



Bundesamt  
für Sicherheit in der  
Informationstechnik

Deutschland  
**Digital•Sicher•BSI•**

# IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Gesundheits-Apps



Sicher im  
digitalen Alltag

# Änderungshistorie

Version	Datum	Name	Beschreibung
1.0	17.05.2021	Maria Hertleif, Cassini Consulting AG Dustin Huptas, Cassini Consulting AG Jens Neureither, Cassini Consulting AG Andreas Schmidt, Aleri Solutions GmbH Michael Schulze, Bundesamt für Sicherheit in der Informationstechnik Nicolas Stöcker, Bundesamt für Sicherheit in der Informationstechnik Waldemar Welsch, Cassini Consulting AG	Erstversion

*Tabelle 1: Änderungshistorie*

# Inhalt

Inhalt.....	3
Abbildungen.....	5
Tabellen.....	6
1 Zusammenfassung.....	7
2 Einleitung, Ausgangslage und Zielsetzung der Studie.....	11
3 Aufbau und Methodik der Studie.....	13
4 Der Markt für Gesundheits-Apps.....	15
4.1 Marktabgrenzung.....	15
4.2 Gegenwärtige Marktentwicklung.....	17
4.2.1 Marktsegmente.....	18
4.2.2 Downloadzahlen.....	20
4.2.3 Anbieterstruktur.....	20
4.2.4 Herkunft der Anbieter.....	20
4.2.5 Geschäftsmodell der Anbieter.....	22
5 Aktuelle Trends und perspektivische Entwicklung des Marktes.....	23
5.1 Die Nachfrage wächst.....	23
5.2 Die Angebotsbreite und -tiefe nimmt zu.....	23
5.3 Datengetriebene Lösungen und künstliche Intelligenz treiben die technologische Entwicklung...24	
5.4 Konzentration auf einzelne Anbieter nimmt zu.....	25
6 IT-sicherheitstechnische Betrachtung von Gesundheits-Apps.....	26
6.1 Sensibilität der Daten.....	26
6.2 Prüfmechanismen der App Stores.....	26
6.3 Quantitative Anbieterbefragung – IT-sicherheitstechnische Maßnahmen der Anbieter.....	27
6.3.1 Untersuchungsdesign der Befragung und Zusammensetzung der Stichprobe.....	28
6.3.2 Ergebnisse aus der Befragung.....	29
6.3.3 Fazit IT-sicherheitstechnische Maßnahmen der Anbieter.....	37
7 Case Studies – IT-sicherheitstechnische Untersuchung von Gesundheits-Apps.....	38
7.1 Design IT-sicherheitstechnische Untersuchung.....	38
7.2 Ergebnisse aus der IT-sicherheitstechnischen Untersuchung.....	39
7.2.1 Technischer Umgang mit Nutzerpasswörtern.....	39
7.2.2 Anbieterseitiger Umgang mit Nutzerdaten in Cloud-Umgebungen.....	40
7.2.3 Generelle Nutzung von Verschlüsselungsmechanismen.....	40
7.2.4 Angriffe gegen Verschlüsselungsmechanismen.....	41
7.2.5 Klassische anwendungsbezogene Angriffe.....	42
7.2.6 Zugriffseinschränkungen auf sensible Daten.....	42
7.2.7 Bedarfsgerechte App-Berechtigungen.....	42

---

7.2.8	Verarbeitung von benutzerbezogenen Daten.....	43
7.3	Zusammenfassung der Ergebnisse .....	43
8	Zielgruppenspezifische Handlungsbedarfe und Lösungen .....	46
	Literaturverzeichnis.....	49
	Glossar.....	51

# Abbildungen

Abbildung 1: Aufbau und Methodik der Studie .....	13
Abbildung 2: Betriebssysteme der downloadstärksten Apps in Deutschland. Quelle: 42matters 12/2020.....	17
Abbildung 3: Anteil der Marktsegmente nach Anzahl der Apps und Downloadzahlen. Quelle: 42matters 12/2020. ....	19
Abbildung 4: Herkunft der Anbieter (nur Google Play Store). Quelle: 42matters 12/2020.* .....	21
Abbildung 5: Anzahl der Apps nach Marktsegmenten für deutsche Anbieter. Quelle: 42matters 12/2020.* ...	21
Abbildung 6: In welchen Bereich würden Sie Ihre App eingliedern? (n=84) .....	29
Abbildung 7: Welche Datenkategorien werden erhoben? (n=78) .....	30
Abbildung 8: Welche Entscheidungsmöglichkeit haben die Nutzer/-innen hinsichtlich der Erfassung und Verarbeitung von Daten? (n=78).....	30
Abbildung 9: Wie wird IT-Sicherheit im Softwareentwicklungsprozess berücksichtigt? (n=70).....	31
Abbildung 10: Nutzen Sie Sie Security for Android Developers (SfAD)? Nutzen Sie das iOS Security Framework (ioSSF)? (n=70).....	32
Abbildung 11: Welche Anforderungen setzen Sie an ein User-Passwort? (n=51).....	32
Abbildung 12: Nehmen Sie Maßnahmen vor, um Daten und Datentransfers zu verschlüsseln? (n=54) .....	33
Abbildung 13: Verschlüsseln Sie Daten auf dem Endgerät und wenn ja, in welcher Stufe? (n=54) .....	33
Abbildung 14: Welchen TLS-Standard verlangen Sie mindestens für die Kommunikation zwischen App und Cloud-Infrastruktur? (n=54).....	34
Abbildung 15: Haben Sie in Bezug auf sicherheitsrelevante Updates einen Prozess zur Erkennung von notwendigen Updates für Bibliotheken Dritter? (n=54).....	34
Abbildung 16: Haben Sie Verfahrensweisen, wie mit der Meldung einer Schwachstelle beispielsweise durch Sicherheitsforscherinnen und -forscher umgegangen wird? (n=54).....	35
Abbildung 17: Gibt es verbindliche Vorgaben zu Zeiträumen, in denen Sicherheitslücken geschlossen werden? (n=54) .....	35
Abbildung 18: Wurden Maßnahmen gegen Reverse Engineering getroffen? (n=51) .....	36
Abbildung 19: Wurden Maßnahmen zur Erkennung von Manipulation (root / jailbreak) der Geräte vorgenommen? (n=51).....	37
Abbildung 20: Testkategorien der IT-sicherheitstechnischen Untersuchung.....	39
Abbildung 21: Übersicht Handlungsbedarfe und Lösungen.....	46

---

# Tabellen

Tabelle 1: Änderungshistorie.....	2
Tabelle 2: Abgrenzung von Gesundheits-Apps, Medizin-Apps und DiGA.....	16
Tabelle 3: Kategorisierung von Gesundheits- und Medizin-Apps am Beispiel zweier App Store Betreiber.....	18

# 1 Zusammenfassung

Gesundheits-Apps wie Fitness Tracker, Diätstagebücher oder Entspannungshilfen erfreuen sich großer Beliebtheit und sind auf vielen mobilen Endgeräten in Deutschland installiert. Sie richten sich vor allem an gesundheitsbewusste Nutzerinnen und Nutzer und unterstützen im Bereich von Prävention, Aufklärung und Gesundheitsförderung. Mit Blick auf die gängigen App Stores machen sie den Großteil der Apps in den Kategorien „Health und Fitness“ und „Medical“ aus. Tagtäglich kommen neue Anwendungen hinzu und der Markt weist eine hohe Dynamik auf.

Ein bedeutender Anteil der Apps verarbeitet personenbezogene Daten und Gesundheitsdaten, die aufgrund ihrer Sensibilität besonders schützenswert sind. Denn: wurden Daten über den Gesundheitszustand einer Nutzerin oder eines Nutzers erst einmal veröffentlicht, lässt sich der Schaden nur selten beheben oder kompensieren. Je nach Leistungsumfang der mobilen Anwendung, werden aber auch besondere Anforderungen an die Verfügbarkeit gestellt, wenn es beispielsweise um Erinnerungsfunktionen geht. Das BSI hat deshalb 2020 die technische Richtlinie „Sicherheitsanforderungen an digitale Gesundheitsanwendungen“ (TR-03161<sup>1</sup>) veröffentlicht, die Entwicklerinnen und Entwicklern von Gesundheits-Apps als Leitfaden bei der Entwicklung sicherer Apps unterstützen soll.

Anders als bei Medizin-Anwendungen, wird der Aspekt der IT-Sicherheit bei Gesundheits-Apps bisher allerdings kaum diskutiert. Die vorliegende Studie möchte deshalb für die aktuelle Marktsituation und für die derzeitige Wahrnehmung von Standards und Maßnahmen der IT-Sicherheit durch Marktteilnehmer sensibilisieren. Im Fokus stehen Status quo und Perspektiven des Marktes, IT-sicherheitstechnische Risiken sowie Handlungsbedarfe und Lösungen, die sich hieraus ergeben.

Zur Erhebung der vorliegenden Studienergebnisse wurden verschiedene Methoden genutzt. Der methodische Aufbau umfasst eine Analyse von Sekundärdaten und Sekundärliteratur, qualitative Interviews mit Marktexpertinnen und -experten sowie Entwicklerinnen und Entwicklern, eine quantitative Befragung von App-Anbietern, bei denen vor allem die Nutzung IT-sicherheitstechnischer Maßnahmen abgefragt wurde, sowie eine IT-sicherheitstechnische Untersuchung, bei der sieben ausgewählte Gesundheits-Apps getestet wurden.

Bisher existiert auf nationaler oder europäischer Ebene keine einheitliche Definition zu „Gesundheits-Apps“. Aufbauend auf Ansätzen aus der Fachliteratur wird im Rahmen der Studie deshalb eine eigene Abgrenzung gegenüber Medizin-Apps und „Digitalen Gesundheitsanwendungen“ (DiGA) vorgenommen. Die Abgrenzung erfolgt auf Basis der Berücksichtigung von drei zentralen Perspektiven: der Nutzerperspektive, der technologischen Perspektive und der regulatorischen Perspektive.

Gesundheits-Apps richten sich anders als Medizin-Apps und DiGA vor allem an gesundheitsbewusste Nutzerinnen und Nutzer und bieten Unterstützung im Bereich von Prävention, Aufklärung und Gesundheitsförderung. Sie richten sich in der Regel nicht an medizinisches Fachpersonal. Aus technologischer Perspektive liegt ihr Schwerpunkt auf der Erfassung, Aufzeichnung, Verarbeitung und Veranschaulichung von gesundheitsbezogenen Daten der Nutzerinnen und Nutzer. Ein nicht unbedeutender Teil der Apps fokussiert sich auf die reine Vermittlung von Wissen. Mit Blick auf die regulatorische Perspektive ist festzuhalten, dass Gesundheits-Apps in der Regel in Abgrenzung zu Medizin-Apps oder DiGA keiner konkret-spezifisch verpflichtenden Regulierung unterliegen.

Für die Marktanalyse wurden die 1.000 downloadstärksten Gesundheits-Apps auf dem deutschen Markt analysiert, die über die beiden bedeutendsten App-Marktplätze angeboten werden. Fitness-Apps machen aktuell das mit Abstand größte Segment aus. Bei den analysierten 1.000 downloadstärksten Gesundheits-Apps entfallen knapp die Hälfte der Downloads auf „Fitness-Apps“. Dieses Segment umfasst insbesondere Anwendungen im Bereich Instruktion und Nachverfolgung von Trainings sowie die Vermittlung sonstiger Fitness-Informationen. Weitere bedeutende Segmente sind „Entspannung und Achtsamkeit“ (Meditation,

---

<sup>1</sup> vgl. <https://www.bsi.bund.de/TR-03161>

Stressbewältigung etc.), „Ernährung & Gewicht“ (Diät & Fasten, Kalorienzählen etc.) oder „Schwangerschaft, Verhütung und Kinderwunsch“ (Zyklus- und Schwangerschaftstracking etc.).

Der Markt für Gesundheits-Apps ist hoch dynamisch und wird in Deutschland aller Voraussicht nach auch perspektivisch weiterwachsen und an Bedeutung gewinnen. Ein Treiber ist die wachsende Nutzernachfrage. Diese steigt u. a., weil Nutzerinnen und Nutzer die eigene Gesundheit verstärkt selbst in die Hand nehmen und Gesundheitsinformationen nachfragen (E-Patient) sowie eigene Körpermessdaten dokumentieren, analysieren und austauschen (Quantified Self).

Gleichzeitig ist ein Trend hin zu einem Wachstum der Angebotsbreite und -tiefe zu erkennen. Mit Blick auf die Angebotsbreite fokussieren sich Anbieter zunehmend nicht mehr nur auf ein Anwendungsgebiet, sondern verbinden mehrere dieser miteinander: beispielsweise „Entspannung und Achtsamkeit“ mit „Fitness“. Apps zum „ganzheitlichen Gesundheitsmanagement“ gewinnen hierdurch an Bedeutung. Gleichzeitig deutet sich für die befragten Expertinnen und Experten eine stärkere Integration der Angebote entlang der Wertschöpfungskette an. Schritt für Schritt erweitern Anbieter von Gesundheits-Apps dabei den Funktionsumfang ihrer App auch in Richtung medizinischer Anwendungsgebiete. Hierdurch könnten auch die Grenzen zum Bereich von Medizin-Apps und DiGA abnehmen.

In technologischer Sicht beeinflussen datengetriebene Lösungen und der steigende Einsatz von künstlicher Intelligenz (KI) die Entwicklung im Markt. Die zunehmende Erfassung und Analyse von Körpermessdaten bietet die Basis für die Entwicklung neuer Anwendungskontexte. KI-Systeme ermöglichen es den Nutzerinnen und Nutzern, individuelle Hinweise für ein gesundheitsförderndes Verhalten zu geben. Ein Bedeutungsgewinn von KI-basierten Anwendungen begünstigt die weitere Konzentration der Download- und Nutzerzahlen auf einzelne Anbieter mit einem vorhandenen Datenpool.

Aufbauend auf diesen grundlegenden Beobachtungen zum Markt erfolgt die Analyse und Bewertung der IT-sicherheitstechnischen Risiken. Die Tragweite eines IT-sicherheitstechnischen Angriffs für Nutzerinnen und Nutzer ist von vielen Faktoren abhängig. Mitentscheidend für die Nutzerrisiken ist, ob und welche Daten verarbeitet werden sowie in welcher Art und an welchem Ort dies erfolgt. Das Risiko, das für einzelne Verbraucherin oder Verbraucher von der Nutzung einer Gesundheits-App ausgeht, ist deshalb differenziert zu betrachten und muss individuell von App zu App beurteilt werden. Die potenzielle Schadenshöhe und damit das Risiko für Verbraucherinnen und Verbraucher kann im Bereich der Gesundheits-Apps abhängig von der Bedeutung bzgl. Vertraulichkeit, Verfügbarkeit und Integrität jedoch besonders hoch sein.

Mit Blick auf vorhandene Sicherheitsmechanismen im Markt wurden auch die Prüfmechanismen der App Store Betreiber beleuchtet. Diese sind verpflichtet, Maßnahmen zur Überprüfung der Qualität der eingereichten Apps durchzuführen. Der Aspekt der IT-Sicherheit steht bei der Prüfung allerdings nicht im Fokus. In den jeweiligen Richtlinien für den Prüfungsprozess werden kaum Informationen darüber veröffentlicht, welche Anforderungen die App Store Betreiber an die Sicherheitsvorkehrungen der Anbieter haben. Mit Blick auf die Gesamtmenge der täglich geprüften Anwendungen ist davon auszugehen, dass die Prüfung automatisiert und deutlich oberflächlicher erfolgt als bei der Prüfung durch Sicherheitsforscherinnen und -forscher. Es ist daher davon auszugehen, dass die Prüfmechanismen der App Stores deshalb in der Regel nicht ausreichen, um Nutzerinnen und Nutzer vor unsicheren Gesundheits-Apps zu schützen.

Im Rahmen einer quantitativen Anbieterbefragung wurde untersucht, welche Maßnahmen Anbieter von Gesundheits-Apps mit Blick auf die IT-Sicherheit ihrer Anwendungen einsetzen. An der Befragung nahmen 84 Anbieter von Gesundheits-Apps teil, die mittels direkter Ansprache und Veröffentlichung der Umfrage über die Kommunikationskanäle des BSI adressiert wurden. Die Stichprobe ist nicht repräsentativ für die Grundgesamtheit (Anbieter von Gesundheits-Apps im deutschen Markt). Erkenntnisse aus der Stichprobenanalyse geben allerdings Hinweise auf mögliche Merkmalsausprägungen innerhalb der Grundgesamtheit.

Nach eigenen Aussagen berücksichtigen 91,4% der Anbieter IT-Sicherheit bereits im Entwicklungsprozess. Die Befragung hat allerdings Aspekte aufgezeigt, in denen Anbieter ihren Umgang mit Fragen der IT-Sicherheit verbessern und professionalisieren können. Die vom BSI im Rahmen der TR-03161 empfohlenen Maß-



nahmen werden nur zum Teil umgesetzt. Einige Beispiele hierfür sind: die Umsetzung des vom BSI empfohlenen Standards für sichere Passwörter, die Verschlüsselung des Datentransfers zwischen App und Cloud-Infrastruktur, die Verschlüsselung der Nutzerdaten auf dem jeweiligen Endgerät, die Einführung eines strukturierten Prozesses für den Umgang mit Schwachstellen und die Definition eines festen Zeitraums für das Schließen von Sicherheitslücken sowie Maßnahmen gegen Reverse Engineering oder zur Erkennung von Geräten, die mittels sog. „roots“ oder „jailbreaks“ manipuliert wurden.

Mit Blick auf die abgefragten Maßnahmen ist kein einheitlicher Umgang mit Fragen der IT-Sicherheit erkennbar und die empfohlenen Maßnahmen werden nur von einem Teil der befragten Unternehmen umgesetzt.

Dieses Ergebnis wird auch durch die IT-sicherheitstechnische Untersuchung bestätigt. Aufbauend auf den Erkenntnissen aus der Marktanalyse und der Anbieterbefragung wurden im Rahmen der Untersuchung sieben ausgewählte Gesundheits-Apps analysiert. Hierfür wurden Apps ausgewählt, die sowohl eine mutmaßlich breite Anwendung unter Nutzerinnen und Nutzern finden als auch eine gewisse Sensibilität der verarbeiteten Daten aufweisen.

Das Prüfschema wurde vom BSI gemeinsam mit der cassini AG entwickelt. Mit einem Prüfkatalog wurden in den drei Kategorien „Netzwerkangriff“, „Angriff am Gerät“ und „Analyse des App-Pakets“ 28 Anforderungen systematisch erfasst und die Apps in einer einheitlichen und daher vergleichbaren Art und Weise untersucht und bewertet.

Im Fokus stand die Analyse von gängigen und wahrscheinlichen Angriffsvektoren. Untersucht wurden Angriffsmöglichkeiten, welche durch Angreifer mit begrenztem Aufwand genutzt werden könnten und sich durch entsprechende Sicherheitsvorkehrungen gemäß der Technischen Richtlinie TR-03161 verhindern ließen. Ziel der Untersuchung war es, den sicherheitstechnischen Gesamtzustand der betrachteten Gesundheits-Apps zu erfassen, um auf dieser Basis Rückschlüsse auf die allgemeine Lage im Markt ziehen zu können. Eine tiefere Analyse, z. B. von Speichermedien oder Code Audits mit Reverse Engineering Techniken erfolgte nicht. Die Untersuchung stellt deshalb keinen vollumfänglichen Test dar und geht nicht mit einer Produktdeklaration oder -zertifizierung einher.

Die Ergebnisse der Untersuchung zeigen, dass die Anbieter eine Auswahl grundsätzlicher Anforderungen an die IT-Sicherheit erfüllen. Beispiele hierfür sind, dass alle Apps für die Verschlüsselung der Kommunikation zwischen den Apps und den Betreiber-Infrastrukturen durchgängig die Transportverschlüsselung Transport Layer Security (TLS) verwenden. Zudem ließen sich im Rahmen der Untersuchung keine erfolgreichen Injection-Angriffe durchführen. Einzelne Apps führten Input-Escaping durch und verhinderten die Ausführung von Programmcode, zeigten den Einsatz weitergehender Schutzmaßnahmen und blockierten Inhalte, die auf Befehlscode hinweisen vollständig.

Die definierten Anforderungen wurden aber in keinem der Fälle in einer Art und Weise abgedeckt, wie es nach TR-03161 zu erwarten gewesen wäre. Die im Prüfkatalog definierten Anforderungen erfüllten die sieben untersuchten Apps im Durchschnitt lediglich zu 49,1%. Über ein durchschnittliches Maß hinausgehende Anstrengungen zur Implementierung von zeitgemäßen IT-Sicherheitsfunktionalitäten waren lediglich im Einzelfall erkennbar. Keine der Apps setzte Sicherheitsmaßnahmen entsprechend des definierten Anforderungskatalogs vollständig um. Einige Beispiele hierfür: sechs von sieben der untersuchten Apps übermittelten Passwörter im Klartext an Authentifizierungsdienste und ebenfalls sechs von sieben Apps konnten mittels eines Man-in-the-Middle Proxy analysiert werden und führten keine erweiterten Schutzmaßnahmen wie Certificate Pinning durch. Die meisten Apps grenzten die Lesbarkeit bzw. den Zugriff auf sensible Daten in den Apps nicht ein, z. B. durch Bildschirmsperren oder PIN-Nutzung und bei keiner der Apps wurden sensible Informationen in der Hintergrundnutzung ausgegraut.

Aus Sicht der technischen IT-Sicherheit muss dieses Ergebnis, insbesondere im Hinblick darauf, dass ein bedeutender Anteil der Apps sensible und besonders schützenswerte Daten verarbeitet, mindestens als kritisch bewertet werden. Denn die Daten der Nutzerinnen und Nutzer werden hierdurch nach Erkenntnissen der Studie nicht ausreichend vor potenziellen Angriffen geschützt.

Für die einzelne Nutzerin respektive den einzelnen Nutzer ist die Tragweite der hierdurch entstehenden Risiken nur schwer zu ermessen. Nur Wenige verfügen über die notwendige Beurteilungskompetenz, um die Risiken bewerten und abwägen zu können. Die hohe Intransparenz und Dynamik des Marktes machen es schwer, sich zu orientieren und die Seriosität und Sicherheit der Angebote zu bewerten. In den vergangenen Jahren wurden deshalb Qualitätssiegel, Kodizes und Datenbanken von Gesundheits-Apps entwickelt, die die Orientierung für Verbraucherinnen und Verbraucher erleichtern sollen. Sie sind allerdings wenig bekannt, betrachten den Aspekt der IT-Sicherheit in der Regel nur am Rande und werden durch das geringe Bewusstsein für die potenziellen Risiken selten angesteuert. Gleichzeitig stoßen sie durch die hohe Dynamik im Markt schnell an ihre Grenzen.

Um die Risiken für Verbraucherinnen und Verbraucher im Kontext von Gesundheits-Apps zu minimieren, erscheint es zielführend über einen ganzheitlichen Ansatz sowohl die Anbieter- als auch die Nutzerseite zu adressieren.

Mit Blick auf die Stärkung der Sicherheit von Gesundheits-Apps sollten Sicherheitsmerkmale als integraler Bestandteil der App verstanden werden. IT-Sicherheitsanforderungen sollten im Sinne eines "Security by Design" Ansatzes bereits im Entwicklungsprozess berücksichtigt werden.

