Schriftenreihe Fachbereich Informatik

2021-2

Informatik
Hauptcampus

HOCHSCHULE TRIER

Datenschutz und IT-Sicherheit logopädischer Android Apps

Konstantin Knorr, Jenny Griffel

Fachbereich Informatik, Hochschule Trier
{knorr, j.griffel}@hochschule-trier.de

Zusammenfassung

Smartphones und Apps werden für Gesundheitsfachberufe immer beliebter. Für die Logopädie ist das in den Geräten verbaute Mikrophon besonders hilfreich, um den Diagnostik- und Therapieprozess zu unterstützen. Gleichzeitig handelt es sich aber bei Sprachdaten um besonders schützenswerte Daten nach der Datenschutz-Grundverordnung. Außerdem werden die Apps oft von minderjährigen Kindern verwendet. Daher spielen der Datenschutz und die IT-Sicherheit dieser Apps eine wichtige Rolle. Der Artikel beschreibt daher mögliche Angreifer und Gefahren sowie eine Methodik, die Gefahren systematisch zu untersuchen. Die Methodik wird auf die 20 beliebtesten Logopädie-Apps für Android angewendet. Während die Netzwerke mittlerweile gut abgesichert sind, geht die größte Gefahr von den Parteien aus, mit denen die App Kontakt aufnimmt. Viele Apps gehen lokal sorglos mit den Sprachdaten um. Gleichzeitig zeigt ein Vergleich mit einer Studie über Diabetes- und Bluthochdruck-Apps, dass durch die kompliziertere Datenerfassung bei logopädischen Apps mehr Daten, insbesondere Sprachdaten lokal gehalten werden. Die Möglichkeiten zur Identifizierung von Lauten und Wörtern werden zurzeit von den Apps kaum genutzt. Die Verwendung des Android-Ökosystems für L-Apps ist aufgrund der Ergebnisse kritisch zu hinterfragen. Die Methodik ist so konzipiert, dass sie von Nutzern angewendet und damit zum Selbstschutz verwendet werden kann. Es werden abschließend Empfehlungen für Nutzer[1] und App-Entwickler ausgesprochen.

1 Einführung

Im Oktober 2021 beinhaltete der Google Play Store rund 2,8 Mio. Apps, davon ca. 44.000 in der Kategorie *Medical*, ~96.000 in der Kategorie *Health&Fitness* und ~270.000 in der Kategorie *Education*[2]. Darunter befinden sich auch zahlreiche logopädische Apps (L-Apps), die bisher kaum auf Datenschutz (DS) und IT-Sicherheit (ITS) hin untersucht worden sind (vgl. Kap. 5). Mit Inkrafttreten des Digitale-Versorgung-Gesetzes 2019 und der Möglichkeit vom Bundesinstitut für Arzneimittel und Medizinprodukte geprüfte Apps vom Arzt verordnet zu bekommen [BfArM] ist ein zunehmender Einsatz von qualitativ hochwertigen Apps für den Bereich der Heilmittelerbringer zu erwarten. Kostenpflichtige deutsche L-Apps, deren Kosten bereits durch einige Krankenkassen übernommen werden, sind z.B. die als Medizinprodukt zertifizierten Neolexon-Apps für Aphasie und Artikulationsstörungen [NeoKost, SpHJ17]. Geißelmann weist in [GE18] drauf hin, dass durch eine veränderte Risikoeinstufung vieler Apps diese Zahl in den nächsten Jahren steigen dürfte.

---

[1] In der folgenden Arbeit wird aus Gründen der besseren Lesbarkeit ausschließlich die männliche Form verwendet. Sie bezieht sich auf Personen beiderlei Geschlechts.

[2] https://www.appbrain.com

Bei den Nutzern der L-Apps handelt es sich um vulnerable Personengruppen wie Menschen mit Beeinträchtigungen in Sprache und Kommunikation, die einerseits durch Eigentraining mit L-Apps besonders von der neuen Technologie profitieren können. Andererseits sind die erfassten Sprachdaten biometrische Daten und damit laut DSGVO besonders schützenswert. Daher ist ein möglicher Mehrwert gegen die Gefahren abzuwägen. Diese Abwägung für technisch nicht versierte Nutzer ist wg. der Komplexität der technischen Infrastruktur i.d.R. nicht durchführbar und sollte auch nicht zu Last der Nutzenden werden.

Der Bundesdatenschutzbeauftragte warnt, dass der Einsatz von Gesundheits-Apps erhebliche Risiken für das Recht auf informationelle Selbstbestimmung birgt. Derzeit erfüllen wenige Datenschutzerklärungen (DSE) die gesetzlichen Anforderungen. Sie sind zu lang oder schwer verständlich. Zu essenziellen Datenschutzfragen enthalten sie nur pauschale Aussagen. Durch die unklaren Regelungen zur Datenverarbeitung entgleiten diese Daten dabei der Kontrolle durch die Nutzer [BfDI19]. Der vorliegende Artikel untersucht, wie stark L-Apps von diesen Problemen betroffen sind, welche Bedrohungen und Angreifer es gibt und welche Gefahren bzgl. DS und ITS bei der Verwendung von L-Apps bestehen. Dazu wird eine Methodik vorgestellt und auf die beliebtesten L-Apps angewendet.

Der Rest des Artikels hat die folgende Struktur: Kap. 2 beschreibt die Grundzüge von L-Apps sowie Gefahren für und Angreifer auf diese Apps aus Sicht der IT-Sicherheit. Außerdem werden bestehende Schutzmaßnahmen von Android thematisiert. In Kap. 3 wird die verwendete Methodik beschrieben inkl. der Auswahlkriterien der Apps, den verwendeten Tools und der Vorgehensweise. Die Ergebnisse der Untersuchung der L-Apps werden in Kap. 4 beschrieben und diskutiert. Verwandte Arbeiten behandelt Kap. 5. Den Abschluss bildet Kap. 6 mit Empfehlungen für Nutzer und App-Entwickler sowie mit einer Beschreibung möglicher zukünftiger Arbeiten.

2 Grundlagen

2.1 Logopädie-Apps

Gesundheits-App sind ein boomender Markt, der sich an Patienten und Therapierende richtet. Das Potenzial, welches Apps in der Logopädie bieten, ist dabei hoch. Zum einen ermöglichen sie durch eine Ergänzung der klassischen Face-to-Face Therapie eine kostengünstige Erhöhung der für den Therapieprozess relevanten Therapieintensität. So können die Patienten nach erfolgter evidenzbasierter Auswahl einer geeigneten App durch das therapeutische Fachpersonal nicht nur in der Therapie, sondern auch zu Hause mittels App selbstständig und selbstwirksam an ihren Therapiezielen weiterarbeiten [StMü18]. Davon können besonders auch ältere, mobilitätseingeschränkte Menschen profitieren. Unter Berücksichtigung des demografischen Wandels und mangelnder logopädischer Versorgung in ländlichen Gegenden können digitale Medien somit eine effektive Versorgung gewährleisten. Zum anderen bieten Apps das Potenzial, durch die Nutzung von Gamification-Elementen und automatisiert angepasster Übungsformate und Rückmeldungen (Kompetenzempfinden) sowie der inhärenten Stärkung von Unabhängigkeit und Selbstbestimmtheit der Nutzer, im Sinne der Self-Determination Theory [RyDe00], die Motivation der Klienten und damit den Therapieerfolg zu steigern.

Je nach Zielsetzung stehen dabei verschiedene Arten von Apps zur Verfügung: spezifische, zweckentfremdete oder motivationale Apps. Spezifische und zweckentfremdete Apps dienen als Lern- bzw. Übungsmittel, Feedbackhilfe oder Kommunikationsmedium, wobei spezifische

Apps speziell für das logopädische Setting entwickelt wurden. Motivations- & Belohnungsapps wiederum zielen nicht auf das aktive Beüben einer Funktion ab, sondern dienen rein der Motivation des Klienten. Besonders bei spezifischen Apps ist neben Aspekten von DS und ITS sowie der Funktionalität auch eine fachliche Expertise bei der Entwicklung der App unabdingbar.

