Freie Universität Berlin

Institut für Informatik

Bachelorarbeit

Automatische Analyse von Datenschutzkonformität in mobilen Apps

Muhannad Aldaadaa

1. Gutachter:	Prof. Dr. Marian Margraf
2. Gutachterin:	Jun.-Prof. Dr.-Ing. Maija Poikela
Betreuerin:	Sandra Kostic
Semester:	Wintersemester 2024
Verfasser:	Muhannad Aldaadaa
Matrikel-Nr.:	5479981
Email:	muhannad.aldaadaa@fu-berlin.de

Berlin den 28.01.2024

Freie Universität Berlin

Fachbereich Mathematik, Informatik und Physik

SELBSTSTÄNDIGKEITSERKLÄRUNG

Name:	Aldaadaa	(BITTE nur Block- oder Maschinenschrift verwenden.)
Vorname(n):	Muhannad	
Studiengang:	Informatik	
Matr. Nr.:	5479981	

Ich erkläre gegenüber der Freien Universität Berlin, dass ich die vorliegende Bachelorarbeit selbstständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt habe.

Die vorliegende Arbeit ist frei von Plagiaten. Alle Ausführungen, die wörtlich oder inhaltlich aus anderen Schriften entnommen sind, habe ich als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch bei keiner anderen Universität als Prüfungsleistung eingereicht.

Datum: 21.01.2025

Unterschrift: 

Würdigung

An erster Stelle möchte ich meiner Betreuerin Sandra Kostic für ihre großartige Unterstützung und Anleitung während der Durchführung der Studie und des Schreibprozesses danken. Weiterhin möchte ich mich bei der Teilnehmer der Umfrage bedanken, die mir mit ihren wertvollen Rückmeldungen zur Verfügung standen.

Muhannad Aldaadaa

Inhaltsverzeichnis

Abstrakt

Die zunehmende Verbreitung mobiler Apps und die damit verbundenen Datenschutzrisiken und Sicherheitsrisiken erfordern innovative Lösungen, um Nutzer bei informierten Entscheidungen zu unterstützen. Diese Bachelorarbeit konzentriert sich auf die Entwicklung und Evaluierung einer Webanwendung, die durch visuelle Sicherheitsindikatoren die Wahrnehmung von App-Berechtigungen verbessert und das Entscheidungsverhalten der Nutzer positiv beeinflusst.

Im Rahmen dieser Arbeit wurde ein dreistufiges Risikobewertungssystem eingeführt, das App-Berechtigungen nach ihrer potenziellen Relevanz in die Kategorien „*niedriges Risiko*“, „*mittleres Risiko*“ und „*hohes Risiko*“ einstuft. Die intuitive Darstellung dieser Informationen sowie die Benutzerfreundlichkeit der Webanwendung wurden in einer empirischen Studie mit 16 Teilnehmern untersucht. Die Ergebnisse haben gezeigt, dass klare visuelle Warnhinweise, wie beispielsweise Farbcodierungen, das Bewusstsein für Sicherheitsrisiken signifikant erhöhen können.

Darüber hinaus wurden Faktoren identifiziert, die das Nutzerverhalten bei der App-Installation beeinflussen. Bewertungen, Rezensionen und technische Aspekte wie Berechtigungen spielen dabei eine zentrale Rolle. Die Studie hat verdeutlicht, dass Sicherheitsindikatoren nicht nur die Wahrnehmung von Risiken verbessern, sondern auch die Bereitschaft der Nutzer steigern, Berechtigungen genauer zu überprüfen.

Diese Arbeit bietet nicht nur einen Einblick in die Gestaltung effektiver Sicherheitsindikatoren, sondern stellt auch Ansätze für die Weiterentwicklung von Standards und gesetzlichen Regelungen vor. Als Ausblick wird die Entwicklung einheitlicher Standards für Sicherheitsindikatoren und Risikobewertungen vorgeschlagen. Dies könnte ein übergreifendes Farbsystem (z. B. Sicherheitsampel) oder detaillierte Bewertungsrichtlinien umfassen. Solche Standards könnten auf europäischer Ebene politisch und gesetzlich diskutiert und eventuell in die DSGVO (EU-Datenschutz-Grundverordnung) integriert werden. Die Ergebnisse dieser Arbeit leisten einen wichtigen Beitrag zur Erhöhung der Sicherheit und Transparenz in digitalen Plattformen und fördern eine informierte und bewusste Nutzung

1 Einleitung

Die zunehmende Verbreitung von mobilen Apps, insbesondere auf Android-Geräten, hat die Diskussion um Datenschutz und Sicherheit intensiviert. Android ist das weltweit dominierende Betriebssystem mit einem Marktanteil von über 74,5 % [1] [2]. Aufgrund der offenen Struktur von Android bietet die Plattform zwar erhebliche Möglichkeiten für Entwickler, birgt jedoch auch erhebliche Risiken für die und Sicherheit der Nutzer. Diese Risiken resultieren aus der wachsenden Zahl von Apps, die umfangreiche Berechtigungen anfordern, um auf sensible Daten wie Kontakte, Standort oder Kamerazugriff zuzugreifen.

Ein weiterer Faktor, der die Bedeutung dieser Problematik hervorhebt, ist die zunehmende Komplexität des Android-Berechtigungssystems. In den letzten Jahren wurden mehrere Updates eingeführt, um den Schutz der Nutzerdaten zu verbessern. Beispielsweise ermöglicht das Laufzeitberechtigungsmodell (Runtime-Permission-Modell) ab Android 6.0 den Nutzern, Berechtigungen zur Laufzeit und nicht während der Installation zu erteilen [1]. Studien zeigen jedoch, dass viele Nutzer Berechtigungsanfragen nicht verstehen oder ihre Bedeutung unterschätzen [3].

Zusätzlich stellt die EU-Datenschutz-Grundverordnung (DSGVO) besondere Anforderungen an App-Berechtigungen, insbesondere bei der Verarbeitung sensibler Daten wie Standort und Kamerazugriff (Art 9, Art. 4 DSGVO). Gemäß Art. 6 Abs. 1 DSGVO müssen Benutzer ein klares und transparentes Verständnis darüber haben, wie diese Daten verwendet werden, um fundierte Entscheidungen zu treffen. Studien zeigen, dass Datenschutzrichtlinien oft inkonsistent sind und viele Apps diese Anforderungen nicht vollständig erfüllen [4] [5] [6] [7].

Die Relevanz dieses Themas zeigt sich auch in der Praxis. Studien haben ergeben, dass viele Apps mehr Berechtigungen anfordern, als für ihre Funktionalität notwendig ist, was als „Over-Privilege“ bezeichnet wird [6]. Dies führt nicht nur zu potenziellen Datenschutzverletzungen, sondern macht die Geräte auch anfällig für Angriffe durch Malware oder andere bösartige Akteure. Daher ist eine tiefgehende Analyse des Android-Berechtigungssystems erforderlich, um sowohl technische als auch organisatorische Ansätze zur Verbesserung der Sicherheit und Privatsphäre zu entwickeln.

Darüber hinaus spielt die Aufklärung der Nutzer eine zentrale Rolle. Viele Benutzer sind sich der Risiken, die mit der Freigabe sensibler Daten verbunden sind, nicht bewusst. Eine Umfrage zum Datenschutzbewusstsein hat gezeigt, dass 35,71 % der Befragten (1.438 von insgesamt 4.025 Teilnehmern) immer die Berechtigungen aller oder einiger Apps lesen, bevor sie diese installieren, während 11,42 % (460 Teilnehmer) haben angegeben, die Berechtigungen niemals zu lesen [8]. Diese Zahlen verdeutlichen die Diskrepanz im Nutzerverhalten und die Bedeutung einer verbesserten Nutzeraufklärung [8].

1.1 Motivation

Die Privatsphäre von Android-Nutzern steht vor immer größeren Herausforderungen. Mit der zunehmenden Nutzung von Smartphones und der Installation von Apps wird die Datenflut, die von mobilen Geräten verarbeitet wird, immer unübersichtlicher. Studien zeigen, dass Android-Nutzer im Durchschnitt mehr als 100 Apps auf ihren Geräten installiert haben, von denen ein erheblicher Anteil umfangreiche Berechtigungen anfordert [3] [9].

Ein Hauptproblem ist das mangelnde Bewusstsein der Benutzer für die Risiken, die mit der Freigabe von Berechtigungen verbunden sind. Beispielsweise benötigen Taschenlampen-Apps häufig Zugriff auf die Kamera und den Standort, auch wenn diese Funktionen nicht erforderlich sind. Diese unnötigen Berechtigungen können zum Sammeln von Daten oder sogar zur Gefährdung des Geräts genutzt werden. Unterdessen zeigen Studien von Almomani und Al Khayer [1] [10] [11] [12], dass viele Benutzer dazu neigen, Berechtigungen ohne Überprüfung zu erteilen, hauptsächlich aus Bequemlichkeit oder Unwissenheit.

Ein weiterer Motivationsfaktor ist die Entwicklung von Sicherheitsangriffen, die gezielt Schwachstellen im Android-Berechtigungssystem ausnutzen. Beispiele wie die „Permission Escalation Attacks“ zeigen, wie Angreifer durch die Kombination von Berechtigungen sensible Daten entwenden können [1] [13]. Solche Angriffe unterstreichen die Notwendigkeit, die Mechanismen zur Berechtigungsvergabe zu stärken und den Nutzern mehr Kontrolle zu geben.

Darüber hinaus erfordert die schnelle Entwicklung des Android-Berechtigungssystems innovative Ansätze, um sowohl Entwickler als auch Nutzer zu unterstützen. Entwickler stehen vor der Herausforderung, die neuesten Sicherheitsanforderungen effizient zu implementieren, während Nutzer die Funktionsweise und Auswirkungen der neuen Mechanismen besser verstehen müssen. Unsere Arbeit greift diese Probleme auf, indem sie ein Tool entwickelt, das App-Metadaten und Berechtigungen analysiert und diese Informationen auf verständliche Weise präsentiert, um die Nutzeraufklärung zu fördern und Entscheidungsprozesse bei der Anwendungsinstallation zu unterstützen.

1.2 Ziel

Das Ziel dieser Bachelorarbeit ist die Entwicklung und Evaluierung eines automatisierten Tools zur Beurteilung der Datenschutzkonformität von mobilen Apps. Die Arbeit verfolgt insbesondere folgende Ziele:

1. Entwicklung einer Webanwendung, die es ermöglicht, App-Metadaten aus dem Google-Play-Store mithilfe des Frameworks „Google-Play-Scraper“ zu analysieren und darzustellen [14].
2. Studie, wie die Darstellung von App-Berechtigungen und Sicherheitsindikatoren gestaltet sein muss, um die Entscheidungsfindung der Nutzer bei der App-Installation zu unterstützen.
3. Analyse des Nutzerverhaltens mithilfe eines Fragebogens und einer Testgruppe, um zu evaluieren, inwieweit die entwickelte Anwendung die Wahrnehmung von Sicherheitsrisiken und die Entscheidungsfindung beeinflusst.
4. Bereitstellung konkreter Handlungsempfehlungen zur Verbesserung der Präsentation von Sicherheitsinformationen und zur Erhöhung des Sicherheitsbewusstseins.

Die Arbeit zielt darauf ab, konkrete Handlungsempfehlungen zu formulieren, die sowohl auf technischer als auch auf organisatorischer Ebene umgesetzt werden können. Dabei werden bestehende Forschungsergebnisse integriert und durch eigene Analysen ergänzt.

1.3 Forschungsfragen

Im Rahmen dieser Bachelorarbeit werden folgende zentrale Forschungsfragen untersucht:

1. **Wie können App-Berechtigungen so dargestellt werden, dass sie das Bewusstsein der Nutzer für Sicherheitsrisiken erhöhen?**
   Ziel ist es, zu untersuchen, welche Visualisierungs- und Präsentationsformen für App-Berechtigungen effektiv sind, um Nutzern fundierte Entscheidungen zu ermöglichen.
2. **Welche Faktoren beeinflussen das Nutzerverhalten bei der Installation von Apps?**
   Hierbei wird analysiert, wie Nutzer Sicherheitsindikatoren und App-Berechtigungen bewerten und in ihre Entscheidungsprozesse einbeziehen.
3. **Inwiefern können Sicherheitsindikatoren das Entscheidungsverhalten von Nutzern beeinflussen?**
   Es soll untersucht werden, ob und wie visuelle Warnhinweise die Wahrnehmung und das Verhalten der Nutzer verändern.
4. **Wie wirksam ist die entwickelte Webanwendung bei der Unterstützung informierter Entscheidungen?**
   Diese Frage zielt darauf ab, die Benutzerfreundlichkeit und Wirksamkeit der entwickelten Lösung zu evaluieren.

Diese Forschungsfragen bieten die Grundlage für die Analyse und Bewertung des Nutzerverhaltens durch die im Rahmen dieser Arbeit entwickelten Webanwendung und durch die Interpretation der erhobenen Daten.

