Zurück zum Inhaltsverzeichnis

Zur Security Awareness bei Nutzern von Smartphones

Philipp Goldberg[1]

Kurzfassung:
Immer mehr Menschen nutzen ein Smartphone. Mittlerweile ist die Anzahl von Nutzern auf gut 3,2 Milliarden angestiegen. Das Thema Sicherheit spielt bei einer derartigen Verbreitung eine wichtige Rolle. Doch wie gut sind die Nutzer über mögliche Risiken und Schutzmaßnahmen informiert? Wie hat sich dies im Laufe der Jahre entwickelt und mit welchen Methodiken wurde dies gemessen? Welche Anstrengungen in der Forschung haben dazu beigetragen, die Security Awareness zu verbessern?
Zur Beantwortung dieser Fragen wird die vorhandene Literatur mit Fokus auf die Security Awareness von Nutzern von Smartphones durchsucht. Hierzu wird ein strukturiertes Literaturreview für die Jahre 2011 bis 2020 durchgeführt. Es werden insgesamt 46 relevante Arbeiten analysiert. Hierbei werden die gängigen Methodiken und Erkenntnisse synthetisiert. Um die zukünftige Forschung zu unterstützen, erfolgt die Auflistung gängiger Limitationen und Hinweise zur weiteren Ausrichtung der Forschungsaktivitäten.

Stichworte: Awareness, Literaturreview, Security Awareness, Sicherheitsbewusstsein, Smartphones, Strukturiertes Literaturreview

1. Einleitung und Motivation

Die Zahl der Smartphone-Nutzer steigt Jahr für Jahr an, auf nunmehr gut 3,2 Milliarden [1]. Durch die zunehmende Verbreitung der Geräte wird es immer wichtiger, dass die Nutzer dabei nicht unnötigen Gefahren ausgesetzt werden. Für den sicheren Umgang mit IT-Ressourcen ist die Security Awareness der Nutzer von Bedeutung. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sieht in seinem IT-Grundschutz-Kompendium [2] vor, dass Mitarbeiter/Nutzer die Sicherheitsziele kennen, dass sie bereit sind diese umzusetzen und fähig sind, in sicherheitskritischen Situationen angemessen zu reagieren.

In seinem Lagebericht zur IT-Sicherheit in Deutschland für das Jahr 2014 merkt das BSI an, dass Smartphones mit ihren Betriebssystemen gut gesichert sind. Eine weitere Komponente für die IT-Sicherheit seien aber auch die Nutzer. Hier wird angemerkt, dass beispielsweise die Berechtigungsabfragen der Apps von den Nutzern in den allermeisten Fällen unreflektiert bestätigt werden. [3]

Hat sich diese Situation geändert? Sind die Nutzer nun besser für den sicheren Umgang mit ihren Smartphones gerüstet? Um diese Fragen zu beantworten und auch zu evaluieren, worauf der Fokus und die Erkenntnisse aus der Forschung liegen, wird in dieser Arbeit ein strukturiertes Literaturreview (SLR) durchgeführt.

[1] Fachbereich Informatik, Hochschule Darmstadt, mail@pgoldberg.de

2. Zielsetzung und Forschungsfragen

Ziel dieser Arbeit soll es sein, einen Überblick darüber zu erhalten, was sich in der Forschung im Bereich der Security Awareness mit Fokus auf Smartphones und deren Nutzer getan hat. Hierfür soll die in den letzten Jahren betriebene Forschung analysiert werden. Neben der Beantwortung der Forschungsfragen soll ein Mehrwert für die zukünftige Forschung generiert werden. So erfolgt die Nennung typischer Limitationen der untersuchten Arbeiten und die Erstellung einer Forschungsagenda.

In der Fragestellung sind 2 Themenschwerpunkte enthalten. Zum einen das Thema Security Awareness, zum anderen auch die Nutzer von Smartphones. Hier stellen sich folgende Fragen:

- Welche Ansätze gibt es, um die Security Awareness zu erhöhen bzw. zu verbessern?
- Mit welchen Methodiken wurde die Security Awareness gemessen?
- Wie wird die Gültigkeit der Aussagen belegt? Welche typischen Limitierungen gibt es?
- Wie hat sich die Security Awareness über die Jahre verändert?

3. Begriffsdefinitionen

In diesem Kapitel werden einige für diese Arbeit wichtige Begriffe definiert.

3.1. Security Awareness

Die gängigen Begriffsdefinitionen zu Security Awareness (deutsch: Sicherheitsbewusstsein) des US-Amerikanischen National Institute of Standards and Technology (NIST) [4] und des BSI [2] nennen ähnliche Punkte. Diese lassen sich auf das Zusammenspiel der Aspekte *Können*, *Wollen* und *Wissen* reduzieren, wie beispielsweise Helisch [5] in seinem Buch erkannt hat.

3.2. Smartphone

Eine allgemeingültige Definition, was ein Smartphone genau ist und was es ausmacht, scheint es aktuell nicht zu geben [6]. Vielmehr gibt es mehrere Definitionen, welche mehr oder minder ähnliche Elemente haben. Hierbei handelt es sich um die Erläuterungen des Duden [7], des Gabler Wirtschaftslexikon [8] und der International Telecommunication Union (ITU) [6].

Nimmt man die Kernpunkte zusammen, so sind die Bedienung über einen Touchscreen, ein modernes/komplexes Betriebssystem, dem eine Vielzahl an Sensoren (beispielsweise GPS) zur Verfügung stehen und die Möglichkeit der Funktionserweiterung mittels Apps, welche durch den Nutzer installiert werden können, Mindestvoraussetzungen für ein Smartphone.

3.3. Strukturiertes Literaturreview

Das Ziel eines SLR ist es, bereits vorhandenes Wissen in Form von relevanten Publikationen zu finden. Es soll durch die Synthese zentraler Aussagen zusammengefasst werden. Weiterhin werden die bisher unternommenen Untersuchungen und Fragestellungen

genannt. Neben der Erstellung einer Forschungsagenda werden die aufgetretenen Limitierungen und methodischen Probleme genannt. Somit können diese bei der weiteren Forschung vermieden werden.

4. Vorgehensweise

In dieser Arbeit wird das Rahmenwerk von Jan vom Brocke et al. [9] genutzt. In ihrer Arbeit gehen sie der Frage nach, ob Literatur Reviews im Bereich der Informatik nachvollziehbar und systematisch durchgeführt werden. Das Ergebnis der Arbeit ist eine Anleitung zur Durchführung eines solchen SLR. Dies war einer der Beweggründe, diese Vorgehensweise zu wählen. Diese teilt sich in 5 aufeinanderfolgende Teilschritte auf, siehe Abbildung 1. Für den generellen Aufbau und die Vorgehensweise wurden auch bereits vorhandene Reviews als Orientierung genutzt, etwa [10].

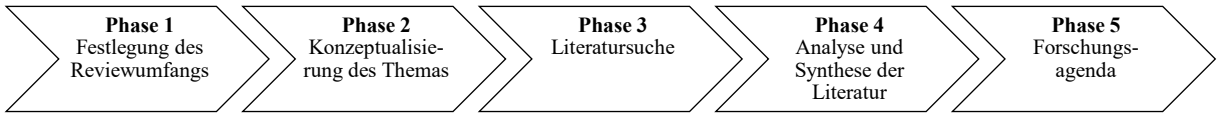

Abbildung 1: Phasen des SLR nach Vom Brocke et al. Quelle: in Anlehnung an [9]

Phase 1: In dieser Phase werden grundlegende Entscheidungen für die Art und Weise des SLR nach der Taxanomie von Cooper [11] festgelegt und in Fettschrift hervorgehoben, siehe Tabelle 1.