L-Apps können bei verschiedenen Erkrankungen zum Einsatz kommen. Zu häufigen logopädischen Störungsbildern bei Erwachsenen gehören Dysarhrien und Aphasien. Diese bezeichnen erworbene, neurologische Störungen, die z.B. nach einem Schlaganfall auftreten können. Bei Dysarthrien ist die Motorik des Sprechvorgangs beeinträchtigt (z.B. Atem-, Kehlkopf- und Zungenmuskulatur), was zu einer undeutlichen Aussprache und Unverständlichkeit führt. Dagegen ist bei Aphasien die Sprachverarbeitung (Lesen, Schreiben, Sprachproduktion, Sprachverständnis) von Lauten/Wörtern/Sätzen/Texten oder auch die Pragmatik betroffen. Dies schränkt die Kommunikationsfähigkeit mitunter erheblich ein. Gesundheitsprobleme, die bei Kindern vermehrt auftreten, sind Artikulations- oder Sprachentwicklungsstörungen. Bei Sprachentwicklungsstörungen erwirbt das Kind das Sprachsystem nicht normal, wobei zumeist mehrere Ebenen betroffen sind (Lautbildung, Wortschatz, Grammatik, Kommunikationsverhalten). Bei isolierten Artikulationsstörungen kann das Kind die Sprachlaute nicht korrekt bilden (phonetische Störung, z.B. Sigmatismus / „Lispeln“) und/oder wendet diese nicht korrekt im Wort an, sondern ersetzt sie z.B. durch einen anderen Laut (phonologische Störung). Stottern hingegen bezeichnet eine im Kindesalter auftretende Redeflussstörung, bei der es zu Unterbrechungen des Redeflusses durch Dehnungen oder Wiederholungen von Lauten oder zu Blockierungen kommt. Dabei treten oft weitere Begleitsymptome wie Kopfmitbewegungen oder Verkrampfungen der Gesichtsmuskulatur auf.

Ist die Kommunikation durch Störungen soweit beeinträchtigt, dass sie die Ausführung von Aktivitäten und die soziale Teilhabe beeinträchtigen, können Kommunikationsmedien aus dem Bereich der Unterstützten Kommunikation (engl. AAC, Augmentative and Alternative Communication) die natürliche Sprache ergänzen oder ersetzen. Elektronische Kommunikationshilfen werden z.B. durch sog. Talker bereitgestellt. Diese ermöglichen einen komplexeren Kommunikationsaustausch durch integrierte Sprachausgabe.

2.2 Gefährdungen und Angreifer

Abb. 2 zeigt Kommunikationsbeziehungen einer typischen L-App. Der initiale Download erfolgt im Play Store. Die App wird dann auf dem mobilen Endgerät installiert. Wird die App verwendet, kann bei vielen L-Apps ein Benutzer-Account beim Web-Server der App eingerichtet werden, wo z.B. kumulierte Daten und Berichte über die Verwendung der App gespeichert werden und abrufbar sind. Beim Betrieb werden zusätzlich Kommunikationsbeziehungen zu Servern des mobilen Ökosystems unterhalten z.B. um Werbung zu platzieren oder das Benutzerverhalten und Abstürze zu analysieren. Die verwendeten Server stammen oft von Amazon oder anderen großen Cloud-Anbieter. Es werden meist die DNS-Server von Google/Alphabet verwendet. Die App unterhält zusätzlich Kommunikationsbeziehungen zu Social Media Seiten, vor allem Facebook. Statt einer eigenen Benutzerverwaltung kann mittels OAuth auch der Facebook- oder Google-Account der Anwender benutzt werden. Einige Apps erlauben den Versand von E-Mails mit logopädischen Daten direkt aus der App hinaus. Manche Apps haben die Spracherkennung an externe Anbieter ausgelagert. Für eine bessere Sprachqualität kann ein externes Mikrophon über Bluetooth oder über USB genutzt werden.

Im beschriebenen Szenario werden unterschiedliche Daten verarbeitet, die sich grob in die folgenden Kategorien einteilen lassen:

D1. Logopädische Daten, hier vor allem Sprachdaten ggf. mit Krankheitsbezug wie Stottern oder Artikulationsstörungen (z.B. Sigmatismus).
D2. Gesundheits-Metadaten wie Zeitpunkte und Dauer der Sprachübungen, Name und Anschrift des Therapeuten
D3. Benutzerdaten wie Vor- und Nachname, Alter, E-Mail-Adresse, Android Werbe-ID, IP- und MAC-Adresse des Geräts

Als mögliche Angreifer auf die Sprach- und Metadaten kommen die folgende Parteien in Frage:

A1. Parteien des mobilen Ökosystems, vor allem Alphabet / Google
A2. Gesundheitsdienste-Anbieter
A3. Angreifer im Netzwerk (WLAN, Bluetooth oder Internet), der vor allem ungeschützten Kommunikationsdaten z.B. auf Vermittlungsknoten oder im Netzwerk abgreifen oder modifizieren kann.
A4. Entwickler von ggf. bösartigen Apps, die auf dem mobilen Endgerät installiert sind und dort auf logopädische Daten zugreifen.

Wir können an dieser Stelle keine tiefere Risikoanalyse vornehmen, da die Einsatzszenarien sich von Nutzer zu Nutzer stark unterscheiden. Im Kapitel 4 werden wir die Parteien nochmals genauer untersuchen.

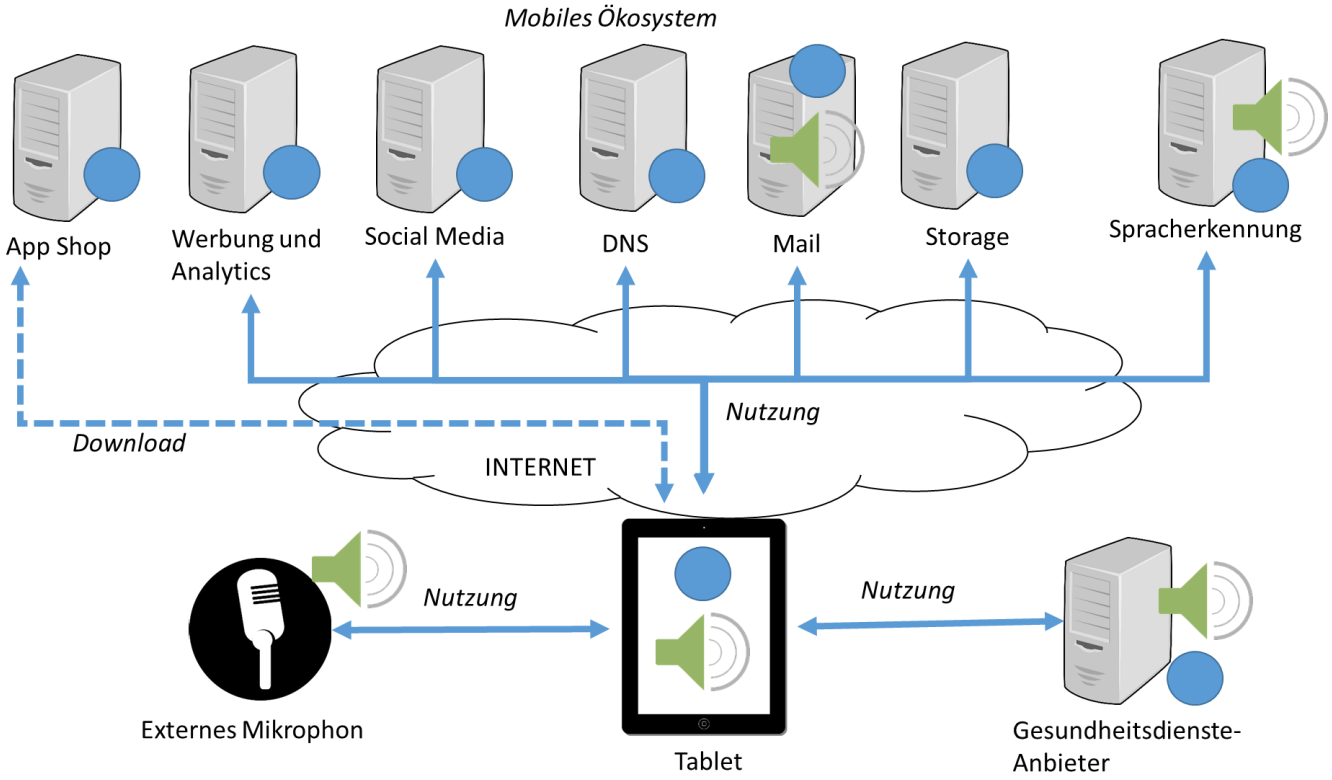

Abbildung 1: Kommunikationsbeziehungen einer Logopädie-App. Das Lautsprecher-Symbol kennzeichnet, an welchen Stellen biometrische Sprachdaten (D1) verarbeitet werden. Der Kreis symbolisiert Gesundheits-Metadaten (D2) oder Benutzer-Daten (D3).