1.4 Aufbau der Arbeit

Die vorliegende Arbeit ist in acht Kapitel gegliedert, die die Entwicklung, Durchführung und Evaluierung der Studie sowie die Ergebnisse und deren Interpretation systematisch darstellen:

- **Kapitel 1: Einleitung**
  Dieses Kapitel bietet eine Einführung in das Thema, beschreibt die Motivation und die Zielsetzung der Arbeit sowie die Forschungsfragen und den Aufbau der Arbeit.
- **Kapitel 2: Verwandte Arbeiten**
  Es wird ein Überblick über bestehende Forschungsarbeiten zur Bewertung und Klassifikation von App-Berechtigungen und zur Entwicklung von Sicherheitsmodellen gegeben. Dabei werden Forschungslücken identifiziert, die den Ausgangspunkt für die vorliegende Arbeit bilden.
- **Kapitel 3: Forschungsmethodik**
  In diesem Kapitel werden die verwendeten Methoden zur Datenerhebung und Analyse erläutert. Es umfasst die Planung und Durchführung von Interviews, die Gestaltung des Fragebogens sowie die Entwicklung und Evaluierung der Webanwendung.
- **Kapitel 4: Beschreibung der Webanwendung**
  Dieses Kapitel beschreibt die Zielsetzung und die technische Umsetzung der entwickelten Webanwendung. Es enthält Details zur Benutzeroberfläche, zur Funktionsweise und zur Visualisierung der Sicherheitsindikatoren.

- **Kapitel 5: Ergebnisse der Studie**
  Hier werden die Ergebnisse der empirischen Studie vorgestellt, die auf den Rückmeldungen der Teilnehmer sowie den beobachteten Interaktionen mit der Webanwendung basieren.
- **Kapitel 6: Diskussion und Interpretation**
  Die Ergebnisse werden in den Kontext bestehender Forschung eingeordnet. Zudem werden die Forschungsfragen beantwortet und praktische Implikationen abgeleitet.
- **Kapitel 7: Einschränkungen der Studie**
  Die methodischen und praktischen Einschränkungen der Arbeit werden dargelegt, um die Generalisierbarkeit und Aussagekraft der Ergebnisse einzuordnen.
- **Kapitel 8: Konklusion und Ausblick**
  Abschließend werden die zentralen Erkenntnisse zusammengefasst, und es wird ein Ausblick auf mögliche zukünftige Forschungsvorhaben und Weiterentwicklungen gegeben.

Diese Struktur bietet eine klare und nachvollziehbare Darstellung des gesamten Forschungsprozesses und der Ergebnisse.

2 Verwandte Arbeiten

Dieser Abschnitt bietet einen Überblick über bestehende Forschungsarbeiten im Bereich der Bewertung und Klassifizierung von App-Berechtigungen sowie der Entwicklung von Sicherheitsmodellen für mobile Apps. Die Betrachtung bestehender Studien hat die Grundlage für die Einordnung und Abgrenzung der vorliegenden Arbeit gebildet.

2.1 Klassifikation von App-Berechtigungen

Die Klassifikation von App-Berechtigungen hat eine zentrale Grundlage für die Risikobewertung mobiler Apps gebildet. Laut Al Jutail et al. [15] hat diese Studie Berechtigungen basierend auf Googles Klassifizierung gefährlicher Berechtigungen in drei Gruppen unterteilt: Berechtigungen, die private Nutzerdaten wie Anrufprotokolle lesen können, solche, die Nutzerdaten wie Kontakte ändern können, und solche, die Funktionen wie GPS-Tracking und Mikrofonzugriff enthalten, die zur Überwachung genutzt werden könnten.

Caushaj und Sugumaran [16] haben Kombinationen von Berechtigungen analysiert, die von Werbenetzwerken und Apps genutzt worden sind, und betont, dass solche Kombinationen häufig das Risiko für die Privatsphäre der Nutzer erhöht haben. Ihre Studie hat gezeigt, dass gefährliche Kombinationen spezifischer Berechtigungen besonders in Bezug auf Werbenetzwerke (Ads Netzwerken) ein erhöhtes Risiko dargestellt haben und die Notwendigkeit einer gezielten Bewertung dieser Berechtigungen unterstrichen.

Atzeni et al. [17] haben ein Framework entwickelt, das statische und dynamische Analysetechniken integriert, um verdächtige Aktivitäten zu identifizieren und diese potenziellen Risikokategorien zuzuordnen. Ihre Methode hat eine umfassende Sicherheitsbewertung ermöglicht, indem verdächtige Aktivitäten in feingliedrige Risikokategorien unterteilt und diese mittels Fuzzy-Logik bewertet worden sind. Dies hat

gezeigt, wie analytische Methoden kombiniert werden können, um ein detailliertes Risikoprofil von Apps zu erstellen.

2.2 Sicherheitsmodelle und Nutzerverhalten

Die Analyse des Nutzerverhaltens in Bezug auf App-Berechtigungen und Sicherheitsindikatoren ist in mehreren Studien thematisiert worden. Laut einer Studie von Al Jutail et al. [15] haben Nutzer oft Schwierigkeiten gehabt, das Risiko von Berechtigungsanfragen richtig einzuschätzen. Diese Erkenntnis hat die Notwendigkeit benutzerfreundlicher Darstellungsformen verdeutlicht.

Das Nutzerverhalten im Umgang mit App-Berechtigungen war ein zentraler Bestandteil bestehender Forschungsarbeiten. Al Jutail et al. [15] haben festgestellt, dass Nutzer häufig Schwierigkeiten gehabt haben, das Risiko bestimmter Berechtigungen einzuschätzen. Dies hat die Bedeutung benutzerfreundlicher Darstellungen verdeutlicht, die eine bessere Informiertheit gewährleistet haben.

Caushaj und Sugumaran [16] haben prädiktive Modelle entwickelt, um das Verhalten von Apps zu analysieren und Benutzer zu ermöglichen, fundierte Entscheidungen basierend auf Sicherheitsindikatoren zu treffen. Diese Modelle haben wertvolle Einblicke in die Funktionsweise von Apps und ihre potenziellen Auswirkungen auf die Privatsphäre geliefert.

Atzeni et al. [17] haben sich auf die Integration von Analyseverfahren konzentriert, die verdächtige App-Aktivitäten erkannt und Risikobewertungen ermöglicht haben. Die Autoren haben betont, dass eine umfassende Methodik für die Sicherheitsbewertung erforderlich ist, um spezifische Risiken besser zu kategorisieren.

2.3 Forschungslücken und Motivation der vorliegenden Arbeit

Obwohl zahlreiche Studien zur Bewertung von App-Berechtigungen existiert haben, hat ein einheitlicher Standard für die Klassifikation und Bewertung dieser Berechtigungen gefehlt. Bisherige Ansätze haben sich häufig auf spezifische technische Implementierungen oder Anwendungsfälle fokussiert. Die vorliegende Arbeit hat das Ziel verfolgt, diese Lücke zu schließen, indem ein flexibles und benutzerfreundliches System zur Risikobewertung von App-Berechtigungen entwickelt worden ist. Dieses System hat die Erwartungen und Bedürfnisse der Nutzer berücksichtigt und klare, visuell unterstützte Informationen zur Entscheidungsfindung angeboten.

3 Forschungsmethodik

Die Methoden dieser Arbeit kombiniert qualitative und quantitative Ansätze, um Nutzerverhalten und deren Wahrnehmung von App-Berechtigungen zu untersuchen. Die Forschungsmethoden werden zunächst allgemein wissenschaftlich beschrieben und anschließend die spezifischen Apps in dieser Studie erläutert.

3.1 Interviews (persönlich und online)

Interviews sind eine bewährte qualitative Forschungsmethode, die detaillierte Einblicke in die Perspektiven und Erfahrungen der Teilnehmer ermöglichen. Sie werden oft genutzt, wenn kontextbezogene und tiefgehende Informationen erforderlich sind, die über die Möglichkeiten von standardisierten Umfragen hinausgehen [18].

3.1.1 Allgemeine Methodik

Interviews lassen sich in drei Hauptkategorien unterteilen:

- **Strukturierte Interviews:** Diese folgen einem klaren Leitfaden mit vordefinierten Fragen, die allen Teilnehmern in gleicher Weise gestellt werden. Sie eignen sich besonders zur Sammlung vergleichbarer Daten [18].
- **Halbstrukturierte Interviews:** Diese kombinieren einen vorbereiteten Leitfaden mit der Flexibilität, auf spontane Themen einzugehen, um tiefere Einblicke zu gewinnen. Sie werden häufig eingesetzt, um qualitative und kontextbezogene Informationen zu sammeln [19].
- **Unstrukturierte Interviews:** Diese bieten maximale Freiheit für die Teilnehmer, ihre Gedanken auszudrücken, sind jedoch schwieriger zu analysieren und weniger standardisiert [18].

Laut Adams und Cox [18] sind halbstrukturierte Interviews besonders nützlich, da sie vorbereitete Fragen mit der Möglichkeit kombinieren, spontan auf neue Themen einzugehen. Diese Interviews bieten die Flexibilität, sowohl unerwartete als auch geplante Erkenntnisse zu gewinnen [19].

3.1.2 Planung und Durchführung

Die Planung und Durchführung von Interviews erfordert mehrere Schritte:

1. **Vorbereitung:** Ein klarer Leitfaden wird erstellt, um sicherzustellen, dass alle relevanten Themen behandelt werden. Zusätzlich wird Raum für spontane Diskussionen gelassen [19].
2. **Durchführung:** Die Interviews werden in einer vertrauensvollen Umgebung durchgeführt. Der Interviewer achtet dabei auf verbale und nonverbale Hinweise, um tiefere Einblicke zu gewinnen [18].
3. **Einleitung:** Zu Beginn des Interviews werden den Teilnehmern die Studienziele erläutert, ihre Zustimmung eingeholt und Anonymität gewährleistet [18].

3.2 Fragebogen (Umfragen)

Fragebogen sind eine bewährte Methode zur systematischen Datensammlung und eignen sich besonders für die Erhebung von Meinungen, Verhalten und Vorlieben der Teilnehmer [18] Ein effektiver Fragebogen erfordert eine klare Struktur, präzise formulierte Fragen und eine Überprüfung der Validität und Reliabilität, um konsistente und aussagekräftige Ergebnisse zu erzielen [20] [21].

3.2.1 Online-/Offline-Fragebogen

Fragebogen können sowohl online als auch offline eingesetzt werden, abhängig von den Anforderungen der Studie und der Zielgruppe.

- **Online-Fragebogen:** Diese bieten eine hohe Reichweite und Flexibilität. Sie ermöglichen schnelle Datenerhebung, kostengünstige Verteilung und automatische Speicherung der Antworten [21] [18]. Plattformen wie Google-Formulare bieten zudem Tools zur Visualisierung und Analyse der Ergebnisse [21].
- **Offline-Fragebogen:** Diese sind ideal für kontrollierte Umgebungen, in denen persönliches Feedback erforderlich ist. Sie gewährleisten eine bessere Kontrolle über den Erhebungsprozess, erfordern jedoch mehr Ressourcen für die Datenerfassung und Daten Eingabe [22].

Laut Prasad Nayak und Narayan [22] sind Online-Fragebogen besonders nützlich für große, geografisch verteilte Zielgruppen, während Offline-Fragebogen für kleinere und spezifischere Studien bevorzugt werden.

3.2.2 Typen von Fragen

Ein effektiver Fragebogen enthält in der Regel eine Kombination aus offenen und geschlossenen Fragen. Geschlossene Fragen, wie Ja/Nein-Optionen oder Likert-Skalen, bieten den Vorteil, dass sie leicht zu analysieren und zu vergleichen sind [22]. Offene Fragen ermöglichen hingegen eine tiefere Einsicht in die Meinungen und Erfahrungen der Teilnehmer, erfordern jedoch eine aufwendigere Analyse [20].

Online-Tools wie Google-Formulare haben die Erstellung und Verteilung von Fragebogen revolutioniert. Laut Couper [23] bietet es ein benutzerfreundliches Design, das die Datenerfassung und Datenanalyse erleichtert. Sie ermöglichen es, Fragen in verschiedenen Formaten wie u.a. Multiple-Choice, Dropdown-Menüs oder Skalen zu gestalten. Die Daten werden automatisch gesammelt und können sofort analysiert werden, was Zeit spart und Fehler reduziert. Google-Formulare ist dabei ein besonders vielseitiges Tool, das sowohl geschlossene als auch offene Fragen unterstützt und die Datenanalyse durch automatische Speicherfunktionen und Exportfunktionen erleichtert [21] [22].

3.2.3 Validität und Zuverlässigkeit

Die Validität eines Fragebogens bezieht sich darauf, inwieweit die gestellten Fragen das messen, was sie messen sollen. Die Zuverlässigkeit beschreibt die Konsistenz der Ergebnisse bei wiederholter Anwendung des Instruments [20]. Eine Pilotstudie wird empfohlen, um die Verständlichkeit und Funktionalität des Fragebogens vor der Hauptstudie zu überprüfen [22].