Merkmal	*Ausprägung*			
Fokus	**Forschungsergebnisse**	**Forschungsmethoden**	Theorien	Anwendungen
Ziel	**Integration**	Kritisieren	**Herausforderungen**	
Perspektive	**Neutrale Wiedergabe**		Standpunkt vertreten	
Abdeckung	**vollständig**	vollständig, selektive Zitation	repräsentativ	zentral bzw. grundlegend
Organisation	historisch	**konzeptionell**	**methodisch**	
Zielgruppe	**Fachleute**	**Wissenschaft**	**Praktiker**	Allgemeinheit

Tabelle 1: Taxanomie dieser Arbeit in Anlehnung an [11]

Phase 2: Hier wird eine Konzeptkarte erstellt. Diese enthält die Kernpunkte dieser Arbeit: *Security Awareness*, *Smartphone* und *User* (Nutzer). Zu allen Begriffen werden beispielsweise Synonyme und weitere verwandte Wörter gesucht und gruppiert.

Phase 3: Suche von Arbeiten und Prüfung auf Relevanz. Die Literatursuche lässt sich wiederum in 4 Subphasen einteilen:

- **Relevante Journale identifizieren**: Computers & Security, Springer Lecture Notes in Computer Science, …
- **Datenbanken suchen**, welche mindestens die oben genannten Journale beinhalten: ACM DL, IEEE DL und dblp.

- **Schlüsselwörter (Keywords) zum Durchsuchen** der Datenbanken nutzen. Diese stammen aus Phase 2.
- **Rückwärts- und Vorwärtssuche**

Phase 4: Nun werden die für relevant befundenen Arbeiten analysiert und synthetisiert. Jede Publikation wird (mehrfach) gelesen, um wichtige Informationen zu extrahieren. Neben dem Forschungsziel der Arbeit wird beispielsweise notiert, wie die Informationen erhoben wurden, wer die Probanden waren und welche Schlüsse gezogen wurden. Um ähnliche Arbeiten miteinander vergleichen zu können, müssen diese gruppiert werden. Dies geschieht mit einer Konzeptmatrix nach Webster und Watson [12].

Phase 5: Schlussendlich erfolgt die Erstellung einer Forschungsagenda. Sie gibt Hinweise darauf, welche Themengebiete weiter Forschung benötigen und auf welche Punkte (methodisch) geachtet werden sollte. Weiterhin werden die eingangs erwähnten Forschungsfragen beantwortet.

5. Durchführung der Literatursuche

Aus den Begriffen der Konzeptkarte (Phase 2) wird eine Suchanfrage formuliert. Sie ist iterativ entstanden, um eine Balance zwischen einer zu breiten respektive zu eingeschränkten Suche zu finden. Weiterhin wurde darauf geachtet, dass die Ergebnismenge für eine Person handhabbar bleibt. Eine Vielzahl der Publikationen der Informatik ist auf Englisch verfasst. Aus diesem Grund wird auch die Suchanfrage auf Englisch formuliert. Diese enthält Variationen der Kernpunkte, welche mit UND verknüpft werden. Etwaige Synonyme und verwandte Begriffe sind mit ODER verbunden:

(smartphone ODER android ODER ios ODER iphone ODER mobile phone) UND (user ODER participant ODER student ODER employee ODER individual) UND (security awareness ODER user awareness ODER personal information ODER information security)

Dieser Suchtext wird für die Suchfunktion jeder Datenbank angepasst. Die primäre Suche wurde am 15.06.2020 durchgeführt und führte zu 506 Ergebnissen. Durch die inhaltliche Relevanzprüfung, die Anwendung der Ein- und Ausschlusskriterien aus Tabelle 2 und die Anwendung weiterer Qualitätskriterien wurden insgesamt 46 Publikationen für die Folgeschritte identifiziert.

Merkmal	*Einschluss*	*Ausschluss*
Veröffentlichung	01.01.2011 bis 31.05.2020	Anderer Zeitraum
Publikationstyp	Vollständiges Paper	Extended Abstracts, Poster, …
Zugriff	Öffentlich zugänglich oder von der Hochschule lizenziert	Kostenpflichtige Artikel
Sprache	Englisch	Andere Sprachen
Fragestellung	Forschungsfragen und ähnliche	Andere Fragestellungen
Nutzereinbindung	Nutzer werden eingebunden	Keine Nutzereinbindung

Tabelle 2: Ein- und Ausschlusskriterien für das SLR (Auszug)

Einige der Ein- und Ausschlusskriterien werden nachfolgend begründet.

Veröffentlichung: Smartphones gibt es bereits seit der Einführung des Apple iPhone im Jahr 2007 [13], was aber nicht bedeutet, dass es seit diesem Zeitpunkt relevante Publikationen geben muss. Das behördliche und somit auch öffentliche Interesse hat im Jahr 2011 stark zugenommen, siehe [14]–[16]. Somit kann ab diesem Zeitpunkt von der Zunahme relevanter Forschungsbeiträge ausgegangen werden. Da diese Arbeit im Juni 2020 begonnen hat, werden nur zuvor veröffentlichte Publikationen betrachtet.

Nutzereinbindung: Im Titel dieser Arbeit werden die Nutzer von Smartphones explizit genannt. Aus diesem Grund sollten auch sämtliche Publikationen den Nutzer einbinden. Dies kann auf vielfältige Weise geschehen. Durch die Einbeziehung des Nutzers können die vorgestellten Verbesserungen oder Aussagen praktisch validiert werden.

Um ähnliche Arbeiten im nächsten Kapitel miteinander vergleichen zu können, müssen diese zuerst gruppiert werden. Parallel zur vorangegangenen Lektüre aller Publikationen wurde eine Konzeptmatrix nach Webster und Watson [12] erstellt. Die Konzepte werden in die beiden Kategorien *Ziel* und *Untersuchungsgegenstand* unterteilt. Als Ziel bzw. Intention einer Publikation konnten die Punkte *Unterstützung des Nutzers*, *Aufklärung und Schulung des Nutzers* sowie *Messen und Analysieren* identifiziert werden. Der Untersuchungsgegenstand bzw. Fokus kann auf den Bereichen *Berechtigungen von Apps, Risikobewertung von Apps*, *Privatsphäre*, *Security Awareness*, *App-Beschreibung* und/oder *Schutz des Smartphones* liegen.

6. Synthese der Arbeiten

Welche Forschungsfragen die Arbeiten bearbeitet haben und zu welchen Schlussfolgerungen sie gekommen sind, ist Teil dieses Kapitels. Zuerst werden die Arbeiten nochmals, basierend auf der Konzeptmatrix, eingeteilt. Dieser Schritt ist notwendig, da die Matrix sehr feingranular ist. Die erneute Einteilung basiert deshalb auf einer höheren Abstraktionsebene. So werden die übergeordneten Ziele bzw. adressierten Probleme identifiziert. Eine eineindeutige Zuordnung ist nicht immer möglich, da jede Arbeit auch (Teil-) Aspekte der übrigen Kategorien ansprechen kann. Die nachfolgenden Abschnitte sind nach dem Hauptziel der Forschungsarbeiten eingeteilt. Diese enthalten wiederum mehrere Unterpunkte. Im nachfolgenden Abschnitt geht es beispielsweise um Arbeiten, welche ihr Hauptaugenmerk auf dem Thema *Berechtigungen von Apps* haben. Innerhalb dieses Kontextes konnten weitere Gruppierungen vorgenommen werden. So wurde beispielsweise das *Verständnis der Nutzer* zum Thema Berechtigungen von Apps untersucht.

6.1. Berechtigungen von Apps

Für den Betrieb benötigen Apps verschiedene Berechtigungen, um auf gewisse Ressourcen zugreifen zu dürfen. Die Arbeiten in diesem Abschnitt befassen sich mit dem Themengebiet der Berechtigungen von Apps.

Verständnis der Nutzer: Wird dieses Berechtigungssystem von den Nutzern verstanden? In einigen Studien wird die Effektivität des Berechtigungsdialogs zur Installationszeit untersucht. Fast alle Android-Nutzer klicken den Dialog weg [17]. Viele Anwender

können nicht erklären, was sich hinter einer Berechtigung verbirgt ([17]–[19]) und welche Möglichkeiten eine Anwendung hierdurch hat.