2.3 Android Sicherheits-Bordmittel

Android bietet viele inhärente Absicherungen, die im Laufe der Versionen kontinuierlich ausgebaut und verbessert wurden. Beispiele sind die Abschottung der App-Dateien durch Linux-

Zugriffsrechte und das Berechtigungskonzept mit expliziter Rückfrage bei „gefährlichen“ Berechtigungen wie z.B. der Nutzung des Mikrophons. Die INTERNET-Berechtigung ist seit Android 4.1 nicht mehr „gefährlich“ und wird so ohne Rückfrage jeder App gewährt. Ein Benutzer kann nicht erkennen oder beschränken, mit wem seine App kommuniziert. Dafür wäre ein gerootetes Gerät notwendig.

Andere Absicherungen obliegen dem Nutzer und werden durch die Auswahl des Gerätes und der Hardware beeinflusst wie z.B. die Verwendung und Wahl der Authentisierung (PIN, Password, biometrische Merkmale), die Festplattenverschlüsselung, welche Daten geloggt werden und die Verwendung eines verschlüsselten Backups.

Weitere Absicherungen liegen in der Verantwortung des Entwicklers der App wie z.B. die korrekte Verwendung von TLS, (G)QUIC, der Speicherort der Daten (z.B. aus der SD-Karte und somit für andere Apps erreichbar), die Auswahl und Verwendung der Berechtigungen oder eine zusätzliche Authentisierung oder Verschlüsselung für die App z.B. über die Eingabe einer PIN.

3 Methodik

Die verwendete Methodik basiert auf der von Knorr und Aspinall [KA15]. Sie wurde 2015 bereits auf Diabetes und Bluthochdruck angewendet [KAW15] und wird hier modifiziert auf L-Apps angewendet. Die Untersuchung wurde auf einem Lenovo tab4 10 PLUS (Lenovo TB-X704F) mit Android 7.1.1 (Kernel 3.18.31) durchgeführt. Das Gerät wurde nicht gerootet. Die Methodik stützt sich auf frei verfügbaren Apps und Tools, die teilweise direkt auf dem mobilen Endgerät verwendet werden, um so auch für App-Nutzer die Nachvollziehbarkeit der Untersuchung zu ermöglichen.

Da in der logopädischen Therapie zumeist an der zwischenmenschlichen Kommunikation gearbeitet wird, eignen sich Apps, die Mikrophon-Aufnahmen zur Evaluation des Outputs nutzen. In dieser Arbeit wurden deshalb spezifische Übungs- und Kommunikationsapps untersucht, die eine Mikrophon-Berechtigung erfordern. Als Übungsapp wurden Applikationen verstanden, in denen der Nutzer direkt Aufgaben (z.B. Wort-Bild-Zuordnungen, Hören bzw. Aussprechen von Lauten) bearbeiten kann und Feedback bekommt. Die Aufgaben sind dabei nach fachlichen Kriterien aufgebaut (z.B. linguistische Ebene, Wortfrequenz, phonetische Komplexität). Die Apps können zusätzlich spielerische Elemente zur Motivationsförderung enthalten (z.B. Sterne/Sticker sammeln, lustige Selfies machen, Minispiele). Als Kommunikationsapps werden Anwendungen definiert, die im Sinne der Unterstützten Kommunikation (UK) Kommunikationstafeln oder Talker bereitstellen und dadurch die Kommunikation des Nutzers ergänzen oder ersetzen.

3.1 Auswahlkriterien

- Android App im Google Play Store
- Die Mikrofon-Berechtigung wird verlangt.
- Fachliche Eignung der App (spezifisch logopädisch oder zweckentfremdet), geprüft durch akademische Sprachtherapeutin
- Sprachen der Apps: Deutsch oder Englisch
- Hohe Installationszahlen ≥ 1.000 für deutsche und ≥ 10.000 für englischsprachige Apps

- Die App wurden über folgende Suchbegriffe im Google Play Store gefunden: Sprachtherapie / Logopädie / Speech Therapy, Stottern / Stutter/ Stammering, Aphasie/ Aphasia, Dysarthrie / Dysarthria
- Übungsapp, kein Diagnostiktool, keine reine Informationsapp
- Kostenlos, Demo-Accounts und In-App Käufe sind zulässig

Basierend auf diesen Auswahlkriterien wurden im März 2020 n=20 Apps identifiziert. Die Apps stammen von 15 verschiedenen Herstellern aus Deutschland, Indien, Israel, Kanada, Malaysia, Tschechien, der Türkei und den USA. Die App „Speech Blubs: Language Therapy“ ist mit über einer halben Millionen Installationen die beliebteste. 7 Apps sind in deutscher Sprache gestaltet, die übrigen in Englisch. Die Apps stammen aus den Play Store-Kategorien Medical (8), Education (6), Health & Fitness (2). Abb. 2 zeigt beispielhaft Screenshot von drei dieser Apps.

Eine vollständige Liste der L–Apps inklusive der Package-Namen, Versionen und der vollständigen Untersuchungsdaten ist unter https://seafile.rlp.net/d/7c033313c5e94d069c10/ verfügbar.

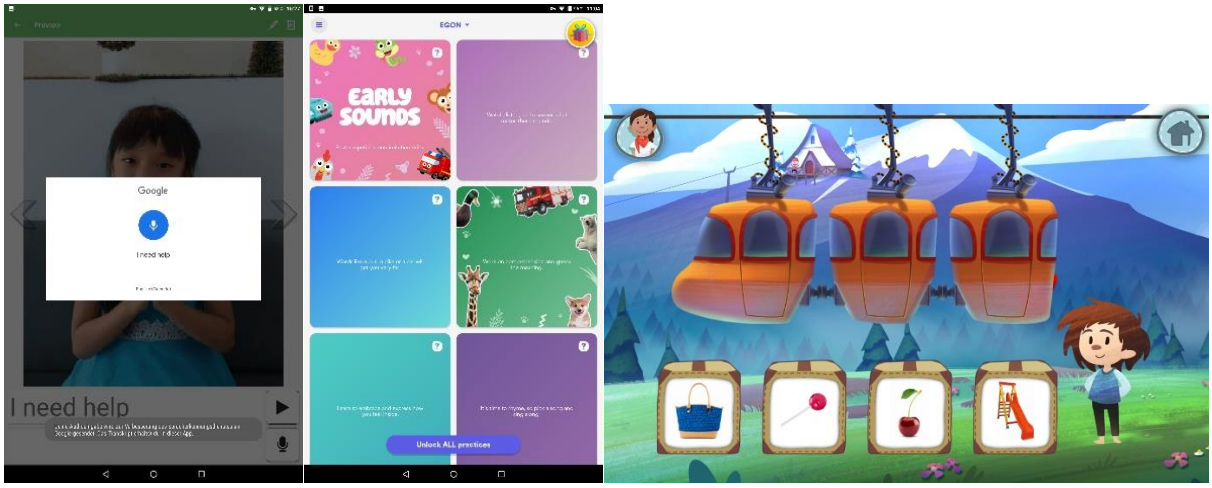

Abbildung 2: Beispiele für L-Apps (von links): “HelpMeTalk” mit Google Spracherkennung, die beliebteste App „Speech Blubs: Language Therapy“ und „neolexon Artikulationsstörungen“