3.3 Studienformat

Das Studienformat basiert auf einem gemischten Ansatz, der qualitative und quantitative Methoden kombiniert, um ein umfassendes Bild der Benutzerwahrnehmung von App-Berechtigungen und Sicherheitsindikatoren zu erhalten.

Die Kombination aus Interviews, einer eigens entwickelten Webanwendung und ein Fragebogen über Google-Formulare haben eine umfassende Datenerhebung ermöglicht. Ergänzend wurde eine Pilotstudie durchgeführt, um die Validität und Zuverlässigkeit der Fragebogen zu gewährleisten [20] [22]. Zur Erfassung ausreichender Informationen und zur Aufrechterhaltung des Interesses der Teilnehmer hat jedes Interview 10 bis 15 Minuten gedauert [24].

3.4 Ablauf der Studie

Die durchgeführte Studie bestand aus mehreren Phasen:

1. **Interviews (persönlich und online):** Halbstrukturierte Interviews wurden durchgeführt, um qualitative Daten zur Wahrnehmung und Entscheidungsfindung der Teilnehmer zu sammeln. Die Interviews haben sowohl persönlich als auch online über Zoom stattgefunden. Vorab haben die Teilnehmer eine Einführung in die Studienziele und den Ablauf des Tests von dem Interviewer erhalten.
2. **Fragebogen**[1] **:** Ein zweigeteilter Fragebogen wurde verwendet, der quantitative Daten gesammelt hat. Der erste Abschnitt des Fragebogens hat Informationen zur Wahrnehmung von App-Berechtigungen erfasst. Und der zweite Abschnitt hat sich auf die Erfahrungen der Teilnehmer mit der entwickelten Webanwendung und deren Feedback zu Sicherheitsindikatoren konzentriert. Abschließend wurden demografische Daten gesammelt. Der Fragebogen wurde mit Google-Formulare durchgeführt, was eine schnelle Verteilung und einfache Datenanalyse ermöglicht hat und der Fragebogen wird so gestaltet, dass er eine Mischung aus geschlossenen und offenen Fragen enthält. Geschlossene Fragen erleichtern die Datenauswertung, während offene Fragen detaillierte Einblicke ermöglichen [20] [18].
3. **Webanwendung**[1] **:** Die entwickelte Webanwendung hat es den Teilnehmern ermöglicht, Sicherheitsindikatoren und App-Berechtigungen interaktiv zu erleben. Nach der Interaktion mit der Webanwendung haben die Teilnehmer ihre Erfahrungen bewertet und Feedback gegeben, das in den zweiten Abschnitt des Fragebogens aufgenommen wurde.

4. **Pilotstudie:** Eine Pilotstudie wurde mit einem Teilnehmer durchgeführt, um die Verständlichkeit des Fragebogens und die Funktionalität der Webanwendung zu überprüfen. Die Pilotstudie hilft, potenzielle Probleme vor der Hauptstudie zu identifizieren und anzupassen [22]. Basierend auf den Erkenntnissen wurden kleinere Anpassungen vorgenommen, bevor die Hauptstudie mit 16 Teilnehmern durchgeführt wurde.

Dieses Studienformat hat sichergestellt, dass eine umfassende Sammlung von Daten sowohl auf individueller als auch auf Gruppenebene ermöglicht wurde, indem qualitative Erkenntnisse mit quantitativen Analysen kombiniert wurden, um ein vollständiges Bild der Wahrnehmungen und Entscheidungsprozesse der Benutzer zu liefern.

3.5 Fragebogensdesign

Der Fragebogen[1] enthält:

- **Geschlossene Fragen**: Diese dienen der strukturierten Datenerfassung und umfassen Likert-Skalen und Ja/Nein-Optionen [21] [23].
- **Offene Fragen**: Diese ermöglichen es den Teilnehmern, ihre Meinungen und Erfahrungen detailliert zu schildern [20] [18].
- **Klare Struktur**: Die Fragen werden logisch angeordnet und mit klaren Anweisungen versehen, um Missverständnisse zu vermeiden [23].

3.6 Stichprobenauswahl

Die Teilnehmer werden gezielt ausgewählt, um eine breite demografische Verteilung zu gewährleisten. Laut Nayak und Narayan [22] erhöht eine repräsentative Stichprobe die Verallgemeinerbarkeit der Ergebnisse. Die Auswahl basiert auf Alter, Geschlecht und technischem Hintergrund.

3.7 Datenerhebungsmethoden

3.7.1 Schriftliche Antworten in Google-Formulare

Google-Formulare ermöglicht eine effiziente Datenerhebung. Die geschlossenen Fragen sammeln präzise und vergleichbare Daten, während offene Fragen den Teilnehmern die Möglichkeit bieten, ihre Meinungen detailliert zu schildern [20] [23].

Mit Hilfe unseres Fragebogens wurden Daten zu den nachfolgenden Themen gesammelt:

- Methoden zur Identifizierung von Apps
- Faktoren, die bei der Installation von Entscheidungen berücksichtigt werden müssen
- Sicherheitsbewusstsein

- Verhalten bei der Berechtigungsprüfung
- Schwerpunkte auf Benutzerfreundlichkeit und Sicherheit

3.7.2 Ablauf des Interviews

1. **Einführung und Kontext**: Der Interviewer erklärt den Teilnehmern die Ziele der Studie und den Ablauf des Tests.
2. **Erster Teil des Fragebogens**: Die Teilnehmer beantworten Fragen zu ihrer Wahrnehmung von App-Berechtigungen.
3. **Test der Webanwendung**: Die Teilnehmer interagieren mit der entwickelten Webanwendung, die auch eine simulierte Dummy-App anzeigt, und testen Funktionen zur Anzeige von Berechtigungen und Sicherheitsindikatoren.
4. **Zweiter Teil des Fragebogens**: Nach dem Test bewerten die Teilnehmer ihre Erfahrungen mit der Webanwendung und geben Feedback zu den dargestellten Sicherheitsindikatoren.

4 Beschreibung unserer Web-Anwendung[1] (Analysis Tool)

4.1 Zielsetzung der Anwendung

Wie erwähnt, die Webanwendung wurde entwickelt, um Benutzer eine transparente und leicht verständliche Demonstration der Sicherheit und des Datenschutzes mobiler Apps zu bieten. Der Fokus liegt auf der Analyse und Visualisierung von App-Berechtigungen, um Benutzer eine fundierte Entscheidungsgrundlage zu bieten, bevor sie eine Anwendung installieren.

Durch die Integration der vom „Google-Play-Scraper“ Framework [14] erfassten Metadaten aus dem Google-Play-Store kann die Webanwendung diese Informationen strukturiert darstellen. Die Ergebnisse werden in einer intuitiven Benutzeroberfläche angezeigt, die klare Sicherheitsindikatoren enthält, beispielsweise ein „Sicherheitsampelsystem“, das potenzielle Risiken visuell hervorhebt.

Die Anwendung dient auch als Forschungsinstrument, um zu untersuchen, wie unterschiedliche Darstellungsformen von Sicherheitsinformationen das Entscheidungsverhalten der Nutzer beeinflussen. Dabei wurde unter anderem eine simulierte Dummy-App „HighRisk Social App“ eingebunden, um das Sicherheitsbewusstsein der Nutzer für kritische Berechtigungen zu stärken. Ziel ist es, nicht nur technische Informationen bereitzustellen, sondern auch das allgemeine Verständnis und Bewusstsein für Sicherheitsrisiken bei der Nutzung von mobilen Apps zu erhöhen.

4.2 Benutzeroberfläche und Funktionen

Einfache Suche: Das Tool ermöglicht die Suche nach Apps (siehe Abb. 1), indem der Name der App in ein Suchfeld eingegeben wird. Daraufhin werden die Metadaten aus dem Google-Play-Store durchsucht, und relevante Ergebnisse werden präsentiert (siehe Abb. 2).

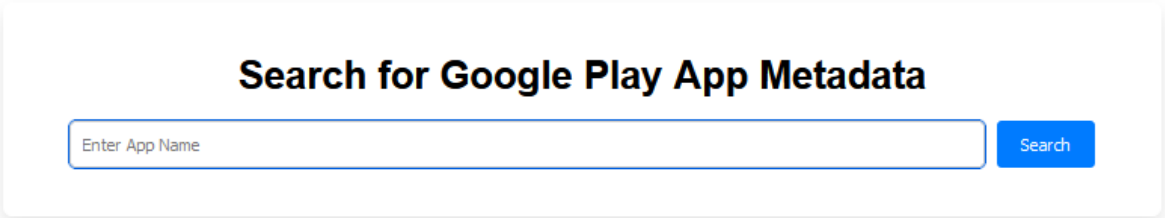

Abbildung 1: Oberfläche des Tools mit Suchfeld zur App-Suche.

4.3 Übersichtliche Ergebnisdarstellung

Hauptergebnis (siehe Abb. 2)**:**

- Hervorgehobene Darstellung der relevantesten Anwendung
- Klare visuelle Darstellung mit App-Symbol
- Grundlegende Informationen wie:
    - App-Name
    - Aktuelle Version
    - Anzahl der Installationen
    - Sicherheitsindikator

Sicherheitsampel-Konzept: Zur Visualisierung der Sicherheitsbewertung wird ein intuitives Farbsystem verwendet (siehe Abb. 2):

- *Grüner* Sicherheitsindikator (Sicherheitssymbol): App erscheint sicher
- *Roter* Sicherheitsindikator (Risikosymbol): Potenzielle Risiken erkennbar

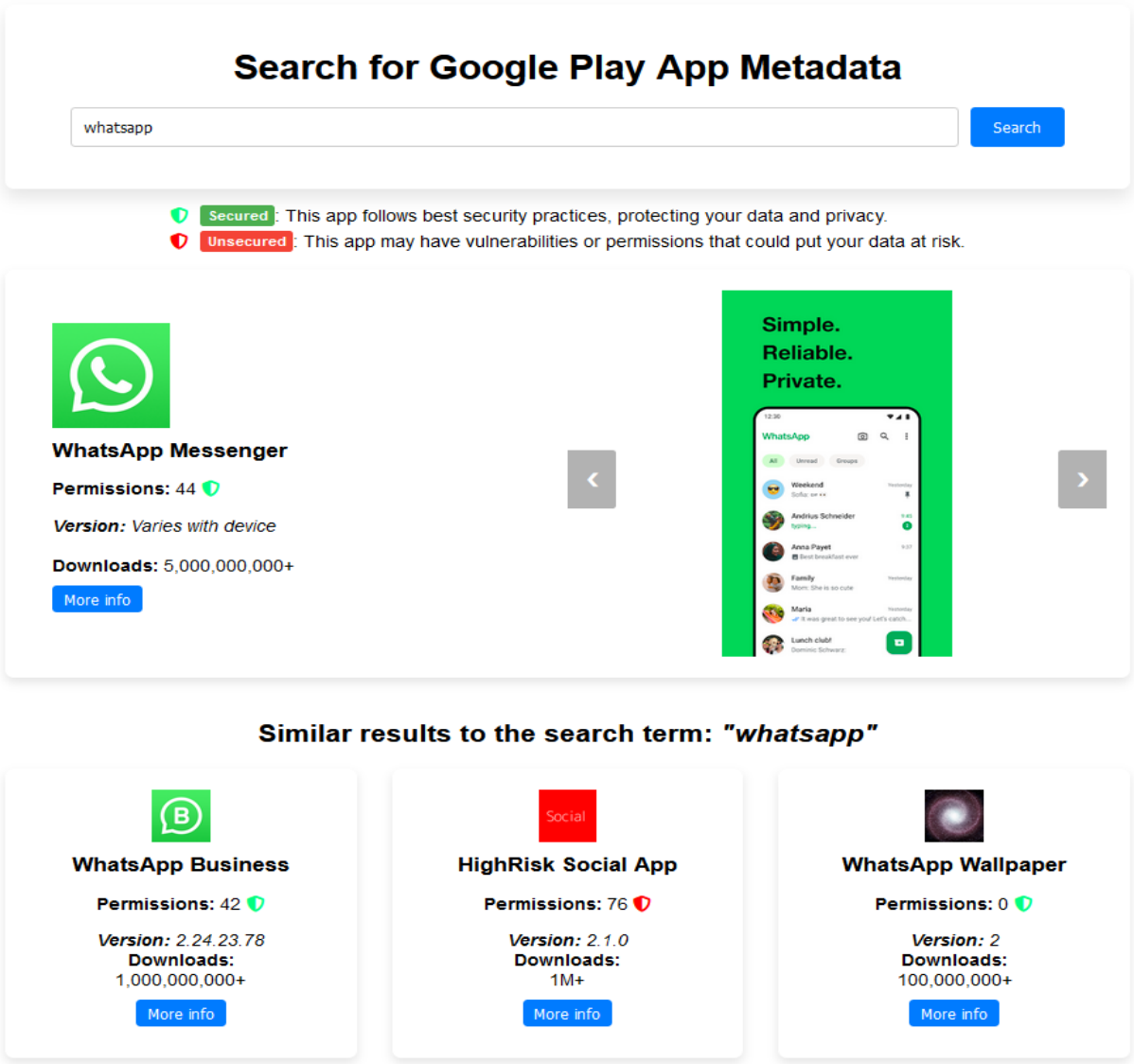

Abbildung 2: Suchergebnisse für die App „whatsapp“

Detaillierte App-Informationen: Über die Schaltfläche „More Info“ können folgende Inhalte abgerufen werden (siehe Abb. 3 und 4):

- Vollständige App-Informationen und Beschreibung.
- Detaillierte Berechtigungsübersicht.
- Risikobewertung der Berechtigungen.
- Erklärungen zu möglichen Datenschutz- und Sicherheitsrisiken.