Zu viele Berechtigungen: Furini et al. [20] nennen ein weiteres Indiz dafür, dass das Berechtigungssystem nicht verstanden wird. Die Apps der Probanden besitzen in vielen Fällen weit mehr Berechtigungen, als sie für die Ausführung ihrer Kernaufgabe benötigen. Ein Beispiel hierfür liefert Alani [21]. Fast 40 % seiner Befragten haben eine Taschenlampen-App installiert, welche insgesamt über 20 Berechtigungen einfordert. Hierunter auch solche, um den Inhalt des Speichers zu lesen. Derartige Berechtigungen werden laut Alani meist für Werbezwecke genutzt. Gratis-Apps haben im Vergleich zur Bezahlvariante meist mehr Berechtigungen, mit denen personenbezogene Daten ausgelesen werden können [22].

Hilfe bei Berechtigungen: Ein Teil der Arbeiten möchte dem Nutzer im Hinblick auf die von einer App geforderten Berechtigungen helfen. Diese Arbeiten betrachten fast alle Smartphones mit Android als Betriebssystem. Eine Vielzahl von ihnen (beispielsweise [23]–[25]) erfordert für die korrekte Funktionsweise Anpassungen am Betriebssystem selbst oder dem von Google betriebenen Play Store ([26], [27]). Die Entscheidung, welche Berechtigung entzogen respektive gewährt wird, kann vom Framework auf zwei unterschiedliche Arten getroffen werden. [23]–[25], [28] und [29] setzen zur Lösungsfindung auf **Crowdsourcing**, also die Intelligenz der Masse an Nutzern. Diese werden in verschiedene Privatsphäre-Profile eingeteilt. Somit sollen die Vorschläge für die Einstellungen von Nutzern mit ähnlichen Vorstellungen bezüglich der Privatsphäre kommen, um die Akzeptanz zu erhöhen. Agarwal und Hall haben in ihrer Arbeit untersucht, ob es einen Unterschied macht, ob ein initiales Set an Experten die Vorschläge macht oder diese gänzlich durch Crowdsourcing entstehen. Die Ergebnisse sind in beiden Fällen identisch. Ähnlich gute Vorschläge lassen sich auch **lokal** erzeugen, indem der Nutzer einige Fragen beantwortet. So werden sie bei [30] und [31] gefragt, für welche App-Kategorie (Art von App) sie welche Berechtigungen plausibel finden. [32] erstellen anhand von allgemeineren Fragen ein Privatsphäre-Profil. So wird den Nutzern aufgezeigt, welche Anwendungen ihren eigenen Vorstellungen widersprechen. Alle Apps unterbreiten dem Anwender daraufhin passende Vorschläge oder setzen diese teils automatisiert um.

6.2. Auswahl von Apps

Der Nutzer kann sein Smartphone um weitere Apps aus den App Stores für Android (Google Play Store) und iOS (Apple App Store) erweitern. Welche Ansätze es gibt, um dem Nutzer bei der Wahl einer App mit Fokus auf Sicherheit und Datenschutz zu helfen, ist Teil dieses Abschnittes. Die Notwendigkeit solcher Maßnahmen wird in Abschnitt 6.3 nochmals explizit aufgefasst. Neben der Begrenzung der Berechtigungen zur Laufzeit (vgl. vorherigen Abschnitt) setzen einige Arbeiten einen Schritt vorher an, nämlich bei der Auswahl einer App.

Berechtigungen und deren Auswirkungen visualisieren: Die Motivation dieser Arbeiten ist identisch: Die benötigten Berechtigungen werden entweder nicht verstanden oder ignoriert. Kelley et al. [27] rücken die benötigten Berechtigungen in den Fokus,

indem sie diese direkt auf der Detailseite einer App im Google Play Store anzeigen. Zudem wandeln sie die Liste an Berechtigungen, welche teils technisch klingen, in eine Checkliste um. So soll auch der Vergleich mehrerer Anwendungen vereinfacht werden. Harbach et al. [26] belassen die Anzeige dort wo sie ist (nach dem Klick auf Download), erweitern diese aber. Sie zeigen die Auswirkungen einer Berechtigung an. Beim Zugriff auf den Speicher wird beispielsweise ein Bild aus der Galerie des Nutzers gezeigt. Somit wird ihm verdeutlicht, welche Tragweite die einzelnen Berechtigungen haben. Benton et al. [33] versuchen Ähnliches. Auch sie passen den Dialog an, erweitern ihn aber mit mehr Text. Dies zeigt allerdings keinen statistisch signifikanten Effekt. Eine visuelle Darstellung wie von [34] ist effektiver.

Beschreibung anpassen: Wu et al. [35] passen die Beschreibung für vom Nutzer als kritisch empfundene Berechtigungen an seine Personalität an. Die so generierten Texte sind verständlicher und reicher an Informationen für den Nutzer. Zhang et al. [36] analysieren das Verhalten der App und geben diese (technischen) Informationen zusätzlich zur vom Entwickler bereitgestellten Beschreibung an den Nutzer weiter. Die Forscher geben an, dass durch ihren Text die tatsächliche Funktion der App beschrieben wird. Beide Arbeiten geben an, dass sie dabei helfen können, maliziöse Apps zu identifizieren.

Anleitung für die Wahl einer App: In [37] wird ein Flyer entworfen, welcher Hinweise darauf gibt, auf was man bei der Wahl im Google Play Store achten sollte. Er informiert die Leser weiterhin darüber, dass auch ihre Daten von Interesse sind und nicht nur diejenigen von bekannten Persönlichkeiten. Neben der Plausibilitätsprüfung der Berechtigungen sollte man zusätzlich auf weitere Apps des Entwicklers und das Datum der letzten Aktualisierung der App, zwecks Sicherheitsupdates, achten. Die Entscheidungen der Probanden werden dadurch nicht zwingend besser, aber fundierter.

Risiko einer App darstellen: Eine weitere Hilfestellung ist die Berechnung und Visualisierung des Risikos einer App. Es wird im Store bei der Auswahl von Apps angezeigt. Hiermit sollen ähnliche Anwendungen vergleichbar werden. Alle Darstellungsvarianten nutzen als Basis für die Berechnung die Anzahl kritischer Berechtigungen. [38] und [39] nutzen eine Skala zur Kommunikation des Risikos. [22] nutzt einen numerischen Wert. Zusätzlich wird bei einem Update im Google Play Store angezeigt, ob die App nun mehr oder weniger in die Privatsphäre eingreift. Ungeachtet der Art der Darstellung geben alle Autoren an, dass sich die Anwender für die bessere Anwendung entscheiden. Zumeist ist das diejenige mit weniger sensitiven/gefährlichen Berechtigungen bei gleicher oder ähnlicher Funktionalität.

6.3. Security Awareness der Nutzer

Die Erhebung der Daten erfolgt in fast allen Fällen subjektiv durch die Nutzung von Fragebögen oder der Durchführung von Interviews. Lediglich 2 Arbeiten ([40] und [41]) erfassen die benötigten Daten automatisiert und objektiv. Die Messung konzentriert sich in den meisten Fällen darauf, ob die Nutzer gängige Sicherheitsmechanismen kennen und auch anwenden. Einige in vielen Arbeiten abgefragte Punkte werden nachfolgend erläutert.

Zugriffsschutz: Ein simpler Schutz ist die Einrichtung einer Displaysperre, um den Zugriff auf das Smartphone und dessen Daten vor unbefugten Dritten zu schützen. Laut Breitinger et al. [42] nutzen 93 % der Generation Z/Y einen Lockscreen. Er merkt weiterhin an, dass solche Maßnahmen eher ergriffen werden als der Schutz der Privatsphäre. Gut 7 Jahre zuvor nutzten lediglich rund 60 % der Nutzer einen Lockscreen (siehe [43] und [44]).

Fehlendes Wissen über Schutzmechanismen: Ein oft genannter Punkt ist, dass den Nutzern das Wissen über die Existenz bestimmter Schutzmaßnahmen oder empfohlener Verhaltensweisen fehlt (beispielsweise [45]–[48]). Vecchiato und Martins [41] fordern von den Herstellern sicherere Standardeinstellungen. Denn laut ihnen haben selbst Personen, welche viele Einstellungen korrekt getätigt haben, weniger als die Hälfte aller Empfehlungen umgesetzt. Die Tendenz, dass IT-affine Personen die notwendigen Einstellungen eher kennen und anwenden, bestätigen auch Watson und Zheng [49]. Sie fordern, die Nutzer gezielt über solche Vorkehrungen zu informieren.