Da sich Art und Umfang von Angriffen stetig und mit hoher Geschwindigkeit weiterentwickeln, bedarf es gleichzeitig einer kontinuierlichen Auseinandersetzung mit den IT-Sicherheitsanforderungen nach aktuellem Stand der Technik. In diesem Kontext gilt es auch, das generelle Bewusstsein der Anbieter für ihre Verantwortung gegenüber Nutzerinnen und Nutzern und die Auswirkungen ihres Handelns zu stärken. Einen Ansatz bietet in diesem Kontext die Sensibilisierung für „Corporate Digital Responsibility“, die die bereits seit geraumer Zeit diskutierte „Corporate Social Responsibility“ um den Aspekt der digitalen Verantwortung erweitert. Unternehmen sollten Verantwortung durch eine ganzheitliche Betrachtung der IT-Sicherheit übernehmen. Neben der Vertraulichkeit, also dem sorgfältigen Umgang mit den Daten ihrer Nutzerinnen und Nutzer, dem sicheren Verwalten und Schutz vor Angriffen, sind auch die Integrität und Verfügbarkeit in den Fokus zu nehmen. Durch die stärkere Berücksichtigung des Aspektes der IT-Sicherheit steigt die Resilienz und Reaktionsgeschwindigkeit der App-Anbieter gegenüber Angriffen. Kundinnen und Kunden sowie Geschäftsmodelle und Reputation der App-Anbieter werden besser geschützt.

Mit der TR-03161 hat das BSI im Jahr 2020 Entwicklerinnen und Entwicklern von Gesundheits-Apps eine Orientierungshilfe für die Entwicklung solcher mobilen Anwendungen an die Hand gegeben. Die Implementierung dieser technischen Richtlinie in die IT-Sicherheitskonzepte der Anbieter ist nach Erkenntnissen dieser Untersuchung noch in einem Anfangsstadium. Das BSI setzt sich dafür ein, dass die Orientierung an der Richtlinie erhöht wird. In diesem Zusammenhang ist ein Dialog mit Entwicklerinnen und Entwicklern angedacht, der Hürden bei der Umsetzung identifizieren und die Richtlinie auf Basis des Dialogs entsprechend weiterentwickeln soll.

Gleichzeitig setzt sich das BSI dafür ein, Verbraucherinnen und Verbraucher für Risiken im Umgang mit digitalen Gesundheitsanwendungen zu sensibilisieren. Hierfür sollten entsprechend Informationen, Leitfäden und Hilfestellungen zur Verfügung gestellt werden. Damit Chancen sowie potenzielle Risiken der Anwendungen erkannt und besser bewertet werden können, sollte die Beurteilungskompetenz der Verbraucherinnen und Verbraucher als immanenter Bestandteil des lebenslangen Lernens gefördert werden.

## 2 Einleitung, Ausgangslage und Zielsetzung der Studie

Mobile Endgeräte (Smartphones, Tablets etc.) sind längst Teil unseres Alltags und die Nutzung mobiler Anwendungen (kurz Apps) gehört zur täglichen Routine. Großer Beliebtheit erfreuen sich dabei Apps, die helfen sollen, unsere Gesundheit zu wahren sowie zu fördern und durch einen benutzerfreundlichen, orts- und zeitunabhängigen Zugriff gekennzeichnet sind. Fitness Tracker, Diätstagebücher und Entspannungshilfen sind beliebte Anwendungen und auf vielen mobilen Endgeräten in Deutschland installiert.

Apps mit Fokus Gesundheit unterscheiden sich dabei in Nutzerperspektive, technologischen Aspekten sowie der Regulierung gravierend. Auf der einen Seite stehen Medizin-Apps, welche durch medizinisches Fachpersonal sowie Patientinnen und Patienten genutzt werden und medizinische Daten vor allem zu Diagnose- und Therapiezwecken verarbeiten. Diese unterliegen in der Regel einer entsprechenden Regulierung. Auf der anderen Seite steht eine tagtäglich wachsende Zahl von Gesundheits-Apps, die sich an gesundheitsbewusste Nutzerinnen und Nutzer richten, Wissen vermitteln und gesundheitsbezogene Daten zu Präventionszwecken erfassen und verarbeiten.

Sowohl Medizin-Apps als auch Gesundheits-Apps verarbeiten besonders schützenswerte und sensible Daten ihrer Nutzerinnen und Nutzer. Wurden sensible Daten über den Gesundheitszustand erst einmal veröffentlicht, lässt sich der Schaden nur selten beheben oder kompensieren. Das Thema IT-Sicherheit wird bisher allerdings vor allem im Kontext von Medizin-Apps rege diskutiert und hat durch die Einführung der Digitale-Gesundheitsanwendungen-Verordnung (DiGAV) hohe Dynamik und Aufmerksamkeit gewonnen. Anbieter von Medizin-Apps und Digitalen Gesundheitsanwendungen (DiGA) unterliegen von Rechtswegen einer Konformitätserklärung u. a. hinsichtlich ihrer IT-Sicherheit, machen aber nur einen kleinen Teil der Medizin- und Gesundheitsanwendungen im Markt aus. Bei dem Gros der Apps, die in den gängigen App Stores in den Kategorien „Health & Fitness“ und „Medical“ angeboten werden, handelt es sich um Gesundheits-Apps, die anders als in der Regel Medizin-Apps und DiGA keiner konkret-spezifischen, verpflichtenden Regulierung unterliegen.

Für Anwenderinnen und Anwender stellt sich der Markt weitestgehend intransparent dar. Die Gründe hierfür sind verschieden: Der Markt unterliegt einer besonders hohen Dynamik – es erscheinen kontinuierlich eine Vielzahl neuer Anwendungen, während parallel dazu täglich Anwendungen wieder verschwinden. Gleichzeitig erfolgt in den App Stores und auch im öffentlichen Diskurs keine einheitliche Systematisierung und Abgrenzung – sowohl in der Unterscheidung zwischen Medizin-Apps und Gesundheits-Apps als auch innerhalb des Marktes für Gesundheits-Apps. Die Kategorien in den App Stores dienen vor allem der optimalen Vermarktung der Anwendungen. Der Aspekt der Datensicherheit im Sinne der IT-Sicherheit spielt in der Darstellung der Apps in den App Stores bisher keinerlei Rolle. Ende 2020 führte Apple mit den „App Privacy Labels“ eine Neuerung ein. Diese Labels helfen Nutzerinnen und Nutzern dabei die Datenschutzpraktiken einer App besser zu verstehen, bevor sie die App herunterladen.<sup>2</sup> Informationen zu IT-Sicherheitseigenschaften einer App suchen Verbraucherinnen und Verbraucher jedoch in der Regel vergeblich.

**Die vorliegende Studie des BSI möchte für die aktuelle Marktsituation und für die derzeitige Wahrnehmung von Standards und Maßnahmen der IT-Sicherheit durch Marktteilnehmer sensibilisieren.**

Im Fokus der Studie stehen Gesundheits-Apps (vgl. 4.1 Marktabgrenzung), Medizin-Apps und DiGA sind explizit nicht Teil der Untersuchung. Ziel ist es, zentrale Marktstrukturen und potenzielle IT-sicherheitstechnische Risiken für Verbraucherinnen und Verbraucher aufzuzeigen und hieraus Handlungsbedarfe und -empfehlungen für Staat, Wirtschaft und Gesellschaft abzuleiten. Hinsichtlich der Bewertung der Risiken liegt das Augenmerk vor allem auf dem Aspekt der IT-Sicherheit der Anwendungen. Eine Orientierungshilfe für Anbieter hat das BSI im Jahr 2020 mit der Technischen Richtlinie 03161 vorgelegt, welche „Sicherheitsanforderungen an digitale Gesundheitsanwendungen“ definiert (BSI, 2020).

---

<sup>2</sup> <https://developer.apple.com/app-store/app-privacy-details/>

Die Studie steht im Kontext der Aufgabe des digitalen Verbraucherschutzes beim BSI. Durch die Einrichtung eines neuen eigenen Organisationsbereichs „Digitaler Verbraucherschutz, Cyber-Sicherheit für Gesellschaft und Bürger“ wird der Bereich aktuell gestärkt und z. B. um Aktivitäten im Bereich der Marktbeobachtung ergänzt. Hier knüpft die vorliegende Studie zur „IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Gesundheits-Apps“ an.

Im nachfolgenden Kapitel 3 werden Aufbau und Methodik der Studie erläutert. Hieran schließt sich die Darstellung des untersuchten Marktes für Gesundheits-Apps an.<sup>3</sup> Kapitel 4.1 stellt dabei zentrale Möglichkeiten der Strukturierung des Marktes und der Abgrenzung insbesondere gegenüber medizinischen Anwendungen dar. Kapitel 4.2 gibt einen Überblick über den Markt in Deutschland und zeigt mit Hilfe von zentralen Kennzahlen die Bedeutung von verschiedenen Marktsegmenten, Anbietern und Geschäftsmodellen auf. Verschiedene Trends deuten darauf hin, dass der Markt auch in den kommenden Jahren weiterhin von einer hohen Dynamik geprägt sein wird. Kapitel 5 zeigt die zentralen Treiber der Entwicklung auf Seiten von Nachfrage und Angebot auf und identifiziert zentrale technologische Trends, die die Entwicklung der Lösungen im Markt in den kommenden Jahren prägen könnten. Teil der Betrachtung ist auch die perspektivische Entwicklung der Anbieterstruktur im Markt.

Die Kapitel 6 und 7 untersuchen die IT-sicherheitstechnischen Risiken von Gesundheits-Apps. In Kapitel 6 werden hierfür zentrale Parameter betrachtet: die Sensibilität der erfassten und verarbeiteten Daten (Kapitel 6.1) sowie die Prüfmechanismen der Apps Stores und IT-sicherheitstechnischen Maßnahmen der Anbieter (vgl. Kapitel 6.2 und 6.3). Die Erkenntnisse zu den Maßnahmen der Anbieter basieren auf einer im Rahmen der Studie durchgeführten quantitativen Anbieterbefragung zu Gesundheits-Apps.

Zusätzlich wurde für sieben ausgewählte Gesundheits-Apps eine IT-sicherheitstechnische Untersuchung durchgeführt. Kapitel 7 gibt eine Übersicht über die zentralen Ergebnisse sowie die Detailergebnisse aus den verschiedenen Schwerpunktbereichen der Untersuchung.

Aufbauend auf den Erkenntnissen aus der Marktanalyse und der Untersuchung der IT-sicherheitstechnischen Risiken von Gesundheits-Apps werden in Kapitel 8 zielgruppenspezifische Handlungsbedarfe und Lösungen zum Schutz von Verbraucherinnen und Verbrauchern diskutiert und bewertet.

---

<sup>3</sup> Aufgrund der verfügbaren Datenlage und der Marktabdeckung wird hier auf die Apps des Google Play Stores und des Apple App Stores abgestellt.

### 3 Aufbau und Methodik der Studie

Zur Erhebung der vorliegenden Studienergebnisse wurden verschiedene empirische Methoden mit einer IT-sicherheitstechnischen Analyse kombiniert. Abbildung 1 veranschaulicht den Aufbau und den Methodenmix dieser Studie.

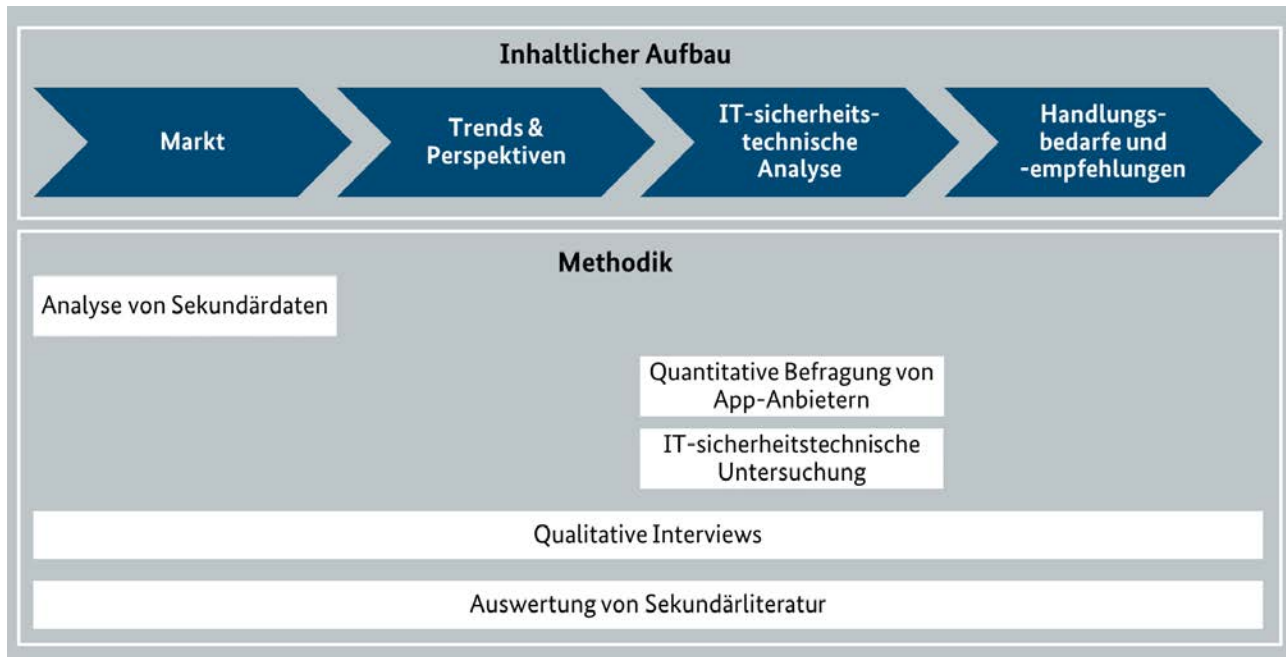


Abbildung 1: Aufbau und Methodik der Studie

Die **Analyse von Sekundärliteratur** lieferte Aufschluss über bisherige wissenschaftliche Erkenntnisse zum Markt für Gesundheits-Apps und unterstützte die Erarbeitung der inhaltlichen Bausteine in allen Schritten der Studie. So wurden vorliegende Erkenntnisse zur Abgrenzung des Marktes analysiert und dienten gemeinsam mit den Erkenntnissen aus der Analyse von Marktdaten als Basis für die Entwicklung einer eigenen Abgrenzung. Im Kontext der IT-sicherheitstechnischen Betrachtung lieferten vorliegende Studien Ansätze zur Einschätzung der Risiken für Verbraucherinnen und Verbraucher (u. a. auf Basis der Sensibilität der verarbeiteten Daten und der Sicherheitsmechanismen der App Stores) sowie zur Bewertung von Handlungsbedarfen und der Praxistauglichkeit verschiedener Handlungsansätze.

Für die Analyse der gegenwärtigen Marktentwicklung (Kapitel 4.2) erfolgte eine **Analyse von Sekundärdaten**. Hierfür wurden Daten der Marktdatenplattform 42matters<sup>4</sup> ausgewertet. Die Auswahl der Apps erfolgte auf Basis der Kriterien „Verfügbarkeit im Apple App Store oder Google Play Store“, „Verfügbarkeit in den Kategorien Health & Fitness und/oder Medical“, „Verfügbarkeit in Deutschland“, „Listing in den deutschen Top App Charts“ und „Anzahl der monatlichen Downloads in Deutschland<sup>5</sup>“. Da die App Stores in den benannten Kategorien nicht nur Gesundheits-Apps aufführen, wurden Apps, welche nicht der dieser Studie zugrunde liegenden Definition entsprechen (vgl. Kapitel 4.1 Marktabgrenzung), herausgefiltert. Aus dem verbleibenden Datensatz wurden die 1.000 Apps mit den meisten monatlichen Downloads in Deutschland für die Analyse ausgewählt.

Darüber hinaus wurden im Rahmen der Studie sechs **qualitative Interviews** mit Marktexpertinnen und -experten sowie Entwicklerinnen und Entwicklern sowie Anbietern von Gesundheits-Apps geführt. Der Befragungszeitraum lag zwischen Oktober und Anfang November 2020. Im Fokus der Gespräche standen zum einen Fragen nach Abgrenzung, Status quo und Perspektiven des Marktes. Zum anderen Fragen der Transparenz des Marktes sowie der sich eventuell hieraus ergebenden Handlungsbedarfe und

<sup>4</sup> <https://42matters.com/>

<sup>5</sup> Monatliche Downloads: durchschnittliche Anzahl der Downloads in Deutschland für die letzten 30 Tage (Stichtag: 1.12.2020)

-empfehlungen im Kontext des Verbraucherschutzes. Darüber hinaus wurde mithilfe dieser Interviews auch das Befragungsdesign der quantitativen Anbieterbefragung validiert und geschärft.

Im Rahmen einer **quantitativen Befragung von App-Anbietern** wurden zwischen November 2020 und Januar 2021 insgesamt 84 Anbieter von Gesundheits-Apps online befragt. Im Fokus der Befragung stand, welche IT-sicherheitstechnischen Maßnahmen Anbieter von Gesundheits-Apps derzeit einsetzen. Das Untersuchungsdesign und die Zusammensetzung der Stichprobe werden in Kapitel 6.3.1 dargestellt. Die Erkenntnisse werden in den Kapiteln 6.3.2 und 6.3.3 erläutert.

Aufbauend auf den Erkenntnissen der Analyse des Marktes und der potenziellen Risiken für Verbraucherinnen und Verbraucher wurden insgesamt sieben Apps für eine **IT-sicherheitstechnische Untersuchung** ausgewählt. Das Untersuchungsdesign wird in Kapitel 7.1 erläutert. Die Ergebnisse der Untersuchung werden in Kapitel 7.2 dargestellt und in Kapitel 7.3 zusammengefasst.

## 4 Der Markt für Gesundheits-Apps

Der Markt der Gesundheits-Apps ist hoch volatil und in großen Teilen keiner spezifischen Regulierung unterworfen. Diese Sachverhalte bedingen, dass im Rahmen der Studiendurchführung eine ausführliche Marktbeobachtung als Grundlage für die Entwicklung des Untersuchungsdesigns und der Bewertung von Beobachtungen und Trends durchgeführt werden musste. Die wesentlichen Erkenntnisse dieser Marktanalyse werden im vorliegenden Kapitel dargestellt.

### 4.1 Marktabgrenzung

Für Nutzerinnen und Nutzer von Smartphones und Tablets stellen die gängigen App Stores ein breites Spektrum an Gesundheits-Apps mit diversen Schwerpunkten und Funktionalitäten bereit. Von Fitness-, Ernährungs-, Wellness- und Lifestyle-Apps bis hin zu Apps zur Prävention und Milderung von spezifischen Krankheiten zielen Gesundheits-Apps auch unter dem Einsatz von „Smart Wearables“ auf den Erhalt und die Stärkung der allgemeinen Gesundheit und die Gesundheitsförderung der Nutzerinnen und Nutzer ab. Studien zeigen, dass das App-Angebot sich dabei nicht zuletzt durch die rasante Entwicklung neuer Technologien sehr dynamisch entwickelt, wodurch der Markt sowohl für Nutzerinnen und Nutzer sowie App-Entwicklerinnen und -Entwickler als auch für regulierende Institutionen zunehmend intransparenter geworden ist (Albrecht, et al., 2016) (Evers-Wölk, et al., 2018).

Erschwerend kommt hinzu, dass bis dato keine einheitliche Definition zu „Gesundheits-Apps“ auf nationaler oder europäischer Ebene existiert. In der Fachliteratur finden sich zahlreiche Versuche einer Definition, deren prominenteste Vertreter nachfolgend in drei Perspektiven eingeordnet werden.

#### Nutzerperspektive:

- Als Gesundheits-Apps werden solche Anwendungsprogramme für mobile Endgeräte, insbesondere Smartphones und Tablets, verstanden, deren Ziel es ist, positiv auf die Gesundheit des Anwenders einzuwirken (Evers-Wölk, et al., 2018) (Albrecht, et al., 2016) (Albrecht, 2016).
- Gesundheits-Apps richten sich primär an gesunde Nutzerinnen und Nutzer und wollen diese bei einem gesundheitsförderlichen Lebensstil unterstützen (Evers-Wölk, et al., 2018) (Albrecht, et al., 2016) (Albrecht, 2016).
- In Abgrenzung zu Medizin-Apps, welche durch medizinisches Fachpersonal genutzt werden und / oder durch ihre medizinische Indikation als Medizinprodukt eingestuft werden müssen, richten sich Gesundheits-Apps in der Regel direkt an Nutzerinnen und Nutzer und werden eigenständig durch diese verwendet (Evers-Wölk, et al., 2018) (Albrecht, et al., 2016) (Albrecht, 2016).

#### Technologische Perspektive:

„Gesundheits-Apps ermöglichen die Erfassung, Aufzeichnung Verarbeitung und Veranschaulichung von gesundheitsbezogenen Daten. Dies können Daten zu Nährwerten (Kalorien), Mengen und Zusammensetzung der konsumierten Speisen, von Alkohol, Wasser, Kaffee oder Nikotin, oder aber auch Körperdaten wie Schritte, Puls, Kalorienverbrauch, Blutzucker/Glukose, Temperatur, Gewicht, Atmung oder Schlafqualität sein. Weiterhin zählen Daten physischer Aktivität, wie Sport, Schlaf oder Sex, sowie emotionale oder psychische Befindlichkeiten zu den erfassten und verarbeiteten Daten. Nicht zuletzt werden Umgebungs- und Ortsdaten einbezogen“ (Evers-Wölk, et al., 2018) nach (Barcena, et al., 2014).

**Regulatorische Perspektive:**

- In Abgrenzung zu Gesundheits-Apps gelten als medizinische oder Medizin-Apps mobile Anwendungen, die der Diagnose oder Therapie einer Erkrankung dienen und als Medizinprodukt zugelassen und mit dem CE-Kennzeichen versehen sind. Weitere Ansatzpunkte zur Abgrenzung liefert §3 Nr. 1 des Medizinproduktegesetzes.
- Mit dem Inkrafttreten des Digitale-Versorgung-Gesetzes können Medizin-Apps für gesetzlich Versicherte zu einer Kassenleistung werden. Diese gelten als "digitale Gesundheitsanwendungen" (DiGA) und werden vom BfArM geprüft, zugelassen und in einem gesonderten Verzeichnis gelistet.

Tabelle 2: Abgrenzung von Gesundheits-Apps, Medizin-Apps und DiGA

	Gesundheits-Apps	Medizin-Apps	DiGA
<b>Nutzung</b>	<ul style="list-style-type: none"> <li>• Von gesundheitsbewussten Nutzerinnen und Nutzern verwendet zur Prävention, Aufklärung und Gesundheitsförderung</li> </ul>	<ul style="list-style-type: none"> <li>• Von medizinischem Personal und Patientinnen/Patienten genutzt</li> <li>• Zur Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten</li> </ul>	<ul style="list-style-type: none"> <li>• Von Patientin/Patient oder von Leistungserbringer und Patientin/ Patient gemeinsam genutzt</li> <li>• Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder Kompensierung von Verletzungen oder Behinderungen</li> </ul>
<b>Technologie</b>	<ul style="list-style-type: none"> <li>• Erfassung, Aufzeichnung Verarbeitung und Veranschaulichung von gesundheitsbezogenen Daten der Nutzerinnen und Nutzer</li> <li>• Wissensbereitstellung</li> </ul>	<ul style="list-style-type: none"> <li>• Jegliche Form der Einflussnahme auf Daten (Erfassung, Aufzeichnung Verarbeitung und Veranschaulichung) von medizinisch relevanten Daten der Patientin/des Patienten</li> </ul>	<ul style="list-style-type: none"> <li>• Erfassung, Aufzeichnung Verarbeitung und Veranschaulichung von medizinisch relevanten Daten der Patientin/des Patienten</li> <li>• Auch Erhebung und Anbindung von Daten über externe Hardware (Pulsmesser, EKG-Sensorik etc.)</li> </ul>
<b>Regulierung</b>	<ul style="list-style-type: none"> <li>• Keine Regulierung</li> </ul>	<ul style="list-style-type: none"> <li>• §3 MPG</li> <li>• CE-Kennzeichnung nach §6 MPG</li> </ul>	<ul style="list-style-type: none"> <li>• Gesundheitsanwendungsverordnung (DiGAV)</li> <li>• § 33a Fünftes Buch Sozialgesetzbuch (SGB V)</li> </ul>

Bisher konnte sich, auch vor dem Hintergrund der dynamischen Entwicklung des Angebotes, keine eindeutige Abgrenzung von Gesundheits-Apps durchsetzen. Zur Abgrenzung des Untersuchungsgegenstands dieser Studie wurden alle drei benannten Perspektiven herangezogen.