Risikobewertung von App-Berechtigungen: Die Anwendung bewertet App-Berechtigungen nach einem dreistufigen Risikobewertungssystem (siehe Abb. 4):

- Niedriges Risiko (*grün*)
- Mittleres Risiko (*gelb*)
- Hohes Risiko (*rot*)

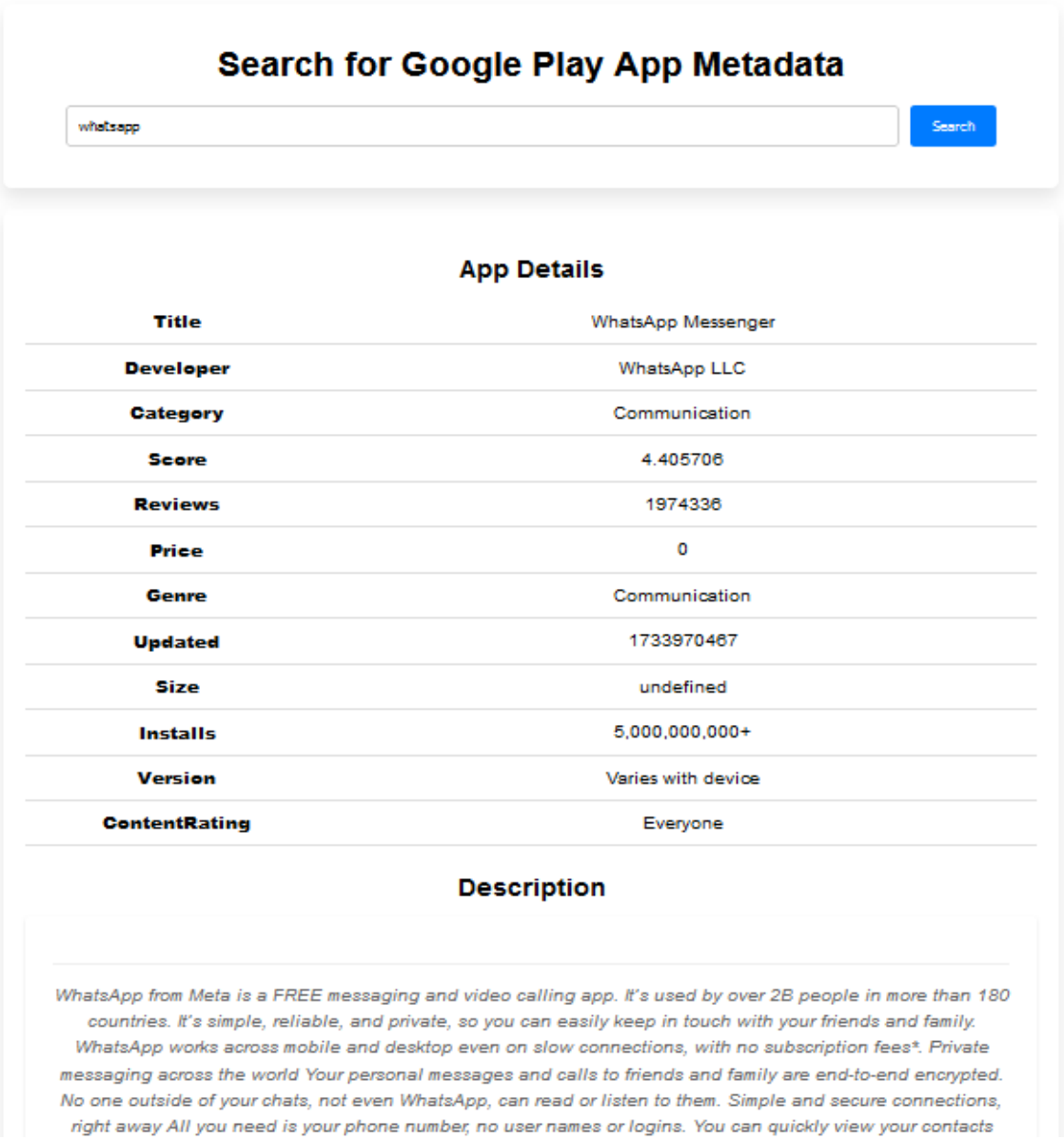

Abbildung 3: Anzeige der vollständigen App-Informationen und Beschreibung nach Auswahl von „More Info“.

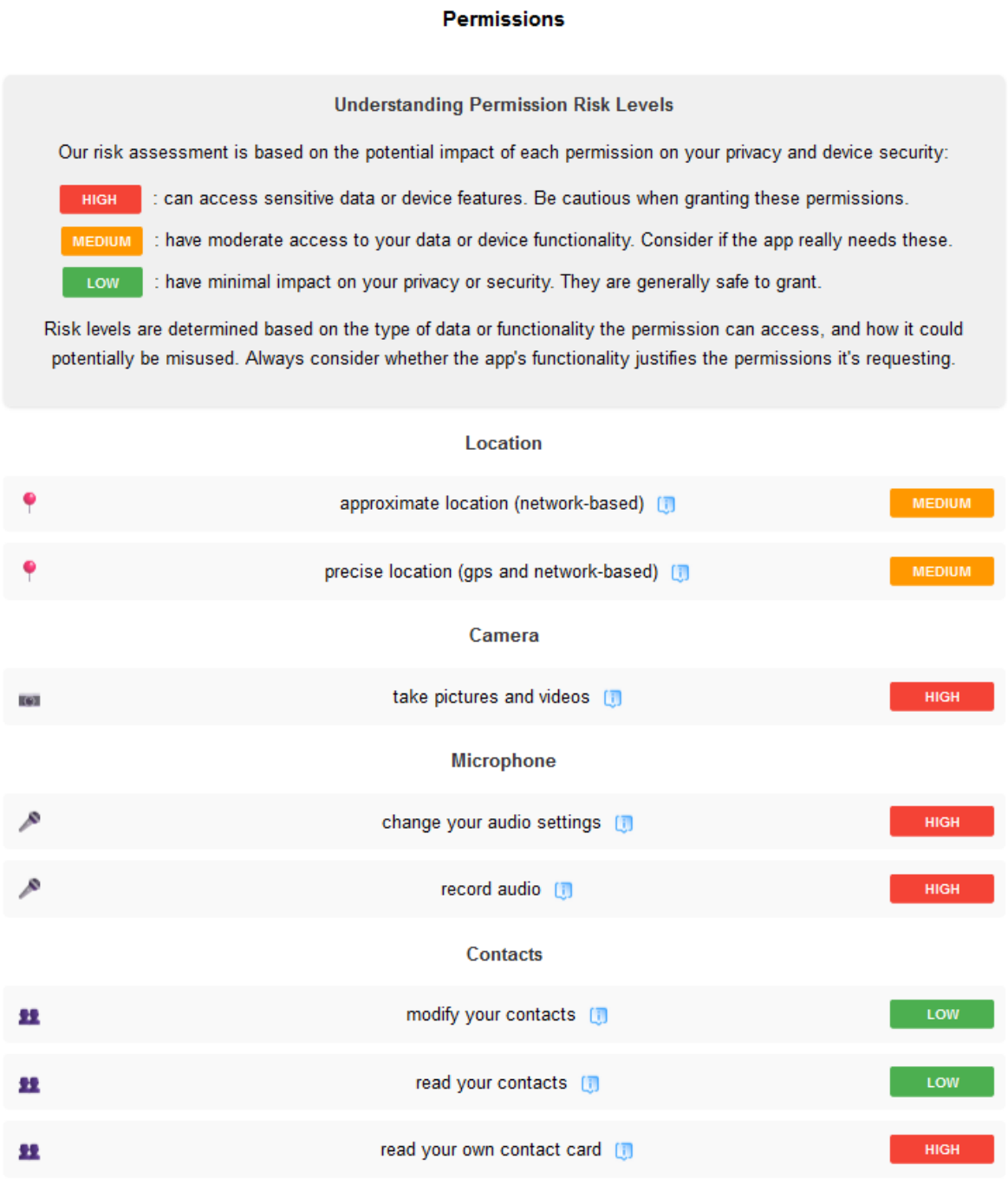

Abbildung 4: weitere Detaillierte Berechtigungsübersicht und Risikobewertung.

Begründung von Risikobewertung: Durch das Überfahren mit der Maus (Hover) über eine der Berechtigungen wird eine zusätzliche Begründung der Risikobewertung (in unserem Fall „Low“, Niedriges Risiko) angezeigt (siehe Abb. 5).

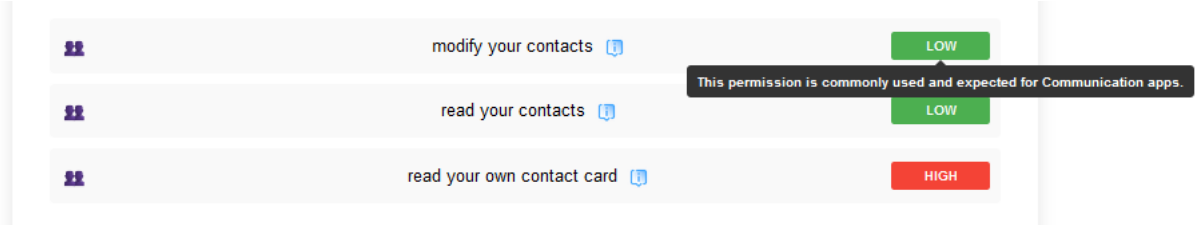

Abbildung 5: Begründung von Risikobewertung

Beschreibung von Berechtigung: Dies ist eine grundlegende Beschreibung der Berechtigung, sie wird beim Überfahren mit der Maus (Hover) über ein Info-Symbol erscheint (siehe Abb. 6).

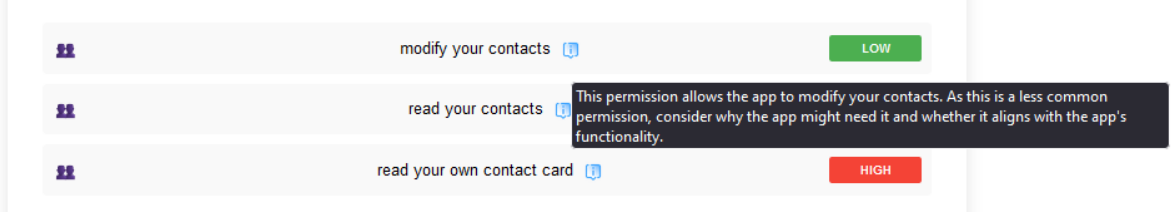

Abbildung 6: Beschreibung von Berechtigungen

4.4 Beschreibung unserer Risiko-Bewertungssystem

Eine umfassende Analyse wissenschaftlicher und technischer Quellen zeigt, dass bislang kein einheitlicher Standard für die Bewertung von App-Berechtigungen existiert, obwohl verschiedene Ansätze vorgestellt wurden. Studien wie die von Al Jutail et al. [15] zeigen, dass App-Berechtigungen basierend auf Googles Klassifizierung in Kategorien wie Zugriff auf private Daten, Änderung von Daten und Überwachung des Standorts eingeteilt werden können. Andere Studien, beispielsweise von Caushaj und Sugumaran [16], unterstreichen die Rolle von Berechtigungskombinationen und Werbenetzwerken (Ads Netzwerken) bei der Bewertung des Datenschutzrisikos. Atzeni et al. [17] haben darüber hinaus ein System entwickelt, das statische und dynamische Analysetechniken kombiniert, um Berechtigungen in feingranulare Risikokategorien einzuordnen. Diese Vielfalt an Ansätzen zeigt, dass die Bewertung von App-Berechtigungen stark von den Zielen der jeweiligen Forschung abhängt.

4.4.1 Methodische Überlegungen

Basierend auf den identifizierten Forschungslücken wurde ein eigenes Risikobewertungssystem entwickelt. Diese orientiert sich an drei wesentlichen Faktoren:

1. Projektspezifische Ziele: Was soll mit dieser Bewertung erreicht werden?

   Das System dient dazu, die potenziellen Auswirkungen von Berechtigungen auf die Privatsphäre und auf den Datenschutz zu analysieren. Dabei wird betont, dass Berechtigungen nicht allgemein als sicher oder unsicher kategorisiert werden. Vielmehr

hängt die Bewertung von Kontext/Kategorie der App ab. Beispielsweise erscheint es logisch und sicher, wenn eine Kommunikations-App wie WhatsApp Kamerazugriff anfordert, während dieselbe Berechtigung bei einer Taschenrechner-App als kritisch und unsicher eingestuft wird.