Benutzbarkeit muss bedacht werden: Dass eine Schutzmaßnahme nicht genutzt wird, kann verschiedene Gründe haben. Einige Befragte geben an, dass die Anpassungen im Alltag lästig sind [50]. Andere finden, dass diese eine schlechte Benutzbarkeit aufweisen [45], [51]. Sie geben an, dass sie solche Schutzmechanismen nutzen würden, wenn deren Benutzbarkeit steigt. In der Studie von Alsaleh et al. [46] halten einige Probanden die Nutzung solcher Mechanismen für Zeitverschwendung, da die Daten auf dem Gerät nicht relevant sind. Weiterhin wird angegeben, dass einem noch nie das Smartphone entwendet wurde und man aus diesem Grund beispielsweise auf einen Lockscreen verzichten kann.

Virenschutzprogramme: Ein im Zuge einiger Umfragen oft gefragter Punkt ist, ob die Nutzer auf ihrem Smartphone eine Antiviren-Software installiert haben. Dies ist bei wenigen Befragten der Fall. Die Forscher sind über dieses Ergebnis verwundert. Viele Teilnehmer geben an, dass sie wichtige oder gar sensible Daten auf dem Smartphone speichern, vgl. [42]. Weiterhin seien sie um die Sicherheit ihrer Daten besorgt, vgl. [51]. Die Nutzung von Antivirus-Apps ist dennoch eher gering (vgl. [42], [43], [52] und andere). Während Computer in der Regel mit einem Virenschutz ausgestattet sind, ist dies bei Smartphones eher die Ausnahme (beispielsweise [44]).

Sicherheitsempfinden von PC und Smartphone: Die Anwender schätzen Smartphones im Vergleich zum PC weniger sicher ein (beispielsweise [45]). Sie nennen auch mögliche Gründe hierfür. So seien PCs schon länger auf dem Markt und die Technik ausgereift und bekannt. Zudem seien vielen die Möglichkeiten von Smartphones auch mit Hinblick auf deren Rechenleistung nicht bekannt. Banking-Angelegenheiten werden laut Chin et al. bewusst am PC erledigt [53]. Sozialversicherungsnummer, Gesundheitsdaten und ähnlich sensible personenbezogene Daten werden ungern am Smartphone eingegeben, anders als am PC, so die Studie weiter. Gründe hierfür seien unter anderem die Angst vor einem Verlust des Gerätes.

Auch wenn die Nutzer mögliche Gefahren kennen, so handeln sie nicht immer entsprechend sicher. Einige Studierende aus der Studie von Jones et al. nutzen Online-Banking, haben aber nicht zwingend einen Lockscreen gesetzt. [54]

Auswahl von Apps: In Bezug auf die Security Awareness fragen viele Studien ihre Teilnehmer, nach welchen Kriterien sie sich für oder gegen eine App entscheiden. Für viele stehen die Punkte Sicherheit und Privatsphäre nicht im Mittelpunkt [44]. Vielmehr spielt die Empfehlung von Bekannten ([27]) oder die Bewertungen und Beliebtheit sowie Werbeanzeigen ([27], [53]) einer App eine primäre Rolle bei der Wahl. Viele nehmen fälschlicherweise an, dass es in den offiziellen App-Stores keine bösartigen Apps gibt (beispielsweise [18], [51]). Die Dialoge, welche die Berechtigungen einer App auflisten (seit Android Marshmallow gibt es diese Dialoge nicht mehr), werden von den meisten Nutzern ignoriert und helfen ihnen somit nicht bei der Entscheidung für oder gegen eine App [17], [18], [43]. Liccardi et al. [22] geben an, dass die reine Anzahl an Berechtigungen dazu führen kann, dass eine App nicht genutzt wird. Es sind allerdings nicht alle Berechtigungen eine Gefahr für die Sicherheit oder Privatsphäre. Selbst Apps mit legitimen Gründen für die Nutzung bestimmter Ressourcen werden nicht installiert.

Einflüsse und Zusammenhänge: Laut Bitton et al. [40] lassen demografische Eigenschaften keinen Rückschluss auf die Security Awareness zu. Sie haben aber einen Zusammenhang zwischen der Installation eines Virenscanners und der Security Awareness identifiziert. Sprache und Kultur haben keinen Einfluss [44]. Auch Bagga et al. [51] konnten keine signifikanten Unterschiede zwischen diversen Altersgruppen feststellen, ähnlich auch Jones et al. [54]. Wobei Jones et al. einräumen, dass sie nur eine Altersgruppe (17 bis 24 Jahre) untersucht haben. Diese Aussagen werden aber nicht von allen Autoren geteilt. So verhalten sich jüngere Menschen laut Alsaleh et al. [46] und Parker et al. [55] tendenziell sicherer. Weiterhin widersprechen Parker et al. der These, dass Sprache, Ethnie und Alter keinen Einfluss haben. Sie geben allerdings zu bedenken, dass deren Probanden meist junge Nutzer von Android-Smartphones sind und das demografische Profil somit nicht ausgewogen sei. Personen mit mittlerem Interesse an Cybersicherheit weisen sichereres Verhalten auf [42]. So erstellen diese beispielsweise häufiger Backups, was im Schadensfall hilfreich sein kann. Einige Studien (beispielsweise [46], [51], [55]) geben an, dass Männer risikoreicher handeln und Frauen nicht alle (tief in den Einstellungen versteckten) Sicherheitsmechanismen aktivieren. Die einzige Studie mit Kindern [56] zeigt ein umgekehrtes Bild. Hier sind die weiblichen Probanden sorgloser im Umgang mit ihrem Smartphone.

6.4. Aufklärung und Schulung der Nutzer

Arbeiten aus dieser Kategorie haben zum Ziel, den Nutzer aufzuklären.

Häufigkeit von Zugriffen: Schlegel et al. [34] visualisieren dem Nutzer am Beispiel seines Standortes, wie oft Anwendungen auf diese Ressource zugreifen. Trotz legitimer Gründe kann eine gehäufte Abfrage die Privatsphäre der Anwender verletzen. Durch die Visualisierung der Häufigkeit kann der Nutzer entscheiden, ob er diese Information weiterhin teilen möchte.

Auswirkungen von Berechtigungen: Meist bleibt es dem Anwender verborgen, welche Informationen übertragen werden. Eling et al. [19] zeigen mit ihrer App auf, welche Daten durch die gewährten Berechtigungen gelesen werden können. In ihrer Arbeit zeigt sich erneut, dass die Nutzer die Tragweite der Berechtigungen nicht kennen oder diese gar nicht erst gelesen haben. Zeigt die App an, auf welche Informationen sie zugreifen möchte, lehnen gut 60 % diese Anfrage ab. Dies kommt laut den Autoren einer Ablehnung der durch die Installation gewährten Berechtigung gleich. Dies bedeutet, dass der Nutzer nicht (mehr) mit seiner Entscheidung einverstanden ist oder schlicht nicht wusste, dass diese Informationen gelesen und versendet werden können. Furini et al. [20] möchten den Nutzer ebenfalls über Berechtigungen aufklären. Auch hier zeigte sich, dass die Vorstellungen der Nutzer von den Möglichkeiten der Berechtigungen abweichen. Zusätzlich analysieren sie die installierten Apps und kommen zu dem Schluss, dass viele Berechtigungen nicht zur primären Funktion der App benötigt werden. Sie fordern, den Nutzer weiter aufzuklären, damit er seine Privatsphäre schützen kann.

Dedizierte Lern-Apps: Bahrini et al. [57] klären den Nutzer spielerisch über Einstellungen zum Schutz seiner Privatsphäre auf. Die zumeist jungen (25 Jahre) Probanden haben durch die App weniger Neues gelernt, da Android in den letzten Jahren viel zur benutzbaren Sicherheit beigetragen hat, so die Autoren. Ähnliches machen Gerber et al. [58]. Sie wollen den Nutzer allerdings dazu animieren, stetig die App zum Lernen zu benutzen. Dies wollen sie mit einem Belohnungssystem erreichen.

