Mobiler Datenschutz: Nutzerzentrierte Gestaltung der AndProtect-App

Susen Döbelt[1], Josephine Halama[1]

Professur für Allgemeine Psychologie und Arbeitspsychologie, TU Chemnitz[1]

susen.doebelt@psychologie.tu-chemnitz.de, josephine.halama2@psychologie.tu-chemnitz.de

Zusammenfassung

Mobile Applikationen bieten nicht nur vielfältige Möglichkeiten der Unterstützung im Alltag, sondern verwenden oft personenbezogene Daten und leiten diese an Dritte weiter. Hinweise zu App-Berechtigungen existieren, sind aber oft unverständlich und werden wenig beachtet. Zudem fehlen NutzerInnen detaillierte Informationen zu Umfang und Weiterleitung der Daten. Mithilfe von gebrauchstauglich aufbereiteten Ergebnissen aus statischen und dynamischen Analyseverfahren sollte im Forschungsvorhaben AndProtect ein Werkzeug geschaffen werden, das NutzerInnen qualifizierte Aussagen über datenschutzrelevante App-Datenflüsse ermöglicht. Innerhalb dieses Beitrages werden einzelne Schritte des nutzerzentrierten Gestaltungsprozesses für das Analysewerkzeug – die AndProtect-App – beschrieben. Die Beschreibung kann als Vorlage für ähnliche Entwicklungsvorhaben dienen und soll mit Workshop-TeilnehmerInnen aus Wissenschaft und Praxis diskutiert werden.

1 Einleitung

Die Anzahl der Applikationen (Apps) im Google Play Store steigt monatlich und liegt aktuell bei über drei Millionen (AppBrain, 2018). Apps bieten NutzerInnen nicht nur vielfältige Möglichkeiten der Unterhaltung und Unterstützung im Alltag, sondern verwenden oft personenbezogene Daten oder leiten diese an dritte Parteien weiter. Den Zugriff auf Daten bekommen Apps über erteilte Berechtigungen (Permissions). Hinweise zu den Permissions und Datenschutzbestimmungen existieren, sind aber für NutzerInnen umständlich, unverständlich und werden in den meisten Fällen wenig beachtet und erinnert (Kelley et al., 2012; 2013; Felt et al., 2012). Ist eine App installiert und der Zugriff auf private Daten gewährt, sind alle weiteren Verarbeitungsschritte für den/die NutzerIn nicht mehr nachvollziehbar.

Ab Android 6.0 wurde, anstatt alle Berechtigungen zur Installation abzufragen, ein Runtime-Permission-Modell eingeführt. Hier wird während der Nutzung einer App die Verwendung von Permissions durch den/die NutzerIn genehmigt oder verweigert. NutzerInnen sind oft

Veröffentlicht durch die Gesellschaft für Informatik e. V. 2018 in
R. Dachselt, G. Weber (Hrsg.):
Mensch und Computer 2018 – Workshopband, 02.–05. September 2018, Dresden.
 https://doi.org/10.18420/muc2018-ws09-0547

unsicher bezüglich der Angemessenheit von Berechtigungsanfragen (Kelley et al., 2013) und gewinnen mit einer zusätzlichen Erklärung Sicherheit (Lin et al., 2012; Android Open Source Project, 2018). Bereits für iOS konnte jedoch gezeigt werden, dass diese Möglichkeit von Entwicklerseite häufig nicht genutzt wird (Tan et al., 2014). Zudem kann trotz Runtime-Modell ein Großteil von Permissions, die Android-seitig als „*nicht gefährlich*“ eingestuft werden, von NutzerInnen nicht verweigert werden, ohne ganz auf die App zu verzichten.

Berechtigungen liefern zudem nur auf einen Teil des App-Verhaltens Hinweise. In welchem Umfang die Berechtigungen genutzt werden und wohin die erhobenen Daten weitergeleitet werden, bleibt für den/die NutzerIn intransparent. Die Schwierigkeit, eine qualifizierte Aussage über das datenschutzrelevante Verhalten von Apps zu treffen, besteht daher weiter und wurde im Forschungsvorhabens AndProtect adressiert. Ziel war es, die Transparenz der Datenverarbeitungsvorgänge und die Risikobewertung für NutzerInnen zu verbessern. Der AndProtect-Ansatz gebrauchstauglich aufbereiteter Ergebnisse statischer und dynamischer Analyseverfahren sollte Einblick in diese Informationen ermöglichen.