2. Projektumfang: Welchen Detaillierungsgrad erfordert die Analyse?

   Die Analyse erfordert eine sorgfältige Unterscheidung zwischen verschiedenen Arten der Berechtigungen.

3. Zielgruppe: Wer sind die Adressaten und Nutzer dieser Bewertung?

   Das Risikobewertungssystem wurde so gestaltet, dass es für technisch weniger versierte Nutzer verständlich ist und fundierte Entscheidungen erleichtert.

4.4.2 Konzeptioneller Ansatz

Im Mittelpunkt stand die Entwicklung eines Bewertungskriteriums, das die potenziellen Auswirkungen von App-Berechtigungen auf die Privatsphäre der Nutzer und sein Datenschutz systematisch erfasst. Die Studie von Al Jutail et al. [15] hebt hervor, dass Nutzer Schwierigkeiten haben, technische Begriffe zu verstehen, was die Notwendigkeit einer klaren und verständlichen Darstellung der Risiken unterstreicht. Die Einteilung der Berechtigungen in Kategorien wie Standortzugriff, Kamerazugriff und Kontaktzugriff ermöglicht eine differenzierte Bewertung. Diese Herangehensweise geht über einfache Bewertungen hinaus und integriert kontextsensible Faktoren, um den Nutzern eine fundierte Entscheidungsgrundlage zu bieten.

Kategorisierung von Berechtigungen: Berechtigungen werden in verständliche Kategorien unterteilt:

- Standortzugriff.
- Kamerazugriff.
- Kontaktzugriff.
- Netzzugriff.
- Und weitere.

Zielgruppe: Die Anwendung richtet sich an:

- Smartphones-Benutzer.
- Eltern, die Apps für Kinder überprüfen möchten.
- Personen, die sich für Datenschutz interessieren
- Menschen, die mehr über die Apps-Sicherheit erfahren möchten.

Mehrwert für Nutzer: Transparente Darstellung von App-Risiken.

- Verständliche Erklärungen ohne technische Fachsprache.
- Unterstützung bei informierten Installationsentscheidungen.
- Sensibilisierung für Datenschutz und App-Sicherheit.

Das Ziel der Webanwendung besteht darin, komplexe technische Informationen aus den Metadaten von Google-Play-Apps in leicht verständliche Erkenntnisse umzuwandeln. Damit soll ein bewussterer Umgang mit mobilen Apps gefördert und die Wahrnehmung für Sicherheitsaspekte geschärft werden.

5 Ergebnisse der Studie

In diesem Abschnitt werden die zentralen Ergebnisse der Studie dargestellt. Die Resultate basieren auf der Analyse der gesammelten demografischen, quantitativen und qualitativen gesammelten Daten aus den Fragebogen, den Beobachtungsnotizen sowie den Rückmeldungen zur Nutzung der entwickelten Webanwendung.

5.1 Demografische Daten

Die Stichprobe hat Teilnehmer unterschiedlichen Alters, unterschiedlichen Bildungsniveaus und unterschiedlicher technischer Fähigkeiten umfasst. Die Teilnehmerverteilung erfolgt wie folgt:

Altersgruppen: Die Mehrheit der Teilnehmenden war zwischen 21 und 48 Jahre alt, wobei es weniger ältere Teilnehmer gegeben hat. Die meisten Teilnehmer waren zwischen 28 und 32 Jahre alt (siehe Abb. 7).

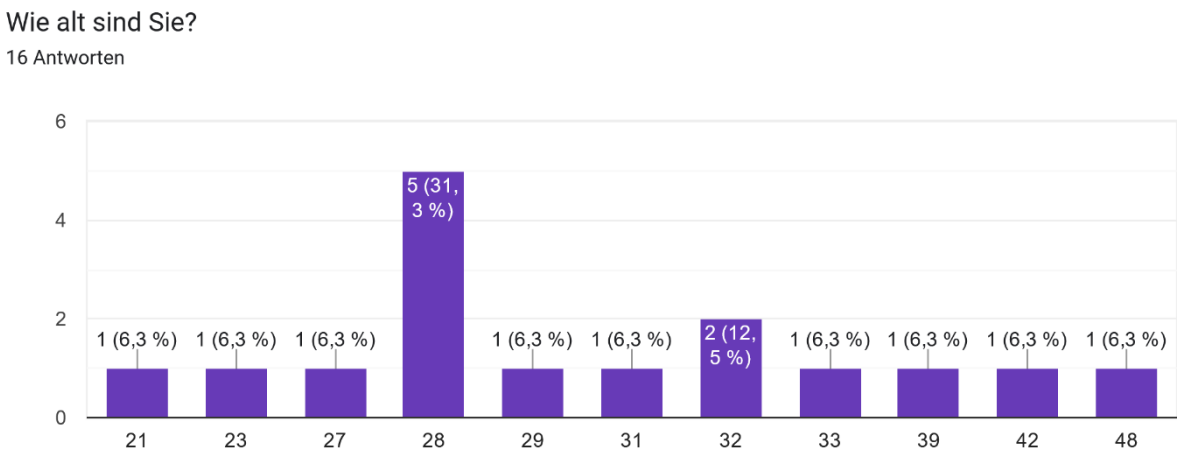

Abbildung 7: Ergebnisse der Umfrage zur Überprüfung des Alters der Teilnehmer

Bildungsniveau: Ein Großteil der Teilnehmenden verfügt über ein hohes Bildungsniveau. Insgesamt haben 31,3 % der Teilnehmer (5 Teilnehmer) über einen Bachelor-Abschluss erworben und 18,8 % über einen Master-Abschlusserworben. Darüber hinaus haben 31,3 % der Teilnehmenden (5 Teilnehmer) über eine abgeschlossene Berufsausbildung absolviert und 18,8 % (3 Teilnehmer) haben als höchsten Bildungsabschluss ein Abitur oder eine Hochschulreife angegeben. Diese Verteilung deutet auf ein relativ hohes Bildungsniveau in der Stichprobe hin (siehe Abb. 8).

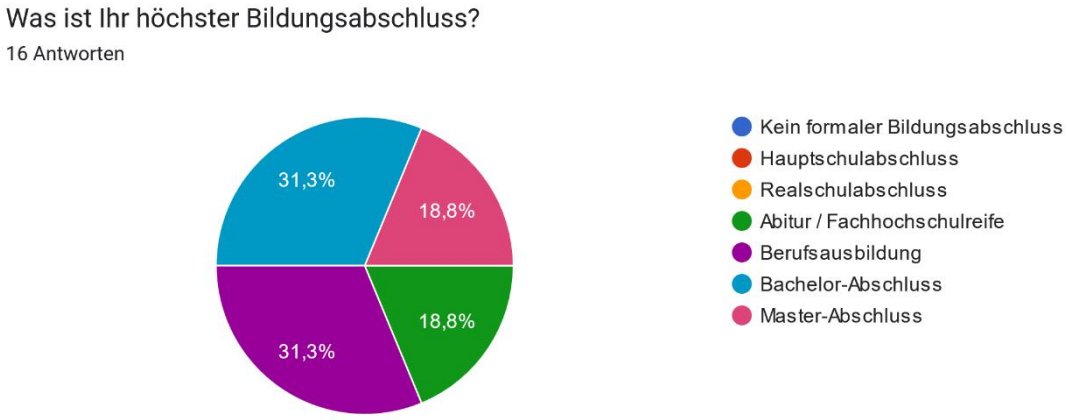

Abbildung 8: Ergebnisse der Umfrage zur Überprüfung des Bildungsniveaus der Teilnehmer.

Beschäftigungsstatus: Die Teilnehmer haben unterschiedliche berufliche Status gehabt. Der größte Anteil der Teilnehmenden war berufstätig, nämlich 50 % (8 Teilnehmer). Weitere 12,5 % (2 Teilnehmer) haben angegeben, selbstständig zu sein, während 12,5 % der Teilnehmer (2 Teilnehmer) haben auch angegeben, auf Arbeitssuche zu sein. Darüber hinaus waren 6,3 % der Teilnehmenden (1 Teilnehmer) Schüler, Studenten, Rentner oder Hausfrauen (siehe Abb. 9).

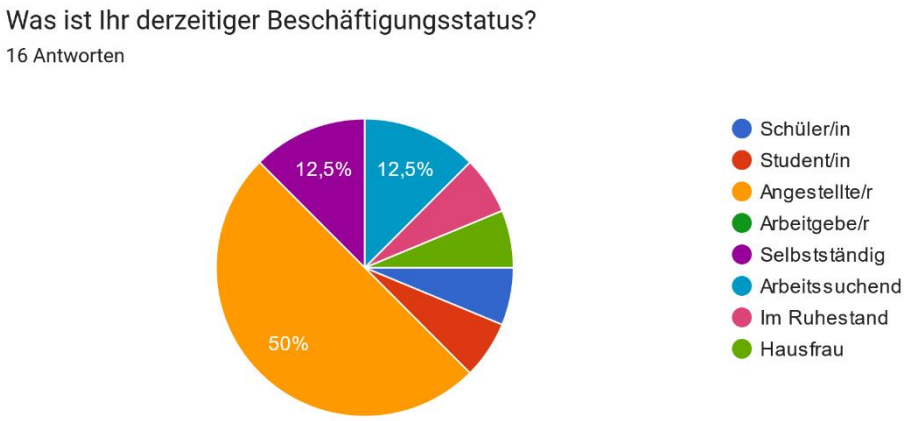

Abbildung 9: Ergebnisse der Umfrage zur Überprüfung des Beschäftigungsstatus der Teilnehmer.

Berufsfelder: Die meisten Berufsteilnehmer arbeiten in verschiedenen Bereichen. 22,2 % der Teilnehmenden (2 Teilnehmer) arbeiten in der IT-Branche und 22,2 % (2 Teilnehmer) auch in der Industrie. Weitere Berufsfelder sind technische Service für Industriemaschinen, Lehre,

Transportdienstleistungen und Energietechnik mit jeweils 11,1 % (1 Teilnehmer) der Angaben. Diese Vielfalt hinsichtlich Alter, Bildungsstand und beruflicher Tätigkeit hat es erlaubt, differenzierte unterschiedliche Einblicke in die persönlichen Entscheidungsprozesse und das Sicherheitsbewusstsein der Teilnehmenden im Zusammenhang mit der Anwendungsnutzung (siehe Abb. 10).

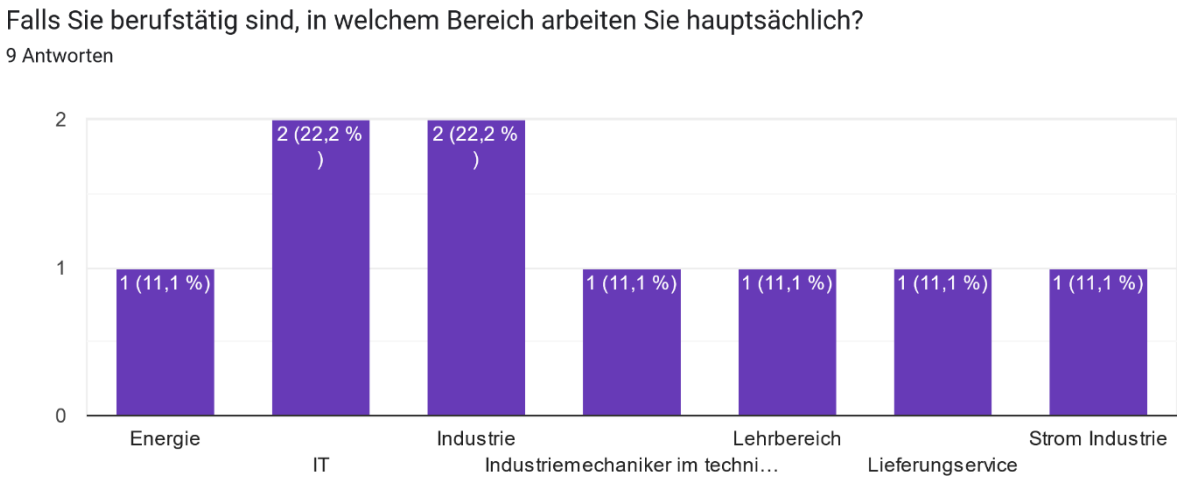

Abbildung 10: Ergebnisse der Umfrage zur Verteilung der Teilnehmer auf verschiedenen Arbeitsbereichen.

5.2 Einflussfaktoren bei der Installation von Apps

Die Ergebnisse der Fragebogen verdeutlichen, welche Kriterien für Nutzer bei der Entscheidung zur Installation einer App von Bedeutung sind (hier wurde die Mehrfachauswahl erlaubt) (siehe Abb. 11):

Hinweis: Die Prozentsätze beziehen sich nicht auf die Teilnehmerzahl (16 Teilnehmer), sondern auf die Gesamtheit der abgegebenen Nennungen, da Mehrfachauswahl erlaubt wurde.

