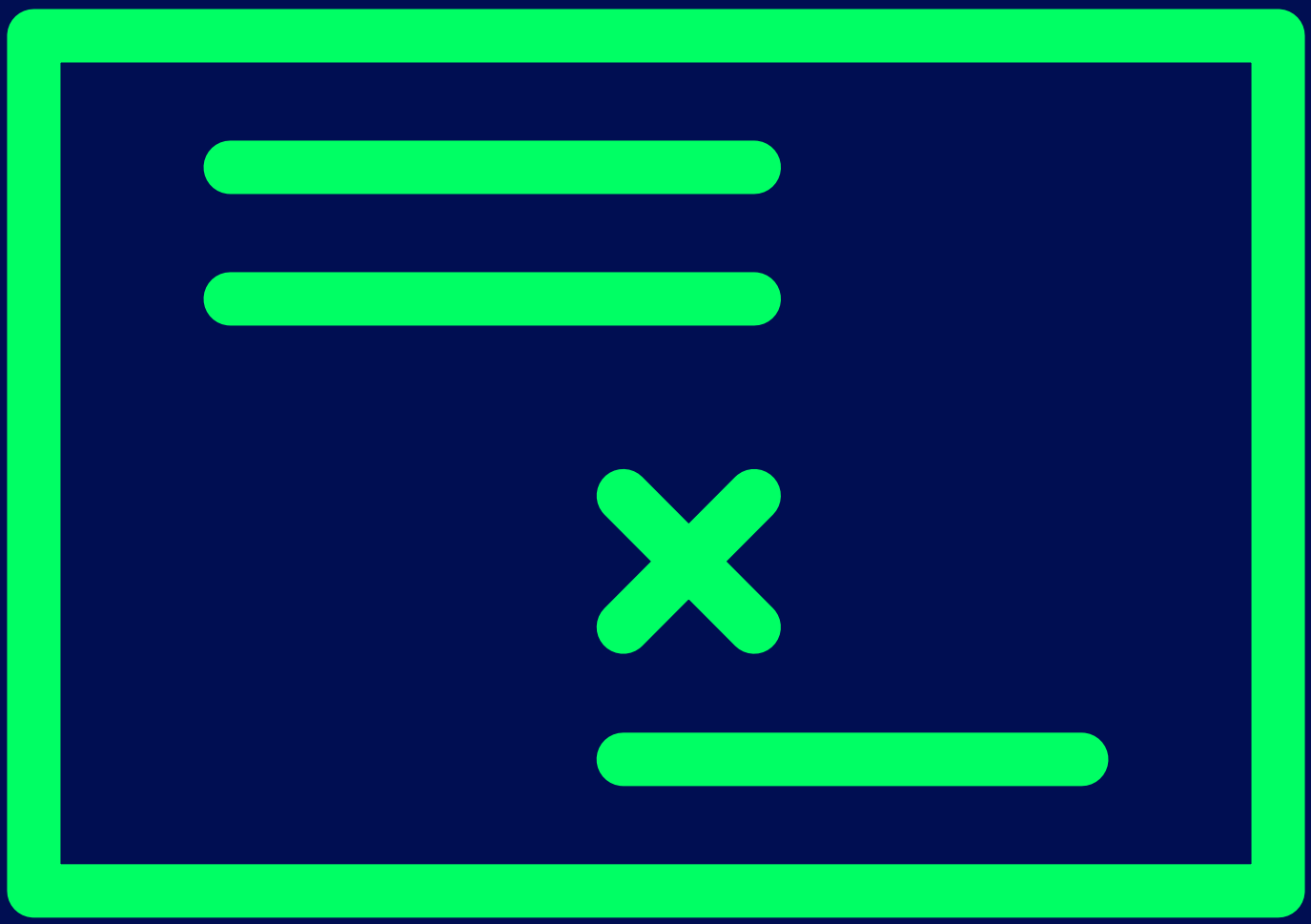
E-Rezept

gematik



# Datenschutz-Folgenabschätzung

für die E-Rezept-App der gematik – Anlage 1: Risikoanalyse

# Verarbeitungstätigkeiten

| ID | Bezeichnung | Beschreibung Verarbeitungstätigkeit |
|---|---|---|
| **V01** | **Installation/ Deinstallation der App** | Zunächst muss die App auf das Endgerät des Nutzers heruntergeladen und installiert werden. Hierzu muss der Nutzer ein bestehendes Nutzer-Konto für den von ihm genutzten Vertriebsplattform für Apps nutzen. Hierfür stehen der Apple App Store, der Google Play Store und die Huawei App Gallery zur Verfügung. Im Rahmen des Downloads und der Installation der App werden vom Betreiber der jeweiligen Vertriebsplattform in eigener Verantwortung Login- und Zugriffsdaten verarbeitet. Es besteht auch die Möglichkeit, die E-Rezept-App über GitHub im apk-Format für Android-Smartphones zu beziehen. Technisch versierte Nutzer können die App damit auf einem Android-Smartphone installieren, nachdem sie in den Betriebssystemeinstellungen die Installation aus „unbekannten Quellen“, d. h. von außerhalb des Google Play Stores, freigegeben haben. |
| **V02** | **Start und Einrichtung der App** | Bei jedem Startvorgang der App erfolgt eine Prüfung auf Anzeichen einer Modifikation zum Zwecke der Warnung von unwissenden Nutzern vor kompromittierten Umgebungen (sog. Rooting bzw. Jailbreaking). Wenn eine Modifikation des Betriebssystems erkannt wird, wird dem Nutzer in der App eine Warnung angezeigt, wobei die weitere Nutzung der App durch die erkannte Modifikation app-seitig nicht beschränkt wird. Zur optionalen Absicherung des Zugriffs auf die App wird die Authentifizierung des Nutzers gegenüber der App durch die für sein Endgerät verfügbaren betriebssystemseitigen biometrischen Authentifizierungsverfahren (z. B. Face ID oder „Entsperren per Fingerabdruck“) sowie die app-seitige Absicherung mittels eines Kennworts abgefragt. Bei Wahl der Absicherung mittels Kennwort zeigt ein Indikatorbalken den Grad der Sicherheit des eingegebenen Kennworts an. Ist die Authentifizierung beim Start der App nicht erfolgreich, wird der misslungene Authentifizierungsversuch in der App angezeigt und gezählt. Der Nutzer kann die Authentifizierung erneut und beliebig oft starten. Im Zuge des Onboardings muss der Nutzer ein lokales Profil einrichten. Der Nutzer kann mehrere Profile anlegen, was ihm die Möglichkeit gibt, als Vertreter (bspw. für Familienangehörige) die E-Rezepte von anderen Personen auf seiner App zu verwalten. Das Eingabefeld für den Profilnamen ist so konfiguriert, dass es der entsprechenden Funktion des Betriebssystems erlaubt, ein automatisches Ausfüllen der Profilnamen zu unterstützen (sofern der Nutzer diese Funktion des Betriebssystems aktiviert hat). Nachdem der Nutzer eine beliebige Zeichenfolge als Nutzernamen eingegeben und den „Weiter“-Button betätigt hat, wird diese Zeichenfolge lokal gespeichert. |

| ID | Bezeichnung | Beschreibung Verarbeitungstätigkeit |
|---|---|---|
| **V03** | **Anmeldung Fachdienst (und Identity Provider)** | Für die Authentifizierung gegenüber dem E-Rezept-Fachdienst mittels eGK gibt der Nutzer die Card Access Number (CAN) und PIN seiner eGK ein. Anschließend ruft die App den Identitätsdienst (IDP) auf. Ist der Aufruf des IDP erfolgreich, wird die NFC-Funktion des Betriebssystems zur kontaktlosen Datenübertragung aufgerufen oder aktiviert. Der Nutzer scannt seine eGK per NFC und es werden die benötigten Identitätsdaten ausgelesen und an den IDP übermittelt. Für die Authentifizierung gegenüber dem E-Rezept-Fachdienst mittels ePA-App wählt der Nutzer zunächst die jeweilige Krankenkasse aus einer Liste. Nachdem der Nutzer seine Auswahl getroffen hat, öffnet sich die ePA-App der jeweiligen Krankenkasse, ggf. nach erstmaliger Installation. Wird die App durch eine ePA-App aufgerufen, erhält sie von der ePA-App einen Identifizierungstoken, der sie gegenüber dem IDP validiert. Ist die Autorisierung durch den Server erfolgreich, erhält die App vom IDP einen SSO-Token. Der SSO-Token wird auf dem Endgerät des Nutzers gespeichert. Nach Erlangung des SSO-Token wird beim IDP ein Zugriffstoken für den E-Rezept-Server angefragt. Ist die Autorisierung durch den Server erfolgreich, erhält die App vom IDP einen Zugriffstoken (Access Token) für den E-Rezept-Server. Auch der Access Token wird auf dem Endgerät des Nutzers gespeichert. Vor Anfragen an IDP und E-Rezept-Server ermittelt die App zunächst die Gültigkeit vorhandener Token und löscht ungültige. Die SSO Token für den IDP sind 12 Stunden gültig, die Access Token für den E-Rezept-Server 5 Minuten. Bei Ungültigkeit des Access Tokens wird vom IDP ein neuer Zugriffstoken angefordert. Bei Ungültigkeit des SSO Token wird eine Neuauthentifizierung des Nutzers initiiert. Zugriffe auf IDP und E-Rezept-Server werden bei Ungültigkeit abgelehnt. Liegt ein gültiger Access Token vor, wird eine Verbindung mit dem Fachdienst aufgebaut, und es werden Rezepte, Nachrichten, Medikationsausgaben und Protokolleinträge an den Endpunkten des E-Rezept-Servers geladen und verschlüsselt auf dem Gerät gespeichert. Es erfolgt ein Hinweis an den Nutzer zu den Aktualisierungen und die neuen Daten werden in der App angezeigt.<br><br>Zur Verbesserung des Bedienkomforts bietet die App dem Nutzer nach erfolgreicher Authentifizierung die Option „Zugangsdaten speichern“ zum Speichern der Zugangsdaten der eGK an, sofern das Betriebssystem des Endgeräts des Nutzers über eine Vorrichtung verfügt, mit dem Daten auf dem Endgerät in einem speziellen Bereich sicher gespeichert werden können (Secure Module). Nachdem sich der Nutzer erfolgreich authentifiziert hat, erhält die App die Zugangsschlüssel für die Anmeldung am E-Rezept-Fachdienst. Wenn der Nutzer die Option „Zugangsdaten speichern“ nicht nutzt, muss er sich nach Ablauf seiner Zugangstoken erneut am E-Rezept-Fachdienst anmelden. |