Nudging: Almuhimedi et al. [59] weisen den Nutzer auf den in Android 4.3 bis 4.4.2 integrierten (experimentellen) Berechtigungsmanager hin. Durch Nudging bekommen sie regelmäßig Hinweise, wie oft eine App in der letzten Zeit welche Ressource genutzt hat. Der reine Hinweis auf den Berechtigungsmanager hat viele Nutzer dazu gebracht, diesen zu nutzen. Ähnlich verfahren Liu et al. [30]. Auch sie zeigen dem Nutzer regelmäßig an, welche App welche Zugriffe fordert und wollen ihn so stetig dazu animieren, die erteilten Berechtigungen zu prüfen.

Nutzer zu sichererem Verhalten animieren: Wie man die Nutzer dazu bewegen kann, gängige Sicherheitsmechanismen einzusetzen wurde auch untersucht. Van Bruggen et al. [60] wollen durch gezielte Nachrichten zur Nutzung einer Displaysperre animieren. Die verschiedenen Arten von Nachrichten (abschreckend, moralische oder eine Belohnung) haben keinen wirklichen Erfolg erzielt. Die Autoren geben an, dass der Aufwand nicht im Verhältnis zum Ergebnis steht. Albayram et al. [50] zeigen den Nutzern ohne Lockscreen ein Video, welches die möglichen Folgen eines ungeschützten Smartphones zeigen. Die Aufklärung über mögliche Risiken hat gut die Hälfte der Testgruppe zum Umdenken bewegt.

7. Diskussion der Arbeiten

Aus den Limitierungen und Forschungslücken aller Publikationen können Erkenntnisse für die zukünftige Ausrichtung und Fokussierung der Forschung gewonnen werden. Weiterhin werden jene Arbeiten oder Konzepte identifiziert, welche einen praktischen Einfluss hatten.

7.1. Limitierungen und Forschungslücken der Arbeiten

Ziel dieses Abschnittes ist es, die über alle Arbeiten hinweg aufgefallenen Limitierungen (ob explizit genannt oder durch die Analyse erkannt) und Forschungslücken aufzuzeigen. Wären einige dieser Einschränkungen nicht vorhanden, würde sich das mutmaßlich positiv auf die Forschung auf dem Themengebiet auswirken.

Verlass auf die korrekte Aussage von Befragten: Dass es einen Unterschied zwischen dem genannten Verhalten (subjektiv) der Probanden und deren tatsächlichem Handeln (objektiv) gibt, haben Bitton et al. [40] in ihrer Arbeit herausgefunden. Sie haben zuerst das geplante Handeln erfragt und anschließend in einem mehrwöchigen Experiment am Gerät des Nutzers das tatsächliche Handeln automatisiert erfasst. Sie kommen zu dem Schluss, dass die objektiven Werte präziser als die Selbsteinschätzung sind. Als Grund nennen sie, dass die Angaben auf Fragebögen entweder falsch sind oder die Frage falsch verstanden wurde. Dieser Punkt wird auch von [54] als mögliche Limitierung genannt.

Vernachlässigung von iOS: Von den analysierten Arbeiten hat nur [25] iOS-Nutzer betrachtet. Alle anderen Veröffentlichungen beschäftigen sich mit Android-Nutzern. Dies wird zumeist damit begründet, dass die Mehrheit Android nutze (beispielsweise [39], [58] und [23]). Bei allgemeineren Befragungen waren dennoch iOS-Nutzer vertreten. Die Vernachlässigung bezieht sich daher zumeist auf Arbeiten, welche eine praktische Implementierung vornehmen.

Kurze Studienzeit: Weiterhin fällt der Untersuchungszeitraum vieler Arbeiten kurz aus. Das haben beispielsweise [26] in ihrer Arbeit genannt und verweisen darauf, dass hiermit nur belegt werden kann, dass der Nutzer das vermittelte Wissen im Kurzzeitgedächtnis gespeichert hat. Ob man sein Verhalten langfristig ändern konnte, sei ungewiss. Es kann auch nicht ausgeschlossen werden, dass die Probanden sich durch die Forschungssituation anders verhalten als sonst (beispielsweise [38]). Die kurze Zeit zum Sammeln von Daten nennen auch [30] als mögliche Einschränkung.

Nicht repräsentative Wahl der Probanden: Viele der untersuchten Arbeiten, welche sich nicht explizit mit jungen Studierenden beschäftigen wollen, taten dies durch die Auswahl der Probanden dennoch (beispielsweise [58]). Einige dieser Arbeiten nennen die Probandenwahl ausdrücklich als limitierenden Faktor. Anders sieht es bei Veröffentlichung von [45] und anderen aus, welche gezielt junge Menschen im Fokus haben. Es sollte nicht nur im universitären Umfeld nach Teilnehmern gesucht werden, denn diese seien laut [39] zumeist höher gebildet. Aus diesem Grund sind die Aussagen meist nicht generalisierbar. Nur wenige Arbeiten treffen die Aussage, dass die Wahl der Probanden in etwa der Nutzerschicht von Android entspricht, etwa [53].

Beschränkung auf technisch versierte Nutzer: Ein ähnliches Problem ergibt sich dadurch, dass die Experimente nur mit einer eingeschränkten Gerätebasis stattfinden können. So müssen beispielsweise für einige Arbeiten die Geräte gerootet sein [25] oder eine spezielle Version des Betriebssystems genutzt werden [59]. Ein regulärer Nutzer wird somit ausgeschlossen, da dies in der Regel nur ein meist auf Sicherheit spezialisierter Nutzerkreis tut und diese meist mehr Wissen in Bezug auf Sicherheit vorweisen können [30].

Fehlende Alltagstauglichkeit: Viele Arbeiten machten sinnvolle Vorschläge, wie man das Sicherheitsbewusstsein der Nutzer verbessern oder ihnen helfen kann. Es sind einige Anwendungen, wie *Protect my privacy* [25], entstanden und erfolgreich mit echten Nutzern erprobt worden. Viele dieser Ideen haben sich aber mutmaßlich nicht durchgesetzt. Das mag am oben genannten Problem liegen, dass man für die Installation selbst Expertenwissen benötigt. Neben den Änderungen am Betriebssystem werden oft Anpassungen an Komponenten gefordert, auf die man keinen direkten Einfluss hat, etwa die Oberfläche des Google Play Store.

7.2. Einflussreiche Forschungsbeiträge

Die Vorschläge, Konzepte und Kritiken einiger Arbeiten haben seit ihrer Veröffentlichung einen praktischen Einfluss gehabt. Ob die Änderungen beispielsweise am Betriebssystem tatsächlich auf diese Arbeiten zurückzuführen sind, ist ungewiss. Dennoch dürfte es nicht abwegig sein, dass auch die Entwickler von Google (Android) und Apple (iOS) diese Publikationen gelesen haben und dadurch zu einigen Anpassungen motiviert wurden.

Verbessertes Berechtigungskonzept bei Android: Felt et al. [17] unterbreiten in ihrer Arbeit von 2012 den Vorschlag, dass Berechtigungsabfragen zur Laufzeit besser wahrgenommen werden könnten. Eling et al. [19] merken ebenfalls in ihrer Arbeit an, dass (feingranulare) Berechtigungsabfragen zur Laufzeit für den Nutzer nützlicher sind, als jene zum Installationszeitpunkt. Mit Android 6 (Marshmallow) hält diese Funktion erstmals offiziell Einzug in das Betriebssystem[2]. Somit muss der Nutzer nicht mehr, wie in früheren Versionen üblich, bereits mit der Installation allen Berechtigungen zustimmen. Weiterhin ist es seit dieser Android-Version möglich, erteilte Berechtigungen auch wieder zu entziehen. Dies haben beispielsweise die Arbeiten im Abschnitt 6.1 (Hilfe bei Berechtigungen) bereits ermöglicht.