Der Fokus dieses Beitrages liegt auf der Darstellung des Vorgehens der Nutzerforschung und kann als Vorlage für ähnliche Entwicklungsvorhaben dienen. Auf eine detaillierte Ergebnisdarstellung wird verzichtet, da dies den Beitragsrahmen übersteigt und die Darstellung des Vorgehens im Vordergrund stehen soll.

2 Fragestellungen

Ziel des Forschungsvorhabens AndProtect war es, ein benutzerfreundliches Werkzeug zu schaffen, welches qualifizierte Aussagen über datenschutzrelevante Informationsflüsse von Apps ermöglicht. Im Zuge des nutzerzentrierten Gestaltungsprozeses ergaben sich schrittweise u. a. folgende Fragestellungen: 1.) Welchen Informationsbedarf haben NutzerInnen hinsichtlich datenschutzrelevanten App-Verhaltens? und 2.) Wie alltagstauglich ist das entwickelte Werkzeug und welche Veränderungen bewirkt es in der Praxis?

Zur Identifikation des Informationsbedarfs wurde eine Nutzerbefragung und zur Überprüfung der Alltagstauglichkeit ein Feldversuch durchgeführt.

3 Methode

3.1 Nutzerbefragung

Die Nutzerbefragung wurde mittels eines Online-Fragebogens realisiert. Nach 10 Wochen konnten $N = 227$ vollständig bearbeitete Fragebögen ausgewertet werden. Das Ausfüllen des Fragebogens dauerte im Mittel 30 Minuten. Nach Begrüßung und Aufklärung über das Ziel der Befragung wurde die Nutzung vier unterschiedlicher App-Gruppen (Karten/Navigations-, Messenger-, Wetter-, und Shopping-App) erfragt. Im Falle der Nutzung einer spezifischen App der genannten App-Gruppen, wurden Fragen zur Bedrohlichkeit für die eigene Privats-

phäre bei Verwendung von 15 zuvor definierten Datenarten gestellt (z. B. Standortdaten, Kameradaten, etc.). Je nach App-Gruppe waren diese Datenarten für die Funktionalität erforderlich, teilerforderlich oder nicht erforderlich. Zudem wurde zwischen einer Datenerfassung während der Interaktion mit einer App (im Vordergrund), oder während die App im Hintergrund abgelegt ist, unterschieden. Im mittleren Teil der Befragung konnten Verbesserungsvorschläge zum Privatsphärenschutz im mobilen Kontext offen formuliert werden. Abschließend wurden stichprobenbeschreibende Variablen (z.B. Technikaffinität, Wissen über Apps, Privatsphärenbedenken) und demographische Angaben (Alter, Bildung, etc.) erfragt. Als Motivation zur Teilnahme an der Befragung fand eine Verlosung statt.

3.2 Feldversuch

Der Feldversuch war in eine zweiwöchige Baseline-Phase und eine vierwöchige Versuchsphase aufgeteilt, um einen Vergleich des TeilnehmerInnen-Verhaltens ohne und mit der AndProtect-App zu ermöglichen. Die Versuchsphase begannen N = 26 TeilnehmerInnen, welche mehrheitlich durch die „*Unterstützung von Forschung und Entwicklung*“ zur Teilnahme motiviert wurden. Die TeilnehmerInnen bildeten eine heterogene Stichprobe, welche eine Bandbreite von Personen mit unterschiedlich ausgeprägten demographischen Variablen beinhaltete. Über den Feldversuch hinweg gab es sieben Befragungszeitpunkte. Die Links zu den wöchentlichen Befragungen wurden per Email an die TeilnehmerInnen verschickt. In der Versuchsphase waren die Nutzung sowie die Gebrauchs- und Alltagstauglichkeit der AndProtect-App (näher Beschreibung der AndProtect-App findet auf der Projektwebseite) im Fokus der Erhebungen. Eine der sieben Befragungen fand in den Laborräumen der AAP statt. Zu diesem Termin wurden die TeilnehmerInnen gebeten, die AndProtect-App zu installieren und den ersten Eindruck mittels Lautem Denken zu schildern. In den weiteren Befragungen davor und danach wurden individualisiert Variablen wie bspw. Gründe für die (De-) Installation von Apps erfragt. Nach Abschluss der Basline- und der Versuchsphase erhielt jedeR TeilnehmerIn eine Aufwandsentschädigung ausgezahlt.