| ID | Bezeichnung | Beschreibung Verarbeitungstätigkeit |
|---|---|---|
| **V04** | **Rezepte einlösen** | Für die Online-Einlösung von E-Rezepten muss der Nutzer zunächst eine Apotheke in der Apothekensuche auswählen. Nach Auswahl der Apotheke kann der Nutzer wählen, ob er seine Medikamente reservieren, von einem Boten liefern oder gesendet bekommen möchte. Wählt der Nutzer die Lieferung, entnimmt die App die Lieferadresse dem jeweiligen Rezept, wobei der Nutzer eine alternative Lieferadresse angeben kann. Wählt der Nutzer die Botendienstlieferung, wird eine Telefonnummer zur Ermöglichung der Kommunikation des Boten mit dem Nutzer abgefragt. Alternative Lieferadresse und Kontaktrufnummer werden verschlüsselt in der App gespeichert und im Rahmen der Bestellungen an die Apotheke bzw. an den Botendienst übermittelt. Schließt der Nutzer die Bestellung ab, erhalten die Rezepte zu den erstellten Medikamenten in der App den Status „in Bestellung“; die Bestelldaten werden verschlüsselt an den E-Rezept-Server übermittelt und dort in einer sicheren Umgebung weiterverarbeitet (Vertrauenswürdige Ausführungsumgebung – VAU). Gleichzeitig wird ein Hintergrundprozess ausgelöst, wodurch die App fortlaufend beim E-Rezept-Server nach neuen Mitteilungen und Statusänderungen in Bezug auf die Bestellung anfragt. Hat der Nutzer Rezepte eingelöst, die er zuvor vom Fachdienst bezogen hat, so werden die eingelösten Rezepte für fünf Minuten in der App mit dem Status „in Einlösung“ angezeigt, und die Synchronisation mit dem Fachdienst initiiert. Wird nicht innerhalb dieses Zeitraums durch die empfangende Apotheke eine Statusänderung über den Fachdienst bewirkt, wird der lokale Status „in Einlösung“ beendet, sodass der Nutzer das Rezept einer anderen Apotheke zuweisen könnte, bis eine Apotheke das Rezept bearbeitet hat. Rezepte, die nicht mehr einlösbar sind, wandern in die Ansicht „Archiv“.<br><br>Für die Einlösung von E-Rezepten in der Apotheke vor Ort muss der Nutzer diese zunächst per Scan importieren. Stimmt der Nutzer dem Zugriff auf die Kamera zu, analysieren die entsprechenden Funktionen der Betriebssysteme das Videobild in Echtzeit und suchen nach den abgedruckten 2D-Codes (DataMatrix Code – DMC) auf den Rezepten. Der Nutzer erhält über das Betriebssystem seines Smartphones Feedback über erkannte Rezepte und kann diese zur App hinzufügen, so dass sie lokal gespeichert werden. In der Apotheke vor Ort kann der Nutzer die in der App gespeicherten Rezepte anzeigen und von den Apothekenmitarbeitern einscannen lassen. Anschließend werden die Rezepte in der App in das „Archiv“ verschoben und der Nutzer wird darüber informiert. Bei jeder Anmeldung am E-Rezept-Fachdienst werden die eingescannten Rezepte durch die Daten des Fachdienstes überschrieben. Wenn dabei fremde Rezepte abgerufen werden, werden korrespondierende Profile automatisch angelegt. |
| **V05** | **Apothekensuche und -bestimmung** | Für die Einlösung von Rezepten oder losgelöst davon im Menüpunkt "Apotheken" kann der Nutzer mit einem Freitext-Eingabebereich für Name oder Adresse nach Apotheken suchen und Filterfunktionen verwenden. Die Anfrage wird an die Server für das Apothekenverzeichnis als Teil des Verzeichnisdienstes der TI (Apothekenverzeichnis) übermittelt und dort unter Berücksichtigung von Fehleingaben (Umlaute, Trennzeichen) ausgewertet. Stimmt der Nutzer der Standortfreigabe zu, fragt die App vom Betriebssystem eine Geoposition ab und übermittelt diese ebenfalls an das Apothekenverzeichnis als weiteren Suchparameter. Das Apothekenverzeichnis generiert als Suchergebnis eine Liste der Apotheken, welche die Kriterien erfüllen, die von der App abgerufen wird. |
| **V06** | **Mitteilungsfunktion** | Für die Abwicklung der Online-Einlösungen kann der Nutzer über eine Mitteilungsfunktion mit Apotheken kommunizieren. Im Menüpunkt „Mitteilungen“ wird ihm ein Eintrag in einer Bestelllliste angezeigt und er kann über das Bestellelement auf die entsprechenden Rezepte zugreifen. Die Bestellliste wird zusammengesetzt aus Kommunikationselementen, die vom Fachdienst abgerufen wurden. Das kann ein Freitext, ein Abholcode, eine Shopping-URL oder Kombinationen aus diesen sein. Kommunikationselemente mit gleichlautendem Inhalt, gleichem Bestellbezug und ähnlicher Sendezeit werden von der App automatisch zusammengefasst. Der Download von neuen Kommunikationselementen kann durch den Nutzer initiiert oder indirekt ausgelöst werden. Stehen neue Kommunikationselemente zur Verfügung, werden dem Nutzer Hinweise auf neue Elemente (Badges) angezeigt. Bei Auswahl des Navigationselements öffnet sich die Bestellübersicht und es wird über einen Badge angezeigt, welche Bestellung neue Informationen hat. Bei Auswahl der Bestellung wird der neue Eintrag in der Kommunikation angezeigt. |

| ID | Bezeichnung | Beschreibung Verarbeitungstätigkeit |
|---|---|---|
| **V07** | **E-Rezepte verwalten und teilen** | Die App gibt dem Nutzer die Möglichkeit, Einsicht in seine auf dem E-Rezept-Server gespeicherten Daten zu nehmen. Sofern der Nutzer am Fachdienst angemeldet ist, kann er sich alle Datenzugriffe für ein bestimmtes Profil anzeigen lassen. Wählt er im Profil „Zugriffstoken“, werden die von der App verwendeten SSO Token und Access Token angezeigt. In der Detailansicht eines Rezeptes werden die ausgegebenen Medikamente angezeigt. Ist der Nutzer nicht am E-Rezept-Server angemeldet, wird ihm eine Mitteilung angezeigt, dass die Daten möglicherweise nicht aktuell sind.<br><br>Die App gibt dem Nutzer die Möglichkeit, Rezepte über Funktionen des Betriebssystems an andere Personen weiterzureichen. Hierzu wählt der Nutzer im Menüpunkt „Rezepte“ ein Rezept und sodann den Teilen-Button. In dem sich öffnenden Betriebssystemdialog wählt er die E-Rezept-App oder eine beliebige andere Anwendung zum Teilen aus. Die App teilt eine URL als direkten Aufrufparameter zur E-Rezept App, inklusive Rezeptcode. Hat der versendende Nutzer die E-Rezept App zum Teilen ausgewählt, öffnet sich ein Eingabedialog zur Erfassung der Krankenversichertennummer (KVNR) des Empfängers. Die zuletzt genutzten KVNRs werden gespeichert und es können Namen dazu angegeben werden (Adressbuch). Im Anschluss an das Teilen erhält der Nutzer unter Mitteilungen einen Eintrag, dass das Rezept an die KVNR/an den Empfänger geschickt wurde. Dem empfangenden Nutzer wird in der vom sendenden Nutzer ausgewählten Anwendung angezeigt, dass er eine E-Rezept-App-URL empfangen hat. Wählt er diese aus, öffnet das Betriebssystem die verbundene URL (https://www.das-e-rezept-für-deutschland.de/share). Dort sind Steuerungsinformationen für Mobilgeräte hinterlegt, die durch mobile Browser ausgewertet werden, und dazu führen, dass eine App geöffnet wird. Ist die App installiert, so wird sie geöffnet und der Rezeptcode von ihr gespeichert. Die App zeigt das empfangene Rezept als gescanntes Rezept an. Hat der empfangende Nutzer die App nicht installiert, öffnet sich die jeweilige Vertriebsplattform für Anwendungssoftware. |
| **V08** | **Nutzungsanalyse** | Der Nutzer kann im Menü „Einstellungen“ mit einem Umschalter die Nutzungsanalyse aktivieren, die standardmäßig deaktiviert ist. Der Umschalter wird flankiert von einem Datenschutzhinweis, mit dem der Nutzer in knapper Form über die Zwecke der Nutzungsanalyse (Verbesserung des Nutzungserlebnisses, Fehleranalyse nach Abstürzen) informiert wird. Wenn der Nutzer den Umschalter aktiviert, erscheint ein weiterer, ausführlicherer Datenschutzhinweis inklusive Hinweis auf die jederzeitige Möglichkeit zur Deaktivierung der Nutzungsanalyse. Aktiviert der Nutzer die Nutzungsanalyse durch „Zustimmen“, schließt sich die Dialogbox. Wählt der Nutzer „Ablehnen“ oder schließt er die Dialogbox mit der Fenster-Schließen-Schaltfläche (Kreuz-Symbol), bleibt die Nutzungsanalyse deaktiviert. (nach Rückmeldung zu Contentsquare entsprechend zu ergänzen) |