Im Fokus der Untersuchung stehen:

- auf dem deutschen Markt verfügbare Gesundheits-Apps,
- die vorrangig von gesundheitsbewussten Nutzerinnen und Nutzern zur Prävention, Aufklärung und Gesundheitsförderung verwendet werden,
- gesundheitsbezogene Daten erfassen, aufzeichnen, verarbeiten und darstellen oder Wissen bereitstellen und
- nicht reguliert werden, also weder als Medizin-App noch als DiGA zugelassen sind.



## 4.2 Gegenwärtige Marktentwicklung

Der Markt der App Stores wird im Wesentlichen durch die beiden herstellerabhängigen Plattformen Google Play Store und Apple App Store dominiert. Weltweit werden im Google Play Store heute 3,4 Millionen und im Apple App Store 1,8 Millionen Apps angeboten.<sup>6</sup> Gesundheits-Apps finden sich vor allem in den Kategorien „Health & Fitness“ und „Medical“. Im Google Play Store entfallen 4,8% (163.000) und im Apple App Store 6,9% (121.000) auf diese Kategorien.<sup>7</sup> In den Kategorien werden auch Medizin-Apps und DiGA angeboten. Sie machen allerdings gegenüber den Gesundheits-Apps nur einen kleinen Anteil aus.

Die Anzahl der im Markt verfügbaren Apps und deren Downloadzahlen sind in den letzten Jahren deutlich gestiegen. Allein zwischen 2013 und 2018 stieg die Anzahl der weltweiten Downloads von mobilen Gesundheitsanwendungen von 1,7 Milliarden auf 4,1 Milliarden (Statista nach Research2Guidance, 2020). Bereits 2017 nutzten laut einer Umfrage des deutschen IT-Verbandes Bitkom 45% der Deutschen Gesundheits-Apps. Ebenso viele nutzten sie zwar noch nicht, konnten sich aber vorstellen, Gesundheits-Apps in Zukunft zu nutzen (Bitkom, 2017).

Treiber der hohen Dynamik im Markt ist auf der einen Seite die wachsende Nachfrage nach Gesundheitsanwendungen. Auf der anderen Seite sorgen die geringen Markteintrittsbarrieren für Anbieter für eine tagtägliche Erweiterung des Angebots. Als weiterer Verstärker der Marktentwicklung erwies sich im Jahr 2020 die Corona-Pandemie. In Europa stiegen die Downloads von Fitness-Apps im 1. und 2. Quartal 2020 um 25% an (Apptopia, 2020).

Für die vorliegende Analyse wurden Apps aus dem Apple App Store und dem Google Play Store aus den Kategorien „Health & Fitness“ und „Medical“ berücksichtigt, wobei die 1.000 downloadstärksten (monatlich<sup>8</sup>; in Deutschland) Gesundheits-Apps analysiert wurden.

Weltweit und auch in Deutschland werden im Google Play Store zahlenmäßig mehr Gesundheits-Apps angeboten. Dennoch generieren die Apps im Apple App Store im Schnitt mehr Downloads (vgl. Abbildung 2), sodass etwa zwei Drittel der analysierten Apps auf dem iOS Betriebssystem basieren.

**Betriebssysteme der downloadstärksten Apps in Deutschland (n=1000)**

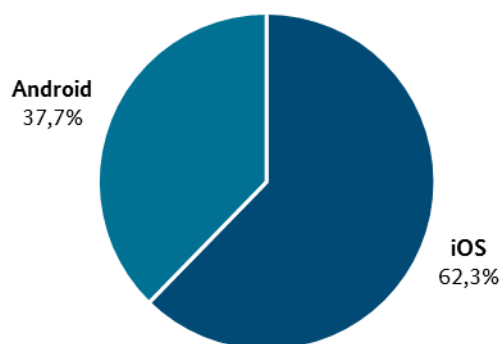


Abbildung 2: Betriebssysteme der downloadstärksten Apps in Deutschland. Quelle: 42matters 12/2020

<sup>6</sup> Diese statistischen Erhebungen sagen alleinstehend nichts über die Qualität der Apps oder über die Zufriedenheit der Marktakteure aus. Auch lässt sich an diesen Zahlen aufgrund der vielen Einflussfaktoren kein Rückschluss auf den Wettbewerbserfolg des jeweils betroffenen mobilen Betriebssystems ableiten. Vielmehr handelt es sich hierbei um eine Entscheidungshilfe hinsichtlich der Relevanz von App-Plattformen auf dem deutschen Markt.

<sup>7</sup> Stand 12/2020. Quelle: 42matters

<sup>8</sup> Monatliche Downloads: durchschnittliche Anzahl der Downloads in Deutschland für die letzten 30 Tage (Stichtag: 1.12.2020)

## 4.2.1 Marktsegmente

Ebenso wie für die Abgrenzung des Marktes, gibt es auch über seine Segmentierung bisher keinen eindeutigen Konsens.

Das Angebot von Gesundheits-Apps wird von zwei großen App-Plattformbetreibern dominiert. Smartphone-Nutzerinnen und -Nutzer haben in den zugehörigen Stores die Möglichkeit, kostenlose und zahlungspflichtige Apps mit dem Fokus Medizin und Gesundheit zu beziehen. Folglich orientieren sich Nutzerinnen und Nutzer in erster Linie an den Kategorisierungen der App Stores.

Plattformbetreiber kategorisieren das App-Angebot auf ihren digitalen Marktplätzen in der Regel nach Themenschwerpunkten. Die Segmentierung unterhalb der für den Bereich Gesundheits-Apps relevanten Kategorien erfolgt jedoch nicht einheitlich über die verschiedenen Marktplätze hinweg und unterliegt einer dynamischen Entwicklung. So werden jeweils für einen gewissen Zeitraum Trendthemen (z. B. Apps für CrossFit Fans) hervorgehoben und beworben (vgl. Tabelle 3). Eine Abgrenzung zu zertifizierten Medizin-Apps oder DiGA ist für Nutzerinnen und Nutzer aktuell nicht möglich oder direkt ersichtlich.

Tabelle 3: Kategorisierung von Gesundheits- und Medizin-Apps am Beispiel zweier App Store Betreiber.

<i>App Store I</i> <i>Kategorie „Gesundheit &amp; Fitness“</i>	<i>App Store II</i> <i>Kategorie „Gesundheit und Fitness“</i>
Premium Apps	Top-Einzelempfehlungen
Meditation	Unsere Lieblingsapps
Lifestyle	Gesund essen
Fit bleiben	Kein Studio? Kein Problem
Lauf-Apps	Apps fürs Intervallfasten
Fitness-Tracker	Yoga für jedes Level
Workout-Timer	Live-Workout-Kurse
Karten & GPS	Achtsamkeit und Meditation
Dein neuer Look	Entspannt schlafen und aufwachen
Besser schlafen	Joggen, laufen, Rad fahren
Gesundheit & Fitness	Im Spotlight
Reisen & Lokales	Fit mit der Apple Watch
Tools & Dienstprogramme	Training nach Muskelgruppen
Radfahren & Radsport	Apps für CrossFit-Fans
Rund um Versicherungen	Smoothies

Stand 25.08.2020

Auch in der Fachliteratur finden sich Ansätze einer möglichen Marktsegmentierung. Am häufigsten erfolgt die Untergliederung dabei nach Themen und Anwendungsfeldern (Evers-Wölk, et al., 2018) (Albrecht, et al., 2016) (Knöppler, et al., 2016). Hierbei konnte sich allerdings bisher keine einheitliche Segmentierung durchsetzen. Mögliche Gründe hierfür sind:

- die hohe Dynamik im Markt mit ständig wechselnden und neu hinzukommenden Themen und Anwendungsfeldern,
- die hohe Bedeutung der App-Marktplätze, die die Apps nach ihren eigenen Systematiken gliedern und dabei vor allem nachfrageorientiert vorgehen,
- das Fehlen einer Vor-Systematisierung (in den App Stores oder über andere Wege), die die Übertragung einer Segmentierung in reale Marktverhältnisse nur über manuelle Zuordnung möglich macht.

Auch weil die Übertragung der Segmentierungen in reale Marktverhältnisse nur über eine manuelle Zuordnung erfolgen kann, hat sich in der Fachliteratur bisher kein einheitlicher Ansatz der Marktgliederung etabliert. Im Rahmen der vorliegenden Untersuchung wurde deshalb, basierend auf den vorliegenden Ansätzen der Fachliteratur und den Erkenntnissen aus der durchgeführten Marktanalyse mit 1.000 betrachteten Apps, ein eigener Ansatz entwickelt:

- Fitness: Instruktionen und Tracking Workouts, sonstige Fitness-Informationen
- Ernährung & Gewicht: Diät & Fasten, Kalorienzähler, Ernährungsinformationen
- Schwangerschaft, Verhütung, Kinderwunsch: Zyklus- und Schwangerschaftstracking, Informationen
- Entspannung & Achtsamkeit: Meditation, besser schlafen, Stressbewältigung, Gedächtnistraining
- Krankheitsmanagement: Umgang mit bestimmten Krankheiten: Suchtkranke, Diabetes, Herzgesundheit
- Warnung & Erinnerung: Terminbuchung und -erinnerung, Erinnerungshilfe z. B. für Wasser trinken
- Sonstiges: Online-Apotheke, Erste Hilfe, Inhaltsstoffe-Check für Kosmetika etc.

Fitness-Apps machen mit einem Anteil von 45,8% an den betrachteten 1.000 Apps und 49,8% an den durchschnittlichen monatlichen Downloads das mit Abstand bedeutendste Marktsegment aus (Abbildung 3). Hierunter fallen u. a. Lauf-Apps oder Portale für Workout-Instruktionen. Apps im Bereich „Entspannung und Achtsamkeit“ stellen ein bedeutendes und wachsendes Segment dar. Sie machen 14,8% der Apps und 11,6% der Downloads aus. Apps, die sich mit dem Thema „Ernährung und Gewicht“ befassen, machen 9,3% der Apps aus und sind mit einem Anteil von 14,6% an den Downloads vergleichsweise stark vertreten.

Anders sieht das Bild bei Apps im Bereich „Krankheitsmanagement“ aus: Apps, die beispielsweise bei der Raucherentwöhnung unterstützen oder Hilfestellung für Diabetikerinnen und Diabetiker bieten, machen einen zahlenmäßigen Anteil von 9,1% aus, generieren aber lediglich 2,5% der Downloads, weil ihre jeweilige Zielgruppe insgesamt kleiner ist. Gegensätzlich sieht das Bild demgegenüber bei Apps aus, die Lösungen im Bereich des „ganzheitlichen Gesundheitsmanagements“ anbieten – mit einem zahlenmäßigen Anteil von 6,2% gegenüber einem Anteil von 12,3% an den Downloads. Hierunter fallen auch Apps von Smartphone-Herstellern, die standardmäßig eigene Lösungen für Tracking und Analyse der eigenen Gesundheitsdaten anbieten.

Anteil der Marktsegmente nach Anzahl der Apps und Downloadzahlen (n=1000)

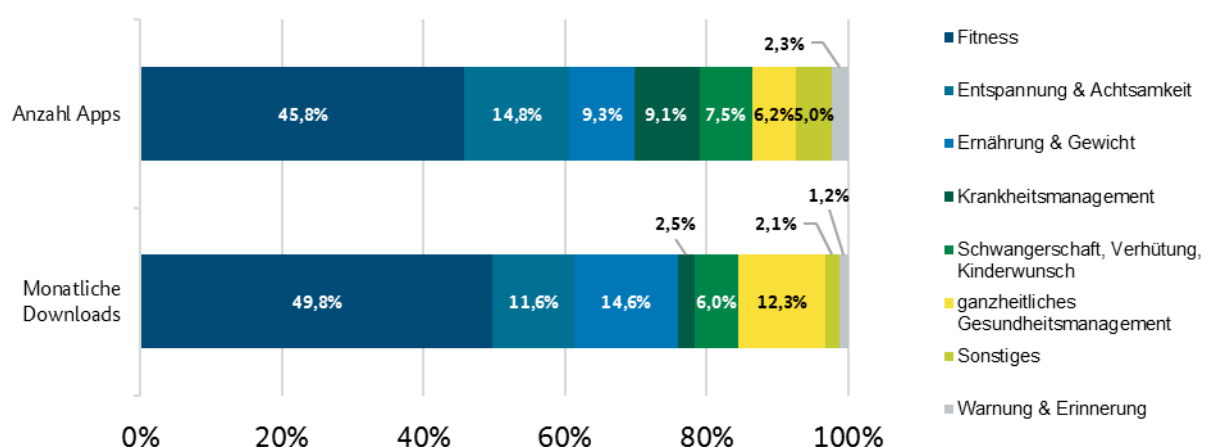


Abbildung 3: Anteil der Marktsegmente nach Anzahl der Apps und Downloadzahlen. Quelle: 42matters 12/2020.

## 4.2.2 Downloadzahlen

Die Verteilung der Downloads je App spiegelt den hohen Wettbewerb und die bereits bestehende Konzentration im Markt wider: Die 1.000 downloadstärksten Apps werden im Mittel 8.271-mal pro Monat heruntergeladen. Allein die 30 downloadstärksten Apps vereinen etwa 51% aller Downloads auf sich und werden im Schnitt 140.857-mal pro Monat heruntergeladen. Die 10 downloadstärksten Apps in Deutschland vereinen bereits in Summe einen Anteil von 21% an den monatlichen Downloads auf sich.

## 4.2.3 Anbieterstruktur

Die hohen Potenziale, die dem Markt für Gesundheits-Apps zugeschrieben werden, sowie die geringen Markteintrittshürden für Anbieter führen sowohl zu einer hohen Dynamik und Vielfalt der angebotenen Apps als auch zu einer hohen Anzahl verschiedener Anbieter im Markt. Etablierte Player aus dem Gesundheitswesen machen dabei nur einen kleinen Anteil aus. Zu möglichen Gründen treffen Evers-Wölk et al. folgende Einschätzung (Evers-Wölk, et al., 2018):

„Etablierte Akteure aus dem Gesundheitswesen tun sich aufgrund fehlender Technologiekompetenzen dagegen eher schwer, ihre Erfahrungen in der Gesundheitsförderung und -beratung für die Entwicklung neuer Gesundheits-Apps und mHealth<sup>9</sup>-Angebote nutzbar zu machen.“

Demgegenüber handelt es sich beim Großteil der Anbieter im Markt um privatwirtschaftliche Akteure. Hierunter befinden sich auch viele Startups: In einer Umfrage von Research2Guidance gaben 54% der befragten Anbieter von Gesundheits-Apps an, dass sie erst in den vergangenen drei Jahren in den Markt eingetreten seien (Evers-Wölk, et al., 2018) nach (Research2Guidance, 2015).

Der Markt ist geprägt von spezialisierten Anbietern, die sich auf ein Anwendungsgebiet fokussieren und folglich meist nur eine App anbieten. Sechs von zehn der Top Gesundheits-App-Anbieter in Deutschland haben nur eine Anwendung pro mobilen Technologiebereich im Portfolio. Die Zuordnung ist dabei nicht immer eindeutig, da Anbieter die Apps zum Teil unter einem abgewandelten Namen anbieten oder durch verschiedene Tochtergesellschaften vertreiben.

## 4.2.4 Herkunft der Anbieter

Abbildung 4 gibt einen Einblick in die Herkunft der Anbieter. Die Analyse beschränkt sich aufgrund der Datenlage auf Apps und Anbieter aus dem Google Play Store. Diese machen 377 der insgesamt 1.000 analysierten Apps aus.

<sup>9</sup> mHealth steht für Mobile Health und meint Gesundheitsanwendungen, die auf mobilen Geräten angeboten werden.

**Herkunft der Anbieter (nur Google Play Store) (n=377)**

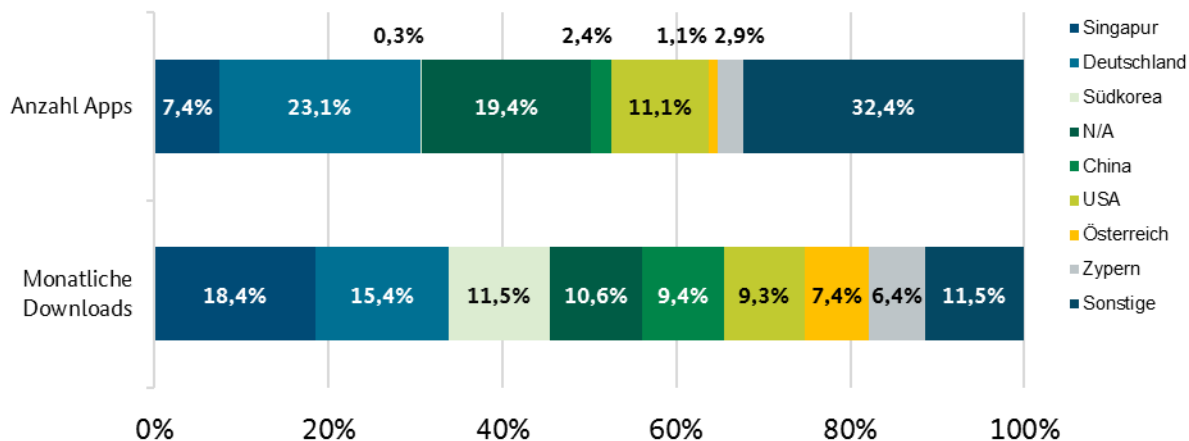


Abbildung 4: Herkunft der Anbieter (nur Google Play Store). Quelle: 42matters 12/2020.\*

\*Aufgrund der Datenlage kann die Herkunft der Anbieter nur für den Google Play Store analysiert und dargestellt werden. Die Anteile für beide Stores können deshalb abweichen.

Auch wenn sich dies nicht unmittelbar in der Abbildung zeigt, spiegelt die Analyse der Herkunftsländer die bereits gezeigte hohe Konzentration der Downloadzahlen auf einzelne Anbieter im Markt wider. Besonders deutlich zeigt sich dies z. B. bei den Anbietern aus Singapur. Während lediglich 7,4% bzw. 27 der Apps von Anbietern aus Singapur angeboten werden (26 hiervon vom selben Anbieter), generieren diese 18,4% der monatlichen Downloads im Google Play Store.

Deutsche Anbieter stellen im Google Play Store die größte Anbietergruppe dar und generieren hier im Schnitt 9.153 monatliche Downloads pro App. Vier von ihnen sind unter den Top 10 der downloadstärksten Apps des deutschen Marktes zu finden. Eine Auswertung der 87 Apps deutscher Anbieter im Google Play Store zeigt, dass diese Anbieter mit 18,4% überdurchschnittlich häufig Apps aus dem Segment Krankheitsmanagement und mit 29,9% unterdurchschnittlich häufig Fitness-Apps im Vergleich zu Anbietern aus anderen Herkunftsländern anbieten (vgl. Abbildung 5).

**Anzahl der Apps nach Marktsegmenten für deutsche Anbieter (nur Google Play Store) (n=87)**

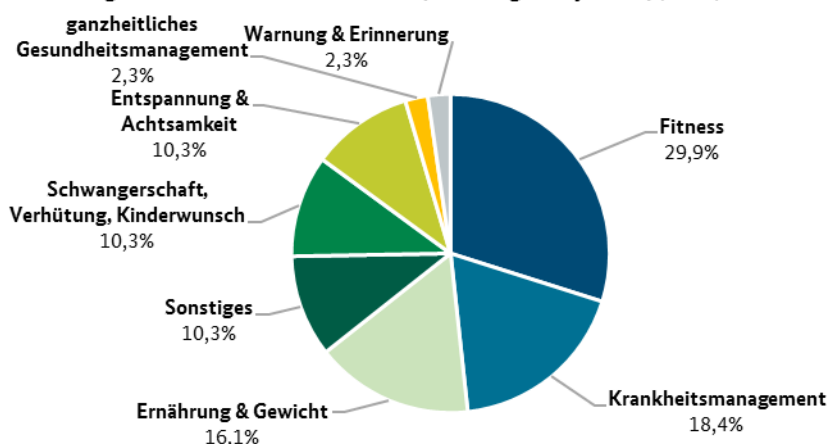


Abbildung 5: Anzahl der Apps nach Marktsegmenten für deutsche Anbieter. Quelle: 42matters 12/2020.\*

\*Aufgrund der Datenlage kann die Herkunft der Anbieter nur für den Google Play Store analysiert und dargestellt werden. Die Anteile für beide Stores können deshalb abweichen

## 4.2.5 Geschäftsmodell der Anbieter

Sowohl die eigene Marktanalyse als auch die Literatur kommen zur Erkenntnis, dass ein Großteil der Anbieter von Gesundheits-Apps nur geringe Umsätze über direkte Erlösmodelle – den Verkauf von Apps, In-App-Käufe oder Abo-Modelle – erzielen können. Folgende Gründe können in diesem Kontext diskutiert werden:

- der hohe Wettbewerbsdruck im Markt mit niedrigen Eintrittsbarrieren und einer tagtäglich rasant steigenden Zahl konkurrierender Produkte und Anbieter sowie eine hohe Konzentration auf einzelne Anbieter und Apps,
- die in Deutschland vergleichsweise geringe Zahlungsbereitschaft für gesundheitsbezogene Zusatzleistungen,
- die generell geringe Zahlungsbereitschaft für digitale Anwendungen (Evers-Wölk, et al., 2018),
- die insgesamt geringe Bedeutung direkter Erlösmodelle gegenüber indirekten Erlösmodellen (insbesondere aus der Nutzung der erhobenen Nutzerdaten).

Von den 1.000 analysierten Apps wird lediglich eine App (0,1%) nicht kostenfrei angeboten. In der gesamten Kategorie „Health & Fitness“ ist der Anteil mit 6% im iOS Store und 3% im Google Play Store etwas höher. Direkte Erlöse generieren die Anbieter vor allem über In-App-Käufe – einmalige Käufe z. B. zur Freischaltung von Zusatzfunktionen oder Abonnements. 56% der analysierten Apps bieten In-App-Käufe an. Der Einstiegspreis liegt dabei im Android Store bei durchschnittlich 1,87 Euro<sup>10</sup>. Maximal können Käufer hier im Schnitt 25,23 Euro pro In-App-Kauf ausgeben. Dabei sind die Unterschiede zwischen den im Detail verlangten Preisen allerdings sehr hoch: der höchste Preis für einen In-App-Kauf liegt für die untersuchte Stichprobe bei 336 Euro (42matters 12/2020).

Darüber hinaus monetarisieren viele Anbieter ihre Apps über Erlösflüsse außerhalb der App Stores. Zu den wichtigsten Erlösquellen zählen die Schaltung von Werbung, der Verkauf verwandter Produkte wie Arznei- oder Nahrungsergänzungsmittel, bei denen die App rein als Mittel zur Kundenakquise genutzt wird, und der Verkauf von Nutzerdaten, um (individualisierte) Werbung für die Nutzerinnen und Nutzer zu schalten.