3.2 Vorgehensweise

Die Vorgehensweise setzt sich aus vier Teilen zusammen:

(A) Statische Analyse der App
(B) Dynamische Analyse der App
(C) Untersuchung der Datenschutzerklärung der App
(D) Untersuchung der Web-Applikation der App (falls vorhanden)

Die Ergebnisse wurden in Tabellen erfasst. Die erfassten Daten wurden durch Kontrollfragen in Ja/Nein-Form geprüft. „Ja“ deutet auf ein mögliches DS- oder ITS-Problem hin, bspw. „Nutzt die App Youtube-Erklärvideos aus der App heraus?“ Die „Jas“ werden zum Vergleich zu einem einfachen Score zusammengezählt. (A)-(C) wurden auf alle Apps angewendet (vgl. Tabellen 1-3), (D) nur auf Apps mit Benutzerkonto auf dem App-Server (vgl. Tab. 4). Je höher der Score, desto kritischer / schlechter das Ergebnis. Teilweise mussten Fragen unbeantwortet bleiben, weil die verwendeten Tools kein Ergebnis lieferten. In diesem Fall bleibt die Antwort offen oder ein „?“ wurde verwendet. Dies erhöht den Score nicht.

(A) Die statische Analyse basiert auf den Informationen, die in der APK[3]-Datei enthalten sind wie bspw. das Manifest[4] inkl. der Android Berechtigungen und der kompilierte Code. Addons Detector[5] wurde benutzt, um Werbe- und Analytic-Bibliotheken im Code zu identifizieren. Lumen Privacy Monitor[6] wurde für die Extraktion der Berechtigungen verwendet.

(B) Dynamische Analyse. Wir verwendeten einen imaginären Patienten mit Sprach- bzw. Sprechstörungen, für den wir im Vorfeld ein Facebook-, Twitter-, Dropbox- und Gmail-Konto angelegt haben. Bei der ersten Verwendung der App wurde, falls möglich, ein Benutzerkonto angelegt. Dann wurde die App zum Sprach-/ Sprechtraining verwendet und dabei primär die Features der App, die eine Sprachaufnahme verlangen. Im Falle einer Spracherkennung wurde analysiert, ob fremde Dienste in Anspruch genommen wurden. Im Anschluss wurde versucht, die erfasstem Daten zu exportieren (z.B. per E-Mail oder auf die SD-Karte). Mittels Tpacketcapture Pro[7] und Lumen wurde der Netzwerkverkehr aufgezeichnet und anschließend mit Wireshark[8] analysiert. Es wurde u.a. getestet, ob YouTube-Videos eingebettet waren, ob eine Gesichtserkennung beinhaltet war, ob die App ohne WLAN genutzt werden konnte, ob es in der App eine Möglichkeit gab, alle gespeicherten Daten zu löschen, ob die DSE in der App einsehbar war und ob die im Manifest angeforderten Berechtigungen, insbesondere die Verwendung des Mikrophons, nachvollziehbar waren. Mittels der Android Debugger Kommandos `adb logcat` wurde getestet, wie stark geloggt wurde und ob die Logs medizinische Daten enthalten. Nach gespeicherten Sprach- und Bilddaten wurde mit einem Filemanager und `adb` gesucht.

(C) Datenschutzerklärung: Für alle Apps wurde die im Play Store angegeben DSE nach folgenden Punkten untersucht: Mittels Privacy Badger[9] auf Firefox wurde die Anzahl der Web-Tracker auf der DSE- und Produkt-Seite protokolliert. Weitere Punkte sind die Länge der DSE, das Veröffentlichungsdatum und die verwendete Sprache. Da auch außereuropäische Apps untersucht wurden, wurden statt der DSGVO ausgewählte Prinzipien der OECD Privacy Guidelines[10] als Grundlage verwendet, die sich aber in weiten Teilen auch in der DS-GVO wiederfinden. Die Prüfung fand nur anhand von Stichpunktfragen statt, da eine tiefere rechtliche Prüfung der DSEn den Rahmen der Arbeit sprengen würde.

(D) Untersuchung des Web-Servers der App. Für Apps mit einem Benutzerkonto auf einem L-App-Server (n=9) wurde ein Benutzerkonto eingerichtet und dann Folgendes getestet: Welches Protokoll wird für die Übertragung der Daten verwendet? Welche Daten werden im Klartext übertragen? Welche Passwortkomplexität wird verlangt? Kann ein Facebook- oder Google-Konto zum Anmelden verwendet werden? Aus den PCAPs wurde mittels Wireshark zudem die verwendete TLS Version extrahiert.

---

[3] APK = Android Package. Ein Archiv, das den Source Code und alle anderen benötigten Dateien einer Android App enthält.

[4] Vgl. https://developer.android.com/guide/topics/manifest/manifest-intro

[5] https://play.google.com/store/apps/details?id=com.denper.addonsdetector

[6] https://play.google.com/store/apps/details?id=edu.berkeley.icsi.haystack

[7] https://www.taosoftware.co.jp/en/android/packetcapture/ erlaubt die Speicherung des Traffics pro App

[8] https://www.wireshark.org/

[9] https://privacybadger.org/

[10] https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

Tab. 1: Ergebnisse der statischen Analyse (A) mit kumuliertem Score (n=20)

Package Name	Anzahl 3rd Party Libs (Addon Detector)	Davon Werbung	Werbebibliotheken im Code enthalten	Davon Analytic	Analytics-Bibliotheken im Code enthalten	Anzahl Berechtigungen (Lumen + Addons Detector)	Mehr als 5 Berechtigungen	Anzahl "Dangerous" Berechtigunen (Lumen)	Mehr als 1 gefährliche Berechtigungen	Score	Anmerkungen / Kritische Punkte
com.neolexon.neolino	3	0	N	0	N	4	N	2	J	1	Kamera-Berechtigung
com.ionicframework.patientapp613489	2	0	N	0	N	7	J	4	J	2	
com.neolexon.therapeut	2	0	N	0	N	7	J	4	J	2	
de.speechcare.moveapp	11	0	N	0	N	15	J	4	J	2	Kamera-Berechtigung
com.pmqsoftware.logopedie2.de	2	0	N	0	N	7	J	2	J	2	
com.stamurai.stamurai	39	1	J	5	J	21	J	7	J	4	Kamera-Berechtigung, READ_PHONE_STATE
com.otsimo.speech	32	0	N	6	J	31	J	2	J	3	Kamera-Berechtigung
com.tactustherapy.apraxiatherapy.lite	5	0	N	1	J	6	J	3	J	3	
com.tactustherapy.languagetherapy.lite	7	0	N	0	N	6	J	3	J	2	
com.tactustherapy.conversationtherapy.lite	10	0	N	1	J	4	N	1	N	1	
com.pmqsoftware.logopadie.de	2	0	N	0	N	7	J	2	J	2	
com.speechessentials.speechessentials	8	0	N	2	J	11	J	4	J	3	
org.blubblub.app.speechblubs	33	0	N	5	J	16	J	5	J	3	Kamera-Berechtigung
com.constanttherapy.android.main	42	1	J	3	J	16	J	5	J	4	Kamera-Berechtigung
com.hycsapp.hlpmetlk	15	2	J	1	J	14	J	4	J	4	Kamera-Berechtigung
com.pmqsoftware.game.childrencards.de	2	1	J	0	N	2	N	1	N	1	Kein INTERNET-Berechtigung
com.elelad.comboard	17	0	N	3	J	10	J	4	J	3	
com.shmoontz.commboards.lite	15	0	N	2	J	10	J	2	J	3	
org.me.alexicomaac	1	0	N	0	N	5	N	3	J	1	Kamera-Berechtigung
com.jabstone.jabtalk.basic	0	0	N	0	N	7	J	3	J	2	Kamera-Berechtigung

Tab. 2: Ergebnisse der dynamischen Analyse (B) mit kumuliertem Score (n=20)