Prüfung von Anwendungen durch App-Stores: In einigen Arbeiten gaben die Nutzer an, dass sie annehmen, dass es in den offiziellen App-Stores von Apple und Google keine schädlichen Apps gibt. Die Autoren dieser Arbeiten geben an, dass es einen solchen Mechanismus nicht gibt (beispielsweise [18], [51]). Google hat seitdem viel getan, um schädliche Anwendungen im Google Play Store zu identifizieren [61]–[63]. Diese Maßnahmen gehen alle in die richtige Richtung. Auch Apple gibt an, dass diverse Sicherheitsmechanismen dafür sorgen, dass Apps frei von bekannten Schadprogrammen sind [64]. Allerdings kann die Zuverlässigkeit dieser Mechanismen angezweifelt werden, da es immer wieder Beiträge über den Fund von Schadsoftware gibt. Laut einem Blogartikel von Avast aus dem Oktober 2020 wurden 21 Malware-Apps (Adware) im Google Play Store gefunden [65]. Die Sicherheitsforscher von Wandera haben im Oktober 2019 17 maliziöse Apps im App Store von Apple gefunden [66].

[2] https://www.android.com/intl/de_de/versions/marshmallow-6-0/ (besucht am 27.08.2020)

8. Fazit und Forschungsagenda

In diesem letzten Kapitel wird diese Arbeit nochmals reflektiert. Zuerst wird ein Fazit gezogen. Anschließend werden die Forschungsfragen beantwortet und basierend auf den vorherigen Kapiteln eine Empfehlung für die zukünftige Forschung gegeben.

8.1. Fazit

Diese Arbeit hat mithilfe der Durchführung eines SLR und der Analyse von 46 Arbeiten den Stand der Forschung auf dem Themengebiet der Security Awareness von Smartphone-Nutzern aufgezeigt. Es wurden die verschiedenen Forschungsschwerpunkte beleuchtet. Einige Schwächen zeigten sich bei der Wahl der Probanden, der Art der Datenerhebung und der Vernachlässigung von iOS-Nutzern. Meist lag der Fokus der Publikationen auf den Themengebieten Berechtigungen von Apps, Auswahl von Apps, Security Awareness der Nutzer und Aufklärung und Schulung der Anwender. Einen neuralgischen Punkt stellt das Berechtigungssystem von Android dar. Den Nutzern war es meist nicht bewusst, auf welche Daten eine Anwendung durch die erteilten Berechtigungen zugreifen darf. Wie im vorherigen Abschnitt erwähnt, wurden einige Vorschläge aus den Arbeiten in die Betriebssysteme integriert. Weiter ist aufgefallen, dass den Nutzern das Wissen für einen sicheren Umgang mit ihrem Smartphone fehlt oder sie ihre Daten nicht als schützenswert ansehen. In der Synthese hat sich ergeben, dass hier bessere und sicherere Standardwerte bei einigen Einstellungen hilfreich sein können. Hiervon profitieren alle Nutzer.

8.2. Beantwortung der Forschungsfragen

Auf die Fragen wurde in den vorangegangenen Kapiteln implizit eingegangen. Diese Erkenntnisse werden nun explizit genannt.

Welche Ansätze gibt es, um die Security Awareness zu erhöhen bzw. zu verbessern? Im Bereich Berechtigungen versuchen viele Arbeiten den Nutzer zu entlasten, indem sie Aufgaben automatisieren. Einen anderen Ansatz bilden Apps, welche den Nutzer spielerisch an das Thema Sicherheit heranführen. Meist genügt es auch, mögliche Risiken aufzuzeigen und Lösungsmöglichkeiten zu nennen, wie man diese effektiv verhindert.

Mit welchen Methodiken wurde die Security Awareness gemessen? Zumeist wurde auf Fragebögen oder ähnliche Methoden gesetzt. Hierbei müssen sich die Probanden selbst einschätzen. Einen allgemeinen Standard oder gar eine Skala gibt es mutmaßlich nicht. Das Messen der Security Awareness durch die Auswertung des tatsächlichen Verhaltens über einen längeren Zeitraum scheint die sinnvollste Variante zu sein (vgl. [40]).

Wie wird die Gültigkeit der Aussagen belegt? Welche typischen Limitierungen gibt es? Meist werden die getroffenen Aussagen, etwa zur Wirksamkeit einer App, mit einem Nutzertest belegt. Vielfach werden auch Fragebögen benutzt oder Interviews durchgeführt. Typische Limitierungen bilden meist die Anzahl und die Auswahl der Probanden oder die Korrektheit der getätigten Aussagen und Angaben. Weiterhin bilden viele Studien nur eine (kurze) Momentaufnahme ab. Länger angesetzte Studien bilden die Ausnahme.

Wie hat sich die Security Awareness über die Jahre verändert? Wie bereits bei der zweiten Forschungsfrage angesprochen gibt es keine einheitliche Skala. Somit ist die Beantwortung dieser Frage nicht trivial. An einigen Eckpunkten aus Abschnitt 6.3 lässt sich jedoch eine Tendenz ablesen. Ein in vielen Studien abgefragter Aspekt ist, ob eine Displaysperre gesetzt ist. Dieser ist über die Jahre von rund 60 % auf 93 % (Generation Z/Y) gestiegen. Hier ist ein positiver Trend zu erkennen. Bahrini et al. [57] ziehen in ihrer Arbeit das Fazit, dass die Betriebssysteme vermehrt den Fokus auf benutzbare Sicherheit legen. Damit begründen sie, dass ihre Probanden durch ihre App nicht viel Neues gelernt haben, da sie bereits über dieses Wissen verfügen.

8.3. Forschungsagenda

Aus den vorherigen Kapiteln lassen sich einige Empfehlungen für zukünftige Arbeiten auf diesem Gebiet ableiten. So sollten bei der Durchführung von Studien möglichst viele Daten automatisiert erhoben werden, um deren Aussagekraft zu erhöhen. Eine manuelle bzw. subjektive Erfassung durch die Nutzer kann zusätzlich erfolgen, um deren geplantes mit dem tatsächlichen Verhalten zu vergleichen. Weiterhin sollte die Auswahl von Probanden mehr an die tatsächlichen demografischen Rahmenbedingungen der Nutzer von Smartphones angepasst werden. Hierbei kann es zusätzlich von Interesse sein, verschiedene Nationalitäten zu betrachten, um etwaige regionale Unterschiede aufzudecken. Einige Arbeiten mussten aus der Betrachtung ausgeschlossen werden, da diese den Nutzer nicht involvierten. So haben einige Arbeiten plausible Konzepte und Ansätze geliefert, diese aber nicht durch die Nutzer verifiziert. Allgemein sollten bei Entwicklungen für eine bestimmte Zielgruppe immer Tests mit dieser durchgeführt werden, um zu überprüfen, ob diese auch alltagstauglich sind. Für die Feststellung der Security Awareness von Nutzern sollte ein allgemeingültiges Rahmenwerk erarbeitet werden. Dieses sollte so gestaltet werden, dass die Ergebnisse miteinander vergleichbar sind. Hierdurch kann die Veränderung der Security Awareness über die Jahre oder auch der Vergleich von verschiedenen Gruppen oder Nationalitäten einfacher erfolgen. Hierzu könnte das von Bitton et al. [40] vorgeschlagene automatisierte Framework zur Berechnung des Information Security Awareness Scores als Basis dienen.

Literaturhinweise

[1] „Newzoo's Global Mobile Market Report: Insights into the World's 3.2 Billion Smartphone Users, the Devices They Use & the Mobile Games They Play", *Newzoo*. https://newzoo.com/insights/articles/newzoos-global-mobile-market-report-insights-into-the-worlds-3-2-billion-smartphone-users-the-devices-they-use-the-mobile-games-they-play/ (zugegriffen Okt. 16, 2020).

[2] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kompendium". Zugegriffen: Okt. 16, 2020. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf?__blob=publicationFile&v=6.

[3] Bundesamt für Sicherheit in der Informationstechnik, „Die Lage der IT-Sicherheit in Deutschland 2014". Dez. 15, 2014, Zugegriffen: Okt. 21, 2020. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile&v=2.

[4] M. Wilson und J. Hash, „Building an Information Technology Security Awareness and Training Program", National Institute of Standards and Technology, NIST Special Publication (SP) 800-50, Okt. 2003. doi: https://doi.org/10.6028/NIST.SP.800-50.