Diese Weitergabe von Daten ist insbesondere mit Blick auf die IT-Sicherheit sowie die mögliche Sensibilität der erfassten Daten im Gesundheitsbereich als kritisch anzusehen. Mit einer steigenden Anzahl an Schnittstellen nehmen die potentiellen Angriffsvektoren zu. Dadurch steigt auch das Risiko eines ungewollten Abflusses von Daten.

Nach Aussage der im Rahmen dieser Studie befragten Expertinnen und Experten planen einige der deutschen Start-ups im Markt einen mittelfristigen Wechsel vom Markt für Gesundheits-Apps in den Markt für Medizin-Apps. Sie starten mit einer Gesundheits-App und nutzen die Fokussierung auf Endbenutzerinnen und -nutzer für die Erprobung und Weiterentwicklung ihrer Anwendung. In diesem Zusammenhang planen sie auch die Monetarisierung ihrer App über eine Aufnahme in das DiGA-Verzeichnis. Die Zulassung fokussiert momentan allerdings vor allem auf Anwendungen im Bereich von Therapie und Diagnose.

<sup>10</sup> Angabe im Datensatz in US-Dollar. Umrechnungskurs vom 15.03.2021

## 5 Aktuelle Trends und perspektivische Entwicklung des Marktes

Zentraler Treiber für das nachfrageseitige Wachstum des Marktes war in den vergangenen Jahren die von Jahr zu Jahr steigende Marktdurchdringung von Smartphones und anderen mobilen Endgeräten. 2019 besaßen 81,8% der Deutschen<sup>11</sup> ein Smartphone. 2012 waren es erst 36% (Statista, 2021). Mit den wachsenden Nutzerzahlen von Smartphones stieg auch die Zahl der Nutzerinnen und Nutzer von Gesundheits-Apps.

Auch wenn dieser Markttreiber für die kommenden Jahre aufgrund der mittlerweile hohen Marktdurchdringung nur noch eine nachgeordnete Rolle spielt, wird sich das dynamische Wachstum, welches der Markt für Gesundheits-Apps in den vergangenen Jahren weltweit und in Deutschland gezeigt hat, auch auf absehbare Zeit weiter fortsetzen. Dieses Wachstum zeigt sich u. a. in den stetig steigenden Download- und Nutzerzahlen, der steigenden Aufmerksamkeit, welche Hubs und Gründerzentren im Themenfeld Digital Health erhalten, sowie in den hohen Summen, die gegenwärtig in diesen Markt investiert werden.

### 5.1 Die Nachfrage wächst

Gesellschaftliche Trends werden auch in den kommenden Jahren für eine positive Entwicklung der Nachfrage an mobilen Anwendungen im Gesundheitsbereich sorgen. Begriffe wie „E-Patient“ oder „Quantified Self“ umschreiben das veränderte Verhältnis der Nutzerinnen und Nutzer zu ihrer eigenen Gesundheit. Dieses ist von einem zunehmend selbstbestimmten und aktiven Umgang mit der eigenen Gesundheit geprägt und sorgt sowohl im Bereich von Gesundheits-Apps als auch bei Medizin-Apps für eine wachsende Nachfrage. Verbraucherinnen und Verbraucher – ganz gleich ob gesund oder krank – nehmen zunehmend ihre eigene Gesundheit selbst in die Hand und fragen aktiv Gesundheitsinformationen nach (E-Patient). Eigene Körpermessdaten werden zudem dokumentiert, analysiert und ausgetauscht (Quantified Self) (Knöppler, et al., 2016).

### 5.2 Die Angebotsbreite und -tiefe nimmt zu

Mit Blick auf das Angebot werden nach Einschätzung der befragten Expertinnen und Experten die aktuell ohnehin eher diffusen Grenzen zwischen den einzelnen Segmenten im Markt für Gesundheits-Apps sowie zwischen Gesundheits- und Medizinanwendungen abnehmen. Hierfür sprechen auch Vorhaben des Gesetzgebers, wie beispielsweise das Digitale-Versorgung-Gesetz oder das Digitale-Versorgungs-und-Pflege-Modernisierungs-Gesetz.

Im Markt für Gesundheits-Apps zeigt sich dies besonders im erwarteten Bedeutungszuwachs von Apps im ganzheitlichen Gesundheitsmanagement. Ihr Marktanteil wird voraussichtlich weiter zunehmen, da App-Anbieter unterschiedliche Themen und Anwendungsbereiche (Fitness, Ernährung, Achtsamkeit etc.) miteinander verbinden und damit die Angebotsbreite einzelner Anwendungen erhöhen.

Gleichzeitig wird eine stärkere Integration von Angeboten entlang der Wertschöpfungskette und damit eine Erhöhung der Angebotstiefe erwartet. Sprich: Anbieter fokussieren sich nicht mehr nur auf Lösungen zur Prävention, sondern erweitern ihre Lösungen Schritt für Schritt in Richtung medizinischer Anwendungen für Diagnose und Therapie. Sichtbar ist dies bereits heute: So wurde beispielsweise bei einer App, welche die Buchung von Arztterminen ermöglicht und Nutzerinnen und Nutzer an diese erinnert, das Leistungsangebot Schritt für Schritt ausgeweitet, sodass heute u. a. auch digitale Arztprechstunden über die Anwendung durchgeführt werden können.

---

<sup>11</sup> Personen ab 14, die ein internetfähiges Smartphone oder Handy besitzen.

Durch die systematische Erweiterung der Anwendungsgebiete von Gesundheits-Apps nicht nur auf andere Marktsegmente, sondern auch auf medizinische Anwendungen wird die dynamische Entwicklung den Wettbewerbsdruck auf Anbieter im klassischen Gesundheitsmarkt erhöhen. Die Kopplung von Gesundheits-Apps, die Körpermessdaten erfassen, visualisieren und analysieren, mit Medizinanwendungen ermöglicht die stärkere Individualisierung und Personalisierung von Medizin und Gesundheit. Hierdurch bietet sich ein hohes Innovationspotenzial, dass zukünftig voraussichtlich stärker genutzt wird.

### 5.3 Datengetriebene Lösungen und künstliche Intelligenz treiben die technologische Entwicklung

Technologische Trends, die in vielen Branchen und Märkten für Innovationsimpulse sorgen, treiben auch die Entwicklung im Markt für Gesundheits-Apps (Knöppler, et al., 2016). Einer dieser Trends war bereits in den vergangenen Jahren die „Gamification“ der Anwendungen:

„Indem der menschliche Spieltrieb durch die Apps aktiviert wird, sollen erwünschte gesundheitsbezogene Verhaltensänderungen hervorgerufen, die Motivation gesteigert, positive Angewohnheiten unterstützt und verfestigt werden. Wesentlich bei der Gamification ist der Einsatz von Elementen, die auch in herkömmlichen Computerspielen zu finden sind: Hierzu zählen narrative Elemente im Sinne eines fortlaufenden Handlungsstranges, das Sammeln von virtuellen Gegenständen, digitale und realweltliche Belohnungen, aber auch sozialer Druck, die erzielten Ergebnisse mit anderen zu teilen.“ (Evers-Wölk, et al., 2018)

Beliebte Gamification-Anwendungen in Gesundheits-Apps sind beispielsweise virtuelle Orden oder Punkte, die Nutzerinnen und Nutzer für besondere Leistungen (gelaufene Strecken, absolvierte Übungen etc.) erhalten und das Teilen der Erfolge mit der Community, welche die Nutzerin oder den Nutzer wiederum durch das „Liken“ der Leistungen motiviert (Duttweiler, et al., 2016).

Ein zentraler Trend ist zudem die zunehmende Erfassung und Analyse von Körpermessdaten. Dieser wird nachfrageseitig durch das wachsende Gesundheitsbewusstsein in der Bevölkerung mit spezifischen Ausprägungen wie der Quantified Self-Bewegung (s. o.) getrieben. Hier werden alle Sensoren und Schnittstellen des Smartphones verwendet, wobei die hieraus erfassten Daten der stetigen Entwicklung neuer Anwendungskontexte für Gesundheits-Apps dienen. So wird zum Beispiel die Stimmerkennung des Smartphones genutzt, um Schlafanomalien bei der Nutzerin bzw. dem Nutzer zu erkennen. Gleiches gilt für Aktivitätsdaten aus „Wearables“, also tragbaren, teilweise in Kleidung eingearbeiteten Sensoren, welche in den vergangenen Jahren an Bedeutung gewonnen haben.

Die immer größeren Datenmengen – Stichwort „Big Data“ – schaffen die Grundlage für den zunehmenden Einsatz von Künstlicher Intelligenz (KI). KI wird vor allem als Innovationstreiber für medizinische Anwendungen ein riesiges Potenzial zugeschrieben (z. B. im Bereich der individuellen Diagnose und Therapie), aber auch bei Gesundheits-Apps wird sie in kommenden Jahren die Entwicklung im Markt treiben.

Über KI-Systeme eröffnen sich für Anbieter von Gesundheits-Apps neue Wege, um Daten (auch aus unterschiedlichen Quellen) zu analysieren und Prognosen zu entwickeln. Verschiedene Daten, z. B. Alter, Gewicht, Geschlecht oder Ernährungsgewohnheiten, werden mit Messergebnissen des Smartphones oder eines Wearables kombiniert und gemeinsam ausgewertet. Hierdurch sind Apps u. a. in der Lage, den Nutzerinnen und Nutzern ein umfassendes Bild der eigenen Gesundheit aufzuzeigen und ihnen individuelle Hinweise für ein gesundheitsförderndes Verhalten zu geben (Evers-Wölk, et al., 2018).

Die enormen Chancen, die KI-Anwendungen für die Entwicklung von Gesundheits-Apps bieten, können durch den Großteil der Anbieter im Markt allerdings bisher nicht genutzt werden. Anbieter mit vergleichsweise geringen Download- und Nutzerzahlen, welche den Großteil der Anbieter im Markt ausmachen, stehen aktuell noch vor der Herausforderung, dass sie nicht auf die hierfür notwendigen Daten zurückgreifen



können, um ihre KI-Anwendungen zu trainieren. So gibt es kaum Zugänge zu gesicherten, auf klaren Standards basierenden Daten und Datenpools, über die verschiedene Daten miteinander verknüpft werden können.

## 5.4 Konzentration auf einzelne Anbieter nimmt zu

Bereits heute schaffen es einige wenige Anbieter, vor allem in Segmenten mit einer breiten Nutzerbasis wie Fitness oder Ernährung, hohe Marktanteile zu erzielen. Diese Entwicklung wird sich aller Voraussicht nach auch perspektivisch weiter fortsetzen.

Ein wichtiger Treiber für diese Entwicklung ist die technologische Entwicklung hin zu KI-gestützten Anwendungen. Über die hierfür notwendigen großen Datenpools verfügen bisher nur die großen Anbieter im Markt für Gesundheits-Apps sowie etablierte Tech-Unternehmen, die ihre Aktivitäten im Markt gegenwärtig verstärkt ausbauen. Die etablierten Tech-Unternehmen verfügen bereits über eine hohe Nutzerbasis und damit große Datenpools aus anderen Anwendungsfeldern, auf welche sie beim Eintritt in den Markt für Gesundheits-Apps zurückgreifen können.

Gleichzeitig begünstigt auch der Trend hin zu einer Erweiterung der Angebotsbreite und der Verbindung verschiedener Anwendungsbereiche (Fitness, Ernährung, Achtsamkeit etc.) (vgl. 5.2), eine weitere Konzentration der Download- und Nutzerzahlen auf einzelne Anbieter im Markt. Denn die Entwicklung ganzheitlicher Lösungen erfordert ein gegenüber Nischenlösungen deutlich höheres Investitionsbudget. Über dieses verfügen vor allem große Anbieter.

Um sich in diesem dynamischen Wettbewerbsumfeld positionieren zu können, sind eine schnelle Entwicklung und eine hohe Marktpräsenz wichtig, welche sich große Anbieter auch durch die Übernahme kleinerer Anbieter sichern können. Um in diesem Marktgefüge dennoch einen Platz einnehmen zu können, suchen Start-ups bereits heute häufig Partnerschaften mit großen Tech-Unternehmen, über die sie ihre Produkte am Markt platzieren.

Eine Konzentration der Download- und Nutzerzahlen auf einzelne Anbieter ist allerdings nicht gleichbedeutend mit einer Konsolidierung der Anbieterstrukturen im Markt auf einzelne wenige Anbieter, die einen Großteil der Apps anbieten. Eine solche Konsolidierung ist aktuell noch nicht sichtbar, könnte sich aber perspektivisch entwickeln.

## 6 IT-sicherheitstechnische Betrachtung von Gesundheits-Apps

Aufbauend auf dem Überblick über die aktuelle Marktsituation und die perspektivische Entwicklung des Marktes für Gesundheits-Apps werden die Apps im Folgenden aus der Perspektive der IT-Sicherheit betrachtet. In Kapitel 6 erfolgt die Betrachtung auf Ebene des Marktes, in Kapitel 7 auf Ebene einzelner Apps, die im Rahmen einer IT-sicherheitstechnischen Untersuchung analysiert wurden.

### 6.1 Sensibilität der Daten

Das Risiko, dass durch die Nutzung von Gesundheits-Apps für die einzelne Nutzerin respektive den einzelnen Nutzer entsteht, wird u. a. dadurch determiniert, ob und welche Daten verarbeitet werden. Nicht alle Gesundheits-Apps verarbeiten (personenbezogene) Daten. Die funktionale Bandbreite der Angebote reicht von der reinen Vermittlung von Wissen bis zur umfassenden Verarbeitung von Gesundheitsdaten.

Wenn Daten verarbeitet werden, ist die Sensibilität der verarbeiteten Daten mitentscheidend darüber, welche mögliche Tragweite ein IT-sicherheitstechnischer Angriff für die einzelne Nutzerin oder den einzelnen Nutzer erlangt.

Um das Risiko, das durch die Nutzung einer bestimmten Anwendung, beispielsweise einer Gesundheits-App, entsteht, bewerten zu können, ist immer eine individuelle Prüfung erforderlich. Eine solche Prüfung sollte eben auch durch den Betreiber der jeweiligen App bereits im Rahmen des Entwicklungsprozesses vollzogen werden, sodass entsprechende Schutzmaßnahmen entsprechend des notwendigen Schutzbedarfs konzipiert und berücksichtigt werden können. Orientierung für diese Schutzbedarfsfeststellung kann der BSI-Standard 200-2 „IT-Grundschutz-Methodik“ bieten. In diesem wird der Schutzbedarf in die Kategorien „normal“, „hoch“ und „sehr hoch“ untergliedert. Sofern in Gesundheits-Apps eine Datenerfassung erfolgt, ist in der Regel aber von einem hohen oder sehr hohen Schutzbedarf auszugehen.

Wie die Marktanalyse zeigte, ist der Markt der Gesundheits-Apps von hoher Volatilität geprägt. Damit verbunden ist, dass sich das Angebot von einzelnen Apps über den Lebenszyklus hinweg weiterentwickelt und ausgeweitet bzw. ergänzt wird. Die Bewertung der Schutzbedürftigkeit von Daten und der Verfügbarkeit von Systemen ist somit kein einmaliger Schritt im Rahmen der initialen Produktentwicklung, sondern sollte als immanenter Systembestandteil verstanden werden.

### 6.2 Prüfmechanismen der App Stores

Die Betreiber von App Stores ergreifen ebenfalls Maßnahmen zur Überprüfung der Qualität eingereicherter Apps. Dabei prüfen sie die Apps, soweit möglich den Programmcode sowie das Verhalten bezüglich einer Reihe von erwünschten bzw. unerwünschten Eigenschaften.

Für die Entwicklerinnen und Entwickler von mobilen Apps stellen die Plattformbetreiber entsprechende Informationen auf Ebene von Richtlinien und Best Practices zur Verfügung. Diese werden jedoch nicht mit konkreten technischen Prüfkriterien hinterlegt.

Mit Blick auf die Gesamtmenge der Apps, die in den App Stores eingereicht wird, ist davon auszugehen, dass der größte Teil der Prüfungen automatisiert erfolgt. Bei solchen automatisierten Prüfungen ist zu erwarten, dass diese auf bekannte schädliche Inhalte, wie Trojaner, Codefragmente oder nachladende Funktionen, abzielen. Im Vergleich zu einer manuellen Prüfung durch Sicherheitsforscherinnen und -forscher ergibt sich zwangsläufig eine geringere Prüftiefe.

Für die App Store Betreiber liegt der Fokus nicht primär auf der IT-Sicherheit, sondern es stehen Kriterien wie die Gesamtqualität der Nutzererfahrung, der Konformitätscheck zum eigenen Geschäftsmodell oder

auch die Markensicht des Herstellers im Vordergrund. Im Folgenden werden die Erkenntnisse aufgeführt, die sich über die Prüfkriterien und -verfahren der beiden Plattformen aufgrund öffentlich zugänglicher Dokumentation ermitteln ließen.

Apple stellt seine Richtlinien für den Prüfungsprozess bereit (App Store Review Guidelines) und beschreibt darin Anforderungen für die Aufnahme von Apps in den App Store (Apple Inc., 2021).

Die Anforderungen gliedern sich in die Bereiche Sicherheit (im Sinne einer gefahrlosen Nutzung und angenehmen, unschädlichen Nutzererfahrung), Performanz, geschäftliche Aspekte (vor allem bzgl. Bezahlvorgängen), Design und rechtliche Rahmenbedingungen.

Die meisten Überschneidungen mit den Inhalten dieser Studie ergeben sich in den Abschnitten für Sicherheit und rechtliche Rahmenbedingungen. So beinhaltet der Teil zur Sicherheit eine breite Sicht, die beispielsweise auch auf physische Schäden und den Schutz von Minderjährigen eingeht. Der Abschnitt zu den Themen IT-Sicherheit / Datenschutz ist vergleichsweise kurz und verweist hauptsächlich darauf, dass die Sicherheitsvorkehrungen und die Verarbeitung von Nutzerdaten in Einklang mit dem „Apple Developer Program License Agreement“ stehen müssen. Dieses Agreement ist jedoch nur im Rahmen des „Apple Developer Program“ für angemeldete Entwicklerinnen und Entwickler einsehbar.

Des Weiteren existiert eine „Übersichtsseite zur Sicherheit bei Apps“ (Apple Inc., 2021). Auf dieser werden einige allgemeine Sicherheitsrichtlinien von Apple-Systemen erklärt und verschiedene Sicherheitsfunktionen vorgestellt. Die Informationen beziehen sich jedoch primär auf Sicherheitsmaßnahmen der Geräte selbst, nicht auf Prüfmechanismen des App Stores.

Als Schutzmechanismus im Google Play Store existiert „Google Play Protect“ (Google, 2021). Es handelt sich dabei um einen multifunktionalen Dienst, der primär auf dem jeweiligen Endgerät läuft. Google Play Protect prüft dabei u. a. Apps der Nutzerinnen und Nutzer bei Installation auf den Endgeräten (on-device protection), aber auch Apps, die Entwicklerinnen und Entwickler in den Google Play Store einstellen wollen (cloud-based security). Neben Sicherheitstests werden Kompatibilitäts- und Konformitätstest durchgeführt. Hierzu wurden Programmrichtlinien für Entwicklerinnen und Entwickler veröffentlicht, die sich in folgende Bereiche gliedern (Google, 2021):

- Inhaltsbeschränkungen,
- Geistiges Eigentum,
- Datenschutz, Täuschung und Missbrauch von Geräten,
- Unerwünschte Software für Mobilgeräte,
- Monetarisierung und Werbung,
- Store-Eintrag und Werbung,
- Spam und Mindestanforderungen an die Funktionalität und
- Durchsetzung von Richtlinien.

Vor Aufnahme in den App Store durchlaufen die Apps eine zentrale Überprüfung. Wie genau das Unternehmen dabei vorgeht, wird nicht kommuniziert. Unabhängige Untersuchungen haben jedoch gezeigt, dass die Erkennungsquoten von Apps, die Schadcode enthalten, durch Play Protect deutlich geringer ausfallen als bei anderen Lösungen (z. B. Bitdefender Mobile Security, Norton Mobile Security) (tom's guide, 2021).

## 6.3 Quantitative Anbieterbefragung – IT-sicherheitstechnische Maßnahmen der Anbieter

Anbieter von Gesundheits-Apps wenden verschiedene Maßnahmen an, um ihre Apps vor Angriffen zu schützen. So werden z. B. durch die verschlüsselte Ablage und den verschlüsselten Transfer von Daten, die

Authentisierung ihrer Nutzerinnen und Nutzer, automatische Updates für Bibliotheken Dritter oder Maßnahmen zur Verhinderung von Reverse Engineering bereits sehr wirkungsvolle Maßnahmen umgesetzt.

Um Einsichten darüber zu gewinnen, in welchem Umfang die Anbieter von Gesundheits-Apps gängige Maßnahmen zum Schutz ihrer Apps vornehmen, wurde im Rahmen der Studie eine standardisierte Befragung von Anbietern durchgeführt.

### 6.3.1 Untersuchungsdesign der Befragung und Zusammensetzung der Stichprobe

Die Befragung wurde als Online-Umfrage durchgeführt und fand über einen achtwöchigen Zeitraum zwischen November 2020 und Januar 2021 statt. Die Rekrutierung der Teilnehmenden erfolgte über die direkte Ansprache von Anbietern und über die Veröffentlichung des Befragungslinks auf den Internetkanälen des BSI. Für die direkte Ansprache wurden Anbieter von Gesundheits-Apps identifiziert und über die im jeweiligen App Store hinterlegte Kontaktadresse per E-Mail angeschrieben.

An der Befragung nahmen 84 Anbieter von Gesundheits-Apps teil. Über eine Eingangsfrage wurde verifiziert, dass alle teilnehmenden Anbieter eine Gesundheits-App im Portfolio haben.

Insgesamt 50 Teilnehmerinnen und Teilnehmer beantworteten alle Fragen, während 34 die Befragung frühzeitig beendeten. Für die beantworteten Fragen wurden dennoch alle Antworten ausgewertet. Die Stichprobengröße divergiert hierdurch zwischen den einzelnen Fragen. Die Teilnehmenden konnten die Fragen auch durch die Auswahl der Option „keine Angaben“ überspringen. Der jeweilige Anteil der Befragten, die keine Angaben zur Frage machten, wird in den Grafiken aufgeführt.

Im Fokus der Befragung stand die Abfrage zu den IT-sicherheitstechnischen Maßnahmen der Anbieter. Darüber hinaus wurden auch generelle Informationen zum Anbieterunternehmen bzw. der angebotenen App sowie das Interesse an einem Austausch mit dem BSI abgefragt. Da keine gezielte Ansprache von Einzelpersonen erfolgte und im Rahmen der Befragung keine Fragen zum Hintergrund der teilnehmenden Unternehmensvertreterinnen und -vertreter gestellt wurden, kann keine Aussage über die Position oder die technische Expertise der oder des Befragten im Unternehmen getroffen werden und somit nicht beurteilt werden, ob alle Befragten über das notwendige fachliche Know-how für die Beantwortung jeder einzelnen Frage verfügten.

Als Basis für die Entwicklung der technischen Fragestellungen diente u. a. die Technische Richtlinie des BSI TR-03161 zu "Sicherheitsanforderungen an digitale Gesundheitsanwendungen"<sup>12</sup>. Hier werden zentrale Prüfaspekte benannt, die im Rahmen der Befragung adressiert wurden.