4 Ergebnisse

4.1 Nutzerberfragung

Die Ergebnisse der Nutzerbefragung zeigten Unterschiede in der Bewertung der Datenarten, je nach deren Erforderlichkeit für eine App-Gruppe. Dabei wurde erwartungsgemäß die Verwendung nichterforderlicher Daten von den NutzerInnen als deutlich bedrohlicher für die eigene Privatsphäre eingeschätzt, als die Verwendung teilerforderlicher und erforderlicher Daten. Zudem offenbarte sich ein Unterschied in den Nutzerbewertungen zwischen der Verwendung von Daten im Vordergrund im Vergleich zur Verwendung im Hintergrund. Die Befragten bewerteten es erwartungsgemäß als bedrohlicher für die eigene Privatsphäre, wenn Daten im Hintergrund verwendet werden. Stichprobenbeschreibende und demographische Variablen (Alter, Technikaffinität, Wissen, negative Erfahrungen) spielten erstaunlicherweise keine Rolle für die Bewertung der Bedrohlichkeit. Lediglich die Variable Privatsphären-

bedenken zeigte positive Zusammenhänge zur Bewertung der Bedrohlichkeit. Grundsätzlich wurde jegliche Verwendung von Daten als sehr kritisch bewertet. Dies unterstrich die Relevanz eines transparenzerhöhenden Werkzeuges.

4.2 Feldversuch

Die Antworten der TeilnehmerInnen in der Versuchsphase zeigten, dass u. a. die AndProtect-App gezielt genutzt wurde um Apps zu überprüfen, allerdings in der ersten Woche häufiger als in den darauffolgenden Wochen. Als Grund für die Nichtnutzung wurden v. a. „*kein Bedarf/Mehrwert*“ und „*mangelnde Zeit*“ genannt. Am besten wurden die im Bericht enthaltenen Informationen zum App-Verhalten sowie die Farbkodierung des App-Risikos bewertet. Von den TeilnehmerInnen konnten deutlich weniger Nachteile als Vorteile der AndProtect-App genannt werden. Als nachteilig wurden bspw. lange Wartezeiten, mangelnde Handlungsoptionen (konkrete Empfehlungen für Riskominimierung, Permissions aus der AndProtect-App heraus verändern) und mangelnde Informationen zur Bedienung der App empfunden. Zur Erfassung der Usability und User Experience wurden verschiedene Fragebögen (bspw. der ISONORM Fragebogen, Prümper & Anft, 1993, der UEQ, Laugwitz et al., 2008; und der PET-USES, Wästlund et al.; 2009) eingesetzt. Die Bewertung der AndProtect-App fiel hier insgesamt „*gut*“ aus. Nach Einschätzung des überwiegenden Teils der TeilnehmerInnen bewirkte die AndProtect-App eine Veränderung im App-Nutzungsverhalten. Dies bezog sich auf die genauere Prüfung von Permissions bzw. auf das Entziehen von Permissions. Der Anteil der Apps, bei denen Permissions entzogen wurden, stieg um 10%. Dieser Anstieg war bei TeilnehmerInnen zu verzeichnen, die diese Funktion bereits vor dem Feldtest nutzten. Besonders zu Beginn der Versuchsphase war zudem ein Anstieg von Deinstallation zu verzeichnen. Begründet wurden diese damit, dass kein Bedarf mehr für die deinstallierte App bestand oder dass die Informationen der AndProtect-App zur Deinstallation motivierten. Der Deinstallationseffekt zeigte sich (ähnlich wie bei den Permissions) nicht für alle TeilnehmerInnen: Etwa ein Drittel gab an, keine Veränderung im Umgang mit Apps durch die AndProtect-App bemerkt zu haben.

5 Zusammenfassung und Diskussion

Innerhalb des Forschungsvorhabens AndProtect wurde ein nutzerzentrierter Gestaltungsansatz verfolgt um ein Werkzeug zu entwickeln, welches den/die NutzerIn befähigt, eine qualifizierte Aussage über datenschutzrelevantes App-Verhalten zu treffen. Zur Erhebung des Informationsbedarfs und der Untersuchung der Alltagstauglichkeit wurden eine Nutzerbefragung und ein Feldversuch durchgeführt.

