Wo-Rona App

IT-Risiken

1. Inhaltliche falsche oder inkorrekte Regelungsdefinitionen.

   Beschreibung:
   Die falsche Übernahme und damit verbundene Verbreitung falscher gesetzlicher Vorgaben, könnte dazu führen, dass sich die Nutzer regelungswidrig verhalten. Folge könnte die Belegung des Nutzers mit einem Bußgeld oder schlimmer noch eine Ansteckung mit dem Corona-Virus sein.
   Daneben würde das Ansehen der App massiv leiden.

   Mitigation:
   Der Prozess der Datenerfassung muss möglichst fehlerfrei ablaufen. Dazu würde es Sinn machen, wenn die einzelnen Normgeber ihre Beschlüsse in einem Musterformular elektronisch an die für die Aktualisierung zuständige Stelle weiterleiten würden. Durch die einheitliche Erfassung der Regelungen, dürften bei der Übernahme der Daten weniger Fehler passieren. Zudem wird durch die Einreichung der Daten durch den jeweiligen Normgeber ein Teil der Verantwortung an diesen abgegeben. Eingereichte Daten sollten dennoch nochmals überprüft werden.

2. Ausspähung der lokal gespeicherten Daten, z.B. durch andere App etc.

   Beschreibung:
   Eine Drittapp könnte versuchen lokal gespeicherte Daten abzugreifen. Da die App keine besonders relevanten Daten speichern wird, ist der zu erwartende Schaden durch die Veröffentlichung solcher Daten eher gering. Dagegen wäre der zu erwartende Imageschaden als sehr groß einzuschätzen.

   Mitigation:
   Grundsätzlich werden alle Daten nur verschlüsselt gespeichert. Daneben wird das Prinzip der Datensparsamkeit angewandt. In der Grundausführung der App wird nur der manuell eingegeben Standort sowie die nicht vertraulichen Regelungsdefinitionen lokal gespeichert.
   Sollten auch die Tracker-Funktionen genutzt werden, müssen Daten gespeichert werden, welche Rückschlüsse auf das Verhalten einer Person zulassen. Dies werden wie erwähnt verschlüsselt abgelegt.

3. Die gleichzeitige Aktualisierung der Regelungsdefinitionen vieler Nutzer führt zu einer Überlastung der Server.

   Beschreibung:
   Sollten zu viele Nutzer gleichzeitig Updates herunterladen, könnte es dazu kommen, dass die Update-Server überlastet ausfallen.

   Mitigation:
   Die Server sollten mit einem geeigneten Mechanismus für Load-Balancing ausgestattet werden. Wird ein bestimmter Grenzwert an Serverauslastung erreicht, so sollten keine Update-Requests mehr angenommen werden, sondern ein Queueing stattfinden.

4. Ein Angriff auf die Update-Server legt diese lahm (z.B. aus dem Umfeld von Corona-Leugnern)

   Beschreibung:
   Zur finalen Lesung bez. des Infektionsschutzgesetzes wurden Mitarbeiter des Bundestages mit tausenden Mails überflutet.[1] Diese Attacke erfolgte mutmaßlich aus dem Umfeld sog. Corona-Leugner. Es steht zu befürchten, dass aus diesem Umfeld auch Attacken gegen die Nutzbarkeit der hiesigen App erfolgen könnten.

   Mitigation:
   Einem sog. Denial of Service-Angriff kann auf unterschiedliche Weise begegnet werden. Je nachdem wie dieser ausgestaltet ist, reicht tlw. schon die Änderung der IP-Adresse eines Servers. Grundsätzlich ist es wichtig, Angriffe möglichst frühzeitig zu erkennen. Aufgrund dessen sollte durchgehend auf die Vitalitätsparameter der Server geachtet werden.

5. Die Rechteanforderungen der genutzten Betriebssysteme verunsichern den Nutzer (s. Corona Warn-App).

   Beschreibung:
   In älteren Android-Versionen geht z.B. die Nutzung der Bluetooth-Funktion mit der Standortberechtigung einher. Das kann Nutzer verunsichern.

   Mitigation:
   Berechtigungen sollten nur dann angefragt werden, wenn diese auch wirklich erforderlich sind. Zudem sollte dem Nutzer eine klare Erklärung angezeigt werden, warum gerade die Berechtigung benötigt wird.

1 s. dazu https://sz.de/1.5118775

Non-IT-Risiken

Der Erfolg der App ist vor allem auch durch Risiken bedroht, die nicht-technischer Art sind. Wie bereits beschrieben, ist das Vertrauen der Bevölkerung in die Integrität der App eine maßgebliche Voraussetzung für deren Erfolg im Sinne einer weiten Verbreitung und Nutzung. Deshalb haben wir weitere non-IT-Risiken erarbeitet, welche dies berücksichtigen.

Verbreitung von Falschinformationen

1. Die App diene dazu, die Einhaltung von Corona-Maßnahmen zu überwachen.

2. Funktionen wie automatische Standortermittlung seien nicht opt-in, sondern dauerhaft aktiv.

3. Es würden nicht nur Daten von den Update-Servern abgerufen, sondern auch Nutzungs- und Bewegungsdaten an die Server übermittelt.

Mitigation:
Der Umgang mit Nutzerdaten sollte übervorsichtig erfolgen, um Gerüchten über die App keinen Nährboden zu bieten. Zudem sollte medial darauf hingewirkt werden, dass die App als sicher wahrgenommen wird.

Riskiomatrix