# Angreifer

| Angreifer | Angreifer ID | Motivation | Know-How | Ressourcen |
|---|---|---|---|---|
| **Fahrlässiger Entwickler** | **A1-Beschäftige** | – Hält Vorschriften für eine sichere Entwicklung nur teilweise ein<br>– Mangelnde Kooperationsbereitschaft bei der Aufklärung von Fehlern | – Sehr viel Erfahrung mit digitalen Benutzeroberflächen (GUI)<br>– Sehr viel Wissen bezüglich IT<br>– Sehr viel Wissen über die IT-Infrastruktur der gematik<br>– Auf die Entwicklung von Software spezialisiert<br>– Verantwortlich für die sichere Entwicklung von Software | – Zugang zur internen Infrastruktur<br>– Eingeschränktes finanzielles Budget<br>– Eingeschränktes zeitliches Budget |
| **Böswilliger Entwickler** | **A1-Beschäftige** | – Versucht, sichere Entwicklung aktiv zu untergraben<br>– Möchte die App durch sein internes Wissen ausnutzen und sich einen persönlichen Vorteil verschaffen<br>– Versucht, Fehler zu vertuschen<br>– Nimmt Kündigung für sein Handeln in Kauf | – Sehr viel Erfahrung mit digitalen Benutzeroberflächen (GUI)<br>– Sehr viel Wissen bezüglich IT<br>– Sehr viel Wissen über die IT-Infrastruktur der gematik<br>– Auf die Entwicklung von Software spezialisiert<br>– Verantwortlich für die sichere Entwicklung von Software | – Zugang zur internen Infrastruktur<br>– Eingeschränktes finanzielles Budget<br>– Eingeschränktes zeitliches Budget |
| **Fahrlässiger Administrator** | **A1-Beschäftige** | – Möchte Aufwand für die Administration minimieren<br>– Mangelnde Kooperationsbereitschaft bei der Aufklärung von Fehlern | – Sehr viel Erfahrung mit digitalen Benutzeroberflächen (GUI)<br>– Sehr viel Wissen bezüglich IT<br>– Sehr viel Wissen über die IT-Infrastruktur der gematik<br>– Auf die Verwaltung von IT spezialisiert<br>– Verfügt über erweiterte administrative Privilegien<br>– Verantwortlich für die sichere Verwaltung und Konfiguration von IT | – Zugang zur internen Infrastruktur<br>– Eingeschränktes finanzielles Budget<br>– Eingeschränktes zeitliches Budget |

| Angreifer | Angreifer ID | Motivation | Know-How | Ressourcen |
|---|---|---|---|---|
| **Böswilliger Administrator** | **A1-Beschäftige** | – Versucht, sichere Konfiguration aktiv zu untergraben<br>– Möchte die App durch sein internes Wissen ausnutzen und sich einen persönlichen Vorteil verschaffen<br>– Versucht, Fehler zu vertuschen<br>– Nimmt Kündigung für sein Handeln in Kauf | – Sehr viel Erfahrung mit digitalen Benutzeroberflächen (GUI)<br>– Sehr viel Wissen bezüglich IT<br>– Sehr viel Wissen über die IT-Infrastruktur der gematik<br>– Auf die Verwaltung von IT spezialisiert<br>– Verfügt über erweiterte administrative Privilegien<br>– Verantwortlich für die sichere Verwaltung und Konfiguration von IT | – Zugang zur internen Infrastruktur<br>– Eingeschränktes finanzielles Budget<br>– Eingeschränktes zeitliches Budget |
| **Technisch unerfahrener Nutzer** | **A2-Nutzer** | – Beabsichtigt die bestimmungsgemäße Nutzung der App<br>– Möchte Rezepte über die App einlösen<br>– Wenig Interesse, den Umgang mit IT zu lernen | – Mangelhafte Erfahrung mit digitalen Benutzeroberflächen (GUI)<br>– Mangelhaftes Wissen bezüglich IT<br>– Kein Wissen über die IT-Infrastruktur der gematik | – Kein Zugang zur internen Infrastruktur<br>– Eingeschränktes finanzielles Budget<br>– Eingeschränktes zeitliches Budget |
| **Fahrlässiger Nutzer** | **A2-Nutzer** | – Frustriert über die Handhabung der App<br>– Wenig Interesse an der Nutzung der App<br>– Mangelnde Kooperationsbereitschaft | – Durchschnittliche Erfahrung mit digitalen Benutzeroberflächen (GUI)<br>– Durchschnittliches Wissen bezüglich IT<br>– Mangelhaftes Wissen über die IT-Infrastruktur der gematik | – Kein Zugang zur internen Infrastruktur<br>– Eingeschränktes finanzielles Budget<br>– Eingeschränktes zeitliches Budget |
| **Betrüger** | **A3-Hacker** | – Möchte die App ausnutzen und sich einen persönlichen Vorteil verschaffen<br>– Nimmt Schädigung von Dritten willentlich in Kauf<br>– Handelt aus Profitgier | – Viel Erfahrung mit digitalen Benutzeroberflächen (GUI)<br>– Versucht das GUI zu seinen Gunsten auszunutzen, auszuhebeln<br>– Durchschnittliches Wissen bezüglich IT<br>– Mangelhaftes Wissen über die IT-Infrastruktur der gematik | – Initial kein Zugang zur internen Infrastruktur<br>– Eingeschränktes finanzielles Budget<br>– Hohes zeitliches Budget |

| Angreifer | Angreifer ID | Motivation | Know-How | Ressourcen |
|---|---|---|---|---|
| **Hacktivist** | **A3-Hacker** | – Beabsichtigt keine bestimmungsmäßige Nutzung der App<br>– Sucht Herausforderung und Anerkennung<br>– Unbefugter Zugriff auf interne Ressourcen<br>– Schädigung von Dritten nicht beabsichtigt | – Sehr viel Erfahrung mit digitalen Benutzeroberflächen (GUI)<br>– Auf das Hacken von IT-Systemen spezialisiert<br>– Viel Wissen bezüglich IT<br>– Initial mangelhaftes Wissen über die IT-Infrastruktur der gematik | – Initial kein Zugang zur internen Infrastruktur<br>– Eingeschränktes finanzielles Budget<br>– Hohes zeitliches Budget |
| **Cracker** | **A3-Hacker** | – Möchte die App ausnutzen und sich einen persönlichen Vorteil verschaffen<br>– Handelt aus Profitgier oder Zerstörungslust<br>– Unbefugter Zugriff auf interne Ressourcen<br>– Nimmt Schädigung von Dritten willentlich in Kauf oder beabsichtigt diese | – Sehr viel Erfahrung mit digitalen Benutzeroberflächen (GUI)<br>– Auf das Hacken von IT-Systemen spezialisiert und ist in der Lage Malware zu schreiben, bzw. anzupassen<br>– Sehr viel Wissen bezüglich IT<br>– Initial mangelhaftes Wissen über die IT-Infrastruktur der gematik | – Initial kein Zugang zur internen Infrastruktur<br>– Eingeschränktes finanzielles Budget<br>– Hohes zeitliches Budget |
| **Betreiber Betriebssysteme** | **A4-Service Provider** | – Verfolgen kommerzielle Interessen<br>– Wägen wirtschaftlichen Erfolg gegen Datenschutz ab<br>– Weitergabe von Daten an andere Drittparteien | – Sehr viel Erfahrung mit digitalen Benutzeroberflächen (GUI)<br>– Sehr viel Wissen bezüglich IT<br>– Mangelhaftes Wissen über die IT-Infrastruktur der gematik | – Stellt technische Infrastruktur bereit<br>– Verfügt über Wartungszugänge zur Infrastruktur<br>– Hohes finanzielles Budget<br>– Hohes zeitliches Budget |
| **Betreiber Nutzungsanalyse** | **A4-Service Provider** | – Verfolgen kommerzielle Interessen<br>– Wägen wirtschaftlichen Erfolg gegen Datenschutz ab<br>– Weitergabe von Daten an andere Drittparteien | – Sehr viel Erfahrung mit digitalen Benutzeroberflächen (GUI)<br>– Sehr viel Wissen bezüglich IT<br>– Mangelhaftes Wissen über die IT-Infrastruktur der gematik | – Stellt technische Infrastruktur bereit<br>– Verfügt über Wartungszugänge zur Infrastruktur<br>– Hohes finanzielles Budget<br>– Hohes zeitliches Budget |
| **Staatliche Behörden** | **A5-Behörden** | – Politische Intervention<br>– Verbrechensbekämpfung<br>– Aufklärung und Abwehr von Bedrohungen (auf staatlicher Ebene) | – Sehr viel Erfahrung mit digitalen Benutzeroberflächen (GUI)<br>– Sehr viel Wissen bezüglich IT<br>– Sehr viel Wissen über die IT-Infrastruktur der gematik | – Gesetzliche Aufklärungsbefugnisse<br>– Hohes finanzielles Budget<br>– Hohes zeitliches Budget |