Die Ergebnisse der Nutzerbefragung zeigten, dass die Information zur Erforderlichkeit der Datenerhebung sowie die Art der Datenerhebung (im Vorder-/Hintergrund) in die Gestaltung der AndProtect-App einbezogen werden mussten. Stichprobenbeschreibende und demographische Variablen (bspw. Technikaffinität, Alter, Wissen) spielten für die Risikobewertung der Datenarten keine Rolle und wurden daher nicht einbezogen. Es wurden jedoch individu-

elle Anpassungsmöglichkeiten hinsichtlich der Bewertung der Datenarten geschaffen, da sich diese je nach Ausprägung der Privatsphärenbedenken geringfügig unterschieden.

Der Feldversuch ergab eine Abnahme der Nutzung der AndProtect-App nach der ersten Woche. Dies erklärt sich durch das abnehmende Informationspotenzial der App über die Zeit: Beim ersten Öffnen lagen unmittelbar Informationen über alle Apps vor, zu denen bereits ein Bericht existierte. Im Verlauf der Versuchsphase trafen nur noch einzelne Berichte zu expltzit angefragten Apps ein. Aus den genannten Nachteilen (lange Wartezeiten, fehlende Handlungsoptionen, keine vorhandene Hilfefunktion) konnten konkrete Verbesserungsmöglichkeiten abgeleitet werden. Zudem zeigte sich, dass das Entziehen von Permissions für einige NutzerInnen eine sinnvolle Verhaltensvariante darstellt, die durch die AndProtect-App angesprochen wurde. Andere Probanden nutzten die Funktion hingegen nicht, was durch die AndProtect-App auch nicht verändert werden konnte. Zudem führte die AndProtect-App zu einem Anstieg von Deinstallationen bei einigen (aber nicht allen) TeilnehmerInnen. Daher ist zu vermuten, dass die AndProtect-App nur für bestimmte Personen einen Effekt hatte. Diese Ergebnisse implizieren eine Weiterentwicklung von der One-Size-Fits-All-Intervention, hin zu einer Nutzertypen-spezifischen Lösung.

Innerhalb des Workshops „*UUX-Praxis im Wandel*“ soll ein Diskurs mit den Workshop-TeilnehmerInnen aus Wissenschaft und Praxis zum dargestellten Vorgehen angestoßen bzw. Erfahrungswerte ausgetauscht werden. Durch die Nutzerbefragung konnten Vermutungen über Informationsbedarfe von NutzerInnen konkret untermauert oder auch widerlegt werden. Der Feldversuch ermöglichte durch den Vergleich einer Baseline- und Versuchsphase tiefe Einblicke in das App-Nutzungverhalten mit und ohne das entwickelte Analysewerkzeug. Diskutiert werden soll, inwieweit die dargestellten Methoden aus einem Forschungsvorhaben in der Praxis nutzbar sind oder inwiefern diese auf Zeit- und Ressourcenbeschränkungen (Bär, Döbelt, Seeling & Dittrich, 2013) in Unternehmen angepasst werden müssten. Mit Workshop-TeilnehmerInnen aus der Wissenschaft möchten wir diskutieren, wie qualitative und quantitative Daten integriert bzw. wie mit widersprüchlichen Daten umgegangen werden kann (Halama & Döbelt, 2017). Wir freuen uns auf einen spannenden Workshop.

Danksagung

Die Inhalte des Beitrages sind Ergebnisse des BMBF geförderten Forschungsvorhabens *AndProtect: Selbstdatenschutz durch statische und dynamische Analyse zur Validierung von Android-Apps* (FKZ: 16KIS0349). Weiterführende Informationen sind auf der Projektwebseite https://www.andprotect.de/ zu finden. Zudem danken wir Paul Schweidler, Timo Jakobi und Michael Burmester für die Rückmeldung zum Beitrag.

Literaturverzeichnis

AppBrain. (n.d.). Anzahl der verfügbaren Apps im Google Play Store in ausgewählten Monaten von Juli 2015 bis Juni 2018 (in 1.000). In Statista - Das Statistik-Portal. Abgerufen am 26.06.2018, von

https://de.statista.com/statistik/daten/studie/74368/umfrage/anzahl-der-verfuegbaren-apps-im-google-play-store/.

Android Open Source Project (2018). Berechtigungen zur Laufzeit angemessen anfordern (in Android ab Version 6.0). Abgerufen am 26.06.2018, von https://developer.android.com/distribute/best-practices/develop/runtime-permissions#best-practices.