Hinsichtlich der Segmentzuordnung machen Anbieter von Apps aus dem Bereich „Krankheitsmanagement“ mit 22,6% den größten Anteil der Befragungsteilnehmenden aus. Auf Basis der Marktanalyse wurde ein realer Anteil von 9,1% ermittelt. Ihr Anteil ist damit in der Stichprobe überrepräsentiert. Im Vergleich zur Marktanalyse unterrepräsentiert sind hingegen Anbieter von Fitness-Apps. In der Marktanalyse wurde ein Anteil von 45,8% ermittelt, während ihr Anteil an der Stichprobe 11,9% beträgt.

---

<sup>12</sup> vgl. <https://www.bsi.bund.de/TR-03161>

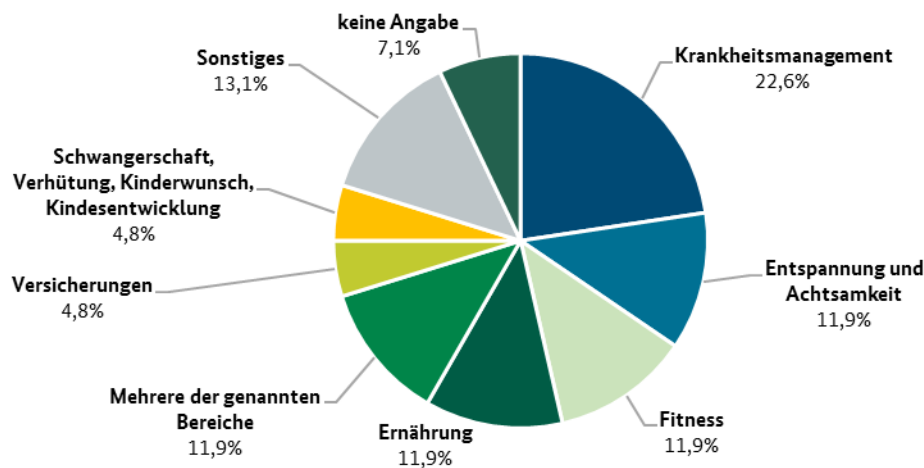


Abbildung 6: In welchen Bereich würden Sie Ihre App eingliedern? (n=84)

Die Mehrheit der befragten Anbieter stellt ihr App-Angebot für mehrere Betriebssysteme bereit: Bei 91,7% der Anbieter ist die App für Android und bei 77,4% für das iOS Betriebssystem erhältlich. Die wichtigsten Vertriebskanäle der befragten Anbieter sind mit 88,1% und 72,6% die App Stores von Google und Apple. 26,1% der Anbieter bieten ihre App auch über ihre eigene Webseite an.

Auf Basis der im Vergleich zur Grundgesamtheit geringen Zahl von Teilnehmenden und der im Vergleich zu Grundgesamtheit abweichenden Branchenzusammensetzung der Stichprobe muss festgehalten werden, dass es sich nicht um eine für die Grundgesamtheit der Anbieter von Gesundheits-Apps im deutschen Markt repräsentative Stichprobe handelt. Erkenntnisse aus der Stichprobenanalyse geben allerdings Hinweise auf mögliche Merkmalsausprägungen innerhalb der Grundgesamtheit.

## 6.3.2 Ergebnisse aus der Befragung

### 6.3.2.1 Verarbeitete Daten

Die Tragweite des Risikos, welches von einem potenziellen Angriff auf Apps ausgeht, wird insbesondere durch die Sensibilität der hier erfassten und verarbeiteten Daten bestimmt. 52,6% der befragten Anbieter geben an, dass sie technische Daten (z. B. Geräteinformationen, Standort, App-Nutzung) erheben; 47,4% persönliche Daten wie z. B. Name, Alter, Geschlecht oder Wohnort und 42,3% gesundheitliche Daten, zu denen z. B. Gewicht, Körpertemperatur oder Erkrankungen zählen. Auch wenn die Ergebnisse der Befragung nicht repräsentativ sind, wird laut der Befragten deutlich, dass bei Weitem nicht alle Gesundheits-Apps technische, persönliche und gesundheitliche Daten der Nutzerinnen und Nutzer verarbeiten. Bei einem nicht unerheblichen Teil der Apps steht die Vermittlung von Wissen (z. B. Instruktionen zu Fitness-Übungen oder Entspannungs-Übungen) im Fokus.

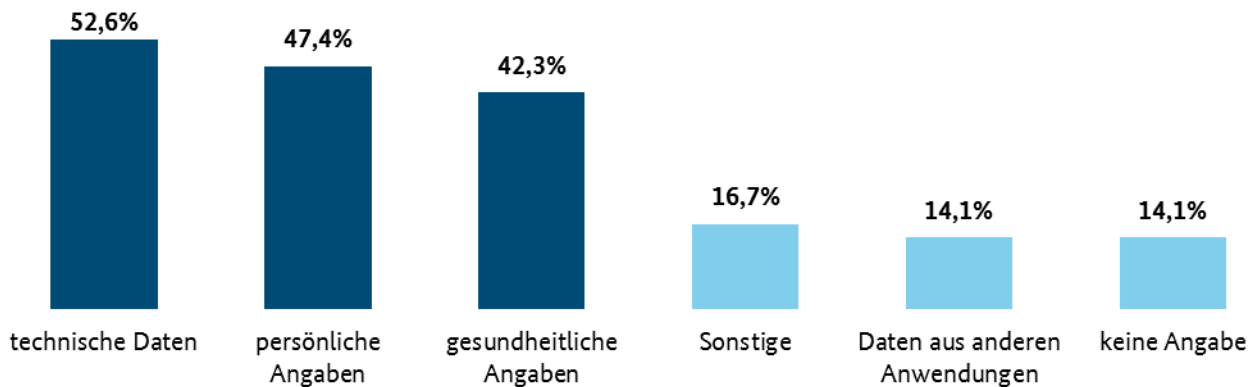


Abbildung 7: Welche Datenkategorien werden erhoben? (n=78)

Gesetzliche Vorgaben regeln, dass Anbieter von Apps ihrer Nutzerinnen und Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten“ unterrichten müssen (Artikel 13, 14 DSGVO).

Der gängigen Praxis entspricht es, dass Nutzerinnen und Nutzer zentral über die Datenschutzbestimmungen informiert werden: Bei 32,1% der Anbieter werden sie über die Datenschutzbestimmungen informiert, können diese jedoch nur akzeptieren. Bei 29,5% der Anbieter können die Nutzerinnen und Nutzer den Datenschutzbestimmungen insgesamt zustimmen oder widersprechen. Lediglich bei 12,8% der Apps können sie der Verwendung in einzelnen Bereichen und bei 2,6% der Apps auf Ebene einzelner Datenpunkte widersprechen.

Im Rahmen der Befragung wurde nicht nach dem genauen Zweck der Datenverarbeitung gefragt – insbesondere, ob die Akzeptanz der Datenschutzbestimmungen notwendig ist, um den vollen Funktionsumfang der App nutzen zu können oder ob es hierfür andere Gründe gibt.

Denkbar ist deshalb, dass die Nutzerinnen und Nutzer die Datenschutzbestimmungen insgesamt akzeptieren müssen, um den vollen Funktionsumfang der Apps nutzen zu können. Wenn sie den Datenschutzbestimmungen widersprechen, müssten sie damit rechnen, die Apps in vielen Fällen nicht oder nur mit eingeschränktem Funktionsumfang in Anspruch nehmen zu können.

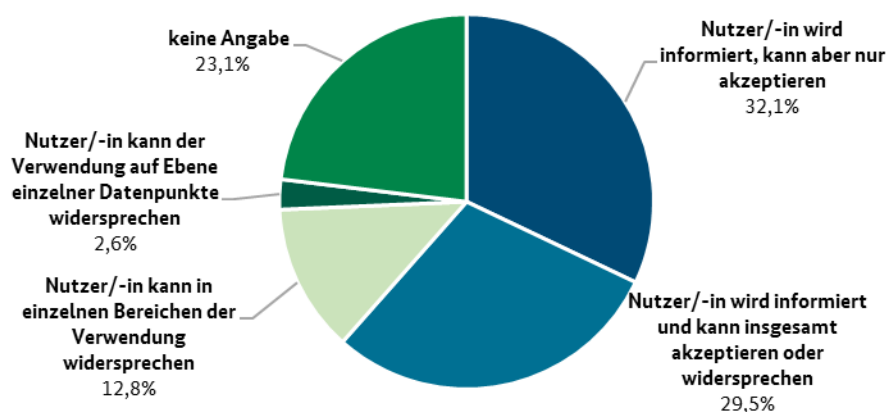


Abbildung 8: Welche Entscheidungsmöglichkeit haben die Nutzer/-innen hinsichtlich der Erfassung und Verarbeitung von Daten? (n=78)

Die Betrachtung der verarbeiteten Daten erfolgte in diesem Kontext nicht mit dem Fokus Datenschutz, sondern zielte eher auf die Bewertung der Schutzziele ab, da die Sensibilität der erfassten, verarbeiteten und ggf. weitergegebenen Daten in einem direkten Zusammenhang mit den IT-Schutzmaßnahmen und deren Bewertung steht.

### 6.3.2.2 IT-Sicherheit im Entwicklungsprozess

Entwicklerinnen und Entwickler sollten bereits im Entwicklungsprozess Sicherheitsanforderungen an ihre Anwendungen berücksichtigen, um spätere Sicherheitslücken im System zu verhindern. Dieses Vorgehen wird unter dem Fachbegriff „Security by Design“ zusammengefasst. Lediglich bei 7,1% der befragten Anbieter findet die IT-Sicherheit im Entwicklungsprozess keinerlei Berücksichtigung, während die große Mehrheit (91,4%) angibt, die IT-Sicherheit direkt im Entwicklungsprozess zu berücksichtigen. Bei den meisten Anbietern wird hierfür kein separates Team eingesetzt, sondern direkt durch die jeweiligen Entwicklerinnen oder Entwickler abgedeckt. Bei 17,1% erfolgt auch eine externe Prüfung.

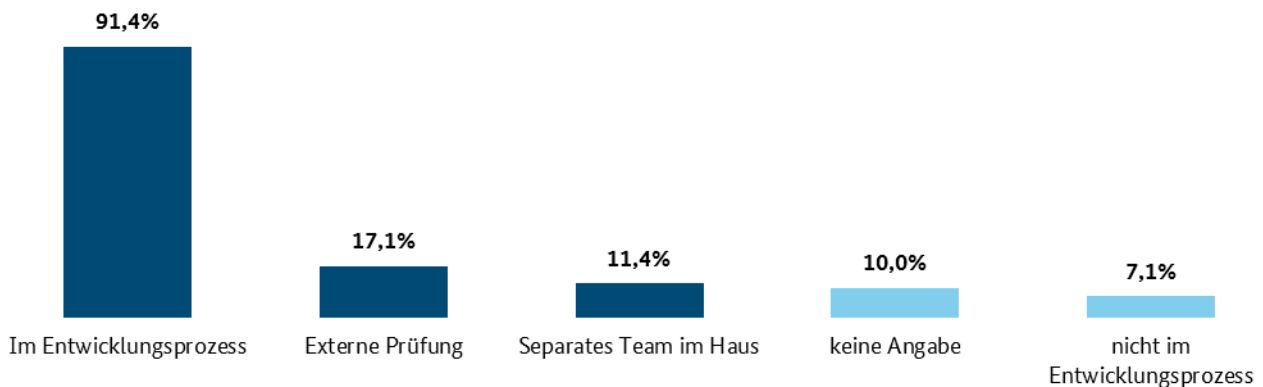


Abbildung 9: Wie wird IT-Sicherheit im Softwareentwicklungsprozess berücksichtigt? (n=70)

Laut Angaben der befragten Anbieter unterscheidet sich der Entwicklungsprozess mit Blick auf den Aspekt IT-Sicherheit überwiegend nicht bei der Entwicklung für verschiedene Betriebssysteme. 67,1% gaben an, dass es hinsichtlich der Berücksichtigung von IT-Sicherheit im Entwicklungsprozess keine Unterschiede gibt. Lediglich 10,0% gaben an, dass es hierbei Unterschiede gibt. 22,9% machten keine Angaben.

### 6.3.2.3 Security Frameworks

Orientierung für die unmittelbare Betrachtung der IT-Sicherheit im Rahmen des Entwicklungsprozesses bieten die Security Frameworks der Plattformen. Hierauf wird auch im Rahmen der BSI TR-03616 verwiesen. Die Befragung zeigt allerdings, dass die Nutzung der Security Frameworks kein Standard ist. 57,2% der Befragten trafen eine Aussage zur Nutzung des Android Frameworks. Davon gaben 24,3% an, das Framework zu nutzen; 32,9% nutzen es nicht. Zum iOS Framework trafen 42,9% der Befragten eine Aussage, von denen 20,0% angaben, das Framework zu nutzen, während 22,9% dies negierten.

Ein möglicher Grund für die geringe Nutzungsrate könnte sein, dass die Frameworks bei den Entwicklerinnen und Entwicklern eher unbekannt sind. Sie werden nicht aktiv durch die Plattformen beworben.

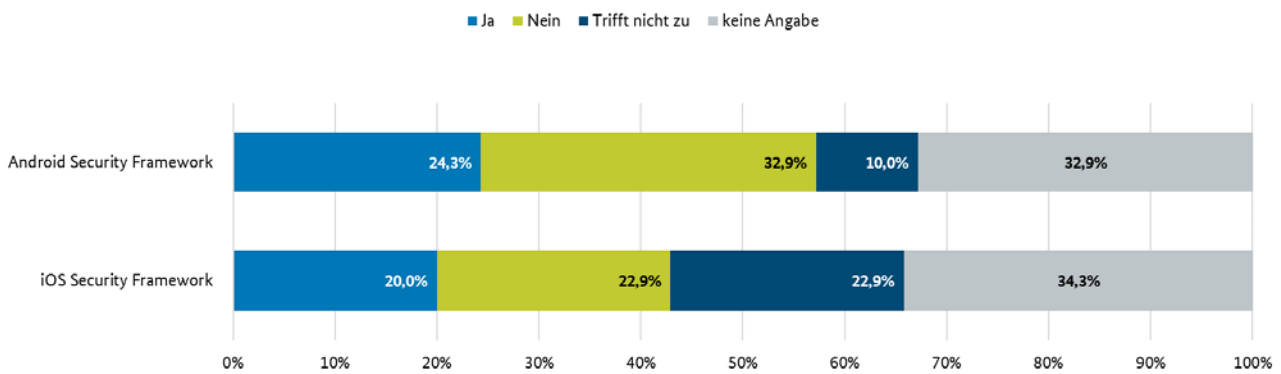


Abbildung 10: Nutzen Sie Sie Security for Android Developers (SfAD)? Nutzen Sie das iOS Security Framework (ioSSF)? (n=70)

### 6.3.2.4 Nutzer-Authentisierung und Passwörter

Das BSI gibt auf seiner Webseite Tipps, worauf Verbraucherinnen und Verbraucher bei der Einstellung eines sicheren Passworts achten sollten (BSI, 2021). Die Passwortempfehlungen fußen auf den Inhalten des IT-Grundschutzes (BSI, 2021).

Empfohlen wird die Verwendung von mindestens acht Zeichen, Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern. 27,5% der Anbieter und damit die größte Gruppe verwenden diesen Standard als Mindestanforderung für die Passwörter ihrer Nutzerinnen und Nutzer.

Allerdings gibt auch ein erheblicher Anteil von 19,6% an, dass sie in ihrer App keinerlei Anforderungen für die Passwörter ihrer Nutzerinnen und Nutzer definieren. Warum ein so großer Anteil keinerlei Anforderungen an die Passwörter stellt, lässt sich auf Basis der Befragung nur vermuten. Ein möglicher Grund könnte darin liegen, dass die Anbieter keine eigene Authentisierung durchführen. Dies gaben 35,3% der Anbieter an. Stattdessen authentisieren einige Anbieter ihre Nutzerinnen und Nutzer über Authentifizierungsframeworks.

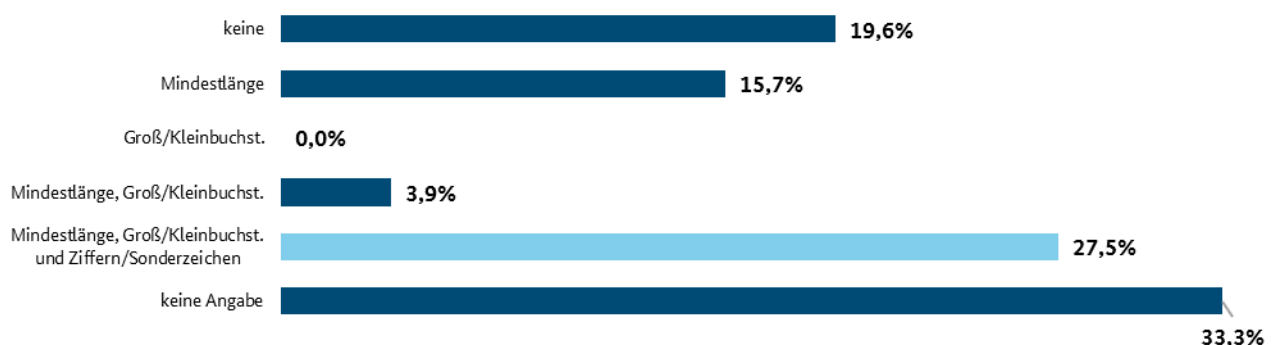


Abbildung 11: Welche Anforderungen setzen Sie an ein User-Passwort? (n=51)

### 6.3.2.5 Verschlüsselung von Daten und Datentransfers

Um zu verhindern, dass sensible Daten der Nutzerinnen und Nutzer ohne berechtigten Zugriff eingesehen werden können, dürfen diese nur verschlüsselt gespeichert und übertragen werden (z. B. zu Public Cloud Dienstleistern). 64,8% der Anbieter nehmen Maßnahmen zur Verschlüsselung von Daten und Datentransfers vor.



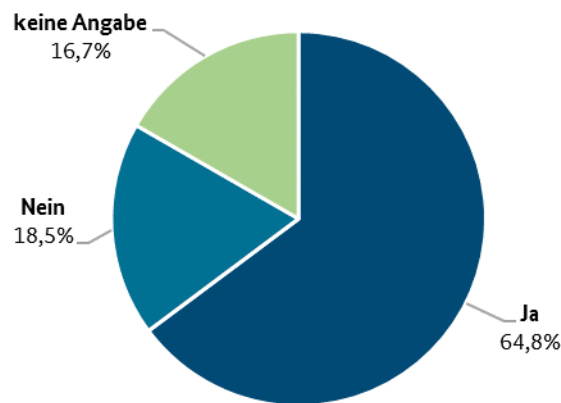


Abbildung 12: Nehmen Sie Maßnahmen vor, um Daten und Datentransfers zu verschlüsseln? (n=54)

Insbesondere für den Fall, dass mobile Endgeräte verloren gehen oder gestohlen werden, ist es wichtig, dass die Nutzerdaten verschlüsselt auf den Geräten abgelegt sind und nicht ausgelesen werden können. 40,8% der Anbieter verschlüsseln die Daten auf dem Endgerät. Hiervon sind bei der Hälfte die gespeicherten Daten erst nach Entsperren durch die Nutzerin oder den Nutzer auslesbar. Mit 38,9% gibt jedoch ein hoher Anteil der Anbieter an, dass sie die Daten unverschlüsselt auf dem Endgerät ablegen – unabhängig davon, ob standardmäßige Verschlüsselungsmechanismen des Betriebssystems vorliegen.

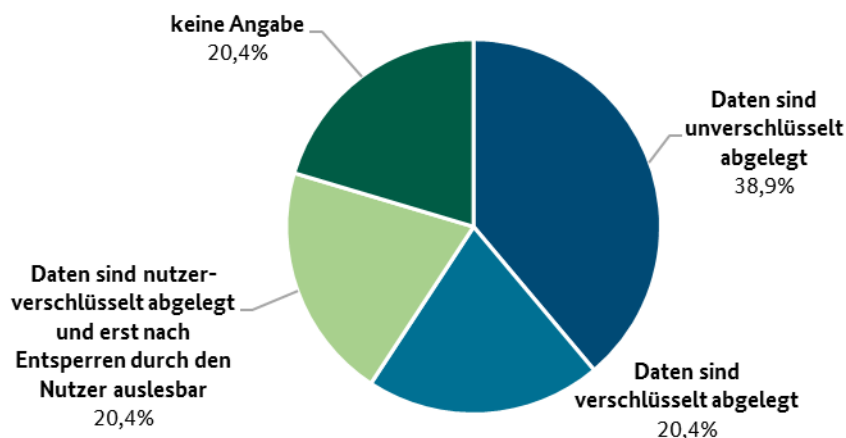


Abbildung 13: Verschlüsseln Sie Daten auf dem Endgerät und wenn ja, in welcher Stufe? (n=54)

Eine gängige Maßnahme, um die Sicherheit der Daten auch im Rahmen von Transfers sicherzustellen, ist die durchgängige Verschlüsselung der Netzwerkkommunikation mit TLS. Die Konfiguration muss dem aktuellen Stand der Technik entsprechen. 25,9% der Anbieter verlangen mindestens den TLS 1.2 Standard für die Verschlüsselung der Kommunikation zwischen App und Betreiber-Infrastruktur. Dieser entspricht aktuell auch dem geläufigsten Standard, welcher die Vorgänger TLS 1.0 und TLS 1.1 abgelöst hat. Der neuere Standard 1.3 wird bisher von vielen Clients noch nicht unterstützt.

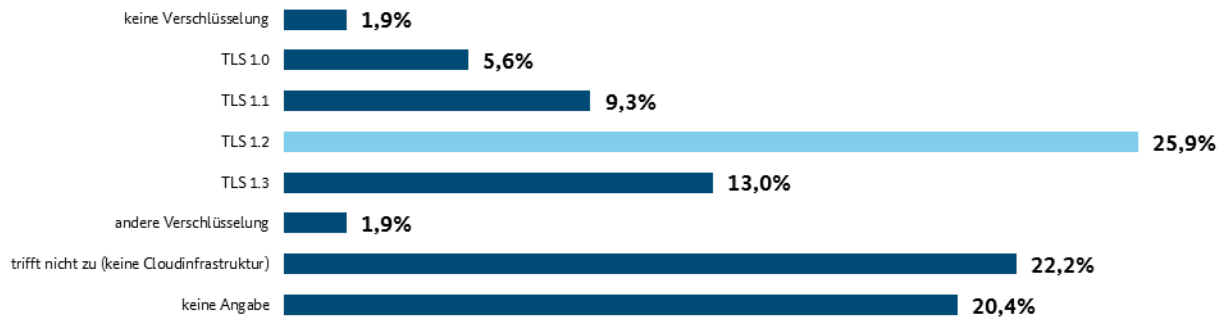


Abbildung 14: Welchen TLS-Standard verlangen Sie mindestens für die Kommunikation zwischen App und Cloud-Infrastruktur? (n=54)

### 6.3.2.6 Updates für Bibliotheken von Dritten

Die Nutzung von Bibliotheken von Drittanbietern erleichtert App-Entwicklerinnen und Entwicklern das Programmieren und ist deshalb eine gängige Praxis in der Softwareentwicklung. Für diese Bibliotheken muss jeweils sichergestellt werden, dass Sicherheitsupdates zeitnah eingespielt werden. Um Updates für Drittanbieter-Bibliotheken zu erkennen und dynamisch durchzuführen, können Anbieter auf sog. „App-Updater“ zurückgreifen. Von den befragten Anbietern nutzen 44,4% einen automatisierten Prozess, um Updates zu erkennen; 35,2% nutzen keinen standardisierten Prozess.