# Etablierte Technische und Organisatorische Maßnahmen

| Maßnahmen ID | Bedrohung | Schwerpunkt Gewährleistungsziel | Beschreibung der Maßnahmen |
|---|---|---|---|
| M-01 | B01-App Spoofing | Vertraulichkeit, Integrität, Nichtverkettung, Transparenz | Die E-Rezept-App ist auf den Vertriebsplattformen eindeutig als gematik-App identifizierbar. Die Versicherten werden von verschiedener Seite und über mehrere Kanäle (z. B. die Webseite der gematik, Ausdruck des Rezept-Codes) darüber informiert, wie sie die E-Rezept-App auf den Vertriebsplattformen identifizieren können. Durch ein gemeinsames Geheimnis (API-Key) zwischen E-Rezept-App und E-Rezept-Fachdienst ist sichergestellt, dass nur die E-Rezept-App auf den E-Rezept-Fachdienst zugreifen kann. Andere Apps können daher nur (in ihrer 2D-Repräsentation) abfotografierte Rezept-Codes verarbeiten, aber nicht auf E-Rezepte zugreifen. Es bestehen vertragliche Vereinbarungen mit den Betriebssystembetreibern über die Nutzung der Vertriebsplattformen; diese Vereinbarungen umfassen jedenfalls teilweise die Prüfung der auf den Vertriebsplattformen angebotenen Apps. |
| M-02 | B02-Veraltete Version | Verfügbarkeit | Die gematik stellt die jeweils aktuelle Version der E-Rezept-App auf den Vertriebsplattformen zur Verfügung und kommuniziert dies über die ihr zur Verfügung stehenden Kanäle (z. B. die Webseite der gematik). Die gematik schließt nicht aktuelle Versionen von der Nutzung des E-Rezept-Fachdienstes aus, z. B. wenn diese Versionen Schwachstellen enthalten oder funktional nicht mehr interoperabel mit dem E-Rezept-Fachdienst sind. Nutzer, die E-Rezepte online einlösen wollen, sind gezwungen, die aktuelle App upzudaten. |
| M-03 | B03-Abhängigkeit von Betriebssystembetreibern | Verfügbarkeit | Es bestehen vertragliche Vereinbarungen mit den Betriebssystembetreibern über die Nutzung der Vertriebsplattformen; diese Vereinbarungen umfassen jedenfalls teilweise die Verfügbarkeit der E-Rezept-App auf den Vertriebsplattformen. Sollte die E-Rezept-App mangels Unterstützung durch Vertriebsplattformen und/oder Betriebssysteme vollständig ausfallen, wäre eine Zuweisung oder Einlösung von E-Rezepten über die App nicht möglich; die Daten auf dem E-Rezept-Server wären noch über die E-Rezept-App für stationäre Geräte (E-Rezept-AdV) einsehbar. |
| M-04 | B04-Mangelhafter Passwortschutz (Biometrie, Passwort) | Vertraulichkeit | Die E-Rezept-App setzt bei der Einrichtung einer Authentifizierung eine Mindeststärke des Passworts voraus. Das vom Nutzer gewählte Passwort wird hierfür mit einer etablierten, ausschließlich lokal verwendeten Softwarebibliothek (lib.zxcvbn) abgeglichen. Das Passwort wird von der E-Rezept-App erst ab "mittlerer" Stärke zugelassen. |
| M-05 | B05-Anwendungsfehler bei der App-Initiierung und beim Einlösen von Rezepten | Verfügbarkeit | Bei der Ausgestaltung der E-Rezept-App wurde entsprechend der Spezifikationen auf eine leichte Bedienbarkeit geachtet, etwa im Onboarding-Prozess. Durch die Berücksichtigung von Nutzer-Feedback über eine eingerichtete Hotline wird die Bedienbarkeit der App ständig verbessert. |

| Maßnahmen ID | Bedrohung | Schwerpunkt Gewährleistungsziel | Beschreibung der Maßnahmen |
|---|---|---|---|
| M-06 | B06-Unsichere Ausführungsumgebung (Jailbreak, Root) | Vertraulichkeit, Verfügbarkeit, Integrität, Transparent, Intervenierbarkeit, Zweckbindung | Bei jedem Start der E-Rezept-App wird überprüft, ob das Gerät mit privilegierten Berechtigungen (Root/Jailbreak) ausgestattet ist. In diesem Fall wird ein Warnhinweis angezeigt, dass das Gerät aus Sicherheitsgründen nicht verwendet werden sollte. |
| M-07 | B07-Nichtverfügbarkeit von IDP- und E-Rezept-Server | Verfügbarkeit | Für den IDP-Dienst und den E-Rezept-Fachdienst fordert die gematik von den Betreibern die höchste in der TI mögliche Verfügbarkeit. Durch georedundante Ausführungen der Dienste ist die Eintrittswahrscheinlichkeit eines Ausfalls aufgrund von Elementarereignissen stark zu reduzieren. Jeder Standort ist über eine mindestens zweifach redundante Anbindung an das Internet anzuschließen. Die Anbieter müssen zudem eine Backup-Strategie entwickeln und umsetzen, die bei einem totalen Ausfall des Dienstes einen Datenverlust minimiert. Ein Ausfall aufgrund von Versuchen, die Dienste zu überlasten, ist durch die Anbieter der Dienste mit Abwehrmethoden nach dem Stand der Technik zu verhindern. Neben den Anbietern der Dienste selbst, überwacht die gematik die Verfügbarkeit der Dienste und Einhaltung der Service Level Agreements und ergreift falls notwendig Maßnahmen, um die Verfügbarkeit wiederherzustellen. Kommt es zu einem Ausfall von IDP- und/oder E-Rezept-Server, wäre die Einlösung von E-Rezepten über den Ausdruck des Rezept-Codes möglich. |
| M-08 | B08-Unbefugter Zugriff auf SSO-/Access-Token | Vertraulichkeit | Der unbefugte Zugriff auf das Token ist nur möglich, wenn physischer Zugriff auf das Gerät möglich ist. Der Nutzer kann eigenverantwortlich darauf achten, wer physischen Zugriff auf sein Gerät erhält. |
| M-09 | B09-Verwendung schwacher Verschlüsselung | Vertraulichkeit | Die kryptographischen Verfahren, die in der Telematikinfrastruktur zum Einsatz kommen dürfen, werden vom BSI vorgegeben (z. B. TR 03116-1). Die gematik nimmt in diesem Rahmen weitere Einschränkungen vor (gemSpec_Krypt). Damit ist gewährleistet, dass die kryptographischen Verfahren bei Bedarf aktualisiert werden und stets dem Stand der Technik entsprechen. Die gematik verfügt über ein Krypto-Notfallkonzept für Fälle, in denen eine Verschlüsselung unerwartet und kurzfristig unsicher wird. |
| M-10 | B10-Fehlschlagen der Authentifizierung | Verfügbarkeit | Die App unterstützt den Nutzer durch eine gerätespezifische Anzeige, wo die Karte an das Smartphone zu halten ist. Dies stellt eine erhebliche Erleichterung in der App-Nutzung dar und befähigt auch ungeübte Nutzer zur richtigen Positionierung der eGK am Smartphone. |
| M-11 | B11-Unrechtmäßige Datenverarbeitung durch Kamerazugriff (ML-Kit) | Vertraulichkeit, Transparent, Datenminimierung, Intervenierbarkeit, Zweckbindung | Die gematik hat mit den Betreibern der Betriebssysteme der Nutzerendgeräte vertragliche Vereinbarungen, durch die die Betriebssystembetreiber verpflichtet sind, die Einhaltung der Gewährleistungsziele sicherzustellen. |
| M-12 | B12-Offenlegung von Rezeptinformationen und Mitteilungen | Vertraulichkeit | Die Anzeige von Daten in der App ist so optimiert, dass funktionsspezifisch Daten angezeigt werden können. So kann bspw. ein in der Nähe stehender Beobachter (etwa in der Warteschlange in der Apotheke) keine Daten aus dem E-Rezept auslesen, wenn nur der Rezeptcode angezeigt wird, der für das Auslesen durch den Apotheker bestimmt. Welche Daten auf dem Smartphone-Bildschirm angezeigt werden, bestimmt der Nutzer letztlich allerdings selbst. Im Sinne eines bewussten Umgangs mit den eigenen Daten kann der Nutzer selbst Maßnahmen ergreifen, um unbeabsichtigten Offenlegungen vorzubeugen und entsprechend darauf achten, welche Daten er sich wann anzeigen lässt. |