Package Name	App nur im Play Store erhältlich	Verwendete externe Spracherkennung z.B. von	Anzahl Flows (Lumen)	Social Media aktiv (Lumen)	Kontakt zu Social Media seite (Lumen)	Ad or Tracker Active (Lumen)	Kontakt zu Ad oder Tracking Seite (Lumen)	Anzahl der Verbindungen zu externen IP-Adressen (Wireshark)	Anzahl der IP-Verbindungen > 0 (Wireshark)	Verwendung von Klartext-Protokollen (Wireshark)	Bild.Dateien für andere Apps zugreifbar im Dateisystem	Speichert Sound-oder Versand therapeutischer Daten per E-Mail	App heraus	Nutzt Youtube-Erklärvideos aus	App nutzt Gesichtserkennung	Verwendet KEIN zusätzliches Pasword zur Authentisierung oder zur Verschlüsselung	KEIN Löschen aller Daten über App möglich	App nur mit Internetverbindung nutzbar	DSE nicht in App erreichbar	Berechtigungen fraglich, vor allem Mikrofonnutzeun	Anzahl der Einträge der App in Logcat	Logeinträge > 2	Score	Anmerkungen / Kritische Punkte
com.neolexon.neolino	J	N	3		N	1	J	12	J		J	N	N	N	J	J	N	N	N	0	N	6	Löschen der Daten nicht im Demo-Modus möglich
com.ionicframework.patientapp613489	J	N	3		N	1	J	NA			N	N	N	N	J	J	N	N	N	0	N	4	Lumen meldet Fingerprint
com.neolexon.therapeut	J	N	3		N	1	J	NA			?	N	N	N	J	J	N	J	N	0	N	5	Lumen meldet Fingerprint
de.speechcare.moveapp	J	J	2		N		N	4	J		N	N	N	N	J	J	J	N	N	0	N	6	Fraunhofer Spracherkennung
com.pmqsoftware.logopedie2.de	J	N	0		N		N	NA			N	N	N	N	J	J	N	J	J	0	N	5	INTERNET-Berechtigung fraglich
com.stamurai.stamurai	J	N	8	1	J	4	J	56	J	N	J	N	J	N	J	J	J	N	N	0	N	9	Dateien auf SDCARD, Überladen mit Videos, NTPv3
com.otsimo.speech	J	N	5	1	J	3	J	34	J	N	N	N	N	J	J	J	J	N	J	0	N	9	Mikrofon-Berechtigung fraglich, Sehr aggressive Werbung für kommerzielle Version, Initial Report zum Ködern, App nutzt Gesichtserkennung
com.tactustherapy.apraxiatherapy.lite	J	N	1		N	1	J	6	J	J	J	J	N	N	J	J	N	N	N	0	N	8	HTTP-Traffic mit App-Namen und Geräteddetails im Klartext, Datensammlung wird per Default zugestimmt
com.tactustherapy.languagetherapy.lite	J	?	1		N		N	1	N	J	N	J	N	N	J	J	N	N	N	15	J	6	Lumen meldet Fingerprint, http mit App-Namen in URL
com.tactustherapy.conversationtherapy.lite	J	?	2		N	1	J	NA			N	J	N	N	J	J	N	N	N	0	N	5	Lumen meldet Fingerprint, http, E-Mail-Reports
com.pmqsoftware.logopadie.de	J	N	0		N		N	NA			N	N	N	N	J	J	N	J	J	0	N	5	INTERNET-Berechtigung fraglich
com.speechessentials.speechessentials	J	N	1		N		N	22	J	J	N	N	J	N	J	J	N	J	J	0	N	8	Mikrofon-Berechtigung fraglich, nutzt Youtube Videos zur Erklärung, MySQL als Klartext-Protokoll, E-Mail Export ist für zukünftige Version geplant
org.blubblub.app.speechblubs	J	N	7	1	J	3	J	54	J	J	J	N	N	J	J	J	J	N	N	0	N	10	HTTP mit App-Namem im Klartext, App nutzt Gesichtserkennung und exportiert dann Fotos in die Galerie
com.constanttherapy.android.main	J	N	2	1	J	0	N	66	J	N	N	N	N	N	J	J	J	N	N	1	N	6	Verwendet eigene Spracherkennung, Link zur DSE beim Anlegen des Accounts
com.hycsapp.hlpmetlk	J	J	1		N		N	7	J	J	N	N	N	N	J	N	J	J	N	13	J	8	Verwendet Google Spracherkennung, Passwort-Schutz, HTTP-Klartext
com.pmqsoftware.game.childrencards.de	J	N	NA		N		N	0	N		N	N	N	N	J	J	N	J	N	0	N	4	Keine Internet-Berechtigung
com.elelad.comboard	J	N	NA		N		N	27	J	N	J	N	N	N	J	N	N	N	N	0	N	4	Analysedienste per Default zugelassen
com.shmoontz.commboards.lite	J	N	NA		N		N	16	J		J	N	J	N	J	N	N	J	J	0	N	7	Mikro wird erst in Volleversion benötigt, YT-Hilfevideos
org.me.alexicomaac	J	N	3		N		N	4	J	N	N	N	N	N	N	N	N	N	N	0	N	2	Mikrophon wird erst nach Umstellen der Settings benötigt (Edit-Mode)
com.jabstone.jabtalk.basic	J	N	NA		N		N	10	J	N	J	N	N	N	J	J	N	J	N	0	N	6	Daten im Backup
Summe	20	2			4		8		13	5	7	3	3	2	19	16	6	8	5		2		

Tab. 3: Auswertung (C) der Datenschutzerklärung (n=20)

