp?
- Werden Ad-IDs (z.B. IDFA, GAID, usw.) verwendet, um nutzerbasierte Werbung auszuspielen?
- Werden Ad-IDs für sonstige Zwecke verwendet?
- Findet ein Tracking von Minderjährigen statt?
- Ist ein potentielles Opt-Out auch innerhalb der App wirksam?

4. Zugriff auf persönliche Daten

- Wird auf folgende Entitäten zugegriffen:
    - Directories des Devices (z.B. Kontaktdaten, Kalender etc.)?
    - Exakte Lokationsdaten (z.B. GPS-Koordinaten)?
    - Hardware des Devices (z.B. Mikrofon, Kamera)?

- Medienspeicher (Fotos, Videos, usw.)?

- Sind die Rechte, welche die App einräumt, für den Funktionsumfang der App von Nöten?

- Ist es möglich, sofern für die Funktionalität der App nicht zwingend notwendig, den oben beschriebenen Zugriff zu beschränken / unterbinden?

- Werden ungefragt Datensätze übermittelt?

5. Übertragung von Stammdaten

- Auf welche Identifier des Devices werden von der App zugegriffen (z.B. IMEI, UDID, etc.) und welche werden versendet?

- Wird die IP-Adresse bei einem Request oder Response übermittelt?

- Wird die MAC-Adresse der Netzwerkschnittstelle des Devices übermittelt?

- Wird die SSID (Name des WLAN-Netzwerkes mit dem das Device verbunden ist) übermittelt?

- Wird der Mobile Carrier (Telefonanbieter: z.B. Telekom, O2, etc.) übermittelt?

- Wird die Telefonnummer des Nutzers übermittelt?

- Wie werden, sofern zutreffend, diese Daten auf dem Device oder serverseitig vom App-Anbieter gespeichert?

III. Datensicherheit – High Security Anforderungen

Für die Begutachtung einer App mit dem High Security Standard der ePrivacyApp Zertifizierung, gibt es zusätzlich zu den bisher genannten Kriterien spezifischere Anforderungen, die gezielter auf den jeweiligen Funktionsumfang der zu prüfenden App anzuwenden sind. Nicht alle aufgelisteten Kriterien sind zwingend erforderlich oder treffen gar zu. Zusätzliche individuelle Tests, insbesonders im Bereich „Exploits“, werden im Testzeitraum durchgeführt, nachdem der volle Funktionsumfang der App bekannt ist und mögliche Schwachstellen ausdefiniert worden sind. Kriterien in diesem Abschnitt verändern sich gemäß dem Stand der Technik fortlaufend und bilden somit lediglich eine konzeptionelle Basis.

1. Erweiterte Nutzerrechte

Sollte das Gerät über erweiterte Nutzungsrechte verfügen, die eine potenzielle Gefahr für Nutzerdaten oder Sicherheit darstellen, muss dies festgestellt werden und ggf. blockiert bzw. die Nutzung der App unterbunden werden. Manipulationen und laufende, gängige Analyseverfahren sollten erkannt und ggf. verhindert werden und/oder der Nutzer auf diese Gefahr hingewiesen werden.

2. Lokaler Speicher

Sensible Daten in jeder Form müssen vor Angreifern geschützt werden. Dies beinhaltet das Speichern von lokalen, sowie externen Daten mit Hilfe der aktuell geltenden Sicherheitsstandards oder darüber hinaus. Es muss der Zugriff auf sensible Daten und deren Extraktion verhindert werden - egal in welchem Zustand sich die App während der Laufzeit befindet.

3. Umgang mit Identifikationen und Authentifizierungen

Bei Anmeldungen bzw. Authentifizierungen muss der aktuelle Sicherheitsstandard verwendet werden, was Technologie und Vorgaben für Anmeldedaten angeht. Der User muss über erfolgreiche oder fehlgeschlagene Anmeldungen informiert werden. Mehrfach falsche Anmeldungen müssen limitiert werden, um Angriffsvektoren auf ein Minimum zu reduzieren. Anmeldedaten, wie Passwörter müssen zusätzlich durch

technische Maßnahmen gesichert sein. Zur Maximierung der Nutzerdatensicherheit sollten Intelligente Vorkehrungen getroffen werden, die Nutzer auch vor unachtsamer Benutzung präventiv schützen.

4. Kommunikation

Netzwerkverkehr muss über eine standardisierte, gesicherte Verbindung erfolgen. Sensible Daten müssen zusätzlich mit einem weiteren Sicherheitsalgorithmus verschlüsselt werden. Generell dürfen keine Verbindungen ohne solche Sicherheitsmaßnahmen zugelassen werden. Zusätzlich verschlüsselte Inhalte müssen ausreichend mit aktuellen Sicherheitsstandards und deren Richtlinien versehen sein. Nachgestellte und oder manipulierte Verbindungen zu einem Backend dürfen weder ausnutzbar noch überhaupt möglich sein.

5. Exploits

Die App darf nicht in unsicheren Modi laufen. Verschlüsselungen müssen Penetrationstests standhalten und mindestens den aktuellen Standards entsprechen. Es muss sichergestellt sein, dass verwendete Bibliotheken oder Frameworks aktuell sind und keine Sicherheitslücke darstellen. Das Manipulieren, Abfangen und Verändern von Verbindungen muss unterbunden werden, sowie ggf. bei Feststellung den Nutzer informieren. Die App und ggf. verwendeten Komponenten müssen ausreichend gegen Manipulation und Reverse Engineering geschützt sein.

6. Social Engineering

Es dürfen keine Informationen, die geheim, vertraulich oder mit deren Hilfe man an solche Informationen gelangt, preisgegeben werden.

Hamburg, ePrivacy GmbH