| Maßnahmen ID | Bedrohung | Schwerpunkt Gewährleistungsziel | Beschreibung der Maßnahmen |
|---|---|---|---|
| M-13 | B13-Verlust des Smartphones | Verfügbarkeit, Vertraulichkeit | Mit der E-Rezept-App auf einem neuen/anderen Smartphone kann der Nutzer seine E-Rezepte weiterhin abrufen und verwenden.<br>Die App erzwingt die Verwendung einer Authentisierungsmethode (z. B. Passwort, biometrisches Merkmal). Dadurch kann ein fremder Benutzer nicht unmittelbar auf die Daten in der App zugreifen.<br>Durch die Aufhebung der Geräteregistrierung kann der Nutzer sicherstellen, dass Unbefugte keine Möglichkeit haben, mit dem Gerät auf den E-Rezept-Fachdienst zuzugreifen. |
| M-14 | B14-Unberechtigte Datenverarbeitung durch Standortzugriff | Intervenierbarkeit, Nichtverkettung | Die App versendet Standortdaten an das Apothekenverzeichnis. Diese Daten werden zweckgebunden für die Apothekensuche verarbeitet.<br>Der Betreiber des Apothekenverzeichnisses wurde von der gematik beauftragt den Dienst gemäß den Spezifikationen der gematik anzubieten und die Einhaltung der Gewährleistungsziele sicherzustellen. Zudem führt die gematik Audits durch, um die Einhaltung der vertraglichen Vereinbarungen zu überprüfen. |
| M-15 | B15-Push Notifications | Vertraulichkeit, Nichtverkettung | Die Nutzdaten der Mitteilungen werden verschlüsselt übertragen.<br>Durch den Versand von Leer-Mitteilungen wird ein Grundrauschen erzeugt, so dass ein Betreiber einer Software, mit der Push Notifications versendet werden, ein Nutzungsverhalten von Nutzern daraus nicht ableiten kann. |
| M-16 | B16-Unabsichtliches Löschen von Mitteilungen | Verfügbarkeit | Einzelne Mitteilungen von Apotheken an Nutzer können nicht gelöscht werden, da Mitteilungen immer fest mit einem E-Rezept verknüpft sind. Nur wenn ein E-Rezept (vom Nutzer oder automatisch) gelöscht wird, werden auch alle damit verbundenen Mitteilungen gelöscht. Mitteilungen vom Nutzer an eine Apotheke können vom Nutzer gelöscht werden; dabei erfolgt eine Bestätigungsnachfrage, ob die Mitteilung wirklich gelöscht werden soll. |
| M-17 | B17-Teilen über unsichere Anwendungen | Vertraulichkeit | Beim Aufruf des Betriebssystemdialogs „Teilen“ wird dem Nutzer ein Hinweis angezeigt, dass ggf. einige der auswählbaren Apps kein angemessenes Schutzniveau für die Übermittlung von Rezeptinformationen bieten. |
| M-18 | B20-Modifikation der Analyseeinstellungen | Datenminimierung, Nichtverkettung | Die Administration der Analyseeinstellungen bei der gematik erfolgt nach dem Vier-Augen-Prinzip. Hierdurch ist der Handlungsspielraum von Einzelpersonen stark limitiert. |
| M-19 | B21-Fehlerhafte Einwilligungs-/ Widerrufsmöglichkeit | Transparenz | Die Nutzungsanalyse ist nach dem Opt-in-Prinzip ausgestaltet. Das bedeutet, dass der Toggle standardmäßig ‚Aus‘ gestellt ist. Es werden kontextspezifische transparente Datenschutzhinweise angezeigt. |
| M-20 | B22-Drittstaatentransfer | Nichtverkettung | Mögliche Drittstaatentransfers sind durch den Abschluss von Standardvertragsklauseln abgesichert. Darüber hinaus findet zum frühestmöglichen Zeitpunkt eine Anonymisierung der Daten statt (ab Eingang der Daten im Network Relay). |

# Risikoanalyse

| Bedrohung ID | Verarbeitungstätigkeit ID | Angreifer ID | Bedrohung | Detaillierte Beschreibung | Etablierte Maßnahmen | Betroffene Personen | Schadensausmaß für betroffene Personen je Gewährleistungsziel: Eintrittswahrscheinlichkeit | Verfügbarkeit | Integrität | Vertraulichkeit | Daten-minimierung | Intervenier-barkeit | Transparenz | Zweckbindung / Nichtverkettung | Risikokategorie | Geplante Maßnahmen | Restrisiko (Risikokategorie) | Erforderlichkeit Konsultation Aufsichtsbehörde (JA/NEIN) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B01 | V01 | A3, A4, A5 | Gefälschte App (App Spoofing) | Cracker oder staatliche Behörden könnten eine betrügerische App im Design der E-Rezept-App entwickeln; aufgrund staatlichen Einflusses auf Betriebssystembetreiber ODER aufgrund mangelnder Design- und Architekturprüfung durch Betriebssystembetreiber könnte die betrügerische App auf der Vertriebsplattform ODER auf einer Webseite zum Download angeboten und vom Versicherten heruntergeladen und installiert werden; hierdurch entstünde das Risiko, dass Angreifer mittels der betrügerischen App Daten unrechtmäßig erheben und verarbeiten. | M-01 | Nutzer | 3 | 1 | 3 | 3 | 3 | 3 | 3 | 3 | 9 | | 9 | NEIN |
| B02 | V01 | A2 | Veraltete Version der App | Versicherte könnten sich eine nicht aktuelle Version der App von einer inoffiziellen Quelle herunterladen und installieren ODER Versicherte könnten es unterlassen, empfohlene Updates zu installieren; hierdurch entstünde das Risiko, dass nicht aktuelle Versionen der E-Rezept-App Daten nicht ordnungsgemäß verarbeiten und Daten bspw. nicht verfügbar sind. | M-02 | Nutzer | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 8 | | 8 | NEIN |
| B03 | V01 | A4, A5 | Abhängigkeit von Betriebssystembetreibern | Für die Installation und den Betrieb der E-Rezept-App auf Smartphones muss die technische Infrastruktur von Betriebssystembetreibern in Nicht-EU-Staaten genutzt werden, wodurch ein Abhängigkeitsverhältnis entsteht; hierdurch entsteht das Risiko, dass z. B. die Verfügbarkeit von Daten in der E-Rezept-App beeinträchtigt werden könnte, bspw. im Falle negativer politischer Entwicklungen. | M-03 | Nutzer | 1 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | | 3 | NEIN |
| B04 | V02 | A2 | Mangelhafter Passwortschutz (Biometrie, Passwort) | Bei der Einrichtung einer Authentifizierung können auch Passwörter vergeben werden, die nicht in jedem Fall einen ausreichenden Schutz bieten; hierdurch entsteht das Risiko eines unberechtigten Zugriffs durch Unbefugte auf die Daten in der App der Versicherten. | M-04 | Nutzer | 2 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 8 | | 8 | NEIN |
| B05 | V02-V04 | A2 | Anwendungsfehler bei der App-Initiierung und beim Einlösen von Rezepten | Aufgrund des mehrstufigen Verfahrens der Einrichtung der App, der Anmeldung am Fachdienst und des Einlösens von Rezepten könnte ein technisch unerfahrener Nutzer nicht in der Lage sein, diese Funktionen korrekt auszuführen; hierdurch entstünde das Risiko, dass Daten nicht verfügbar wären. | M-05 | Nutzer | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 8 | | 8 | NEIN |
| B06 | V02 | A2 | Unsichere Ausführungsumgebung (Jailbreak, Root) | Ein Nutzer könnte die E-Rezept-App unwissentlich auf einem Smartphone mit Jailbreak-, Root-Status ausführen; hierdurch könnte das Risiko entstehen, dass Sicherheitsfunktionen der App nicht ordnungsgemäß funktionieren. | M-06 | Nutzer | 2 | 3 | 0 | 3 | 0 | 0 | 0 | 0 | 6 | | 6 | NEIN |
| B07 | V03 | A3 | Nichtverfügbarkeit von IDP- und E-Rezept-Server | Das ordnungsgemäße Ausführen der Funktionen der E-Rezept-App baut auf dem Funktionieren des IDP- und des E-Rezept-Servers auf; hierdurch entsteht das Risiko, dass Daten aufgrund von Nichtverfügbarkeit von IDP- und E-Rezept-Server in der E-Rezept-App nicht verfügbar sein könnten, bspw. bei Hackerangriffen auf IDP- und E-Rezept-Server. | M-07 | Nutzer | 2 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 6 | | 6 | NEIN |
| B08 | V03 | A3 | Unbefugter Zugriff auf SSO-/Access-Token | Im Zuge der Anmeldung am IDP/Fachdienst werden SSO-/Access-Token an die App übermittelt und auf dem Smartphone der Versicherten gespeichert; dabei liegen die Daten im Arbeitsspeicher unverschlüsselt vor; hierdurch entsteht unter Berücksichtigung der gewählten Absicherung der E-Rezept-App das Risiko des unbefugten Zugriffs auf die Token durch einen Hacker. | M-08 | Nutzer | 1 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 4 | | 4 | NEIN |
| B09 | V03 | A1, A3 | Verwendung schwacher Verschlüsselung | Bei der Kommunikation zwischen verschiedenen Endpunkten (eGK, IDP-Server, E-Rezept-Server) und der E-Rezept-App könnte eine schwache Verschlüsselung eingesetzt werden, bspw. wenn die Verschlüsselungsmethode veraltet ist; hierdurch entstünde das Risiko, dass die übermittelten Informationen abgefangen und offengelegt werden. | M-09 | Nutzer | 1 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 4 | | 4 | NEIN |
| B10 | V03 | A2 | Fehlschlagen der Authentifizierung | Die Authentifizierung gegenüber dem IDP/Fachdienst könnte fehlschlagen, bspw. weil sich die eGK nicht per NFC scannen lässt (Antennen befinden sich an unterschiedlichen Stellen an den Geräten); hierdurch entstünde das Risiko, dass Daten nicht verfügbar sind. | M-10 | Nutzer | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 8 | | 8 | NEIN |