	Basisdaten						Vollständigkeit DSE								Web-Seite					
Package-Name	Anzahl Wörter	Anzahl Zeichen (<- Leerzeichen)	Version / Datum	DSE älter als Mai 2018 oder nicht angegeben	Sprache der DSE	KEIN Datenschutzbeauftragter bzw. KEINE Kontaktadresse / E-Mail für Datenschutz angegeben	KEINE technisch / organisatorischen Schutzmaßnahmen beschrieben	Zweck der Datensammlung und Verwendung der Daten der App NICHT beschrieben	Rechte der Betroffenen NICHT aufgelistet	Gemeinsame DSE für App und Web-Seite	Android Permissions werden NICHT erklärt	Weitergabe von Daten an andere Parteien	DSE erlaubt Werbung für externe Produkte / Dienste?	Anzahl Tracker auf Datenschutzseite (Privacy Badger)	Anzahl Tracker auf Datenschutzseite > 0 (Privacy Badger)	Anzahl Tracker auf Hauptseite (Privacy Badger)	Anzahl Tracker auf Hauptseite > 0 (Privacy Badger)	Score	Anmerkungen / Zitate
com.neolexon.neolino	3538	24035	März 2020	N	DE	N	N	N	N	J	N	N	N	4	J	6	J	3	Die Aufnahmen werden nur für die Dauer der direkten Wiedergabe lokal auf Ihrem Endgerät gespeichert und nicht an neolexon oder andere Personen übertragen. Die Daten werden anonymisiert ausgewertet, um die Effektivität des Trainings zu belegen.
com.ionicframework.patientapp613489	3538	24035	März 2020	N	DE	N	N	N	N	J	N	N	N	4	J	6	J	3	
com.neolexon.therapeut	3538	24035	März 2020	N	DE	N	N	N	N	J	N	N	N	4	J	6	J	3	
de.speechcare.moveapp	4647	31703	KA	J	DE	N	J	J	N	J	J	KA	N	3	J	3	J	7	Es ist kein Beauftragter bestellt. Kontaktinfos werden aber angegeben. Lange Begriffsbestimmugen und Rechteauflistung. Wenig konkretes. "Wir haben technische und organisatorische Maßnahmen getroffen." Wieche?
com.pmqsoftware.logopedie2.de	55	308	29.9.2015	J	E	J	NR	NR	NR	J	J	N	N	0	N	2	J	5	DSE sehr kurz und mit Rechtschreibfehlern, DSB nicht benannt
com.stamurai.stamurai	1224	6531	2019-05-08	N	E	N	J	N	J	J	J	N	N	0	N	4	J	5	We do not sell, trade, or otherwise transfer to outside parties your Personally Identifiable Information.
com.otsimo.speech	4778	25929	KA	J	E	N	N	J	N	J	N	J	J	2	J	6	J	7	Privacy Policy and User Agreement, Electing to share your personal information with carefully selected companies so that they can send you offers and promotions about their products and services
com.tactustherapy.apraxiatherapy.lite	2712	13539	10.4.2020	N	E	N	NR	NR	NR	J	N	N	N	6	J	6	J	3	"Apps: We collect NO personal information", "This recorded information is never transmitted to us.", Privacy Bagder warnt for Facebook
com.tactustherapy.languagetherapy.lite	2712	13539	10.4.2021	N	E	N	NR	NR	NR	J	N	N	N	6	J	6	J	3	Privacy Bagder warnt for Facebook
com.tactustherapy.conversationtherapy.lite	2712	13539	10.4.2022	N	E	N	NR	NR	NR	J	N	N	N	6	J	6	J	3	Privacy Bagder warnt for Facebook
com.pmqsoftware.logopadie.de	55	308	29.9.2015	J	E	J	NR	NR	NR	J	J	N		0	N	2	J	5	DSE sehr kurz und mit Rechtschreibfehlern
com.speechessentials.speechessentials	601	3121	14.11.2015	J	E	N	J	N	J	J	J	N	J	2	J	1	J	8	"We may use your Personal Information to contact you with newsletters, marketing or promotional materials", "The security of your Personal Information is important to us", aber keine Maßnahmen beschrieben.
org.blubblub.app.speechblubs	2554	13361	KA	J	E	N	N	N	N	J	J	N	N	1	J	3	J	5	DSE inkl. Terms of Use, Gesichtserkennung nur lokal. "We will not sell or share personal data about children with third-party companies for marketing purposes."
com.constanttherapy.android.main	941	5114	30.3.2018	J	E	J	J	N	J	J	J	N	N	8	J	8	J	8	"We may collect device-specific information", "If the user provides explicit permission, user's location information might be collected as part of the service."
com.hycsapp.hlpmetlk	162	832	29.3.2019	N	E	N	NR	NR	NR	N	N	N	N	0	N	0	N	0	DSE auf Github, Permissions werden erklärt, "No personal information will be collected when you are using this app."
com.pmqsoftware.game.childrencards.de	675	3294	16.01.2020	N	E	J	NR	NR	NR	J	J	N	N	0	N	2	J	4	
com.elelad.comboard	1200	7200	22.10.2017	J	E	N	N	N	J	J	J	J	J	2	J	2	J	8	"Affiliate: We may disclose information about you to our affiliates for the purpose of being able to offer you related or additional produkt and services"
com.shmoontz.commboards.lite	1595	8149	27.9.2018	N	E	N	J	N	J	J	J	J/2	N	3	J	5	J	6	unique device identifier is collected, "We also reserve the right to transfer your Personal Information in the event we sell, merge or transfer all or a portion of our business or assets. "
org.me.alexicomaac	477	2449	KA	J	E	J	J	N	J	J	J	N	N	5	J	5	J	8	"We do not sell your information or deal in any way with third-parties." " We will not disclose your personal information to any third party, period."
com.jabstone.jabtalk.basic	56	277	KA	J	E	J	NR	NR	NR	J	J	NR	NR	3	J	2	J	6	JABtalk's privacy policy is quite simple. We don't receive or even have a mechanism to receive information about our users. No data is collected. No advertisements are sold.
Summe				10		6	6	2	6	19	12	2	3	0	15	0	19		

Tab. 4: Ergebnisse der Untersuchung (D) der Web-Applikation der App (n=9)

Package-Name	Password Length (Number of	Passwortlänge <=6 möglich	Passwort möglich Nur Buchstaben oder Zahlen als	Facebook möglich Login über	TLS.Version<1.2	Score	Anmerkungen / Kritische Punkte
com.neolexon.neolino	8	N	J	N	N	1	
com.ionicframework.patientapp613489	8	N	J	N	N	1	Konto nur mit Therapeuten
com.neolexon.therapeut	8	N	J	N	N	1	Konto nur für Therapeuten nutzbar
com.stamurai.stamurai	6	J	N	J	N	2	Login alternativ für Facebook-Konto möglich
com.otsimo.speech	6	J	J	J	N	3	Login alternativ für Facebook-Konto möglich, Werbung per E-Mail wird beim Anlegen des Account per Default zugestimmt
org.blubblub.app.speechblubs	8	N	J	N	N	1	
com.constanttherapy.android.main	1	J	J	N	N	2	
com.elelad.comboard	6	J	N	N	N	1	
org.me.alexicomaac	3	J	J	N	N	2	
Summe		5	7	2	0		

4 Ergebnisse und Diskussion

Die Tabellen 1-4 zeigen die Ergebnisse der Untersuchungen. Den Autoren ist klar, dass die Methodik nur einen kleinen Ausschnitt möglicher Probleme aufgreift und mit dem vereinfachten Punktesystem keine Risikobewertung für einzelne Nutzer oder Nutzungsszenarien darstellt. Trotzdem erlaubt die Methodik einen ersten Vergleich der Apps, wobei zwei Gruppen unterschieden werden müssen: L-Apps mit (9) bzw. ohne Web-Account (11).

Die häufigsten Probleme bei (A) sind eine Vielzahl von Berechtigungen insbesondere von „gefährlichen“ Berechtigungen neben der Verwendung des Mikrophons wie z.B. Kamera. Es gibt eine einzige App, die keine INTERNET-Berechtigung hat und daher auch keine Daten übertragen kann. 10 L-Apps habe eine externe Analytic- und 4 eine Werbe-Bibliothek eingebunden. Bei (B) ist die Anzahl der Verbindungen zu unterschiedlichen externen IP-Adressen das häufigste Problem. Es gibt 3 L-Apps, die zu über 50 IP-Adressen Verbindungen aufbauen (max. 66). Lumen weist den Datenfluss zu Social Media Seiten (4, Facebook) und Werbe- und Trackerseiten (8) nach und warnt, dass ein Fingerprint z.B. bestehend aus der Geräte ID gebildet wird (5). Bei 5 Apps wird Klartext-Traffic verwendet, vor allem HTTP mit dem App-Namen in der URL oder im HTTP-Header, einmal auch das MySQL-Protokoll mit allen SQL-Statements im Klartext.

Keine L-App erlaubt die Eingabe eines zusätzlichen Passwortes zur Authentisierung oder Verschlüsselung der Daten, 6 Apps speichern die Sound-Daten für alle anderen Apps zugreifbar. 3 Apps versenden Sound- oder therapeutische Dateien per E-Mail, ohne die Nutzer auf etwaige Probleme hinzuweisen. Nur 6 von 20 Apps erlauben das explizite Löschen aller Sprachdaten aus der App heraus. 8 Apps lassen sich nur mit eingeschaltetem WLAN in vollem Umfang nutzen. Es wurde auch geprüft, ob die App direkt auf der Web-Seite des Herstellers zum Download bereit steht unter Umgehung des Play Stores: kein Hersteller bietet dies an.

(C) Erfreulicherweise hatten alle untersuchten App eine DSE, allerdings von unterschiedlicher Länge und Qualität. Viele Ergebnisse unserer Überprüfung decken sich mit [BfDI19]. Spezifisch für unsere Untersuchung sind folgende Punkte: Der Zweck der Datenverarbeitung und Kontaktadressen werden bei erfreulich vielen DSEn angegeben. Die DSEn sind meist gut verständlich und transparent bzgl. Ihrer Datenerfassung und –nutzung. Werbung und eine Weitergabe von Sprachdaten wird nur vereinzelt genannt. Nur 9 DSEn erläutern die verwendeten Android Berechtigungen, meist nur die gefährlichen Berechtigungen (also nicht von der INTERNET-Berechtigung). 19 von 20 Apps mischen die DSE von App und Web-Seite. Der Privacy Badger zeigt, dass bei 15 der 20 Web-Seiten mit DSEn von externen Trackern überwacht werden, bei den Hauptseiten sind es sogar 19 von 20.