Ein möglicher Grund dafür, warum eine nicht unerhebliche Zahl der Anbieter keinen standardisierten Prozess und keine App-Updater nutzt, ist, dass die automatisch eingespielten Updates die Funktionalität der App beeinträchtigen können. Gleichzeitig sind automatische Updates auch nicht für alle Drittanbieter-Bibliotheken möglich, weil einige der Bibliothek-Anbieter dies durch „Obfuskation“ verhindern. Durch die Obfuskation wird der Programmcode so verändert, dass der Quelltext nicht oder nur schwer eingesehen und verändert werden kann. Hierdurch wollen die Anbieter z. B. Reverse Engineering oder den Diebstahl ihres geistigen Eigentums durch das Kopieren von Programmteilen verhindern.

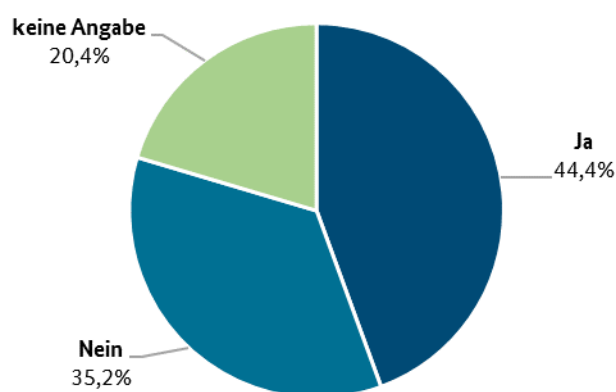


Abbildung 15: Haben Sie in Bezug auf sicherheitsrelevante Updates einen Prozess zur Erkennung von notwendigen Updates für Bibliotheken Dritter? (n=54)

### 6.3.2.7 Schließung von Schwachstellen

Durch Nutzerinnen und Nutzer, aber auch Forscherinnen und Forscher, die gezielt nach Schwachstellen in Systemen suchen, werden regelmäßig Schwachstellen in digitalen Anwendungen identifiziert. Nach der Meldung einer Schwachstelle, sollte diese so schnell wie möglich geschlossen werden. 46,3% der befragten Anbieter von Gesundheits-Apps haben einen Prozess für den Umgang mit einer gemeldeten Schwachstelle. Wie diese Verfahrensweise aussieht und in welcher Art sie formalisiert ist, wurde im Rahmen der Befragung nicht erfasst. 37,0% haben keine Verfahrensweise für den Umgang mit einer gemeldeten Schwachstelle.

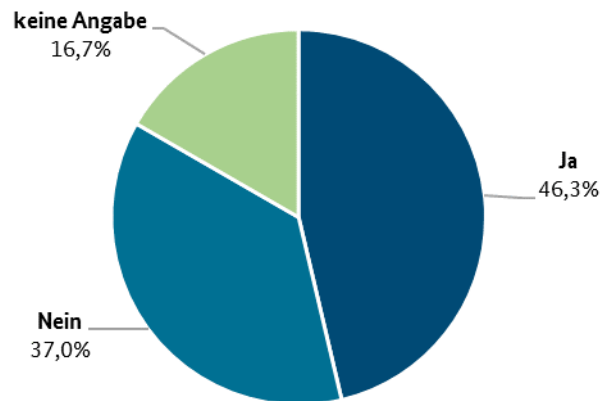


Abbildung 16: Haben Sie Verfahrensweisen, wie mit der Meldung einer Schwachstelle beispielsweise durch Sicherheitsforscherinnen und -forscher umgegangen wird? (n=54)

Der Zeitraum bis zur Schließung der Schwachstelle ist besonders wichtig. Sinnvoll ist es, wenn App-Anbieter für sich konkrete zeitliche Vorgaben definieren und festlegen, in welchem Zeitraum Schwachstellen geschlossen werden sollten. Die Zeiträume sollten sich am Grad der Kritikalität der identifizierten Schwachstellen ausrichten. 63,0% der befragten Anbieter machen keine verbindlichen Vorgaben für die Dauer der Schließung von identifizierten Schwachstellen; 14,8% machen verbindliche Vorgaben. Bei den meisten Anbietern mit verbindlichen Vorgaben, sollen die Schwachstellen, laut eigener Angaben, binnen einer Woche geschlossen werden.

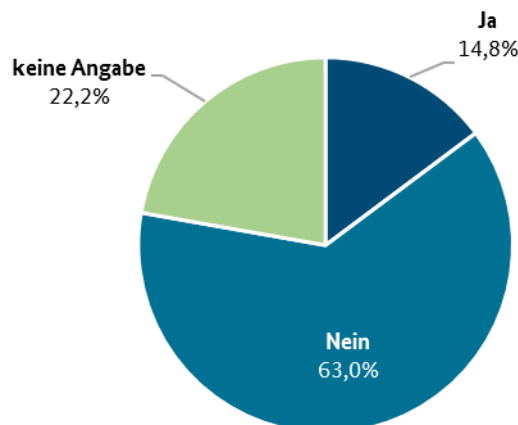


Abbildung 17: Gibt es verbindliche Vorgaben zu Zeiträumen, in denen Sicherheitslücken geschlossen werden? (n=54)

### 6.3.2.8 Reverse Engineering, Bug Bounties und Jailbreaks

„Mittels Reverse Engineering wird versucht, die Funktionsweise einer kompilierten Software zu analysieren, ohne dabei auf den Quelltext oder die Spezifikation der Software zugreifen zu müssen. Als Vorbereitung eines Cyber-Angriffs können z. B. Sicherheits-Updates mittels Reverse Engineering untersucht werden, um Erkenntnisse über Sicherheitslücken zu sammeln, die durch das Update geschlossen werden. Mittels dieser Informationen kann ein Angreifer Rückschlüsse ziehen, wie man diese Schwachstelle auf Systemen ausnutzen kann, die das Update nicht installiert haben.“ (BSI, 2018)

Apps sollten durch Verschleierungsmaßnahmen wie Code-Obfuskation (s. o.) Maßnahmen gegen Reverse Engineering umsetzen, um zu verhindern, dass potenzielle Angreifer Schwachstellen in ihren Systemen ausnutzen. Nur die Hälfte der befragten App-Anbieter (51%) führen solche Maßnahmen gegen Reverse Engineering durch, während ein vergleichsweise hoher Anteil von 31,4% keine Maßnahmen vornimmt.

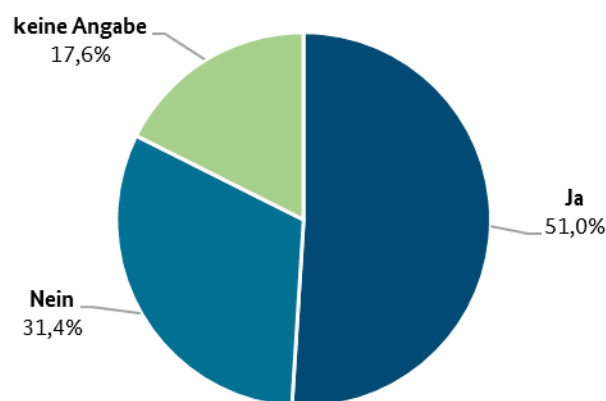


Abbildung 18: Wurden Maßnahmen gegen Reverse Engineering getroffen? (n=51)

Im Rahmen von Bug Bounty Programmen fordern Unternehmen Hacker auf, Schwachstellen in ihren Systemen zu identifizieren und loben hierfür Belohnungen aus. Nach den Erkenntnissen aus der Befragung ist das Durchführen von Bug Bounties bei Gesundheits-Apps nicht üblich. Lediglich 3,9% der Anbieter geben an, dass sie öffentliche Bug Bounties zum Auffinden von Schwachstellen ausschreiben. 82,4% nutzen keine öffentlichen Bug Bounties.

Eine weitere Maßnahme für die Sicherung der App ist das Erkennen und angemessene Reagieren auf sog. „Jailbreaks“ im iOS-Umfeld bzw. „Rooten“ im Fall von Geräten mit Android Betriebssystem:

„In Betriebssystemen von Smartphones und Tablets werden immer wieder Schwachstellen entdeckt, die es ermöglichen, das vom Hersteller etablierte Sicherheitskonzept zu umgehen und somit auf Systemprozesse und geschützte Speicherbereiche zuzugreifen. Dadurch können Programme nicht vorgesehene Berechtigungen erlangen, mit denen sie unerlaubte Aktionen ausführen können. [...] Sogenannte Jailbreaks nutzen diese Schwachstellen aus, um beispielsweise alternative App Stores oder sonstige Erweiterungen nutzen zu können. Jailbreak-Techniken können aber auch von Angreifern verwendet werden, um Schadprogramme zu installieren oder andere schädliche Manipulationen auf dem Gerät vorzunehmen. Schadprogramme können auch Schwachstellen ausnutzen, um sich auf einem Gerät zu installieren oder es zu manipulieren. Hierdurch kann das Betriebssystem anders als vorgesehen genutzt und wichtige Sicherheitsfunktionen können übergangen werden. Insbesondere betroffen sind Daten, die vom mobilen Betriebssystem in geschützten Bereichen gelagert werden, da eine App mit Superuser-Rechten diese unter Umständen auslesen kann.“ (BSI, 2020)

Anbieter sollten deshalb nach Empfehlungen des BSI Maßnahmen implementieren, die es ermöglichen, Manipulationen an den Endgeräten ihrer Nutzerinnen und Nutzer zu erkennen. Anwendungen müssen „roots“

und „jailbreaks“ an Geräte entsprechend des aktuellen Stands der Technik erkennen und angemessen darauf reagieren. Der Großteil der befragten Anbieter von Gesundheits-Apps (58,8%) setzt allerdings keine Maßnahmen zur Erkennung von Manipulationen um; lediglich 25,5% der Anbieter tun dies.

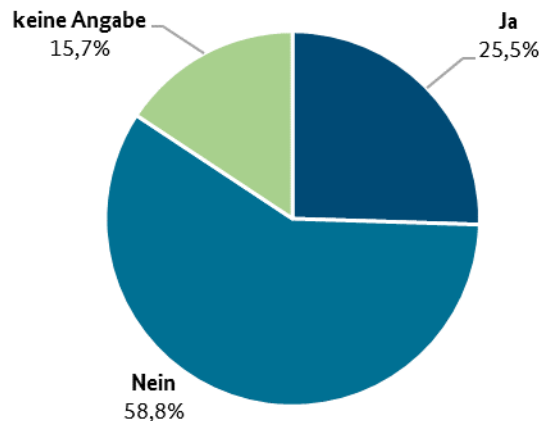


Abbildung 19: Wurden Maßnahmen zur Erkennung von Manipulation (root / jailbreak) der Geräte vorgenommen? (n=51)

### 6.3.3 Fazit IT-sicherheitstechnische Maßnahmen der Anbieter

Im Rahmen der Befragung wurden Anbieter von Gesundheits-Apps zu ihrem grundsätzlichen Umgang mit Kernelementen der IT-Sicherheit befragt. Die Befragung hat gezeigt, dass der Großteil der Anbieter IT-Sicherheit nach eigenen Angaben bereits im Entwicklungsprozess berücksichtigt und verschiedene Maßnahmen zum Schutz der Apps und damit auch der Daten ihrer Nutzerinnen und Nutzer vor externen Zugriffen vornimmt. Die Befragung hat aber auch Aspekte aufgezeigt, in denen Anbieter ihren Umgang mit Fragen der IT-Sicherheit verbessern und professionalisieren können.

Hierzu gehört beispielsweise die Nutzung der Security Frameworks von iOS und Android, die passgenaue Orientierung für die Entwicklung sicherer iOS- und Android-Apps bieten, oder die Einführung eines strukturierten Prozesses für den Umgang mit Schwachstellen, in dem auch ein fester Zeitraum für das Schließen von Sicherheitslücken definiert werden sollte.

Für die Kommunikation zwischen App und Betreiber-Infrastruktur sollte immer eine Version des TLS-Standards genutzt werden, die dem aktuellen Stand der Technik entspricht. Weiterhin besitzt ein bedeutender Anteil der Anbieter bisher keinen Prozess, um Updates von Bibliotheken Dritter zu erkennen und einzubinden. Viele Anbieter fordern bei der Vergabe von Passwörtern nur eine Mindestlänge. Dies überrascht, denn deutlich sicherer wäre die zusätzliche Forderung von Groß- und Kleinbuchstaben und Sonderzeichen, welche vom BSI empfohlen wird. Ausdrücklich empfiehlt das BSI zudem eine „Zwei-Faktor-Authentisierung“, bei der eine zweistufige Überprüfung der Nutzerin respektive des Nutzers erfolgt (BSI, 2021). Anbieter könnten damit auf einem verhältnismäßig einfachen Weg die Sicherheit ihrer Anwendungen erhöhen. Gleiches gilt für den Aspekt des Reverse Engineering. Wenn es sich auch nicht um die Mehrheit handelt, gibt dennoch ein großer Anteil der Anbieter an, keinerlei Maßnahmen gegen Reverse Engineering vorzunehmen. Hier sollten in jedem Fall Maßnahmen ergriffen werden. Es ist zu empfehlen, dass Anbieter Techniken zum Erschweren von Reverse Engineering integrieren, um die Eintrittsschwelle für Angriffe zumindest zu erhöhen. Dies sollte nicht dazu führen, dass man vom Ziel besserer Sicherheitsmaßnahmen abrückt und ist in diesem Sinne als additive Maßnahme zu sehen.

## 7 Case Studies – IT-sicherheitstechnische Untersuchung von Gesundheits-Apps

### 7.1 Design IT-sicherheitstechnische Untersuchung

Applikationen für mobile Endgeräte befinden sich in einem komplexen technischen Zusammenspiel zwischen der eigentlichen Anwendung, dem Smartphone, dem Betriebssystem und den externen Kommunikationsmöglichkeiten des Gerätes. Diese Ausgangssituation erlaubt grundsätzlich sehr unterschiedliche Prüftiefen, welche sich bis hin zur Suche von Angriffsvektoren auf den untersten technischen Ebenen erstrecken kann.

Im vorliegenden Fall zielt die Untersuchung darauf ab, den sicherheitstechnischen Gesamtzustand der betrachteten Gesundheits-Apps zu erfassen, um Rückschlüsse auf die allgemeine Lage am Markt ziehen zu können. Daher wurde zu diesem Zweck ein Vorgehen gewählt, welches gängige und wahrscheinliche Angriffsvektoren in Form eines Prüfkataloges systematisch erfasst und die Möglichkeit bietet, die betrachteten Apps in einer einheitlichen und daher vergleichbaren Art und Weise zu untersuchen und zu bewerten.

Ziel ist es, im Rahmen der Tests die Angriffsmöglichkeiten zu untersuchen, welche durch Angreifer mit begrenztem Aufwand ausgenutzt werden könnten und sich mit dem aktuellen Stand der Technik durch entsprechende Sicherheitsvorkehrungen verhindern ließen. Dabei liegt der Fokus auf Angriffsvektoren auf der Benutzerebene sowie Netzwerk- und klassischen Man-in-the-Middle-Angriffen. Tiefergehende Analysen von z. B. Speichermedien oder Code Audits mit Reverse Engineering Techniken waren nicht Teil der Untersuchung.

Ein vollständiges und detailliertes Bild des IT-sicherheitstechnischen Zustandes der Apps kann auf diese Weise nicht geschaffen werden. Die Betrachtung ermöglicht es aber zu beurteilen, ob App-Hersteller auf einer aggregierten Ebene für ein dem aktuellen Stand der Technik angemessenes Sicherheitsniveau sorgen.

Der Prüfkatalog besteht aus 28 Anforderungen, die den drei Kategorien „Netzwerkangriff“, „Angriff am Gerät“ und „Analyse des App-Pakets“ zugeordnet sind. Der Bereich Netzwerkangriff berührt hauptsächlich Protokollanalysen des Datenverkehrs ausgehend von der App, mit dem Ziel, die Nutzung von Verschlüsselungsprotokollen nach dem Stand der Technik seitens der Endpunkte zu untersuchen. Dies beinhaltet auch die Erfassung von etwaiger Kommunikation zu Drittdiensten sowie die Absicherung von Übertragungsinhalten. Die Kategorie Angriff am Gerät umfasst die Benutzung der App und des Gerätes mit den damit zusammenhängenden sicherheitsrelevanten Aspekten, wie etwa Sichtbarkeit sensibler Daten auf der Benutzeroberfläche, stufenweiser Authentifizierung und Eingabevalidierung. Im Bereich Analyse des App-Pakets stand die Prüfung von technischen Applikationsberechtigungen sowie die Sichtung von Überbleibseln des Software-Entwicklungszyklus im Mittelpunkt (vgl. Abbildung 20).

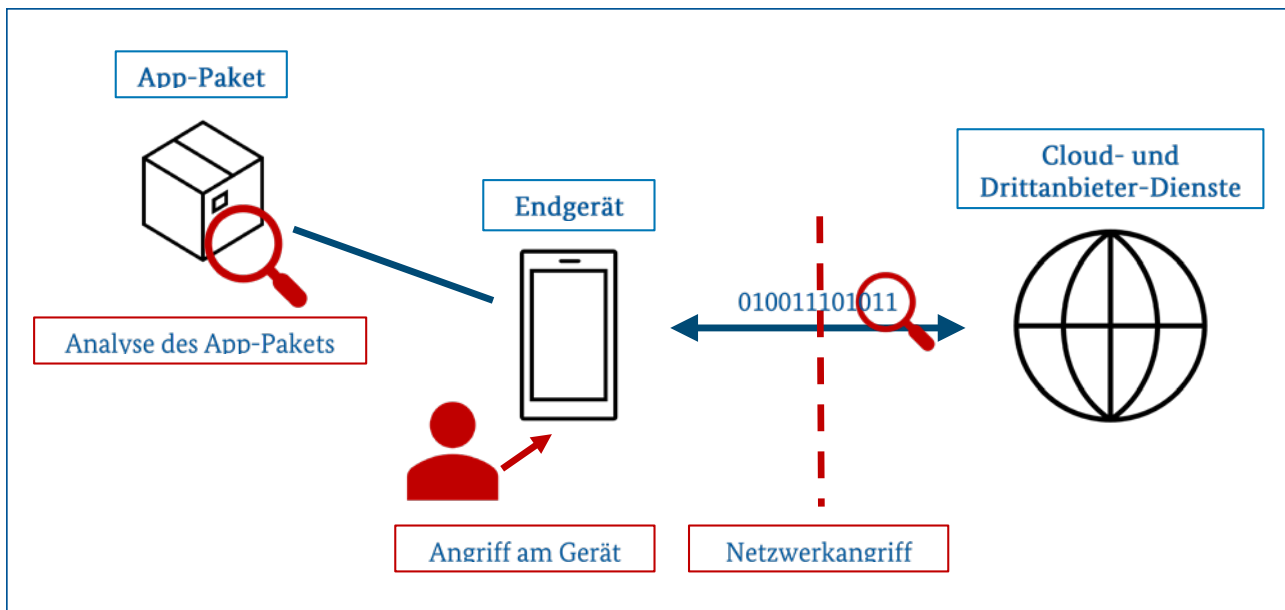


Abbildung 20: Testkategorien der IT-sicherheitstechnischen Untersuchung

## 7.2 Ergebnisse aus der IT-sicherheitstechnischen Untersuchung

Die folgenden Unterkapitel sind nach den zentralen Aspekten der IT-sicherheitstechnischen Untersuchung gegliedert. Auf Basis der jeweiligen Erkenntnisse erfolgt eine Bewertung der zum Zeitpunkt der Untersuchung implementierten Sicherheitsmaßnahmen und es werden ergänzend Hinweise auf Verbesserungspotenziale gegeben.

### 7.2.1 Technischer Umgang mit Nutzerpasswörtern

Der Umgang mit Nutzerpasswörtern spielt auf der technischen Ebene eine entscheidende Rolle, da hiervon der Zugang zum Konto und letztlich die Vertraulichkeit und Integrität der Nutzerdaten abhängen. Aus diesen Gründen ist es essenziell, dass die von den Nutzerinnen und Nutzern auf ihrem Gerät zum Login eingegebenen Passwörter in einer sicheren Art und Weise vom Dienst des Anbieters authentifiziert werden.

Wenn Angreifer in den Besitz von Datenabzügen gelangen, die Klartext-Passwörter enthalten, können persönliche Daten häufig unbemerkt abgegriffen werden. Im schlimmsten Fall kommt es zu Datenveränderungen oder weiteren Schäden, z. B. durch Identitätsdiebstahl.

Damit zu diesem Zweck Passwörter nicht im Klartext an den prüfenden Dienst übertragen werden müssen, hat es sich als Standard erwiesen, spezielle Einweg-Funktionen (sog. Hash-Funktionen) anzuwenden, die das Passwort in einen Hash-Wert umwandeln. Eine Rückkehr vom Hash-Wert zum Passwort wird damit praktisch unmöglich gemacht. Dieses Vorgehen bietet den Vorteil, dass nur der Hash-Wert zur Verifikation an den Anbieter gesendet werden muss und ein Angreifer, der Zugriff auf die Nachricht erhält, keine Rückschlüsse auf das ursprüngliche Klartext-Passwort ziehen kann. In der Verifikationsdatenbank des Anbieters sorgt die ausschließliche Speicherung von Hash-Werten ebenfalls für ein verringertes Risiko des Bekanntwerdens von Nutzerpasswörtern. Neben der Verwendung von Hash-Funktionen existieren weitere gängige Mechanismen, um Passwörter und deren Hash-Werte zusätzlich zu schützen, z. B. Überschlüsselung. Somit ist die Verarbeitung von Klartext-Passwörtern als relevantes Sicherheitsrisiko zu bewerten und möglichst zu vermeiden.

Damit Anbieter keinen eigenen Verifikationsdienst für Login-Daten entwickeln und betreiben müssen, können Authentifizierung-Frameworks wie „OpenID Connect“, „OAuth2“ und Dienste von Drittanbietern

genutzt werden. Diese führen die Authentifikation der Nutzerinnen und Nutzer durch und autorisieren diese, auf die Dienste des Anbieters zuzugreifen.

Bei den betrachteten Apps zeigte sich, dass nicht alle vorhandenen technischen Möglichkeiten zum Schutz von Passwörtern beim Transport genutzt werden. Bei sechs der untersuchten sieben Apps wurden Passwörter im Klartext an den Authentifizierungsdienst übertragen. Diese konnten offengelegt werden, sobald der Datenverkehr im Rahmen der Untersuchung entschlüsselt wurde. Die verwendete Verschlüsselung des Transportweges schützt die Passwörter zwar grundsätzlich vor einer Offenlegung, bietet aber als alleinige Sicherungsmaßnahme keinen hinreichenden Schutz, da verschiedene Angriffe auf das Verfahren vorhanden sind.

Die Mehrzahl der Apps nutzt die angesprochenen Authentifizierung-Frameworks wie OAuth2. Bemerkenswert ist an dieser Stelle, dass auch zu diesen Diensten Passwörter im Klartext übertragen wurden.

## 7.2.2 Anbieterseitiger Umgang mit Nutzerdaten in Cloud-Umgebungen

Die Bauweise moderner Mobilapplikationen bedingt, dass zum einen die IT-Infrastrukturen der Anbieter zum überwiegenden Teil in Cloud-Umgebungen oder anderweitigen Hintergrundsystemen lokalisiert sind – den sogenannten „Backends“. Zum anderen kommunizieren die Apps nicht nur mit dem unmittelbaren App-Anbieter, sondern auch mit Backends von Drittanbietern, welche dedizierte Leistungen erbringen. Dabei kann es sich um Datenbanken, Identifikationsdienste, IT-Infrastrukturen zur Datenauslieferung und Werkzeuge für Marketing und Produktoptimierung handeln. Dies führt dazu, dass alle untersuchten Apps die Hintergrundumgebungen mehrerer Anbieter gleichzeitig nutzen. Eine der untersuchten Apps verwendete ausschließlich die Leistungen von Drittanbietern, d. h. der App-Anbieter betreibt überhaupt kein unternehmenseigenes Backend.