| Bedrohung ID | Verarbeitungstätigkeit ID | Angreifer ID | Bedrohung | Detaillierte Beschreibung | Etablierte Maßnahmen | Betroffene Personen | Schadensausmaß für betroffene Personen je Gewährleistungsziel | | | | | | | | | Geplante Maßnahmen | Restrisiko (Risikokategorie) | Erforderlichkeit Konsultation Aufsichtsbehörde (JA/NEIN) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Eintrittswahr-scheinlichkeit | Verfügbarkeit | Integrität | Vertraulichkeit | Daten-minimierung | Intervenier-barkeit | Transparenz | Zweckbindung / Nichtverkettung | Risikokategorie | | | |
| B11 | V04 | A1, A4 | Unrechtmäßige Daten-verarbeitung durch Kamerazugriff (ML-Kit) | Die Software, mit der die Rezept-Token per Kamera gescannt und Daten zum Zwecke des Hinzufügens von Rezepten verarbeitet werden, steht unter der Kontrolle der Betriebssystembetreiber; hierdurch besteht daher das Risiko, dass die Daten unrechtmäßig (zweckwidrig, intransparent, ohne Rechtsgrundlage) verarbeitet werden; dies gilt insbesondere für Googles „ML-Kit“. | M-11 | Nutzer | 4 | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 8 | | 8 | NEIN |
| B12 | V04-V05 | A2, A3 | Offenlegung von Gesundheitsdaten (Rezeptinformationen, Mitteilungen) | Beim Einlösen von Rezepten in der Apotheke ist das gescannte Rezept in der E-Rezept-App zu präsentieren; hierdurch besteht das Risiko, dass Rezeptinformationen oder Mitteilungen unbeabsichtigt gegenüber Unbefugten am gleichen Aufenthaltsort offengelegt werden, bspw. durch sog. Shouldersurfing oder in dem Fall, dass ein technisch unerfahrener Nutzer weitere Personen um Hilfe bei der Handhabung der E-Rezept-App ersucht. Während des Betriebs der App kann die Screenshot-Betriebssystemfunktion ausgelöst werden; hierdurch besteht das Risiko, dass Daten kopiert werden und Unbefugten gegenüber offengelegt werden. | M-12 | Nutzer | 4 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 12 | Einfügen eines kontextspezifischen Warnhinweises vor Einlösung Rezept. | 9 | NEIN |
| B13 | V04 | A3 | Verlust des Smartphones | Das Smartphone des Nutzers könnte durch Diebstahl oder auf andere Weise in die Verfügungsgewalt Unbefugter gelangen; hierdurch entstünde das Risiko, dass Daten gegenüber Unbefugten offengelegt und missbraucht werden. | M-13 | Nutzer | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 8 | | 8 | NEIN |
| B14 | V05 | A4 | Unrechtmäßige Datenverarbeitung durch Standortzugriff | Die Software, mit der die Standortdaten verarbeitet werden, steht unter der Kontrolle der Betriebssystembetreiber; durch die Übermittlung von Standortdaten könnte ein Profiling von Nutzern durchgeführt werden. Hierdurch besteht das Risiko, dass die Daten unrechtmäßig (zweckwidrig, intransparent, ohne Rechtsgrundlage) verarbeitet werden. | M-14 | Nutzer | 4 | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 8 | | 8 | NEIN |
| B15 | V06 | A4 | Unrechtmäßige Datenverarbeitung durch Push Notifications (Firebase Cloud Messaging) | Die Software, mit der die Push Notifications im Rahmen der Mitteilungsfunktion versendet werden, steht unter der Kontrolle der Betriebssystembetreiber; hierdurch besteht daher das Risiko, dass die Daten zweckwidrig, intransparent, ohne Rechtsgrundlage verarbeitet werden; dies gilt insbesondere für Googles „Firebase Cloud Messaging“ | M-15 | Nutzer | 4 | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 8 | | 8 | NEIN |
| B16 | V06 | A2 | Unabsichtliches Löschen von Mitteilungen | Durch Unachtsamkeit könnten Nutzer Mitteilungen der Apotheken an sie über eingelöste E-Rezepte unabsichtlich löschen; hierdurch entstünde das Risiko, dass Daten nicht verfügbar wären. | M-16 | Nutzer | 1 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | | 3 | NEIN |
| B17 | V07 | A2, A3 | Teilen über unsichere Anwendungen | E-Rezepte könnten über die Teilen-Funktion des Betriebssystems über unsichere, bspw. nicht verschlüsselte Anwendungen weitergegeben werden; hierdurch entstünde das Risiko, dass Daten gegenüber Unbefugten offengelegt würden. | M-17 | Nutzer | 2 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 8 | | 8 | NEIN |
| B18 | V08 | A1 | Zweckwidrige Datenverarbeitung nach Modifikation der Analyseeinstellungen (Usability Tracking) | Ein Beschäftigter führt zweckwidrige Modifikationen in den administrativen Einstellungen der Nutzungsanalyse durch. Hierdurch entstünde das Risiko, dass Daten zweckwidrig und unrechtmäßig verarbeitet werden. | M-18 | Nutzer | 1 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 3 | | 3 | NEIN |
| B19 | V08 | A1, A2 | Fehlerhafte oder intransparente Implementierung der Einwilligungs-/Widerrufsmöglichkeit | Die Einwilligungs-/Widerrufsmöglichkeiten bezüglich der Nutzungsanalyse könnten fehlerhaft oder intransparent implementiert und für den Versicherten nur bedingt nachzuvollziehbar sein; hierdurch entstünde das Risiko dass eine abgegebene Einwilligung unwirksam wäre und die Daten unrechtmäßig verarbeitet würden. | M-19 | Nutzer | 1 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | | 2 | NEIN |
| B20 | V08 | A4, A5 | Unrechtmäßige Verarbeitung von Daten durch Drittstaatentransfer | Daten könnten in Drittstaaten ohne vergleichbares Schutzniveau übermittelt werden. Hierdurch entstünde das Risiko, dass personenbezogene Daten gegenüber Unbefugten offengelegt und unrechtmäßig verarbeitet würden. | M-20 | Nutzer | 1 | 0 | 0 | 2 | 0 | 2 | 2 | 3 | 3 | | 3 | NEIN |