- **Bewertungen**: Der größte Teil der Teilnehmenden 68,8 % (11 Nennung) zieht Bewertungen als Orientierung heran. Diese bieten schnelle, zahlenbasierte Einblicke in die allgemeine Zufriedenheit anderer Nutzer mit der App.
- **Rezensionen**: Mit 62,5 % (10 Nennung) folgen Rezensionen, die eine detailliertere Einschätzung liefern. Kommentare und Erfahrungsberichte sind besonders nützlich, um mögliche Vor- oder Nachteile einer App besser abzuschätzen.
- **App-Beschreibung**: 18,8 % (3 Nennung) achten auf die Beschreibung der App, die meist Informationen zu Funktionen und Anwendungsmöglichkeiten enthält.
- **Entwicklerinformationen**: Für 12,5 % (2 Nennung) spielt der Entwickler der App eine Rolle, was auf die Bedeutung von Vertrauen in die Herkunft der Software hinweist.
- **Berechtigungen, Speichergröße und Installationsstatistiken**: Diese Aspekte wurden jeweils von 6,3 % (1 Nennung) der Teilnehmenden berücksichtigt. Dies deutet darauf

hin, dass technische Details im Entscheidungsprozess oft nur nachrangige Kriterien darstellen.

- **Keine Kriterien**: Ebenso haben 6,3 % (1 Nennung) der Teilnehmenden angegeben, bei der Auswahl einer App keine spezifischen Kriterien zu verwenden.

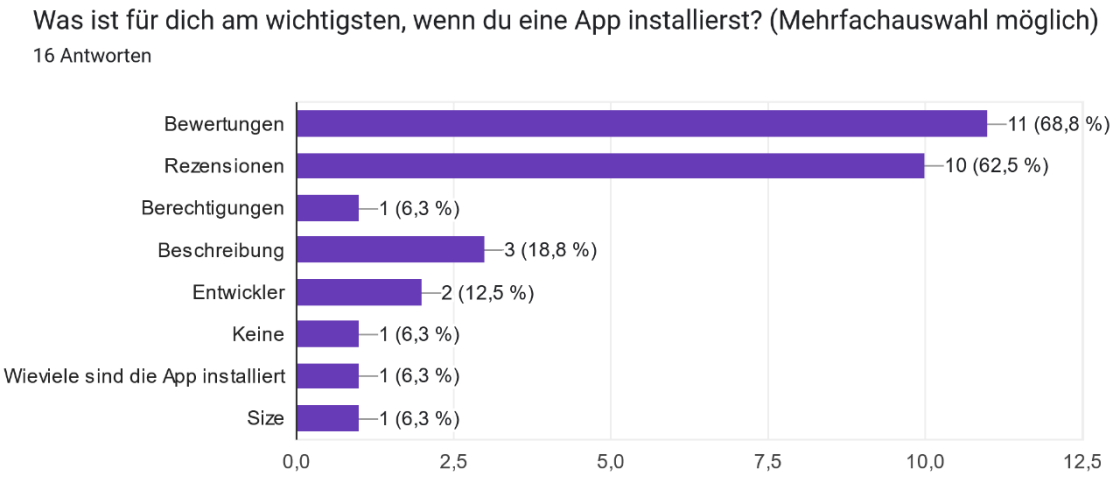

Abbildung 11: Ergebnisse einer Umfrage zu Installationskriterien von Apps.

5.3 Bewertung der App-Sicherheit

Die Einschätzung der Sicherheit einer App wurde auf einer Skala von 1 (unwichtig) bis 5 (sehr wichtig) abgefragt. Die Resultate verdeutlichen eine klare Tendenz zur hohen Priorisierung der Sicherheit (siehe Abb. 12):

- 62,5 % der Teilnehmenden (10 Teilnehmer) haben die Sicherheit der App mit dem höchsten Wert (5) bewertet, was ihre Relevanz unterstreicht.
- 31,3 % (5 Teilnehmer) haben die zweithöchste Bewertung vergeben (4).
- Lediglich 6,3 % (1 Teilnehmer) haben die Sicherheit als mittelmäßig (3) eingestuft.

Insgesamt zeigt sich, dass Sicherheitsaspekte für die Mehrheit der Teilnehmenden eine zentrale Rolle spielen und als entscheidender Faktor bei der Nutzung von Apps gelten.

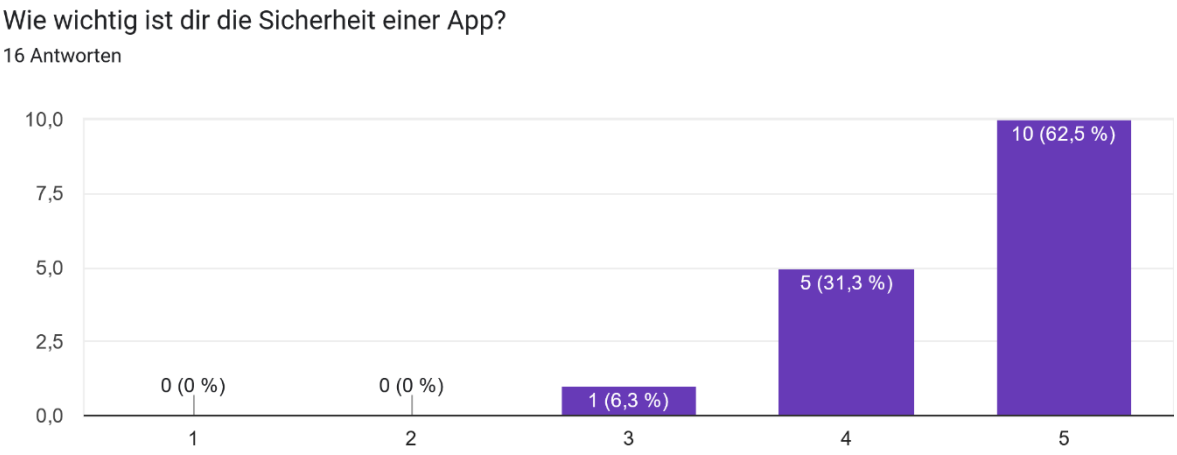

Abbildung 12: Ergebnisse der Umfrage zur App-Sicherheit auf einer 5-Punkte-Skala.

5.4 Umgang mit App-Berechtigungen

Trotz der hohen Bedeutung von Sicherheitsaspekten zeigt sich eine deutliche Diskrepanz zwischen Bewusstsein und Verhalten hinsichtlich der Überprüfung von App-Berechtigungen (siehe Abb. 13):

- 18,8 % der Teilnehmenden (3 Teilnehmer) haben angegeben, die Berechtigungen einer App vor der Installation zu prüfen.
- 81,3 % (13 Teilnehmer) verzichten hingegen auf eine solche Kontrolle.

Dieses Ergebnis weist darauf hin, dass Sicherheitsrisiken zwar stark vorhanden sind, praktische Maßnahmen zur Kontrolle von App-Berechtigungen jedoch oft vernachlässigt werden.

Abbildung 13: Ergebnisse der Umfrage zur Überprüfung von App-Berechtigungen vor der Installation.

5.5 Priorisierung von Benutzerfreundlichkeit im Vergleich zur Sicherheit

Die Fragebogensergebnisse zur Priorisierung von Benutzerfreundlichkeit und Sicherheit zeigen eine klare Präferenz für die Gleichgewichtung beider Aspekte (siehe Abb. 14):

- 93,8 % der Teilnehmenden (15 Teilnehmer) haben Benutzerfreundlichkeit und Sicherheit als gleich wichtig bewertet. Dies deutet darauf hin, dass Nutzer sowohl eine intuitive Nutzung der App als auch ausreichende Sicherheitsmaßnahmen als essenziell erachten.
- 6,3 % (1 Teilnehmer) haben angegeben, dass Sicherheit wichtiger ist. Diese Minderheit legt einen stärkeren Fokus auf den Schutz persönlicher Daten und die Minimierung von Sicherheitsrisiken.
- Es wurde keine Angabe gemacht, dass Benutzerfreundlichkeit wichtiger ist als Sicherheit.

Diese Ergebnisse verdeutlichen, dass Nutzer in der Regel eine ausgewogene Priorisierung der beiden Faktoren erwarten und eine benutzerfreundliche, aber zugleich sichere App bevorzugen.

Die Teilnehmer, die angegeben haben, App-Berechtigungen vor der Installation zu überprüfen, haben unterschiedliche Kriterien unter die Frage „Wenn ja, worauf achtest du am meisten bei den Berechtigungen?“ genannt, die sie bei ihrer Bewertung berücksichtigen:

- Viele Teilnehmer haben betont, dass sie darauf achten, ob die Berechtigungen dem Anwendungszweck der App entsprechen. Beispielsweise wurde angemerkt, dass In-App-Käufe oder der Zugriff auf sensiblere Bereiche wie die Kamera kritisch hinterfragt werden, wenn sie nicht im direkten Zusammenhang mit der Hauptfunktion der App stehen.
- Einige Teilnehmer haben hervorgehoben, dass sie gezielt prüfen, welche Zugriffsrechte die App anfordert, um sicherzustellen, dass diese nicht über das Notwendige hinausgehen.
- Andere haben angegeben, dass sie ein besonderes Augenmerk auf den Zugriff auf persönliche Daten wie Fotos oder die Kamera legen, da solche Berechtigungen potenziell die Privatsphäre gefährden können.

Diese Ergebnisse verdeutlichen, dass die Nutzer, die Berechtigungen überprüfen, vor allem auf die Zweckmäßigkeit und die potenziellen Risiken achten. Besonders sensible Zugriffe werden dabei genauer bewertet, während weniger kritische Berechtigungen oft toleriert werden, wenn sie dem Nutzungskontext entsprechen.

Abbildung 14: Ergebnisse der Umfrage zur Priorisierung von Benutzerfreundlichkeit und Sicherheit.

5.6 Einfluss von App-Berechtigungen auf die Installationsentscheidung

Die Frage, ob zu viele geforderte Berechtigungen zur Nichtinstallation einer App geführt haben, wurde wie folgt beantwortet (siehe Abb. 15):

- 68,8 % der Teilnehmenden (11 Teilnehmer) haben bereits eine App nicht installiert, weil sie zu viele Berechtigungen verlangt hat. Dies zeigt, dass eine Vielzahl der Nutzer bei übermäßigen Berechtigungsanfragen vorsichtig agiert und die Installation ablehnt.
- 31,3 % (5 Teilnehmer) haben hingegen angegeben, dass sie eine App trotz vieler Berechtigungen installiert haben.

Diese Ergebnisse unterstreichen das zunehmende Bewusstsein für Datenschutz und Datensicherheit. Nutzer hinterfragen zunehmend, warum bestimmte Berechtigungen erforderlich sind, und reagieren bei übermäßigen Anforderungen kritisch.

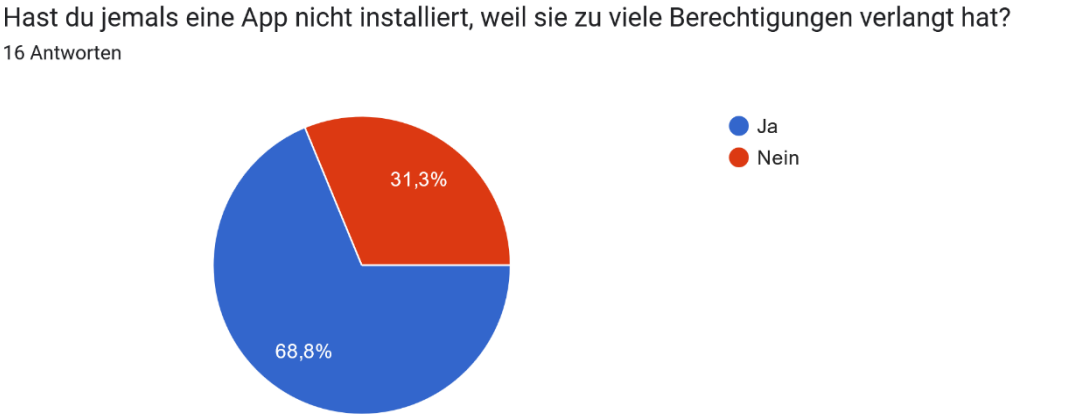

Abbildung 15: Ergebnisse der Umfrage: App-Installation aufgrund von Berechtigungen.

5.7 Wahrnehmung der Sicherheitsindikatoren

Die Ergebnisse der praktischen Testphase hat verschiedene Trends in Bezug auf die Wahrnehmung und das Verständnis von Sicherheitsindikatoren verdeutlicht.

5.7.1 Risikosymbol

Die visuelle Darstellung der Warnhinweise, wie beispielsweise das rote Risikosymbol zur Kennzeichnung einer potenziell risikobehafteten App, wurde von der Mehrheit der Teilnehmenden als effektiv wahrgenommen. Auf einer Skala von 1 (unklar) bis 5 (sehr klar) haben 62,5 % (10 Teilnehmer) der Teilnehmenden die Verständlichkeit des Symbols mit der höchsten Punktzahl bewertet. Weitere 37,5 % (6 Teilnehmer) haben angegeben, dass das Symbol klar verständlich war (Bewertung: 4). Diese Ergebnisse bestätigen die Wirksamkeit der visuellen Gestaltung zur Vermittlung von Sicherheitsinformationen (siehe Abb. 16).