Bär, N., Döbelt, S., Seeling, T. & Dittrich, F. (2013). Zur Notwendigkeit anwendungsspezifischer Usability-Verfahren für betriebliche Software. In H. Brau, A. Lehmann, K. Petrovic, M. Schroeder (Hrsg.), Tagungsband Usability-Professionals 2013. Bremen, pp. 318-321.

Batyuk, L., Herpich, M., Camtepe, S. A., Raddatz, K., Schmidt, A. D. & Albayrak, S. (2011). Using static analysis for automatic assessment and mitigation of unwanted and malicious activities within Android applications. In Malicious and Unwanted Software (MALWARE), 2011 6th Interna-tional Conference. IEEE. pp. 66-72.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E. & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. In Proceedings of the 8th symposium on usable privacy and security. ACM. p.3.

Halama, J. & Döbelt, S. (2017). The Integration of Diverse User Data to derive User Requirements. In: Eibl, M. & Gaedke, M. (Hrsg.), INFORMATIK 2017. Bonn: Gesellschaft für Informatik. pp. 2329-2334.

Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N. & Wetherall, D. (2012). A Conundrum of Permissions: Installing Applications on an Android Smartphone. In Blyth, J., Dietrich, S. & Camp, L. J. (Eds.), Financial Cryptography and Data Security. Berlin: Springer. pp. 63-76

Kelley, P. G., Cranor, L. F. & Sadeh, N. (2013). Privacy as part of the app decision-making process. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM. pp. 3393-3402.

Laugwitz, B., Held, T. & Schrepp, M. (2008). Construction and evaluation of a user experience questionnaire. Symposium of the Austrian HCI and Usability Engineering Group. Berlin: Springer, pp. 63-76.

Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J. & Zhang, J. (2012). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing. ACM. pp. 501-510.

Prümper, J. & Anft, M. (1993). Die Evaluation von Software auf Grundlage des Entwurfs zur internationalen Ergonomie-Norm ISO 9241 Teil 10 als Beitrag zur partizipativen Systemgestaltung—ein Fallbeispiel. In Software-Ergonomie'93. Wiesbaden: Vieweg+ Teubner Verlag. pp. 145-156.

Tan, J., Nguyen, K., Theodorides, M., Negrón-Arroyo, H., Thompson, C., Egelman, S. & Wagner, D. (2014). The effect of developer-specified explanations for permission requests on smartphone user behavior. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM. pp. 91-100.

Wästlund, E., Wolkerstorfer, P. & Köffel, C. (2009). PET-USES: privacy-enhancing technology–users' self-estimation scale. In IFIP PrimeLife International Summer School on Privacy and Identity Management for Life. Springer, Berlin, Heidelberg. pp. 266-274.

Autoren

Döbelt, Susen

Susen studierte Psychologie an der TU Dresden und ist seit 2013 an der TU Chemnitz als wissenschaftliche Mitarbeiterin an der Professur für Allgemeine Psychologie und Arbeitspsychologie angestellt. Im Bereich Mensch-Maschine-Interaktion ist sie in nationalen und internationalen Forschungsprojekten mit der Erfassung nutzerzentrierter Anforderungen, Gestaltung und Evaluation technischer Systeme in verschiedenen Anwendungskontexten betraut. Ihr Forschungsschwerpunkt liegt im Bereich Smart Grid Anwendungen und mobile Applikationen und hier auf der Untersuchung von Privatsphärenaspekten.

Halama, Josephine

Josephine studierte Psychologie an der TU Chemnitz. Seit 2016 ist sie wissenschaftliche Mitarbeiterin an der Professur für Allgemeine Psychologie und Arbeitspsychologie. Ihre Diplomarbeit schrieb sie im Rahmen des hier dargestellten Projektes AndProtect. Während ihres Studiums war Josephine wissenschaftliche Hilfskraft an der Professur und in Forschungsprojekte wie "Gesteuertes Laden V3.0" und "Entwicklung eines Indikators für nutzerrelevante Netzqualität" involviert. Im Rahmen des letztgenannten Projektes schrieb sie ihre Bachelorarbeit mit dem Titel: "Das Verhältnis von nutzerrelevanten Netzparametern und der Erlebnisqualität - Ergebnisse einer Studie zum mobilen Internet".