Diese Situation stellt den derzeitigen Zustand der technischen Entwicklung dar und ist für sich genommen nicht als ungünstig zu bewerten. Allerdings vergrößert sich damit die Komplexität der IT-Architektur und in Bezug auf die IT-Sicherheit steigt das Risiko für mögliche Angriffsszenarien. Angreifer erhalten somit eine wachsende Anzahl an Angriffsvektoren, die sie ausnutzen können. So kann das Kompromittieren eines Drittanbieters auch dazu führen, dass eine Gesundheits-App ebenfalls betroffen ist. Im Hinblick auf den Verbraucherschutz ist diese Situation bedenklich, da es für Nutzerinnen und Nutzer zunehmend schwerer wird, einen möglichen Abfluss der eigenen Daten nachzuvollziehen. Darüber hinaus kann sich das Risikoprofil des App-Anbieters vergrößern, da dieser keine Kontrolle über das Sicherheitsniveau der verwendeten Drittdienste hat. Ein Beispiel für eine hohe Dynamik in diesem Bereich stellt z. B. der Einsatz von GraphQL, als Abfragesprache mit eigenen Sicherheitsrisiken, dar.

In Fachkreisen werden hierzu diverse Best Practice Ansätze diskutiert. Mit Blick auf beispielsweise die fertigen Industriezweige ist es Standard, über Stücklisten die verbauten Einzelteile und deren Herkunft nachvollziehen zu können. Ähnliches kann im Sinne eines Software Bill of Material für eine höhere Transparenz in der Software Supply Chain sorgen. Die OpenSSL Sicherheitslücke Heartbleed zeigte beispielweise eindrücklich, wie immanent eine detaillierte Kenntnis über genutzte Drittkomponenten und deren Abhängigkeiten sind. Ziel des Software Bill of Material ist es, relevante Schwachstellenmeldungen schnell identifizieren und beheben zu können.

## 7.2.3 Generelle Nutzung von Verschlüsselungsmechanismen

Die Datensicherheit bei der Kommunikation im Internet hängt maßgeblich von einer Transportverschlüsselung ab, dem Standard TLS (Transport Layer Security). Bei einer netzwerktechnischen Analyse der Gesundheits-Apps war erkennbar, dass alle Apps durchgängig TLS zur Kommunikation mit den Betreiber-Infrastrukturen verwenden.



Der TLS-Standard umfasst verschiedene Versionen, die im Laufe der Zeit um neue Funktionen wie kryptografische Verfahren, Protokolle und Mitigation möglicher Angriffsmethoden verbessert wurden. So liegt die aktuelle Version TLS 1.3 seit 2018 vor. Ein wichtiger Punkt für Apps und Browser ist die Nutzung von TLS in mindestens der Version TLS 1.2, die seit 2008 existiert. Diese Version verhindert eine Reihe von Angriffsmöglichkeiten.

Aus Kompatibilitätsgründen unterstützen die untersuchten Backends in der Mehrzahl noch zusätzlich zu den aktuellen Versionen die veralteten Versionen TLS 1.0 bzw. TLS 1.1 und vereinzelt kryptografische Verfahren, die mittlerweile als schwach eingestuft wurden. In Kombination von Backend und modernen Apps bzw. Browsern werden allerdings immer die besten verfügbaren Verfahren ausgehandelt.

## 7.2.4 Angriffe gegen Verschlüsselungsmechanismen

Unabhängig von den eingesetzten Versionen der Transportverschlüsselung können Angreifer versuchen, das Kommunikationsprotokoll anzugreifen. Ziel ist es, damit die Vertrauensbeziehung zwischen App und Backend zu unterminieren, um sich selbst als legitimer Kommunikationspartner in die Kommunikation einzuschleusen.

In dieser Angriffsvariante täuscht der Angreifer der App bzw. dem Mobilgerät mit Hilfe eines gefälschten Sicherheitszertifikats vor, der beabsichtigte Kommunikationspartner (z. B. das Cloud-Backendsystem eines App-Anbieters) zu sein (Man-in-the-Middle-Angriff). Ein Schutz vor diesem Angriff stellt das sog. Certificate Pinning dar. Dabei werden die vom Server (ggf. auch von Apps) präsentierten Sicherheitszertifikate anhand ihrer kryptografischen Fingerabdrücke und der ausstellenden Zertifizierungsstelle verglichen, um unbefugten Zugriff zu unterbinden.

Im Rahmen der Untersuchung wurde dieser Umstand genutzt, um den Netzwerkverkehr über einen TLS-Entschlüsselungs-Proxy mittels eines selbst ausgestellten Sicherheitszertifikats zu untersuchen.

Sechs der sieben getesteten Gesundheits-Apps ließen sich mit dieser Methode untersuchen, was darauf schließen lässt, dass diese Apps Certificate Pinning nicht einsetzen. Sie sind damit für derartige Angriffe grundsätzlich verwundbar, in welchen sich ein Angreifer logisch zwischen zwei Kommunikationspartnern positioniert, um die Kommunikation abzufangen, mitzulesen oder zu manipulieren. Lediglich eine App setzte eine Form der Zertifikatsprüfung ein und ließ sich nicht auf diese Art untersuchen.

Für einen erfolgreichen Angriff müssen mehrere Faktoren zusammenkommen. Erst in Kombination mit weiteren Angriffen, in denen auf dem Endgerät der Benutzerin oder des Benutzers eigene bzw. gefälschte Sicherheitszertifikate installiert werden (z. B. durch Malware oder das Auslösen von Benutzerhandlungen, wie der Installation eines vermeintlich sicheren WLAN-Hotspot- oder VPN-Anbieter-Zertifikates) lässt sich eine funktionstüchtige Angriffskette erzeugen.

Ein weiterer Angriffsvektor ergibt sich beim Datenaustausch zwischen App und Backend. Zwar setzen alle Apps eine Transportverschlüsselung ein, die aber wie bereits angesprochen anfällig für Man-in-the-Middle-Angriffe ist. Dieses Risiko lässt sich z. B. durch die Überverschlüsselung, einer zusätzlich zur Transportverschlüsselung auf TLS-Ebene stattfindenden Verschlüsselung der Daten, mindern.

Überverschlüsselung wird nur bei einer der untersuchten Apps für eine bestimmte Untermenge an Informationen angewandt. Im Umgang mit sensiblen Informationen ist ein Einsatz von Überverschlüsselung und die darüberhinausgehende Nutzung von erweiterten Schutzmaßnahmen wie Hardware Security Bausteinen grundsätzlich anzuraten.

## 7.2.5 Klassische anwendungsbezogene Angriffe

Diese Art von Angriffen bezieht sich auf die Anwendungsebene der Mobilapplikation und des Backends der Anbieter. So versuchen Angreifer z. B. durch Injection-Attacken Daten einzuschleusen, die nicht den vorgegebenen Formaten entsprechen oder mit Hilfe von Sonderzeichen die Applikation dazu bewegen sollen, in einen Fehlerzustand zu gelangen und mehr als die intendierten Antworten zu erzeugen.

Über solche Attacken konnten in der Vergangenheit weitreichende Schäden bis hin zu vollständigen Datenabzügen erreicht werden. Aus diesem Grund sichern Anbieter ihre Applikationen dagegen ab. So werden in der App und in Backends Validierungen von Eingabefeldern vorgenommen und es werden nur Daten an Apps zurückgesendet, die z. B. keine Sonderzeichen mehr enthalten.

Im Rahmen der IT-sicherheitstechnischen Untersuchung ließen sich keine erfolgreichen Injection-Angriffe durchführen, da alle Apps eine Art der Eingabevalidierung durchführen.

Bei vier der sieben untersuchten Apps fand Input-Escaping statt: In diesem Fall werden alle Zeichen (auch Sonderzeichen und Teile von Befehlen) unverändert beibehalten, jedoch wird ein z. B. eingeschleuster Programmcode nicht ausgeführt.

Zwei der getesteten Apps zeigten den Einsatz von weitergehenden Schutzmaßnahmen. Hier wurden übermittelte Inhalte, die auf Befehlscode hindeuten, vollständig blockiert und nicht übernommen. Bei einer weiteren App kam eine spezialisierte Firewall (Web Application Firewall, WAF) mit einer Schutzfunktion eines Content-Delivery-Netzwerk-Anbieters zum Einsatz.

## 7.2.6 Zugriffseinschränkungen auf sensible Daten

Gesundheits-Apps verarbeiten sensible und ggf. auch identifizierende Nutzerdaten, z. B. Passwörter, Geburtsdaten und teilweise Gesundheitsdaten. Aus diesem Grund ist es geboten, dass die Apps eng mit den sicherheitstechnischen Möglichkeiten der Hardware interagieren bzw. diese effektiv einsetzen (Beispiel: Sperren). Geschieht dies nicht, besteht für Nutzerinnen und Nutzer die Gefahr, dass Angreifer auf einem nicht gesperrten Gerät Daten der Apps einsehen und dort auch Aktionen auslösen können (z. B. eine Terminanfrage bei einem Arzt).

Die meisten der untersuchten Apps sind nicht oder nur unzureichend vor dieser Art von Angriffen geschützt. So erfordert z. B. keine der Apps die Vergabe einer Geräte-PIN zur Nutzung. Nur eine einzige App im Test bietet die Möglichkeit, eine zusätzliche App-Sperre einzurichten, bei allen anderen Apps ist eine Sperre nicht möglich. Darüber hinaus werden bei keiner der untersuchten Apps auf dem Bildschirm sichtbare und sensible Daten ausgegraut, z. B. wenn die Nutzerin oder der Nutzer die App in den Hintergrund legt.

## 7.2.7 Bedarfsgerechte App-Berechtigungen

Mobile Anwendungen benötigen für ihren Funktionsumfang eine Reihe von Berechtigungen. Beispiele hierfür sind das Recht, auf den Kalender des Gerätes zugreifen zu dürfen (für eine Terminvereinbarung) oder die Kamera zu aktivieren, etwa um eine Videosprechstunde durchzuführen. Apps müssen in ihrem Programmcode grundsätzlich eine Auswahl an Berechtigungen einräumen. Bei der späteren Nutzung der App können sie diese dynamisch bei der Nutzerin oder dem Nutzer anfragen.

Insbesondere im Hinblick auf Gesundheits-Apps ist es wichtig, dass Berechtigungen stets anwendungsfallbezogen und angemessen sind und dem allgemein angebotenen Funktionsumfang entsprechen. Apps sollen beispielsweise nicht auf die im Gerät gespeicherten Kontakte oder Gesundheitsdaten zugreifen können, wenn kein Anwendungsfall vorliegt, welcher dies erfordert. Für App-Anbieter auf dem deutschen Markt gilt zudem, dass die Konformität zur Datenschutz-Grundverordnung (DSGVO) zu wahren ist.

Bei den geprüften Apps sind die Umsetzung und bedarfsgerechte Nutzung von Berechtigungen mit einer Ausnahme zufriedenstellend. Die meisten Apps verlangen nur die Berechtigungen, die auch für den regulären Betrieb notwendig sind. Einzig eine der untersuchten Apps erfordert Berechtigungen, die nicht unbedingt für den angebotenen Funktionsumfang erforderlich sind. In diesem Fall wurden Berechtigungen für den Zugriff auf Bluetooth und den Beschleunigungssensor erfragt, ohne dass der Zugriff der App eine entsprechend ersichtliche Funktionalität bietet.

Generell können Nutzerinnen und Nutzer hier aktiv werden und für Apps in den Geräteeinstellungen die angefragten Berechtigungen einsehen bzw. auch sperren. Gleichzeitig sollten Nutzerinnen und Nutzer aufmerksam werden, wenn Apps Berechtigungen anfragen, ohne dass die App die Nutzung klar darstellt.

## 7.2.8 Verarbeitung von benutzerbezogenen Daten

Alle untersuchten Apps verarbeiten benutzerbezogene Daten. Entweder ergeben sich diese Daten direkt durch Nutzereingabe (z. B. Geburtsdatum, E-Mail-Adresse) oder sie ergeben sich indirekt durch Nutzungstelemetrie und Tracking, d. h. das Nachspüren von nutzerindividuellen Spuren wie IP-Adresse, Gerätetyp oder Betriebssystemversion.

Die meisten der untersuchten Apps verwenden die Dienste von Drittanbietern, um Nutzungstelemetrie zu übermitteln und mutmaßlich auszuwerten. Während Nutzerinnen und Nutzer bei browserbasierten Webseiten in den Datenschutzeinstellungen häufig die Wahl haben, Dienste zu erlauben oder zu blockieren, stehen diese Möglichkeiten bei den untersuchten Apps meist nicht zur Verfügung – lediglich eine App ließ es zu, die Weitergabe von Daten an Dritte auszuschließen.

Der Fluss von Nutzungsdaten umfasst – soweit analysierbar – in den meisten Fällen benutzerbezogene Daten zu Endgeräten und der Softwareausstattung. Die Kombination der Datenpunkte würde ein Fingerprinting der Anwenderinnen und Anwender ermöglichen, wobei ein möglichst eindeutiger digitaler Abdruck der Nutzerin oder des Nutzers erzeugt wird, um ihre bzw. seine Interaktionen zu verfolgen. Die Menge der gesammelten Telemetriedaten ließ sich im Falle der untersuchten Apps nicht mit der angestrebten App-Funktionalität rechtfertigen.

In einem untersuchten Fall wurde ein Benutzerprofil angelegt, ohne dass sich die Nutzerin bzw. der Nutzer registriert. Erfolgt im weiteren Verlauf eine Registrierung, z. B., um eine erweiterte Funktionalität zu nutzen, wird diese mit dem zuvor pseudonym erzeugten Profil verknüpft.

Bei einzelnen Apps ergeben sich darüber hinaus ungünstige Konstellationen zwischen dem Nutzungszweck und den Drittanbietern. Im Beispiel konnte nach Ärzten in der Umgebung gesucht werden. Dafür wurde digitales Kartenmaterial eines Dienstleisters in die App eingebunden. In der Konsequenz kann hierdurch der Dienstleister mitverfolgen, nach welchen Fachärzten eine Nutzerin bzw. ein Nutzer sucht.

Einen erwähnenswerten Fall stellt eine App dar, die einen Drittanbieterdienst einbindet, dessen Kerngeschäft im Bereich der Click-Stream-Analyse liegt, d. h. der Backend-seitigen Auswertung von Screenshots. Die bei der Auswertung gefundenen Artefakte legen nahe, dass Bildschirminhalte bei Nutzerinteraktionen visuell erfasst und ausgewertet werden.

## 7.3 Zusammenfassung der Ergebnisse

Im Rahmen der Studie fand eine IT-sicherheitstechnische Untersuchung von ausgewählten Gesundheits-Apps für die Betriebssysteme Android und iOS statt. Das Prüfschema wurde vom BSI sowie Sicherheitsspezialistinnen und -spezialisten auf der Grundlage von Erfahrungen aus IT-Sicherheitsprojekten verfasst. Die untersuchungsspezifische Prüftiefe der durchgeführten Untersuchung stellt keinen vollumfänglichen Test

der Sicherheitsleistungen der Produkte dar. Die Betrachtung durch die Studie geht nicht mit einer Produktdeklaration oder -zertifizierung einher. Vielmehr verschafft sie in erster Linie einen groben Überblick und eine erste Vergleichbarkeit der Sicherheitseigenschaften von Gesundheits-Apps.

Das BSI beobachtet IT-sicherheitstechnische Aspekte von Systemen und Applikationen auf einer kontinuierlichen Basis, diese Studie soll jedoch zusätzlich einen punktuellen Status erfassen. Die Sicherheit eines Systems hängt auch von externen, sich kontinuierlich verändernden Faktoren ab. Da auch fortlaufend neue Schwachstellen entstehen können, ist es erforderlich, solche Systeme im Rahmen eines sicheren Produktlebenszyklus regelmäßig zu überprüfen.

Um die für diese Studie notwendige Untersuchungsstruktur herzustellen, wurde ein Prüfkatalog erarbeitet, der mittels 28 Prüfschritten einen systematischen Überblick über den IT-sicherheitstechnischen Grundzustand der Apps gibt. Zur Erstellung des Prüfkataloges wurden relevante und wahrscheinliche Angriffsvektoren identifiziert und gegen einschlägige Security Guidelines, wie den „OWASP Mobile Security Testing Guide“ (The OWASP Foundation, 2021), validiert. Alle Apps wurden in einem für diesen Zweck eingerichteten virtuellen Untersuchungslabor analysiert.

Untersucht wurden sieben Apps, davon drei Apps auf Basis des Android Betriebssystems und vier auf Basis von iOS. Zur Auswahl der Apps wurden die Ergebnisse der Marktanalyse sowie der Anbieterbefragung als Basis herangezogen. Es wurden Apps ausgewählt, die sowohl eine mutmaßlich breite Anwendung unter Nutzerinnen und Nutzern finden als auch eine gewisse Sensibilität der verarbeiteten Daten aufweisen.

Die Untersuchung hat gezeigt, dass die Anbieter eine Auswahl grundsätzlicher Anforderungen an die IT-Sicherheit erfüllt haben, diese aber in keinem der Fälle in einer Art und Weise abdecken, wie es nach dem Stand der Technik zu erwarten wäre. Aus Sicht der technischen IT-Sicherheit muss das Ergebnis mindestens als kritisch bewertet werden.

Über ein durchschnittliches Maß hinausgehende Anstrengungen zur Implementierung von zeitgemäßen IT-Sicherheitsfunktionalitäten sind lediglich im Einzelfall erkennbar. So findet sowohl auf Geräteebene, bei der Benutzerführung als auch auf Ebene der Prozesse oder Netzwerkkommunikation keine durchgängige und ausreichende Absicherung statt. Auch der Umgang mit den Benutzerdaten ist insbesondere vor dem Hintergrund, dass zum Teil personenbezogene Gesundheitsdaten erfasst und verarbeitet werden, zumindest bedenklich. Um beispielsweise den jeweiligen Funktionsumfang der Apps nutzen zu können, muss einem beträchtlichen Abfluss von benutzerbezogenen Daten zu Drittanbietern zugestimmt werden. Mit Blick auf die besondere Sensibilität der verarbeiteten personenbezogenen Daten in Gesundheits-Apps ist aus Sicht des BSI die Umsetzung der TR-03161 zu empfehlen.

Positiv hervorzuheben ist, dass alle Apps eine grundsätzliche Transportverschlüsselung mittels HTTPS und aktuellen kryptographischen Algorithmen nutzen. Weiterhin ist anzumerken, dass die überprüften Apps überwiegend nur die für den jeweiligen Funktionsumfang erforderlichen Berechtigungen auf dem Gerät anfordern.

Insgesamt lässt sich festhalten, dass keiner der App-Anbieter eine vollständige Umsetzung der Sicherheitsmaßnahmen nach dem Stand der Technik bieten kann. Dies hat verschiedene Ursachen: Einerseits bieten die App-Anbieter eine Umsetzung von Mindestanforderungen der Richtlinien der App Store Betreiber. Diese legen allerdings keine spezifischen Anforderungen an das IT-Sicherheitsniveau von Gesundheits-Apps fest, so dass für eine angemessene Absicherung weitergehende Sicherheitsmechanismen erforderlich wären. Andererseits entwickelt sich der Funktionsumfang der Apps in Richtung des medizinischen Einsatzbereichs ebenfalls beständig weiter, sodass die Kritikalität der verarbeiteten und miteinander verknüpften Daten weiter zunimmt. Insbesondere im Gesundheitsbereich ist es erstrebenswert, dass Verbraucherinnen und Verbraucher sichere Mobilapplikationen von Anbietern nutzen, die an der Technischen Richtlinie 03161 „Sicherheitsstandards für digitale Gesundheitsanwendungen“ (BSI, 2020) ausgerichtet sind.

Es bedarf einer kontinuierlichen Auseinandersetzung mit den Anforderungen bzgl. des Stands der Technik, da sich Art und Umfang der Angriffe rasant weiterentwickeln. Hierfür ist es empfehlenswert, Sicherheitsmerkmale als integralen Teil des Produktes zu verstehen und im Sinne eines sicheren Produktlebenszyklus

nach ISO/IEC (ISO/IEC 27034:2011, ISO/IEC 12207, ISO/IEC 81001-5-1) fortwährend in der Entwicklung und im Betrieb zu reflektieren. Dieses Vorgehen ermöglicht eine dauerhafte Verringerung der Angriffsvektoren, idealerweise eine gleichzeitige Förderung der Resilienz und Reaktionsgeschwindigkeit auf sich ändernde Anforderungen und schützt nicht nur die Informationen und Daten der Kundinnen und Kunden, sondern auch die Geschäftsmodelle und Reputation der App-Anbieter.

## 8 Zielgruppenspezifische Handlungsbedarfe und Lösungen



	Gesundheits-Apps sicherer machen		Nutzerinnen und Nutzer befähigen
	<ul style="list-style-type: none"> <li>IT-Sicherheitsanforderungen im Sinne eines „<b>Security by Design</b>“-Ansatzes bereits im Entwicklungsprozess berücksichtigen. Die Grundlage hierfür ist mit der <b>TR-03161</b> als Leitfaden für Entwicklerinnen und Entwickler geschaffen.</li> </ul>		<ul style="list-style-type: none"> <li>Verbraucherinnen und Verbraucher <b>für Risiken im Umgang mit digitalen Gesundheitsanwendungen sensibilisieren</b></li> </ul>
	<ul style="list-style-type: none"> <li><b>Dialog mit Anbietern</b> suchen, um eventuelle Hürden bei der Umsetzung der <b>TR-03161</b> zu identifizieren und die Richtlinie <b>entsprechend weiterzuentwickeln</b></li> </ul>		<ul style="list-style-type: none"> <li><b>Beurteilungsvermögen der Nutzerinnen und Nutzer fördern</b>, damit sie Chancen nutzen sowie potenzielle Risiken erkennen und bewerten können</li> </ul>
	<ul style="list-style-type: none"> <li>Bewusstsein der Anbieter für ihre Verantwortung gegenüber Nutzerinnen und Nutzern und die Auswirkungen ihres Handelns durch die Sensibilisierung für „<b>Corporate Digital Responsibility</b>“ stärken</li> </ul>		<ul style="list-style-type: none"> <li><b>Bereitstellung von Informationen, Leitfäden und Hilfestellungen</b> zur Stärkung der digitalen Lösungskompetenz von Verbraucherinnen und Verbrauchern</li> </ul>

Abbildung 21: Übersicht Handlungsbedarfe und Lösungen

Die Ergebnisse der Marktanalyse haben zentrale Strukturen und Entwicklungen im Markt für Gesundheits-Apps aufgezeigt. Der noch junge Markt ist durch eine hohe Dynamik mit ständig wechselnden und sich verändernden Angeboten und Marktteilnehmern gekennzeichnet. Mit Blick auf die Anwendungsbereiche der Apps reicht das Angebot von Fitness-Apps bis hin zu Apps, die die Nutzerinnen und Nutzer bei einem ganzheitlichen Gesundheitsmanagement unterstützen sollen. Funktional reicht die Breite des Angebots von der reinen Vermittlung von Wissen bis zur umfassenden Verarbeitung von Gesundheitsdaten.