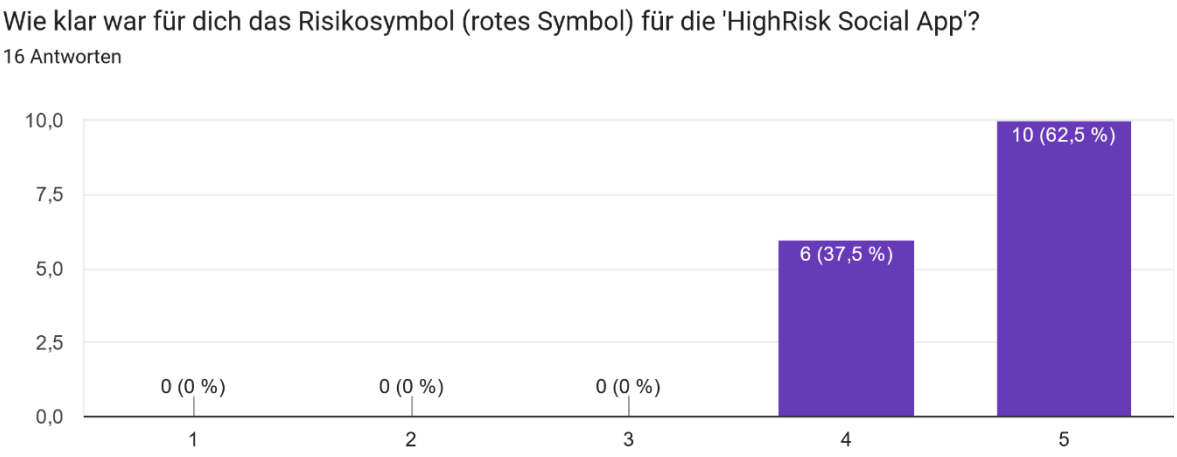

Abbildung 16: Ergebnisse der Umfrage zur Frage „Wie klar war für dich das Risikosymbol (rotes Symbol) für die HighRisk Social App'?“.

5.7.2 Reaktion auf umfangreiche Berechtigungen

Die Antworten der Teilnehmer vor dem Testen der Webanwendung haben ein gemischtes Bild hinsichtlich ihres Verhaltens gegenüber umfangreichen Berechtigungen gezeigt. Auf die Frage „Hast du jemals eine App nicht installiert, weil sie zu viele Berechtigungen verlangt hat?“ haben 68,8 % der Teilnehmer (11 Teilnehmer) mit „Ja“ geantwortet (siehe Abb. 15). Dies hat verdeutlicht, dass ein Großteil der Nutzer Bedenken gegenüber umfangreichen oder sicherheitskritischen Berechtigungen hat. Dennoch haben einige Teilnehmer angegeben, dass ihre Entscheidung stark vom Kontext der App abhängt, da bestimmte Berechtigungen in spezifischen App-Kategorien als weniger kritisch wahrgenommen werden.

Nach der Interaktion mit der Webanwendung haben die Teilnehmer ein verstärktes Bewusstsein für Sicherheitsrisiken geäußert. Die intuitive und klare Darstellung von sicherheitsrelevanten Informationen wurde als hilfreich empfunden, um fundierte Entscheidungen zu treffen. Dies hat gezeigt, dass visuelle Indikatoren, wie beispielsweise Risikosymbole (rote Symbole), die Wahrnehmung von Risiken verbessern können.

5.7.3 Einfluss der Risikosymbole auf der Entscheidung

Die Risikosymbole in der Webanwendung haben einen signifikanten Einfluss auf die Entscheidungen der Teilnehmer gehabt. Auf die offene Frage „Wie würde dieses Symbol deine Entscheidung beeinflussen, eine App zu installieren?“ haben die Teilnehmer vielfältige Antworten gegeben:

- Viele Teilnehmer haben geäußert, dass sie die App aufgrund des roten Risikosymbols nicht installieren würden. Aussagen wie „Ich würde die App niemals installieren“ oder „Das Symbol hat mich davon abgehalten, die App zu installieren“ wurden mehrfach hervorgehoben.
- Einige Teilnehmer haben angegeben, dass das Symbol sie dazu veranlasst hat, die Berechtigungen der App genauer zu überprüfen, bevor sie eine Entscheidung treffen.
- Einzelne Teilnehmer haben das Symbol als nützlich angesehen, um informierte Entscheidungen zu treffen, haben jedoch betont, dass zusätzliche Kontextinformationen hilfreich wären.

Die Frage „War die Anzeige der Berechtigungen und Sicherheitsinformationen klar verständlich?“ haben alle Teilnehmer (16 Teilnehmer) mit „Ja“ beantwortet, was die hohe Benutzerfreundlichkeit und Klarheit der Darstellung unterstrichen hat (siehe Abb. 17).

Abbildung 17: Ergebnisse der Umfrage zur Überprüfung der Klarheit der Berechtigungen und Sicherheitsinformationen.

Die Ergebnisse haben gezeigt, dass gut gestaltete Sicherheitsindikatoren eine wichtige Rolle bei der Entscheidungsfindung spielen und das Bewusstsein für Sicherheitsrisiken deutlich erhöhen können.

5.7.4 Verbesserungsvorschläge

Die Teilnehmer haben wertvolles Feedback zur Webanwendung gegeben, das sowohl positive Aspekte als auch Verbesserungsvorschläge beinhaltet:

Positive Aspekte:

- **Verständlichkeit:** Alle Teilnehmer haben die Anzeige der Sicherheitsindikatoren und Berechtigungen als klar und verständlich empfunden.
- **Nutzerfreundlichkeit:** Die Mehrheit der Teilnehmer hat die einfache und intuitive Bedienbarkeit der Webanwendung hervorgehoben.

Verbesserungsvorschläge:

- Sicherheitsrisiken sollten stärker in den Kontext der jeweiligen App gestellt werden. Beispielsweise wurde angemerkt, dass GPS-Zugriffe bei einer Navigations-App als normal, bei einer Taschenrechner-App jedoch als kritisch einzustufen sind.
- Die Darstellung von Informationen in tabellarischer Form wurde vorgeschlagen, um die Übersichtlichkeit zu erhöhen.
- Die Färbung und Sicherheitsindikatoren wurden als hilfreich bewertet, jedoch wurde angeregt, sie durch kurze Erklärungstexte zu ergänzen, um ihre Aussagekraft weiter zu verbessern.

Die durch die Studie gewonnenen Erkenntnisse haben gezeigt, dass visuelle und intuitive Darstellungen von Sicherheitsinformationen die Wahrnehmung und das Entscheidungsverhalten der Nutzer positiv beeinflussen können. Gleichzeitig bieten die vorgeschlagenen Optimierungen eine Grundlage für die Weiterentwicklung der Webanwendung, um ihre Nutzerfreundlichkeit und Effektivität weiter zu steigern.

5.8 Zusammenfassung der Ergebnisse

Zusammenfassend lässt sich feststellen, dass die Kombination aus Fragebogen, Beobachtungen und Rückmeldungen ein umfassendes Bild des Nutzerverhaltens und Sicherheitsbewusstseins bei der App-Installation ermöglicht hat. Während Sicherheitsindikatoren und visuelle Warnhinweise das Entscheidungsverhalten positiv beeinflussen können, besteht nach wie vor ein Informationsdefizit bei der Bewertung von App-Berechtigungen. Unsere entwickelte Webanwendung trägt dazu bei, dieses Defizit zu verringern, indem sie transparente und verständliche Einblicke in die Sicherheitsrisiken mobiler Apps bietet.

6 Diskussion

In diesem Kapitel werden die Ergebnisse der Studie analysiert, die Forschungsfragen beantwortet und die Implikationen der Erkenntnisse interpretiert. Ziel ist es, die

Haupterkenntnisse in den Kontext bestehender Forschung zu stellen und mögliche Auswirkungen sowie Verbesserungsmöglichkeiten zu diskutieren.

6.1 Beantwortung der Forschungsfragen

Forschungsfrage 1: Wie können App-Berechtigungen so dargestellt werden, dass sie das Bewusstsein der Nutzer für Sicherheitsrisiken erhöhen?

Die Ergebnisse der Studie haben gezeigt, dass die visuelle Darstellung von Sicherheitsindikatoren eine entscheidende Rolle spielt, um das Bewusstsein für Risiken zu schärfen. Besonders das eingeführte dreistufige Risikobewertungssystem mit Farbcodierungen (Sicherheitsampel: grün, gelb, rot) hat sich als effektiv erwiesen. 62,5 % der Teilnehmer (10 Teilnehmer) haben die Risikosymbole als sehr klar verständlich bewertet (siehe Abb. 16). Diese Ergebnisse haben die Bedeutung intuitiver und visuell ansprechender Warnhinweise unterstrichen. Im Vergleich zu bisherigen Studien, die sich oft auf textbasierte Informationen beschränkt haben, liefert diese Arbeit klare Hinweise darauf, dass Farbcodierungen die Wahrnehmung von Risiken positiv beeinflusst haben.

Forschungsfrage 2: Welche Faktoren beeinflussen das Nutzerverhalten bei der Installation von Apps?

Die Studie hat mehrere Schlüsselfaktoren identifiziert, die das Nutzerverhalten beeinflusst haben. Bewertungen und Rezensionen sind von der Mehrheit der Teilnehmer (68,8 % bzw. 62,5 %) als entscheidende Kriterien bei der App-Installation genannt worden (siehe Abb. 11). Gleichzeitig haben 68,8 % der Teilnehmer (11 Teilnehmer) angegeben, Apps nicht zu installieren, wenn diese zu viele Berechtigungen anfordern (siehe Abb. 15). Diese Ergebnisse haben verdeutlicht, dass sowohl soziale Faktoren (Bewertungen und Rezensionen) als auch technische Aspekte (Berechtigungen) das Entscheidungsverhalten entscheidend beeinflusst haben.

Forschungsfrage 3: Inwiefern können Sicherheitsindikatoren das Entscheidungsverhalten von Nutzern beeinflussen?

Die eingeführten Sicherheitsindikatoren, insbesondere die roten Risikosymbole, haben einen signifikanten Einfluss auf die Entscheidungen der Teilnehmer gehabt. Viele haben geäußert, dass sie eine App aufgrund des Risikosymbols nicht installieren würden. Darüber hinaus haben die Sicherheitsindikatoren dazu beigetragen, dass die Teilnehmer die Berechtigungen der Apps genauer überprüft haben. Dies hat gezeigt, dass visuelle Warnhinweise nicht nur die Wahrnehmung von Risiken verbessert, sondern auch das Nutzerverhalten positiv beeinflusst haben.

Forschungsfrage 4: Wie wirksam ist die entwickelte Webanwendung bei der Unterstützung informierter Entscheidungen?

Die entwickelte Webanwendung ist von allen Teilnehmern als klar und verständlich bewertet worden. Insbesondere die intuitive Benutzeroberfläche und die klare Darstellung der Sicherheitsindikatoren sind positiv hervorgehoben worden. Verbesserungsvorschläge wie die Kontextualisierung von Berechtigungen und die tabellarische Darstellung von Informationen haben Ansätze für zukünftige Weiterentwicklungen geboten. Insgesamt haben die Ergebnisse gezeigt, dass die Anwendung die Entscheidungsfindung der Nutzer effektiv unterstützt hat.

6.2 Interpretation der Hauptergebnisse

Die Ergebnisse der Studie haben bestätigt, dass visuelle und intuitive Sicherheitsindikatoren das Bewusstsein für App-Berechtigungen erheblich gesteigert haben. Gleichzeitig ist deutlich geworden, dass viele Nutzer zwar Sicherheitsaspekte als wichtig einstufen, jedoch ihre Entscheidungen oft durch die Benutzerfreundlichkeit oder die wahrgenommene Relevanz der App beeinflusst werden. Dies verdeutlicht die Notwendigkeit, Sicherheitsinformationen im Kontext der jeweiligen App-Kategorie bereitzustellen. Beispielsweise werden GPS-Zugriffe bei Navigations-Apps als akzeptabel wahrgenommen, während sie bei anderen App-Kategorien kritisch betrachtet werden.

6.3 Praktische Implikationen

Die Ergebnisse der Arbeit haben mehrere praktische Implikationen geboten:

- **Für Nutzer:** Die Arbeit hat gezeigt, dass eine bewusste und informierte Entscheidung bei der App-Installation möglich ist, wenn relevante Informationen klar dargestellt werden.
- **Für Forscher:** Die entwickelte Bewertungsmethode hat eine Grundlage für zukünftige Studien zur Verbesserung von Sicherheitsindikatoren geboten.
- **Für Plattformanbieter wie Google-Play-Store und Apple-App-Store:** Plattformen sollten verstärkt auf die visuelle Darstellung von Berechtigungen und Sicherheitsindikatoren setzen, um die Entscheidungsfindung der Nutzer vor der Installation von Apps zu unterstützen. Klare und verständliche Darstellungen könnten das Vertrauen der Nutzer stärken und ihre Bereitschaft erhöhen, Sicherheitsaspekte in ihre Entscheidungen einzubeziehen.