# Bewertung

| Bedrohung ID | Bedrohung | Eintrittswahrscheinlichkeit | Schaden | Risiko |
|---|---|---|---|---|
| **B01** | Gefälschte App (App Spoofing) | – (3) Erwartung, dass mindestens einmal im Jahr eine gefälschte App auftaucht. | – Integrität, Vertraulichkeit, Datenminimierung, Intervenierbarkeit, Transparenz, Zweckbindung/Nicht. (3): Annahme, das beträchtliche Schäden für Versicherte entstehen können für Großteil der Schutzziele. | 9 |
| **B02** | Veraltete Version der App | – (4) Erwartung, dass ein Anteil der der Nutzer die App über eine inoffizielle Quelle bezieht. | – Verfügbarkeit (2): Annahme, dass Probleme nur temporär und behebbar. | 8 |
| **B03** | Abhängigkeit von Betriebssystembetreibern | – (1) Erwartungshaltung, dass es Eintritt ist minimal. | – Verfügbarkeit (4): Wenn es Eintritt wäre der Schaden enorm,<br>– Es gibt keinen Ersatz. | 3 |
| **B04** | Mangelhafter Passwortschutz (Biometrie, Passwort) | – (2) Aufgrund eines mittleren PW-Schutzes, Zugriff auf die App durchaus möglich, bspw. durch trial and error. | – Vertraulichkeit (4): potenzieller Vollzugriff durch den Angreifer | 8 |
| **B05** | Anwendungsfehler bei der App-Initiierung und beim Einlösen von Rezepten | – (4) Aufgrund eines mehrstufigen Verfahrens zum Anmelden stellt regelmäßig eine große Herausforderung für unerfahrene Nutzer dar. | – Betroffen ist die Verfügbarkeit (2), aber Folgen haten sich in Grenzen und sollten nur temporär Natur sein und keine Folgen haben. | 8 |
| **B06** | Unsichere Ausführungsumgebung (Jailbreak, Root) | – (2) Vergeben den niedrigsten Wert, in Kombination mit Maßnahmen unwahrscheinlich, dass ein Nutzer unwissentlich ein Smartphone mit Jailbreak verwendet. | – Verfügbarkeit (3): Fehlende Sicherheitsfkt könnten dazu führen, dass der Apothekendienst nicht erreicht wird.<br>– Aufgrund fehlender Sicherheitsfkt, könnte potenziell ein Vertraulichkeitsproblem (3) entstehen. | 6 |
| **B07** | Nichtverfügbarkeit von IDP- und E-Rezept-Server | – (2) wir gehen davon aus, dass der Dienst aufgrund des aktuell frühen Implementierung Status einmal Jährlich temporär ausfällt. | – Verfügbarkeit (3): Die fehlende Verfügbarkeit kann teilweise schwere Folgen nach sich ziehen. | 6 |
| **B08** | Unbefugter Zugriff auf SSO-/ Access-Token | – (1) Damit sich diese Bedrohung realisiert, ist ein physischer Zugriff auf das Gerät ist notwendig. Niedrigster Wert vergeben. | – Vertraulichkeit (4): Wenn der Zugriff erfolgreich ist, dann hat der Angreifer wiederum zugriff auf alle hinterlegten Daten. | 4 |
| **B09** | Verwendung schwacher Verschlüsselung | – (1) Wir gehen davon aus, dass mindestens einmal in 10 Jahren ein Schwachpunkt in einer Verschlüsselung gefunden. | – Vertraulichkeit (4): Aufgrund von potenziellen technischen Limitation kann dies schwerwiegende Folgen für die Vertraulichkeit haben. | 4 |

| Bedrohung ID | Bedrohung | Eintrittswahrscheinlichkeit | Schaden | Risiko |
|---|---|---|---|---|
| **B10** | Fehlschlagen der Authentifizierung | – (4) Aufgrund der unterschiedlich verbauten NFC Chips in Smartphones gehen wir von regelmäßigen Problemen beim scannen der eGK aus. | – Verfügbarkeit (2): Die Herausforderung zum scannen der Karte kann zu einer Verzögerung der Verfügbarkeit führen, sollte allerdings keine gravierenden oder dauerhaften Schäden nach sich ziehen. | 8 |
| **B11** | Unrechtmäßige Datenverarbeitung durch Kamerazugriff (ML-Kit) | – (4) Es besteht eine starke Abhängigkeit von Betriebssystembetreibern,<br>– Außerdem bereits vorgekommen, dass die Betreiber unrechtmäßig Daten verarbeitet haben,<br>– Aktuell kämpft Google mit einer Strafe bzgl. unrechtmäßiger Verarbeitung von Standortdaten. | – Vertraulichkeit, Datenminimierung, Intervenierbarkeit, Transparenz, Zweckbindung/Nicht. (2): Hier sehen wir eine Vielzahl von Schutzzielen betroffen, allerdings sehen wir hier keine schwerwiegenden Einschränkungen der Schutzziele der Betroffenen,<br>– Wir gehen daher von einer mittleren Schwere aus. | 8 |
| **B12** | Offenlegung von Gesundheitsdaten (Rezeptinformationen, Mitteilungen) | – (4) Aufgrund der frühen Implementierungsstatus und der Tatsache das vor allem ältere Nutzer in der Regel nicht so stark versiert sind, vergeben wir den Höchstwert für die EW. | – Vertraulichkeit (3): Die Offenlegung von Rezeptinformationen kann zu beträchtlichen Schäden führen. | 12 |
| **B13** | Verlust des Smartphones | – (4) Wir gehen davon aus, das regelmäßig Nutzer regelmäßig ihr Smartphone verlieren und vergeben daher die Höchstwertung. | – Verfügbarkeit (2): Der Passwortschutz der App und die Möglichkeit, die Geräteregistrierung aufzuheben. | 8 |
| **B14** | Unrechtmäßige Datenverarbeitung durch Standortzugriff | – (4) Es besteht eine starke Abhängigkeit von Betriebssystembetreibern,<br>– Bereits vorgekommen, dass die Betreiber unrechtmäßig Daten verarbeitet haben,<br>– Aktuell kämpft Google mit einer Strafe bzgl. unrechtmäßiger Verarbeitung von Standortdaten. | – Vertraulichkeit, Datenminimierung, Intervenierbarkeit, Transparenz, Zweckbindung/Nicht. (2): Hier sehen wir eine Vielzahl von Schutzzielen betroffen, allerdings sehen wir hier keine schwerwiegenden Einschränkungen der Schutzziele der Betroffenen. | 8 |
| **B15** | Unrechtmäßige Datenverarbeitung durch Push Notifications | – (4) Es besteht eine starke Abhängigkeit von Betriebssystembetreibern,<br>– Bereits vorgekommen, dass die Betreiber unrechtmäßig Daten verarbeitet haben,<br>– Aktuell kämpft Google mit einer Strafe bzgl. unrechtmäßiger Verarbeitung von Standortdaten. | – Vertraulichkeit, Datenminimierung, Intervenierbarkeit, Transparenz, Zweckbindung/Nicht. (2): Hier sehen wir eine Vielzahl von Schutzzielen betroffen, das Versenden Von Leer-Mitteilungen senkt die Aussagekraft von potenziell ermittelten Daten. | 8 |
| **B16** | Unabsichtliches Löschen von Mitteilungen (Firebase Cloud Messaging) | – (1) Die Spezifikationen und die Bestätigungsnachfrage senken die Eintrittswahrscheinlichkeit signifikant. Vergeben den kleinsten möglichen Wert. | – Verfügbarkeit (3): Falls eine Nachricht versehentlich gelöscht wird, können die Folgen teilweise schwerwiegend sein, wenn die Nachricht wichtige Informationen für ein Rezept beinhaltet haben. | 3 |

| Bedrohung ID | Bedrohung | Eintrittswahrscheinlichkeit | Schaden | Risiko |
|---|---|---|---|---|
| **B17** | Teilen über unsichere Anwendung | – (2) Es besteht eine starke Abhängigkeit von Betriebssystembetreibern,<br>– Funktion kann nicht eingeschränkt werden, allerdings senken die getroffenen Maßnahmen die Eintrittswahrscheinlichkeit teilweise. | – Vertraulichkeit (4): Abhängig von der Anwendung über die das Rezept geteilt wird, kann es schwere eventuell unwiderrufliche Folgen für den Betroffenen nach sich ziehen. | 8 |
| **B18** | Zweckwidrige Datenverarbeitung nach Modifikation der Analyseeinstellungen | – (2) Die Chance, dass wenigstens ein Administrator in 10 Jahren eine Analyseeinstellung zweckwidrig oder fahrlässig anpasst. | – Datenminimierung (3): Die Modifikation der Anlayseeinstellungen führen zu deutlich umfangreicheren Erfassung personenbezogener Daten mit potenziell schweren Folgen für den Versicherten.<br>– Nichtverkettung (3): Die Modifikation der Analyseeinstellungen kann zu einer erheblichen Beeinträchtigung der Privatsphäre führen. | 3 |
| **B19** | Fehlerhafte oder intransparente Implementierung der Einwilligungs-/Widerrufsmöglichkeit | – (1) Es ist theoretisch möglich, aber sehr unwahrscheinlich, dass die derzeitige Implementierung der Einwilligungs-/Widerrufsmöglichkeit nicht gefunden oder nicht verstanden wird. | – Transparenz (2): Dem Versicherten nur mangelhaft über die Verarbeitung personenbezogener Daten informiert. | 2 |
| **B20** | Übermäßige Verarbeitung von Daten durch/nach Drittstaatentransfer | – (1) Es ist theoretisch möglich, aber sehr unwahrscheinlich, dass personenbezogene Daten unrechtmäßig verarbeitet werden. Die relevanten personenbezogenen Daten liegen im Arbeitsspeicher (RAM) des Network Relays. | – Zweckbindung/Nichtverkettung (3): Die Verkettung der Nutzungsdaten durch Behörden eines Drittstaates, kann zu einer erheblichen Beeinträchtigung der betroffenen Personen führen. | 3 |