(D) Während die Übertragung zum Server bei allen 9 Apps mit TLS ≥ v1.2 gut abgesichert war, gilt dies für die Passwörter nicht: 5 Apps erlauben Passwörter mit 6 oder weniger Zeichen, bei 7 kann man nur Zahlen oder Buchstaben verwenden. Bei einer App reicht ein Passwort mit einem Zeichen. Vier Apps erlauben das Login über Google- oder Facebook-Konten.

Betrachtet man die in Kap. 2.2 definierten Angreifer A1-A5, so fällt auf, dass die größte Gefahr vom mobilen Ökosystem allen voran von Google/Alphabet als Betreiber des Play Stores und größtem Anbieter von Werbung und Analyse-Funktionalität ausgeht. Gegen andere Angreifer wie z.B. A3 sind die Apps mittlerweile durch die Verwendung von TLS/(G)QUIC gut geschützt und nur noch vereinzelt treten Klartextprotokolle auf. Selbst DNS wird nicht mehr im Klartext verwendet. Allerdings ist auch hier Google der größte Anbieter von DNS-Servern, die die An-

fragen trotz Transportverschlüsselung immer noch auswerten können. Im mittleren Bereich finden sich A4 und A5. Das Angriffspotential der Anbieter selbst (A2) ist in den DSEn mehr oder weniger gut ablesbar und schwankt pro App von „nicht vorhanden“ bei Apps ohne Netzwerkverkehr bis hin zu „sehr invasiv“ bei Apps mit vielen Netzwerkverbindungen und Weitergabe der Daten.

Enttäuschend ist der Stand der Sprachanalyse in den Apps. Die meisten L-Apps überlassen dem Nutzer die Kontrolle der eigenen Aufnahme bzw. den Abgleich mit einem gespeicherten, abspielbaren Muster. Nur eine App hat eine eigene Spracherkennung implementiert, eine weitere App verwendet eine Fraunhofer-Lösung. Eine App verwendet die Google-Spracherkennung. Rein technisch wären heutige Smartphones zu weit mehr in der Lage.

Die Apps haben reichhaltige Funktionen und unterscheiden sich im Aufbau stark. Die subjektive Einschätzung ist bei (C) am höchsten, gefolgt von (B). (B) hat den höchsten zeitlichen Untersuchungsaufwand. Probleme bei der Untersuchung waren: tpacketcapture „verschluckt“ sich bei eingebundenen Videos (meist von YouTube) und Google-Diensten wie Captchas und kann nicht alle Apps untersuchen. Lumen hat Probleme mit TLS-Verbindungen, die Certificate Pinning verwenden und so den verwendeten Man-In-The-Middle-Ansatz unterbinden.

Tab. 5 zeigt die kumulierten Score der Apps sortiert in aufsteigender Reihenfolge. Alle L-Apps weisen mindestens 9 Probleme in (A-C) auf, der Spitzenreiter hat einen Score von 19. Über (A)-(D) erhöht sich der Maximalwert sogar auf 22. Am besten abgeschnitten haben die Apps neolexon Aphasie, Conversation Therapy Lite und Lernspiele für Kinder. Am schlechtesten abgeschnitten haben die Apps Speech Essentials Therapy App, Otsimo, Constant Therapy, Speech Blubs: Language Therapy und Stamurai. Tab. 5 zeigt auch eine deutliche positive Korrelation zwischen der Anzahl der Downloads und der Höhe des Scores. Eine positive Ausnahme ist die App „Lernspiel für Kinder“. Offenbar treibt das Geschäftsmodell von Android erfolgreiche App-Entwickler zur problematischem Verhalten im Bereich des Datenschutzes.

5 Verwandte Arbeiten

Alber et al. 2020 [ASGL20] haben einen Bewertungskatalog vorgestellt, der v.a. Therapierenden aber auch Nutzern eine adäquate App-Auswahl unter Berücksichtigung von Datenschutz und -sicherheit, Funktionalität und fachlichen Aspekten ermöglicht.

Seit 2019 bietet das Bundesinstitut für Arzneimittel und Medizinprodukte ein Bewertungsverfahren an, das sog. Fast-Track-Verfahren für digitale Gesundheitsanwendungen, das auch DS und ITS adressiert [BfArM]. Allerdings geschieht dies in sehr generischer Forum durch Bezug auf die DSGVO und den BSI-Grundschutz (Baustein APP.1.4: Mobile Anwendungen) und bietet daher keine spezifische Unterstützung für Android oder L-Apps.

Furlong et al. [FMS+18] haben mithilfe der Mobile Application Rating Scale die Qualität von 135 Android-Apps untersucht. Der Fokus lag dabei auf der Qualität und Effizienz der Apps und nicht auf DS und ITS.

Grundy et al. haben in [GCH+19] die Weitergabe von 28 Datensätze bei populären Gesundheits-Apps über Simulation mit fiktiven Patienten und dem Agrigento-Framework untersucht. Ihr Ergebnis: „Data sharing is routine, yet far from transparent.” Vor allem Google/Alphabet profitiert über Werbe- und Analyseplattformen.

HealthOn [HealthOn] unterstützt Nutzer bei der Prüfung von Qualitäts- und Transparenzkriterien. Dabei werden ethische und moralische Kriterien berücksichtigt, Datenschutz und Privatheit sind Beispiele. Unsere Untersuchung deckt die dort genannten Punkte ab, testet deren Praxistauglichkeit für Android L-Apps und bietet eine sinnvolle Erweiterung der im Healthon-Bewertungskatalog gelisteten Punkte zu DS und ITS.

Der Vergleich mit einer ähnlichen Untersuchung von Bluthochdruck- und Diabetes-Apps [KA15, KAW15] von 2015 zeigt viele Gemeinsamkeiten. Die wichtigsten Unterschiede sind: Alle Apps haben mittlerweile DSEn (statt 20%), der Schutz der Daten im Netzwerk hat sich deutlich verbessert (kaum noch HTTP), Blutdruck und –zucker lassen sich als Zahlen speichern und leicht in Statistiken umwandeln und daher leichter und strukturierter auslagern, z.B. auf externe Server. Sound-Dateien bleiben viel häufiger auf dem lokalen Gerät, was aus Datenschutzsicht zu begrüßen ist. Die Durchdringung der Gesundheitsapps mit Google-Diensten hat weiter zugenommen.

Im Jahre 2021 untersuchte Herz ebenfalls mit einer auf [KA15] basierenden Methodik Fitness-Apps [He21]. Auch diese Studie zeigt, dass Angreifer aus dem Netzwerk mittlerweile hauptsächlich kryptographisch geschützten Netzwerkverkehr sehen. Außerdem verlangen die meisten der Fitness-Apps einen Online-Account, um überhaupt genutzt werden zu können. Auch die problematische Korrelation von Download-Zahlen und DS/ITS-Problemen wird bestätigt.

Tab. 5: Gesamt-Score und Download-Zahlen der L-Apps

App Name	(A)-Score	(B)-Score	(C)-Score	Summe (A)-(C)	(D)-Score	Summe (A)-(D)	Downloads
neolexon Aphasie	2	4	3	9	1	10	1.000
Conversation Therapy Lite	1	5	3	9			10.000
Lernspiele für Kinder, Deutsch	1	4	4	9			100.000
neolexon Artikulationsstörungen	1	6	3	10	1	11	1.000
neolexon Therapeut	2	5	3	10	1	11	1.000
SymboTalk - AAC Talker	1	4	8	10	1	11	10.000
Language Therapy Lite	2	6	3	11			10.000
Alexicom AAC for Android	1	2	8	11	2	13	10.000
Logopädie App 2: Übungen zur Aussprache	2	5	5	12			10.000
Logopädie App 1: Übungen zur Aussprache	2	5	5	12			50.000
HelpMeTalk	4	8	0	12			10.000
Apraxia Therapy Lite	3	8	3	14			10.000
MoveApp	2	6	7	15			1.000
CommBoards Lite - AAC Speech Assistant	3	7	6	16			10.000
Stamurai	4	9	5	18	2	20	10.000
Speech Blubs: Language Therapy	3	10	5	18	1	19	500.000
Constant Therapy	4	6	8	18	2	20	100.000
Otsimo | Speech Therapy Pronunciation Articulation	3	9	7	19	3	22	10.000
Speech Essentials Therapy App	3	8	8	19			50.000

6 Empfehlungen und Ausblick

6.1 Empfehlungen für Nutzer und App-Entwickler

Für die Betreiber von App Shops gibt es die folgenden Empfehlungen: Klartextkommunikation sollte vermieden werden, die Verwendung der angeforderten Berechtigungen sollten überprüft

werden sowie eine einheitliche Struktur und Inhaltsvorgaben für DSEn von Gesundheitsapps wäre wünschenswert, um den Nutzern den Vergleich zu erleichtern.