Die Kombination aus empirischen Ergebnissen und theoretischen Überlegungen hat gezeigt, dass die entwickelte Webanwendung einen wichtigen Beitrag zur Sensibilisierung für App-Berechtigungen geleistet hat. Die Forschungsfragen sind beantwortet worden, und praktische Ansätze zur Verbesserung der Benutzerfreundlichkeit und Sicherheit mobiler Apps sind identifiziert worden. Künftige Studien können auf diesen Erkenntnissen aufbauen, um die Effektivität von Sicherheitsindikatoren weiter zu steigern.

7 Einschränkungen der Studie

Obwohl die Ergebnisse informativ sind, weist diese Studie mehrere methodische und praktische Einschränkungen auf, die bei der Interpretation der Ergebnisse berücksichtigt werden müssen:

7.1 Stichprobenzusammensetzung

Das Bildungsniveau der Stichprobe war überdurchschnittlich hoch: 50,1 % der Teilnehmer haben (8 Teilnehmer) über einen Hochschulabschluss verfügt (siehe Abb. 8). Dies kann die Ergebnisse verfälschen, da gebildetere Personen möglicherweise ein höheres Bewusstsein für Sicherheitsfragen haben.

Die Altersverteilung konzentriert sich überwiegend auf Teilnehmer im Alter zwischen 21 und 48 Jahren, wodurch die ältere Nutzergruppe unterrepräsentiert ist (siehe Abb. 7). Dies schränkt die Generalisierbarkeit der Ergebnisse auf andere Altersgruppen ein.

7.2 Methodische Einschränkungen

Die Kombination aus persönlichen Interviews und Zoom-Videogesprächen kann zu unterschiedlichen Interaktionsqualitäten führen und die Vergleichbarkeit der Ergebnisse beeinträchtigen.

Die relative kurze Dauer der Interviews (10–15 Minuten) könnte die Tiefe der gesammelten Informationen eingeschränkt haben, insbesondere bei komplexeren Sicherheitsaspekten.

7.3 Technische Einschränkungen

Die entwickelten Webanwendung basieren vollständig auf Daten aus dem Google-Play-Store, sodass keine Aussagen zum Nutzerverhalten in IOS-Apps oder anderen App-Stores getroffen werden können.

Die Risikobewertung von App-Berechtigungen wird mithilfe eines selbst entwickelten dreistufigen Systems ohne einheitliche Standards durchgeführt. Dies kann die Vergleichbarkeit mit anderen Studien einschränken.

7.4 Verhaltensbeobachtung

Beobachtungen des Nutzerverhaltens werden in kontrollierten Testumgebungen durchgeführt, die das natürliche Installationsverhalten im täglichen Leben möglicherweise nicht vollständig widerspiegeln.

Die Anwesenheit des Interviewers kann zu sozial erwünschtem Antwortverhalten führen, insbesondere bei Fragen zur Sicherheitsbewertung und zum Umgang mit App-Berechtigungen.

7.5 Zeitliche Einschränkungen

Da die Studie eine Momentaufnahme darstellt und keine Aussagen über langfristige Verhaltensänderungen oder die nachhaltige Wirksamkeit der Sicherheitsindikatoren zulässt, konnte auch die Entwicklung des Sicherheitsbewusstseins über Zeit nicht erfasst werden.

Diese Einschränkungen bieten wichtige Ansatzpunkte für zukünftige Forschungsarbeiten, die sich beispielsweise auf spezifische Altersgruppen konzentrieren, längerfristige Verhaltensänderungen untersuchen oder alternative App-Stores einbeziehen könnten. Zudem wäre eine Validierung des entwickelten Risikobewertungssystems durch weitere Studien wünschenswert.

8 Zusammenfassung und Ausblick

Die vorliegende Bachelorarbeit hat einen wichtigen Beitrag zum Verständnis des Nutzerverhaltens bei der App-Installation und zur Entwicklung effektiver Sicherheitsindikatoren geleistet. Unsere entwickelte Webanwendung hat gezeigt, dass visuelle und intuitive Sicherheitsindikatoren das Potenzial haben, das Bewusstsein für App-Berechtigungen zu schärfen und fundierte Installationsentscheidungen zu unterstützen.

8.1 Zusammenfassung der Ergebnisse

Die Ergebnisse unserer Studie haben die Relevanz von Sicherheitsindikatoren und deren Einfluss auf das Nutzerverhalten bestätigt. Die eingeführten visuellen Warnhinweise, wie das dreistufige Farbsystem, haben sich als effektive Methode zur Vermittlung von Sicherheitsrisiken herausgestellt. Mehr als 62 % der Teilnehmer haben die visuellen Indikatoren als sehr klar und verständlich bewertet, während die intuitive Benutzeroberfläche und die kontextsensible Darstellung von Berechtigungen von allen Teilnehmern positiv hervorgehoben wurden.

Darüber hinaus hat die Studie gezeigt, dass Nutzer sowohl soziale Faktoren wie Bewertungen und Rezensionen als auch technische Aspekte wie Berechtigungen in ihre Entscheidungsprozesse einbeziehen. Der Großteil der Teilnehmer hat angegeben, Apps nicht zu installieren, wenn diese übermäßige Berechtigungen anfordern, was ein wachsendes Bewusstsein für Datenschutz und Sicherheit verdeutlicht.

8.2 Praktische Erkenntnisse

Die Arbeit hat praktische Handlungsempfehlungen für verschiedene Zielgruppen hervorgebracht:

- **Für Nutzer:** Die Ergebnisse zeigen, dass eine bewusste und informierte Entscheidung bei der App-Installation möglich ist, wenn relevante Informationen klar und verständlich dargestellt werden.
- **Für Plattformbetreiber:** Anbieter wie Google-Play-Store oder der Apple-App-Store könnten von der Integration klarer visueller Indikatoren profitieren, um Nutzern eine

bessere Entscheidungsgrundlage zu bieten und das Vertrauen in ihre Plattformen zu stärken.

- **Für Forschung und Gesetzgebung:** Die Studie hebt die Notwendigkeit hervor, standardisierte Sicherheitsindikatoren und Risikobewertungssysteme zu entwickeln, die langfristig auch gesetzlich verankert werden könnten.

8.3 Ausblick

Die Ergebnisse dieser Arbeit bieten eine solide Grundlage für zukünftige Forschungen und Entwicklungen. Einige vielversprechende Ansätze für weiterführende Studien sind:

- **Erweiterung auf mobile Plattformen:** Während diese Arbeit sich auf eine Web-Version konzentriert hat, könnten zukünftige Studien die Visualisierung von Sicherheitsindikatoren in mobilen App-Stores wie dem Google-Play-Store oder dem Apple-App-Store untersuchen. Dabei könnten Unterschiede in der Darstellung und Wahrnehmung zwischen Web- und Mobilversionen analysiert werden.
- **Entwicklung von Standards:** Eine mögliche Weiterentwicklung wäre die Erstellung einheitlicher Standards für Sicherheitsindikatoren und Risikobewertungen. Dies könnte ein übergreifendes Farbsystem (z. B. Sicherheitsampel) oder detaillierte Bewertungsrichtlinien umfassen. Solche Standards könnten auf europäischer Ebene politisch und gesetzlich diskutiert und eventuell in die DSGVO (EU-Datenschutz-Grundverordnung) integriert werden.
- **Langzeitstudien:** Eine Studie der langfristigen Auswirkungen von Sicherheitsindikatoren auf das Nutzerverhalten wäre ebenfalls wertvoll. Dabei könnte erforscht werden, ob und wie sich das Sicherheitsbewusstsein der Nutzer über die Zeit entwickelt.

Zusammenfassend lässt sich sagen, dass diese Arbeit einen wichtigen Beitrag zur Verbesserung der Sicherheit und Transparenz mobiler Apps geleistet hat. Die vorgestellten Ansätze und Ergebnisse bieten eine Grundlage für weiterführende Forschungen und Entwicklungen, die das Ziel verfolgen, das Vertrauen der Nutzer in digitale Plattformen zu stärken und eine sicherere Nutzung mobiler Apps zu ermöglichen.

Referenzen

[1] I. M. Almomani und A. Al Khayer, „A comprehensive analysis of the android permissions system,“ Ieee access 8, 2020.

[2] E. Alepis und C. Patsakis, „Unravelling security issues of runtime permissions in android.,“ Journal of Hardware and Systems Security, 2019.

[3] E. Gashi , „Permission-based privacy analysis for android applications.,“ University for Business and Technology - UBT, 2018.

[4] R. McConkey und O. Olukoya, „Runtime and design time completeness checking of dangerous android app permissions against GDPR.,“ IEEE Access, 2023.

[5] A. Senarath und N. A. Arachchilage, „Why developers cannot embed privacy into software systems? An empirical investigation.,“ Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering, 2018.

[6] S. Yilmaz und M. Davis, „Hidden permissions on Android: a permission-based Android mobile privacy risk model.,“ Kingston University, UK, 2023.

[7] G. Danny S. , D. Rodriguez, J. M. del Alamo und J. Such, „Guamán, Danny S., et al. "Automated GDPR compliance assessment for cross-border personal data transfers in android applications.,“ Computers & Security, 2023.

[8] M. M. Alani, „Android users privacy awareness survey.,“ International Journal of Interactive Mobile Technologies, 2017.

[9] . O. Astafeva, D. Kadyrova und I. Osipova, „Research Of Educational Content Implementation Due To Development Of Mobile Apps Market.,“ European Proceedings of Social and Behavioural Sciences, 2020.

[10] M. Hatamian, „Engineering privacy in smartphone apps: A technical guideline catalog for app developers.,“ IEEE Access 8 (2020): 35429-35445., 2020.

[11] M. Alenezi und I. Almomani, „Abusing android permissions: A security perspective.,“ IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)., 2017.

[12] J. Xiao , S. Chen, Q. He, Z. Feng und X. Xue, „An Android application risk evaluation framework based on minimum permission set identification.,“ Journal of Systems and Software, 2020.

[13] L. Shen, „Multifeature-Based Behavior of Privilege Escalation Attack Detection Method for Android Applications,“ Mobile Information Systems, 2020.

[14] R. M. A. Latif, M. T. Abdullah, S. U. Aslam Shah, M. Farhan, F. Ijaz und A. Karim, „Data Scraping from Google Play Store and Visualization of its Content for Analytics,“ International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), 2019.

[15] M. Al Jutail, M. Al-Akhras und A. Albesher, „Associated Risks in Mobile Applications Permissions," College of Computing and Informatics, Saudi Electronic University, Riyadh, KSA., 2019.

[16] E. Caushaj und V. Sugumaran, „Classification and security assessment of android apps," Discover Internet of Things, 2023.

[17] A. Atzeni, T. Su, M. Baltatu, R. D'Alessandro und G. Pessiva, „Android Apps Risk Evaluation: a methodology," EAI Endorsed Transactions on Ubiquitous Environments, 2015.

[18] A. Adams und A. L Cox, „Questionnaires, in-depth interviews and focus groups," The Open University's repository of research publications, 2008.

[19] N. Fox, „Using Interviews in a Research Project," TRENT RDSU, 2006.

[20] S. Jain, S. Dubey und S. Jain, „Designing and validation of questionnaire.," International dental & medical journal of advanced research, 2016.

[21] V. Raju N und N. Harinarayana, „Online Survey Tools: A Case Study of Google Forms," National conference on scientific, computational & information research trends in engineering, GSSS-IETW, 2016.

[22] M. S. D. Prasad Nayak und K. Narayan, „Strengths and weaknesses of online surveys," IOSR Journal of Humanities and Social Sciences (IOSR-JHSS), 2019.

[23] M. P. Couper, „Designing Effective Web Surveys," Cambridge University Press, 2008.

[24] M. Revilla und J. K. Höhne, „How long do respondents think online surveys should be? New evidence from two online panels in Germany.," International Journal of Market Research, 2020.

[25] S. Jain, S. Dubey und S. Jain, „Designing and validation of questionnaire," International dental & medical journal of advanced research, 2016.

Anhang

Links und Ressourcen

In diesem Abschnitt werden relevante Links und Ressourcen bereitgestellt, die als zusätzliche Referenzen und Kontext für diese Arbeit dienen. Dazu gehören Quellcode-Repository und Werkzeuge, die während der Entwicklung und Analyse verwendet wurden.

1. **Code-Repository:**
    - GitHub-Repository der Webanwendung Dieses Repository enthält den Quellcode der entwickelten Webanwendung
2. **Fragebogen-Formular:**
    - Google-Forms-Umfrage Das in dieser Studie verwendete Umfrageformular zur Erhebung von Daten über das Nutzerverhalten und die Wahrnehmung von App-Berechtigungen.