# Eintrittwahrscheinlichkeit

## Identifikation von Bedrohungen

| ID | Frage |
|---|---|
| Q1 | Welche Bedrohungen für die Betroffenen können durch die Nutzung der App entstehen? |
| Q2 | Welche Bedrohungen für die Betroffenen können durch IT-Ereignisse entstehen? |
| Q3 | Welche Bedrohungen für die Betroffenen können sich aus vorsätzlichen Angriffen ergeben? |
| Q4 | Wie kann ein Beschäftigter der gematik die rechtmäßige und sichere Verarbeitung personenbezogener Daten beeinflussen? |
| Q5 | Gibt es besondere Bedrohungen für die Betroffenen durch fremde Anwendungen, IT-Systeme oder strukturelle Gegebenheiten, die nicht der E-Rezept-App zuzuordnen sind? |

## Relevanz

| Relevanz | Erklärung |
|---|---|
| Direkt relevant | Die jeweilige Bedrohung wirkt sich auf die E-Rezept-App und die Verarbeitung personenbezogener Daten mit ihr aus. Sie muss daher in die Dokumentation aufgenommen werden. |
| Indirekt relevant | Die jeweilige Bedrohung kann sich auf die E-Rezept-App und die Verarbeitung personenbezogener Daten mit ihr auswirken, aber die Auswirkungen gehen nicht über andere oder allgemeinere Bedrohungen hinaus. Sie sollte daher nicht in die Dokumentation aufgenommen werden. |
| Nicht relevant | Die jeweilige Bedrohung kann sich nicht auf die E-Rezept-App und die Verarbeitung personenbezogener Daten mit ihr auswirken. Sie darf daher nicht in die Dokumentation aufgenommen werden. |

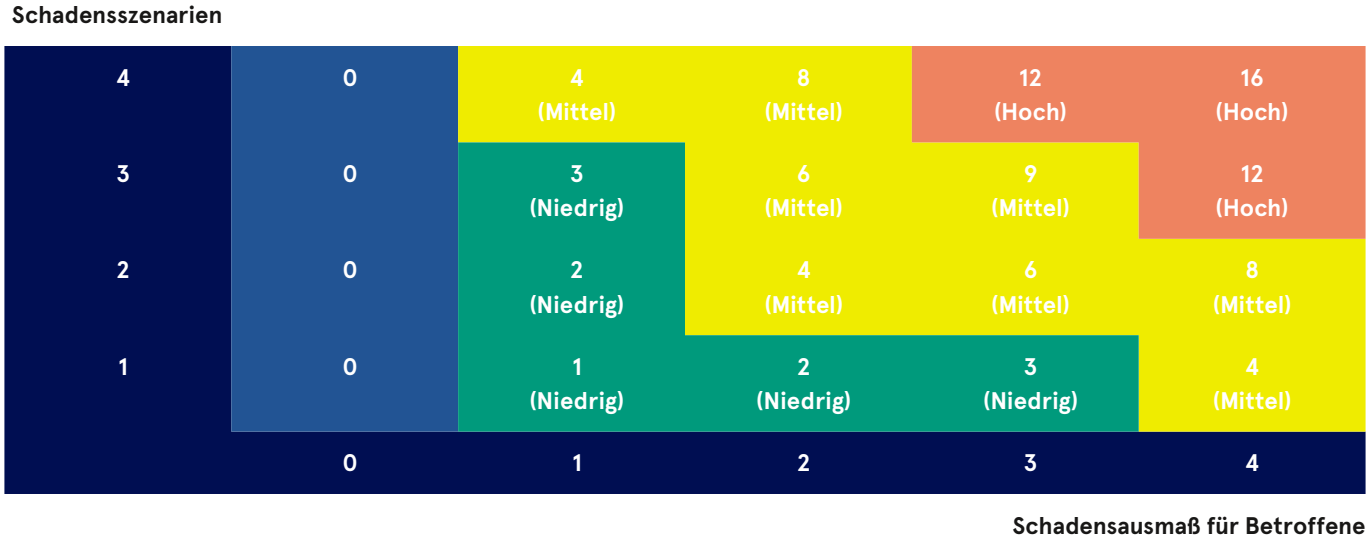
# Eintrittswahrscheinlichkeit

| Eintrittswahr-scheinlichkeit | Eigenschaften |
|---|---|
| 1 - Niedrig | **Tritt seltener als alle 10 Jahre auf.** |
| | Theoretisch möglich, aber sehr unwahrscheinlich. |
| | Die Bedrohung ist in der gematik weitgehend unbekannt. |
| | Ein Angreifer benötigt besondere technische Fähigkeiten und Unterstützung sowie ein sehr hohes Maß an internem Fachwissen und Interaktion mit anderen Personen oder Institutionen, die der Geheimhaltung unterliegen, um das notwendige zusätzliche Wissen zu erlangen, um die persönliche Verbindung herzustellen. |
| 2 - Medium | **Tritt etwa alle 2–10 Jahre auf.** |
| | Seltene Fälle. |
| | Die Bedrohung ist in der gematik bekannt. |
| | Ein Gegner benötigt technische Fähigkeiten und allgemeine Unterstützung sowie Expertenwissen und zusätzliches Wissen durch Interaktion mit Personen (Insider). |
| 3 - Hoch | **Findet einmal pro Jahr statt.** |
| | Vielleicht möglich bis sehr wahrscheinlich. |
| | Die Bedrohung ist einmal aufgetreten oder es ist überzeugend, dass sie in der gematik auftreten kann. |
| | Ein Angreifer benötigt nur wenig spezielles Know-how, zusätzliches Wissen oder kriminelle Energie, um Angriffsvektoren auszunutzen. |
| 4 - Sehr Hoch | **Tritt mindestens mehrmals im Jahr auf.** |
| | Sehr hohe Wahrscheinlichkeit. |
| | Die Bedrohung ist bereits mehrfach in der gematik aufgetreten oder kann jederzeit auftreten. |
| | Ein Gegner braucht keine besonderen Fähigkeiten oder Kenntnisse. |

# Schadenskategorien

| Schadensszenarien | Schadensausmaß für betroffene Personen | | | | |
|---|---|---|---|---|---|
| | 0 – Kein Schaden | 1 – Niedrig | 2 – Medium | 3 – Hoch | 4 – Sehr Hoch |
| **Physisch**<br>(z. B. Falsche medikamentöse Behandlung, weitere physische Schäden) | – Kein Schaden<br>– Nicht anwendbar | – Kurzes Kopfweh<br>– **Vorübergehende**, leichte Beeinträchtigung | – Leichte Erkrankung<br>– **Vorübergehende** Beeinträchtigung | – Langzeittherapie ist notwendig, um Schäden zu kompensieren | – **Dauerhafte** Beeinträchtigung der körperlichen Unversehrtheit<br>– Tod durch (fehlende) medikamentöse Behandlung |
| **Immateriell**<br>(z. B. Kontrollverlust über eigene Daten, Überwachung, Veröffentlichung personenbezogener Daten, Identitätsdiebstahl, unerlaubtes Profiling, Verletzung weiterer Grundrechte (z. B. Meinungsfreiheit)) | – Kein Schaden<br>– Nicht anwendbar | – Angst vor Kontrollverlust über Daten | – **Teilweise, vorübergehende** Verunglimpfung der Person oder Verlust der Anerkennung | – Erhebliches Mobbing<br>– **Beträchtlicher** Imageschaden, der aber mit Mühe überwunden werden kann<br>– Eingeschränkte Teilhabe an der Gesellschaft | – Schwere soziale Diskriminierung,<br>– **Virale** öffentliche Exposition mit grundlegenden, irreversiblen Folgen |
| | – Kein Schaden<br>– Nicht anwendbar | – Unerhebliche Beeinträchtigung der Privatsphäre | – **Erhebliche**, aber vorübergehende Beeinträchtigung der Privatsphäre | – **Erhebliche** Beeinträchtigung der Privatsphäre, aber mit großen Schwierigkeiten zu bewältigen | – **Schwere oder irreversible** Beeinträchtigung der Privatsphäre<br>– Folgen können nicht überwunden werden |
| **Materiell**<br>(z. B. Jobverlust durch berufliche Nachteile, finanzielle Verluste, Schaden am Eigentum) | – Kein Schaden<br>– Nicht anwendbar | – Bis zu 100 Euro | – Bis zu 1.000 Euro | – Bis zu 5.000 Euro oder drei Nettogehälter | – Mehr als drei Nettogehälter oder 5.000 Euro |

# Risikomatrix



**Impressum**

Herausgeber:
gematik GmbH
Friedrichstraße 136
10117 Berlin

Gestaltung: DreiDreizehn GmbH, Berlin