[5] M. Helisch, „Definition von Awareness, Notwendigkeit und Sicherheitskultur", in *Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung*, M. Helisch und D. Pokoyski, Hrsg. Wiesbaden: Vieweg+Teubner, 2009, S. 9–28.

[6] Fredrik Eriksson, „Proposal for a definition of smartphone", *International Telecommunication Union (ITU)*, Aug. 28, 2017. https://www.itu.int/en/ITU-D/Statistics/Documents/events/egh2017/EGH%202017%20background%20document%203%20-%20Definition%20of%20smartphone.pdf (zugegriffen Okt. 21, 2020).

[7] „Duden | Smartphone | Rechtschreibung, Bedeutung, Definition, Herkunft". https://www.duden.de/rechtschreibung/Smartphone (zugegriffen Okt. 21, 2020).

[8] P. D. I. Sjurts, „Definition: Smartphone", Feb. 19, 2018. https://wirtschaftslexikon.gabler.de/definition/smartphone-52675/version-275793 (zugegriffen Okt. 21, 2020).

[9] J. Brocke *u. a.*, „RECONSTRUCTING THE GIANT: ON THE IMPORTANCE OF RIGOUR IN DOCUMENTING THE LITERATURE SEARCH PROCESS", *ECIS 2009 Proceedings*, Jan. 2009, [Online]. Verfügbar unter: https://aisel.aisnet.org/ecis2009/161.

[10] M. Tahaei und K. Vaniea, „A Survey on Developer-Centred Security", in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, Juni 2019, S. 129–138, doi: 10.1109/EuroSPW.2019.00021.

[11] H. M. Cooper, „Organizing knowledge syntheses: A taxonomy of literature reviews", *Knowledge in Society*, Bd. 1, Nr. 1, S. 104–126, März 1988, doi: 10.1007/BF03177550.

[12] J. Webster und R. T. Watson, „Analyzing the Past to Prepare for the Future: Writing a Literature Review", *MIS Quarterly*, Bd. 26, Nr. 2, S. xiii–xxiii, 2002.

[13] „Apple erfindet mit dem iPhone das Mobiltelefon neu", *Apple Newsroom*. https://www.apple.com/de/newsroom/2007/01/09Apple-Reinvents-the-Phone-with-iPhone/ (zugegriffen Nov. 02, 2020).

[14] Bundesamt für Sicherheit in der Informationstechnik, „Die Lage der IT-Sicherheit in Deutschland 2011“. Mai 31, 2011, Zugegriffen: Okt. 16, 2020. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile&v=3.

[15] Bundesamt für Sicherheit in der Informationstechnik, „Wie sicher sind Smartphones?“, Feb. 04, 2011. https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/aeltere_Artikel/Smartphones_24022011.html (zugegriffen Mai 18, 2020).

[16] „Smartphones: Information security risks, opportunities and recommendations for users“. https://www.enisa.europa.eu/publications/smartphones-information-security-risks-opportunities-and-recommendations-for-users (zugegriffen Okt. 15, 2020).

[17] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, und D. Wagner, „Android permissions: user attention, comprehension, and behavior“, in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, Washington, D.C., Juli 2012, S. 1–14, doi: 10.1145/2335356.2335360.

[18] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, und D. Wetherall, „A conundrum of permissions: installing applications on an android smartphone“, in *Proceedings of the 16th international conference on Financial Cryptography and Data Security*, Bonaire, März 2012, S. 68–79, doi: 10.1007/978-3-642-34638-5_6.

[19] N. Eling, S. Rasthofer, M. Kolhagen, E. Bodden, und P. Buxmann, „Investigating Users' Reaction to Fine-Grained Data Requests: A Market Experiment“, in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Jan. 2016, S. 3666–3675, doi: 10.1109/HICSS.2016.458.

[20] M. Furini, S. Mirri, M. Montangero, und C. Prandi, „Privacy perception and user behavior in the mobile ecosystem“, in *Proceedings of the 5th EAI International Conference on Smart Objects and Technologies for Social Good*, Valencia, Spain, Sep. 2019, S. 177–182, doi: 10.1145/3342428.3342690.

[21] M. Alani, „Android Users Privacy Awareness Survey“, *International Journal of Interactive Mobile Technologies (iJIM)*, Bd. 11, S. 130, Apr. 2017, doi: 10.3991/ijim.v11i3.6605.

[22] I. Liccardi, J. Pato, D. J. Weitzner, H. Abelson, und D. De Roure, „No technical understanding required: helping users make informed choices about access to their personal data“, in *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, London, United Kingdom, Dez. 2014, S. 140–150, doi: 10.4108/icst.mobiquitous.2014.258066.

[23] R. Liu, J. Cao, L. Yang, und K. Zhang, „PriWe: Recommendation for Privacy Settings of Mobile Apps Based on Crowdsourced Users' Expectations“, in *2015 IEEE International Conference on Mobile Services*, Juni 2015, S. 150–157, doi: 10.1109/MobServ.2015.30.

[24] B. Rashidi, C. Fung, A. Nguyen, T. Vu, und E. Bertino, „Android User Privacy Preserving Through Crowdsourcing“, *IEEE Transactions on Information Forensics and Security*, Bd. 13, Nr. 3, S. 773–787, März 2018, doi: 10.1109/TIFS.2017.2767019.

[25] Y. Agarwal und M. Hall, „ProtectMyPrivacy: detecting and mitigating privacy leaks on iOS devices using crowdsourcing“, in *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*, Taipei, Taiwan, Juni 2013, S. 97–110, doi: 10.1145/2462456.2464460.

[26] M. Harbach, M. Hettig, S. Weber, und M. Smith, „Using personal examples to improve risk communication for security & privacy decisions“, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Toronto, Ontario, Canada, Apr. 2014, S. 2647–2656, doi: 10.1145/2556288.2556978.

[27] P. G. Kelley, L. F. Cranor, und N. Sadeh, „Privacy as part of the app decision-making process“, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Paris, France, Apr. 2013, S. 3393–3402, doi: 10.1145/2470654.2466466.

[28] Q. Ismail, T. Ahmed, A. Kapadia, und M. K. Reiter, „Crowdsourced Exploration of Security Configurations“, in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, Seoul, Republic of Korea, Apr. 2015, S. 467–476, doi: 10.1145/2702123.2702370.

[29] J. Lin, B. Liu, N. Sadeh, und J. I. Hong, „Modeling users' mobile app privacy preferences: restoring usability in a sea of permission settings“, in *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, Menlo Park, CA, Juli 2014, S. 199–212, Zugegriffen: Juli 08, 2020. [Online].

[30] B. Liu *u. a.*, „Follow my recommendations: a personalized privacy assistant for mobile app permissions“, in *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security*, Denver, CO, USA, Juni 2016, S. 27–41, Zugegriffen: Juli 08, 2020. [Online].

[31] Y. Jing, G.-J. Ahn, Z. Zhao, und H. Hu, „Towards Automated Risk Assessment and Mitigation of Mobile Applications“, *IEEE Transactions on Dependable and Secure Computing*, Bd. 12, Nr. 5, S. 571–584, Sep. 2015, doi: 10.1109/TDSC.2014.2366457.

[32] C. B. Jackson und Y. Wang, „Addressing The Privacy Paradox through Personalized Privacy Notifications“, *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, Bd. 2, Nr. 2, S. 68:1-68:25, Juli 2018, doi: 10.1145/3214271.

[33] K. Benton, L. J. Camp, und V. Garg, „Studying the effectiveness of android application permissions requests“, in *2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, März 2013, S. 291–296, doi: 10.1109/PerComW.2013.6529497.

[34] R. Schlegel, A. Kapadia, und A. J. Lee, „Eyeing your exposure: quantifying and controlling information sharing for improved privacy“, in *Proceedings of the Seventh Symposium on Usable Privacy and Security*, Pittsburgh, Pennsylvania, Juli 2011, S. 1–14, doi: 10.1145/2078827.2078846.