Folgende Empfehlungen richten sich an die Entwickler von L-Apps: Die aufgedeckten Probleme können als Startpunkt für eine Verbesserung der Apps im Bereich des DSs und der ITS verwendet werden. Alle Berechtigungen sollten erklärt werden, insbesondere wie die Sprachdaten weiterverarbeitet werden (lokal oder remote) und für welche Zwecke die INTERNET-Berechtigung verwendet wird. Momentan ist für den Anwender nicht zu unterscheiden, ob Daten an den L-App-Server fließen, an externe Server übertragen oder nur lokal verarbeitet werden. Optimal wäre die Angabe aller externen Verbindungen inkl. des Zwecks der Verbindung. Grundy et al. fordern in [GCH+19] darüber hinaus, die Datenweitergabe an externe Parteien wählbar zu machen. Speziell für Aphasiker ist bzgl. der DSE zu klären, inwieweit die Forderung der DSGVO nach leicht verständlichen Formulierungen noch spezifiziert und angepasst werden muss. Der potenteste Angreifer ist das mobile Ökosystem. Der erfolgversprechendste Schritt wäre, die App über einen anderen Kanal z.B. über die eigene Web-Seite anzubieten. Dies widerspricht aber grundlegend Googles Geschäftsinteressen und verlangt vom Nutzer „Apps aus unbekannten Quellen installieren“ zu akzeptieren, was die meisten Nutzer stark verunsichert.

Dem Nutzer bleibt nur die sorgfältige Prüfung der DSE und der Angaben im Play Store vor der Installation der App. In der Stichprobe gab es nur eine L-App ohne Internet-Berechtigung. Das Abschalten von WLAN ist aber bei einigen L-Apps möglich. Bestehende Siegel für L-Apps beziehen sich neben Datenschutz, meist auf Qualität oder Benutzbarkeit, sind sehr heterogen, (noch) nicht stark verbreitet und bieten daher auch keine Hilfe [HealthOn]. Wie hoffen, dass wir mit der vorgestellten Methodik Nutzern Hilfe zur Selbsthilfe anbieten können.

6.2 Zukünftige Arbeiten

Einige populäre L-Apps wie DiaTrain, Articulation Station Pro und Apraxia RainbowBee sind nur für Apple Geräte erhältlich. Die vorgestellte Methodik könnte daher auf iOS angepasst werden. In der Untersuchung wurden nur „kostenlose“ L-Apps untersucht. Die Analyse könnte auf bezahlte Apps ausgedehnt werden. Bei zwei untersuchten Apps wird das Mikrofon erst in der kommerziellen Version genutzt. Eine Umfrage unter den Entwicklern der L-Apps könnte genauer ausleuchten, welche Motive den aufgezeigten Problemen aus Entwicklersicht zugrunde liegen. Eine weitere zukünftige Arbeit wäre die Übertragung der Untersuchung auf andere Therapiewissenschaften wie z.B. Physiotherapie oder Ergotherapie. Dies würde weitere Vergleiche zwischen verschiedenen Klassen von Therapie-Apps erlauben.

Anders als Arzneimittel oder Behandlungshilfen wie Stützstrümpfe, Spritzen oder Herzkatheter brauchten Medizin-Apps lange Zeit keine Zulassung. In Deutschland wurde mit der Digitale Gesundheitsanwendungen vom Bundesinstitut für Arzneimittel und Medizinprodukte [BfArM] eine Vorgehensweise und ein Verzeichnis vorgestellt, dass diese Lücke schließen soll. Von den untersuchten L-Apps ist dort keine enthalten. Offenbar meiden viele L-App-Entwickler diesen Weg – sei es aus Unkenntnis oder um den Aufwand zu reduzieren. Das ambitionierteste Ziel ist die Arbeit an einem leichtgewichtigen Gütesiegel oder einer Zertifizierung von Gesundheits-Apps. Die medizinischen Zertifikate (wie für Medizinprodukte oder „Digitale Gesundheitsanwendungen“) und Zertifikate aus der IT-Sicherheit (wie die Common Criteria) sind für L-Apps in der Regel zu aufwändig und werden von den Entwicklern daher abgelehnt, weshalb neue Ansätze wie z.B. [HealthOn] zu prüfen und ggf. zu erweitern sind.

Literatur

[ASGL20] B. Alber, A. Starke, J. Griffel, J. Leinweber: Qualität von Apps in der Logopädie/Sprachtherapie. Der Bewertungskatalog für Apps in Sprachtherapie und Sprachförderung (BAS). Forum Logopädie Heft 3 (34) 12-13. https://doi.org/10.2443/skv-s-2020-53020200302

[BfArM] Bundesinstitut für Arzneimittel und Medizinprodukte: Digitale Gesundheitsanwendungen, https://www.bfarm.de/DE/Medizinprodukte/DVG/_node.html

[BfDI19] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: Gesundheits-Apps, Informations-Flyer, https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Gesundheitsapps.pdf?__blob=publicationFile&v=7 (2019)

[FMS+18] L. Furlong, M. Morris, T. Serry, S. Erickson S: Mobile apps for treatment of speech disorders in children: An evidence-based analysis of quality and efficacy. PLoS ONE 13(8): e0201513. https://doi.org/10.1371/journal.pone.0201513 (2018)

[Ge18] K. Geißelmann: Medizinprodukte - Risikoklasse für Apps steigt, Deutsches Ärzteblatt 2018; 115(12): A-538, https://www.aerzteblatt.de/archiv/196980/Medizinprodukte-Risikoklasse-fuer-Apps-steigt

[GCH+19] Q. Grundy, K. Chiu, F. Held, A. Continella, L. Bero, R. Holz: Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. BMJ 2019;364:l920, https://doi.org/10.1136/bmj.l920

[He21] N. Herz: Überprüfung des Datenschutzes und der IT-Sicherheit von Fitness-Apps für Android Geräte, Bachelorarbeit, Fachbereich Informatik, Hochschule Trier, 2021

[HealthOn] HealthOn, Siegel für Gesundheits-Apps: Marktübersicht, https://www.healthon.de/

[KA21] K. Knorr, D. Aspinall: Security Testing for Android mHealth Apps, in Proc. of the 6th international Workshop on Security Testing (SECTEST), co-located with the 8th IEEE International Conference on Software Testing, Verification and Validation (ICST 2015), Graz, Austria, April 13, 2015

[KAW21] K. Knorr, D. Aspinall, M. Wolters: On the Privacy, Security and Safety of Blood Pressure and Diabetes Apps, in Proc. of IFIP SEC 2015 International Conference on ICT Systems Security and Privacy Protection, pp. 571-584, May 26-28, Hamburg, Germany

[KrWA16] M. Krämer, M. Wolters, D. Aspinall. POSTER: Weighing in eHealth Security - A Security and Privacy Study of Smart Scales. Proceedings of the 23rd ACM SIGSAC Conference on Computer and Communications Security (2016)

[NeoKost] Neolexon: Kostenerstattung, https://neolexon.de/kostenerstattung/

[RyDe00] R. M. Ryan, E. L. Deci: Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being. American Psychologist, Vol. 55 (1), 68-78, doi: 10.1037110003-066X.55.1.68

[SpHJ17] M. Späth, E. Haas, H. Jakob. neolexon-Therapiesystem. Forum Logopädie, Heft 3 (31) 20-24 (2017)

[StMü18] A. Starke, J. Mühlhaus. App-Einsatz in der Sprachtherapie. Forum Logopädie Heft 2 (32) 22-26 (2018)