Mitentscheidend für die Nutzerrisiken ist, ob und welche Daten verarbeitet werden sowie in welcher Art und an welchem Ort dies erfolgt. Das Risiko, das für die einzelne Verbraucherin oder den einzelnen Verbraucher von der Nutzung einer Gesundheits-App ausgeht, ist deshalb differenziert zu betrachten und muss individuell von App zu App beurteilt werden. Die potenzielle Schadenshöhe und damit das Risiko für Verbraucherinnen und Verbraucher kann im Bereich der Gesundheits-Apps abhängig von der Bedeutung bzgl. Vertraulichkeit, Verfügbarkeit und Integrität jedoch besonders hoch sein.

Die Ergebnisse der quantitativen Anbieterbefragung und der IT-sicherheitstechnischen Untersuchung ausgewählter Apps haben gezeigt, dass Anbieter im Markt verschiedene Maßnahmen zum Schutz der Apps und damit auch der Daten der Nutzerinnen und Nutzer vor externen Zugriffen vornehmen. Die sieben Apps der IT-sicherheitstechnischen Untersuchung haben eine Auswahl grundsätzlicher Anforderungen an die IT-Sicherheit erfüllt, decken diese aber nicht in einer Art und Weise ab, wie es nach dem Stand der Technik zu erwarten wäre. Die Ergebnisse lassen darauf schließen, dass ein bedeutender Anteil der Anbieter keine Daten- und IT-Sicherheit nach den in der technischen Richtlinie „Sicherheitsanforderungen an digitale Gesundheitsanwendungen“ definierten Standards vollständig umsetzt (BSI, 2020).

Die Gesundheitsdaten der Verbraucherinnen und Verbraucher werden somit nicht ausreichend gegen Angriffe geschützt. Die Tragweite der hierdurch entstehenden Risiken, ist für die einzelne Nutzerin respektive den einzelnen Nutzer nur schwer zu ermessen. Gleichzeitig sind sie individuell nur schwer in der Lage, sich ausreichend gegenüber diesen Risiken zu schützen.

Der Markt weist eine hohe Intransparenz auf und für Nutzerinnen und Nutzer ist es schwer bis unmöglich, sich in der Fülle des Angebots zu orientieren sowie die verschiedenen Anbieter und die Seriosität und Sicherheit der Angebote zu bewerten. Der gängige Weg, um sich über Apps zu informieren und diese auszuwählen, ist für die meisten Nutzerinnen und Nutzer über die jeweiligen App Stores. Diese unterziehen die Apps vor der Aufnahme in ihre Stores zwar einer Überprüfung, Aspekte der IT-Sicherheit stehen hier nach aktuellem Kenntnisstand jedoch nicht im Fokus.

Als Reaktion auf die hohe Intransparenz des Marktes wurden in den letzten Jahren von Verbänden, wissenschaftlichen Institutionen oder privatwirtschaftlichen Akteuren Unterstützungsangebote geschaffen, die Nutzerinnen und Nutzern die Orientierung erleichtern sollen. Hierzu zählen beispielsweise Qualitätssiegel, Kodizes und Datenbanken mit vertrauenswürdigen Apps. Die Angebote sind bei den Nutzerinnen und Nutzern allerdings wenig bekannt und stoßen aufgrund der hohen Dynamik im Markt schnell an ihre Grenzen (Lampert, 2020).

Um Verbraucherinnen und Verbraucher im Markt für Gesundheits-Apps besser zu schützen, bedarf es deshalb eines ganzheitlichen Ansatzes, mit dem sowohl Anbieter- als auch Nutzerseite adressiert werden. Auf beiden Seiten ist das Bewusstsein für die bestehenden Risiken zu schärfen.

Anbieter können mit einer Reihe von Maßnahmen die IT-Sicherheitsstandards ihrer Apps erhöhen und so einen besseren Schutz bieten. Zur Authentisierung der Nutzerinnen und Nutzer sollte seitens der Apps die Vergabe sicherer Passwörter gefordert werden, die den aktuellen Empfehlungen des BSI entsprechen. Zur Identifikation der Nutzerinnen und Nutzer sollte zudem eine 2-Faktor-Authentisierung genutzt werden. Einfache Schutzmaßnahmen sind auch App-Sperren und das Ausgrauen von sensiblen Daten, sobald die App in den Hintergrund gelegt wird. Die Übertragung von sensitiven Klartextinhalten, z. B. Passwörtern, sollte vermieden und wo dies technisch möglich ist, geeignet übergeschlüsselt werden. Um eine weitere Steigerung des Sicherheitsniveaus zu erreichen, empfiehlt sich auch der Einsatz von Funktionalitäten, die in den aktuellen Geräten auf Basis von Hardware-Sicherheitsbausteinen zur Verfügung gestellt werden. Um Man-in-the-Middle-Angriffe abwehren zu können, sollten zeitgemäße Methoden zum Schutz verschlüsselter Verbindungen wie Certificate Pinning eingesetzt werden.

IT-Sicherheitsanforderungen sollten im Sinne eines „Security by Design“-Ansatzes bereits im Entwicklungsprozess berücksichtigt und die Anwendung einer unabhängigen technischen Überprüfung unterzogen werden.

Heutige Software ist häufig hochmodular und mit modernen, vernetzten Programmierschnittstellen (sogenannten application programming interfaces, kurz API) verbunden, wie z. B. bei Cloud-Dienstleistungen und mithilfe von GraphQL. Hierbei ist es wichtig, dass diese vor der Integration mit dem eigenen Risikoprofil abgeglichen werden. Verantwortliche in den Bereichen Softwarearchitektur und Sicherheit müssen neue Technologien in die Prüftätigkeiten im Rahmen des Entwicklungsprozesses mit aufnehmen. Bei sorgfältiger Planung und Umsetzung können somit spätere Sicherheitslücken und ein hieraus resultierender Schaden für die Nutzerinnen und Nutzer sowie letztendlich auch für die Reputation des Anbieters vermieden werden.

Mit der 2020 veröffentlichten Technischen Richtlinie „Sicherheitsanforderungen an digitale Gesundheitsanwendungen“ stellt das BSI Entwicklerinnen und Entwicklern von Gesundheits-Apps einen Leitfaden zur Verfügung, der sie bei der Erstellung sicherer mobiler Anwendungen unterstützen soll. Die Richtlinie listet zentrale Aspekte auf, die aus IT-sicherheitstechnischer Perspektive bei der Entwicklung von Gesundheits-Apps berücksichtigt werden sollten. Um die Bekanntheit der Richtlinie zu stärken und eventuelle Herausforderungen bei der Umsetzung der Technischen Richtlinie zu identifizieren, soll der Dialog mit den Anbietern verstärkt und auf dieser Basis die Richtlinie weiterentwickelt werden.

Einen weiteren wesentlichen Ansatzpunkt, mit dem Anbieter digitaler Anwendungen für IT-sicherheits-technische Risiken sensibilisiert und für die stärkere Berücksichtigung im Entwicklungsprozess motiviert werden können, bietet der Fokus auf den Bereich „Corporate Digital Responsibility“. Hiermit wird die bereits seit geraumer Zeit diskutierte „Corporate Social Responsibility“ als sozial, gesellschaftlich und ökologisch verantwortungsvolles Unternehmenshandeln um den Aspekt der digitalen Verantwortung erweitert. Unternehmen können Verantwortung wahrnehmen, indem sie sorgfältig mit den Daten ihrer Nutzerinnen und Nutzer umgehen, sie sicher verwalten und vor Angriffen schützen. Im Kontext von Gesundheits-Apps heißt dies auch, einen ständigen Blick darauf zu haben, welche Daten verarbeitet werden und ob durch eine Erweiterung des Funktionsumfangs der App eine Erweiterung des Schutzes der Nutzerdaten angezeigt ist. Hierzu zählt auch das Bekenntnis der App-Anbieter zur Bereitstellung regelmäßiger und zeitnaher Sicherheitsaktualisierungen während des Produktlebenszyklus.

„Corporate Digital Responsibility“ kann einen Beitrag leisten, das Bewusstsein von Anbietern digitaler Anwendungen für ihre Verantwortung insbesondere gegenüber ihren Nutzerinnen und Nutzern zu stärken, sie für die Auswirkungen ihres Handelns zu sensibilisieren und hieraus resultierend die notwendigen Schritte zum besseren Schutz ihrer Nutzerinnen und Nutzer zu unternehmen.

Gleichzeitig besteht auch auf Nutzerseite Handlungsbedarf. Ebenso wie auf Seiten der Anbieter muss das Bewusstsein bei Verbraucherinnen und Verbrauchern für Risiken im Umgang mit digitalen Gesundheitsanwendungen geschärft werden. Sie müssen über die Beurteilungskompetenz verfügen, um potenzielle Risiken erkennen und bewerten zu können.

Sowohl die eigene Marktanalyse als auch die Literatur kommen zur Erkenntnis, dass ein Großteil der Anbieter von Gesundheits-Apps nur geringe Umsätze über direkte Erlösmodelle – den Verkauf von Apps, In-App-Käufe oder Abo-Modelle – erzielen können. Insbesondere bei diesen Apps ist es wahrscheinlich, dass gespeicherte Daten oder daraus entstandene Profile weitergegeben und ausgewertet werden. Aus Sicht der IT-Sicherheit gilt es hierbei zu beachten, dass durch eine Zunahme der Datenschnittstellen auch das Risiko eines ungewollten Datenabflusses steigen kann.

Die Entwicklung der notwendigen digitalen Kompetenzen, um die Chancen neuer Technologien zu nutzen und Risiken beurteilen zu können, sollte immanenter Bestandteil des lebenslangen Lernens sein. Gleichzeitig gilt es, Verbraucherinnen und Verbraucher durch die Bereitstellung von Informationen für mögliche Risiken zu sensibilisieren und ihnen nutzerfreundliche Leitfäden und Hilfestellungen an die Hand zu geben, um die Qualität und Vertrauenswürdigkeit von digitalen Gesundheitsanwendungen beurteilen zu können.



# Literaturverzeichnis

**Albrecht, U.-V. 2016.** Kapitel 13. Orientierung für Nutzer von Gesundheits-Apps. In: Albrecht, U.-V. (Hrsg.), Chancen und Risiken von Gesundheits-Apps (CHARISMHA). Medizinische Hochschule Hannover, 2016, S. 282–300. urn:nbn:de:gbv:084-16040812052. <http://www.digibib.tu-bs.de/?docid=60020>

**Albrecht, U.-V.; Höhn, M. & von Jan, U. 2016:** Kapitel 2. Gesundheits-Apps und Markt. In: Albrecht, U.-V. (Hrsg.), Chancen und Risiken von Gesundheits-Apps (CHARISMHA). Medizinische Hochschule Hannover, 2016, S. 62–82. urn:nbn:de:gbv:084-16040811225. <http://www.digibib.tu-bs.de/?docid=60007>

**Apple Inc. 2021.** App privacy details on the App Store. Abgerufen am 31. 03 2021: <https://developer.apple.com/app-store/app-privacy-details/>.

**Apple Inc. 2021.** App Store Review Guidelines. Abgerufen am 31. 03 2021: <https://developer.apple.com/app-store/review/guidelines/>.

**Apple Inc. 2021.** Sicherheit bei Apps – Übersicht. Abgerufen am 31. 03 2021: <https://support.apple.com/de-de/guide/security/sec35dd877d0/web>.

**Apptopia. 2020.** Global Mobile Consumer Trends 2020.

**Barcena, M., Wueest, C. und Lau, H. 2014.** How safe is your quantified self? Abgerufen am 31.03.2021: [https://paper.bobyli.com/Meeting\\_Papers/BlackHat/Europe-2014/eu-14-Wueest-Quantified-Self-A-Path-To-Self-Enlightenment-Or-Just-A-Security-Nightmare-wp.pdf](https://paper.bobyli.com/Meeting_Papers/BlackHat/Europe-2014/eu-14-Wueest-Quantified-Self-A-Path-To-Self-Enlightenment-Or-Just-A-Security-Nightmare-wp.pdf)

**Bitkom. 2017.** Positionspapier - Orientierung im Markt der Gesundheitsapps. Abgerufen am 31.03.2021: <https://www.bitkom.org/sites/default/files/file/import/Bitkom-Orientierung-im-Markt-der-Gesundheitsapps.pdf>

**Bundesamt für Sicherheit in der Informationstechnik (BSI). 2020.** Allgemeine Smartphones und Tablets (Edition 2020). Abgerufen am 31. 03 2021: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium\\_Einzel\\_PDFs\\_2021/07\\_SYS\\_IT\\_Systeme/SYS\\_3\\_2\\_1\\_Allgemeine\\_Smartphones\\_und\\_Tablets\\_Edition\\_2021.pdf?\\_\\_blob=publicationn](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium_Einzel_PDFs_2021/07_SYS_IT_Systeme/SYS_3_2_1_Allgemeine_Smartphones_und_Tablets_Edition_2021.pdf?__blob=publicationn).

**Bundesamt für Sicherheit in der Informationstechnik (BSI). 2021.** IT-GrundschutzKompodium. Abgerufen am 31. 03 2021: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium/IT\\_Grundschutz\\_Kompodium\\_Edition2021.pdf?\\_\\_blob=publicationFile&v=6](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium/IT_Grundschutz_Kompodium_Edition2021.pdf?__blob=publicationFile&v=6).

**Bundesamt für Sicherheit in der Informationstechnik (BSI). 2018.** Register aktueller Cyber-Gefährdungen und -Angriffsformen. Abgerufen am 31. 03 2021: [https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS\\_026.html](https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_026.html).

**Bundesamt für Sicherheit in der Informationstechnik (BSI). 2021.** Sichere Passwörter erstellen. Abgerufen am 31. 03 2021: [https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html).

**Bundesamt für Sicherheit in der Informationstechnik (BSI). 2020.** Sicherheitsanforderungen an digitale Gesundheitsanwendungen. Technische Richtlinie BSI TR-03161. 2020.

**Bundesamt für Sicherheit in der Informationstechnik (BSI). 2021.** Zwei-Faktor-Authentisierung. Abgerufen am 31. 03 2021: [https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html).

- Bundesministerium der Justiz und für Verbraucherschutz. 2021.** Telemediengesetz (TMG) § 13 Pflichten des Diensteanbieters. Abgerufen am 31. 03 2021: [https://www.gesetze-im-internet.de/tmg/\\_13.html](https://www.gesetze-im-internet.de/tmg/_13.html).
- Duttweiler, S., Gugutzer, R., Passoth, J.-H. und Strübing, J. (Hg.). 2016.** Leben nach Zahlen. Self-Tracking als Optimierungsprojekt? Digitale Gesellschaft 10.
- Evers-Wölk, M., Oertel, B. und Sonk, M. 2018.** Gesundheits-Apps. Arbeitsbericht Nr. 179. Büro für Technikfolgenabschätzung beim Bundestag, 2018.
- Google. 2021.** Google Play Protect. Abgerufen am 31. 03 2021: <https://developers.google.com/android/play-protect/>.
- Google. 2021.** Programmrichtlinien für Entwickler (gültig ab dem 1. März 2021). Abgerufen am 12.05.2021: [https://support.google.com/googleplay/android-developer/answer/10477564?hl=de&ref\\_topic=9877065](https://support.google.com/googleplay/android-developer/answer/10477564?hl=de&ref_topic=9877065)
- Knöppler, K. und Neisecke, T., Nölke, L. 2016.** Digital-Health-Anwendungen für Bürger. Kontext, Typologie und Relevanz aus Public-Health-Perspektive. Entwicklung und Erprobung eines Klassifikationsverfahrens. Abgerufen am 31. 03 2021: [https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Studie\\_VV\\_Digital-Health-Anwendungen\\_2016.pdf](https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Studie_VV_Digital-Health-Anwendungen_2016.pdf)
- Lampert, C. 2020.** Ungenutztes Potenzial – Gesundheits-Apps für Kinder und Jugendliche. Bundesgesundheitsbl 63, 708–714 (2020). <https://doi.org/10.1007/s00103-020-03139-2>
- Research2Guidance. 2015.** mHealth App Developer Economics 2015. The current status and trends of the mHealth app market.
- Statista. 2021.** Anteil der Smartphone-Nutzer in Deutschland in den Jahren 2012 bis 2020 nach VuMA und Bitkom. Abgerufen am 31. 03 2021: <https://de.statista.com/statistik/daten/studie/585883/umfrage/anteil-der-smartphone-nutzer-in-deutschland/#:~:text=Der%20Anteil%20der%20Smartphone%2DNutzer,internetf%C3%A4higes%20Smartphone%20oder%20Handy%20besitzen.&text=Fast%20jeder%20Deutsche%2C%20der%20>
- Statista nach Research2Guidance. 2020.** Anzahl der Downloads von mHealth-Apps weltweit in den Jahren 2013 bis 2018 (in Milliarden). Abgerufen am 31. 03 2021: <https://de.statista.com/statistik/daten/studie/695434/umfrage/anzahl-der-weltweiten-downloads-von-mhealth-apps/#:~:text=Die%20Statistik%20zeigt%20die%20Anzahl,1%20Milliarden%20mHealth%2DApplikationen%20heruntergeladen.>
- The OWASP Foundation. 2021.** OWASP Mobile Security Testing Guide. Abgerufen am 31. 03 2021: <https://owasp.org/www-project-mobile-security-testing-guide/>.
- tom's guide. 2021.** Google Play Protect review. Abgerufen am 31. 03 2021: <https://www.tomsguide.com/reviews/google-play-protect>.

# Glossar

## **Authentifizierung**

Bei der Authentifizierung wird der bei der Authentisierung vorgelegte Identitätsnachweis einer Person überprüft. Erst nach erfolgreicher Authentifizierung erfolgt dann eine Autorisierung.

## **Authentisierung**

Bei der Authentisierung legt eine Person einen Nachweis über ihre Identität vor, um ihn von einem System überprüfen zu lassen. Dies kann u. a. durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen, die Authentisierung von Daten z. B. durch kryptografische Signaturen.

## **Backend**

Die meisten Anwendungen verlassen sich für die Verarbeitung und Speicherung von Daten nicht ausschließlich auf die von der Laufzeitumgebung bereitgestellten Ressourcen. Sie lagern diese Aufgaben auf ein zentrales System im Hintergrund (Backend) aus. Neben der Verarbeitung und Speicherung von Daten übernehmen diese Systeme oft auch Aufgaben zur Authentifizierung und Autorisierung von Nutzern oder andere zentrale Tätigkeiten.

## **Certificate Pinning**

Beim Certificate Pinning werden die vom Server (ggf. auch von Apps) präsentierten Sicherheitszertifikate anhand ihrer kryptografischen Fingerabdrücke und der ausstellenden Zertifizierungsstelle verglichen, um unbefugten Zugriff zu unterbinden. Das Certificate Pinning ermöglicht hierdurch einen Schutz vor Man-in-the-Middle-Angriffen (s. u.).

## **Hash-Funktion**

Eine Hash-Funktion ist ein kryptografischer Algorithmus, bei dem Nachrichten beliebiger Länge auf einen Hash-Wert fester Länge (z. B. 160 Bit) abgebildet werden. Bei kryptografisch geeigneten Hash-Funktionen ist es praktisch unmöglich, zwei Nachrichten mit dem gleichen Hash-Wert zu finden (Kollisionsresistenz) und bei einem gegebenen Hash-Wert eine Nachricht zu finden, die durch die Hash-Funktion auf den Hash-Wert abgebildet wird (Einwegigkeit).

## **Hash-Wert**

Ein Hash-Wert ist eine mathematische Prüfsumme, die durch Anwendung einer Hash-Funktion aus einer elektronischen Nachricht erzeugt wird. Da es bei einer kryptografisch geeigneten Hash-Funktion praktisch unmöglich ist, zwei Nachrichten zu finden, deren Hash-Wert identisch ist, bezeichnet man den Hash-Wert auch als "digitalen Fingerabdruck" einer Nachricht.

## **Injection-Angriff**

Bei einem Injection-Angriff versucht ein Angreifer, Befehle in eine Webanwendung oder einen Webservice zu injizieren und auszuführen. Auf diese Weise können unbefugt Befehle zum Auslesen oder Manipulieren von Daten übermittelt werden.

## **Input-Escaping**

Durch Input-Escaping werden alle Zeichen - auch Sonderzeichen und Teile von Befehlen - unverändert beibehalten, jedoch wird ein z. B. eingeschleuster Programmcode nicht ausgeführt.

## **Jailbreak**

Bei einem Jailbreak (deutsch: Gefängnisausbruch) werden Sicherheitsmechanismen des mobilen Betriebssystems iOS außer Kraft gesetzt. Nutzer sowie Apps erhalten so vollen Zugriff auf das Betriebssystem. Für einen Jailbreak werden spezielle Programme verwendet, die Schwachstellen in iOS ausnutzen. [...] Durch Jailbreaks hinaus entstehen zahlreiche Angriffspunkte, weil Anwendungen und Anwender vollen Zugriff auf das Betriebssystem erhalten. Dazu zählt auch, dass nach dem Jailbreak Apps aus ungeprüften Quellen installiert werden können, die möglicherweise Schadsoftware enthalten. Viele Benutzer versäumen es auch, ein neues Root-Passwort zu vergeben - mit der Folge, dass es durch den Jailbreak auf einen allgemein bekannten Standardwert gesetzt wird.

**Man-in-the-Middle-Angriffe**

Ziel bei einem Man-in-the-Middle-Angriff ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehr Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer "in die Mitte" der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und gegenüber dem Empfänger als Sender ausgibt. Als erstes leitet der Angreifer eine Verbindungsanfrage des Senders zu sich um. Im nächsten Schritt baut der Angreifer eine Verbindung zu dem eigentlichen Empfänger der Nachricht auf. Wenn ihm das gelingt, kann der Angreifer unter Umständen alle Informationen, die der Sender an den vermeintlichen Empfänger sendet, einsehen oder manipulieren, bevor er sie an den richtigen Empfänger weiterleitet. Auf die Antworten des Empfängers kann der Angreifer wiederum ebenfalls zugreifen, wenn nicht entsprechende Schutzmechanismen wirksam sind.

**Obfuskation**

Durch die Obfuskation wird der Programmcode so verändert, dass der Quelltext nicht oder nur schwer eingesehen und verändert werden kann. Hierdurch wollen die Anbieter z. B. Reverse Engineering oder den Diebstahl ihres geistigen Eigentums durch das Kopieren von Programmteilen verhindern.

**Rooten**

Der Begriff „Rooten“ wird für das Einräumen erweiterter Benutzerrechte auf mobilen Geräten, wie Smartphones oder Tablets, genutzt. Durch das Rooten des mobilen Geräts werden die ursprünglich von dem Hersteller für den Benutzer begrenzten Rechte zur Veränderung beispielsweise des Betriebssystems oder von vorinstallierten Apps erweitert. Gewöhnlich wird der Begriff Rooten für Linux- oder Android-basierte Geräte verwendet. Zum Rooten der Geräte werden spezielle Programme verwendet, die Schwachstellen in dem Betriebssystem ausnutzen. Beim Root-Prozess können sich Fehler ereignen, welche ein Gerät unbrauchbar machen. Ebenso können Nutzerdaten verloren gehen. Aufgrund der erweiterten Rechte können zudem die Auswirkungen von Malware weitaus umfangreicher sein.

**Schwachstelle**

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementierung, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

**Zwei-Faktor-Authentisierung**

Die Zwei-Faktor-Authentisierung bezeichnet die Kombination von zwei Faktoren aus den drei Bereichen Wissen (zum Beispiel Passwort), Besitz (z. B. Chipkarte) und Biometrie (z. B. Fingerabdruck).