[35] T. Wu *u. a.*, „Catering to Your Concerns: Automatic Generation of Personalised Security-Centric Descriptions for Android Apps“, *ACM Trans. Cyber-Phys. Syst.*, Bd. 3, Nr. 4, S. 36:1-36:21, Sep. 2019, doi: 10.1145/3317699.

[36] M. Zhang, Y. Duan, Q. Feng, und H. Yin, „Towards Automatic Generation of Security-Centric Descriptions for Android Apps“, in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Denver, Colorado, USA, Okt. 2015, S. 518–529, doi: 10.1145/2810103.2813669.

[37] O. Kulyk, P. Gerber, K. Marky, C. Beckmann, und M. Volkamer, „Does This App Respect My Privacy? Design and Evaluation of Information Materials Supporting Privacy-Related Decisions of Smartphone Users“, gehalten auf der Workshop on Usable Security, San Diego, CA, 2019, doi: 10.14722/usec.2019.23029.

[38] C. S. Gates, J. Chen, N. Li, und R. W. Proctor, „Effective Risk Communication for Android Apps“, *IEEE Transactions on Dependable and Secure Computing*, Bd. 11, Nr. 3, S. 252–265, Mai 2014, doi: 10.1109/TDSC.2013.58.

[39] J. Kang, H. Kim, Y. G. Cheong, und J. H. Huh, „Visualizing Privacy Risks of Mobile Applications through a Privacy Meter“, in *Information Security Practice and Experience*, Cham, 2015, S. 548–558, doi: 10.1007/978-3-319-17533-1_37.

[40] R. Bitton, K. Boymgold, R. Puzis, und A. Shabtai, „Evaluating the Information Security Awareness of Smartphone Users“, in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Honolulu, HI, USA, Apr. 2020, S. 1–13, doi: 10.1145/3313831.3376385.

[41] D. Vecchiato und E. Martins, „Experience report: A field analysis of user-defined security configurations of Android devices“, in *2015 IEEE 26th International Symposium on Software Reliability Engineering (ISSRE)*, Nov. 2015, S. 314–323, doi: 10.1109/ISSRE.2015.7381824.

[42] F. Breitinger, R. Tully-Doyle, und C. Hassenfeldt, „A survey on smartphone user’s security choices, awareness and education“, *Comput. Secur.*, Bd. 88, 2020, doi: 10.1016/j.cose.2019.101647.

[43] A. Mylonas, A. Kastania, und D. Gritzalis, „Delegate the smartphone user? Security awareness in smartphone platforms“, *Computers & Security*, Bd. 34, S. 47–66, Mai 2013, doi: 10.1016/j.cose.2012.11.004.

[44] J. Ophoff und M. Robinson, „Exploring end-user smartphone security awareness within a South African context“, in *2014 Information Security for South Africa*, Aug. 2014, S. 1–7, doi: 10.1109/ISSA.2014.6950500.

[45] V. Gkioulos, G. Wangen, S. K. Katsikas, G. Kavallieratos, und P. Kotzanikolaou, „Security Awareness of the Digital Natives“, *Information*, Bd. 8, Nr. 2, Art. Nr. 2, Juni 2017, doi: 10.3390/info8020042.

[46] M. Alsaleh, N. Alomar, und A. Alarifi, „Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods“, *PLOS ONE*, Bd. 12, Nr. 3, S. e0173284, März 2017, doi: 10.1371/journal.pone.0173284.

[47] R. C. Jisha, R. Krishnan, und V. Vikraman, „Mobile Applications Recommendation Based on User Ratings and Permissions“, in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Sep. 2018, S. 1000–1005, doi: 10.1109/ICACCI.2018.8554691.

[48] I. Androulidakis und G. Kandus, „Mobile Phone Security Awareness and Practices of Students in Budapest“, in *Proceedings of the 6th International Conference on Digital Telecommunications*, 2011, S. 17--22, Zugegriffen: Juli 08, 2020. [Online].

[49] B. Watson und J. Zheng, „On the User Awareness of Mobile Security Recommendations“, in *Proceedings of the SouthEast Conference*, Kennesaw, GA, USA, Apr. 2017, S. 120–127, doi: 10.1145/3077286.3077563.

[50] Y. Albayram, M. M. H. Khan, T. Jensen, und N. Nguyen, „“...better to use a lock screen than to worry about saving a few seconds of time”: Effect of Fear Appeal in the Context of Smartphone Locking Behavior“, 2017, S. 49–63, Zugegriffen: Juli 16, 2020. [Online]. Verfügbar unter: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/albayram.

[51] T. Bagga, J. Sodhi, B. Shukla, und M. A. Qazi, „SMARTPHONE SECURITY BEHAVIOUR OF THE INDIAN SMARTPHONE USER“, *MAN IN INDIA*, S. 13, 2017.

[52] I. Androulidakis und G. Kandus, „Differences in users' state of awareness and practices regarding mobile phones security among EU countries", in *Proceedings of the 5th WSEAS international conference on Communications and information technology*, Juli 2011, S. 294–300.

[53] E. Chin, A. P. Felt, V. Sekar, und D. Wagner, „Measuring user confidence in smartphone security and privacy", in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, Washington, D.C., Juli 2012, S. 1–16, doi: 10.1145/2335356.2335358.

[54] B. H. Jones, A. G. Chin, und P. Aiken, „Risky business: Students and smartphones", *TECHTRENDS TECH TRENDS*, Bd. 58, Nr. 6, S. 73–83, Nov. 2014, doi: 10.1007/s11528-014-0806-x.

[55] F. Parker, J. Ophoff, J.-P. V. Belle, und R. Karia, „Security awareness and adoption of security controls by smartphone users", in *2015 Second International Conference on Information Security and Cyber Forensics, InfoSec 2015, Cape Town, South Africa, November 15-17, 2015*, 2015, S. 99–104, doi: 10.1109/InfoSec.2015.7435513.

[56] N. Etaher und G. R. S. Weir, „Understanding children's mobile device usage", in *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Juni 2016, S. 1–7, doi: 10.1109/ICCCF.2016.7740437.

[57] M. Bahrini, G. Volkmar, J. Schmutte, N. Wenig, K. Sohr, und R. Malaka, „Make my Phone Secure! Using Gamification for Mobile Security Settings", in *Proceedings of Mensch und Computer 2019*, Hamburg, Germany, Sep. 2019, S. 299–308, doi: 10.1145/3340764.3340775.

[58] N. Gerber *u. a.*, „FoxIT: enhancing mobile users' privacy behavior by increasing knowledge and awareness", in *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, Orlando, Florida, USA, Dez. 2018, S. 53–63, doi: 10.1145/3167996.3167999.

[59] H. Almuhimedi *u. a.*, „Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging", in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, Seoul, Republic of Korea, Apr. 2015, S. 787–796, doi: 10.1145/2702123.2702210.

[60] D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, und J. D'Arcy, „Modifying smartphone user locking behavior", in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, Newcastle, United Kingdom, Juli 2013, S. 1–14, doi: 10.1145/2501604.2501614.

[61] „Google ‚Bouncer' Now Scanning Android Market for Malware". https://uk.pcmag.com/mobile-apps/66697/google-bouncer-now-scanning-android-market-for-malware (zugegriffen Nov. 05, 2020).

[62] „Google Play Protect für den Schutz vor schädlichen Apps - Google Play-Hilfe". https://support.google.com/googleplay/answer/2812853?hl=de (zugegriffen Nov. 05, 2020).

[63] „Google Play Protect", *Android*. https://www.android.com/intl/de_de/play-protect/ (zugegriffen Nov. 05, 2020).

[64] „Sicherheit bei Apps – Übersicht", *Apple Support*. https://support.apple.com/de-de/guide/security/sec35dd877d0/web (zugegriffen Nov. 30, 2020).

[65] „New Malware Apps on Google Play | Avast". https://blog.avast.com/new-malware-apps-on-google-play-avast (zugegriffen Nov. 28, 2020).

[66] „Trojan malware infecting 17 apps on the App Store“, *Wandera*, Okt. 24, 2019. https://www.wandera.com/ios-trojan-malware/ (zugegriffen Nov. 30, 2020).