# ZUR SECURITY AWARENESS BEI NUTZERN VON SMARTPHONES

**Philipp Goldberg, M. Sc.**
Hochschule Darmstadt – Fachbereich Informatik

17. Deutscher IT-Sicherheitskongress
BSI

# MOTIVATION

- Beliebtheit von Smartphones steigt ständig an → aktuell 3,2 Milliarden Nutzer weltweit [1]
- BSI: „Die Lage der IT-Sicherheit in Deutschland 2014“ [2]
  - Betriebssysteme vergleichsweise gut gesichert
  - Nutzer installieren Apps ohne die Berechtigungsabfragen zu beachten
- Ist diese Aussage auch gut 7 Jahre später noch relevant?

# ZIELSETZUNG UND FORSCHUNGSFRAGEN

- 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?

➔ Beantwortung mittels strukturiertem Literaturreview (SLR)

## STRUKTURIERTES LITERATURREVIEW

# ZIEL UND TAXANOMIE

- Vorhandenes Wissen finden
- Zentrale Aussagen zusammenfassen
- Forschungsagenda

| 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 |

Taxanomie dieser Arbeit in Anlehnung an Cooper [3] (Auszug). Zutreffendes durch **Fettschrift** hervorgehoben.

# LITERATURSUCHE

**Suchanfrage:** Variationen der 3 Kernthemen Security Awareness, Smartphone und Nutzer.

**Primäre Suche** mit 506 Treffern

**Synthese** von 46 Arbeiten

| Merkmal | Einschlusskriterium | Ausschlusskriterium |
|---|---|---|
| **Zeitpunkt der Veröffentlichung** | 01.01.2011 bis 31.05.2020 | Anderer Zeitraum |
| **Sprache der Publikation** | Englisch | Andere Sprachen, Übersetzungen durch Dritte |
| **Einbindung von Nutzern** | Datenerhebung, Verifikation, … | Keine Nutzereinbindung |

Ein- und Ausschlusskriterien (Auszug)

# SYNTHESE DER ARBEITEN

Einteilung und Erkenntnisse

SYNTHESE DER ARBEITEN

# EINTEILUNG IN GRUPPEN

Gruppierung auf höherer Abstraktionsebene

- Identifizierung des übergeordneten Ziels bzw. adressierter Probleme
- Obergruppen:
  - Berechtigungen von Apps
  - Auswahl von Apps
  - Security Awareness der Nutzer
  - Aufklärung und Schulung der Nutzer

## SYNTHESE DER ARBEITEN

# BERECHTIGUNGEN VON APPS

- Nutzer verstehen das Berechtigungssystem und dessen Auswirkungen nicht [5 u.a.]
  - Berechtigungen können nicht immer erklärt werden
  - Dialoge mit Hinweisen zu Berechtigungen werden nicht beachtet
  - Anwender installieren Apps mit zu vielen Berechtigungen [bspw. 6]
- Forschung: Vorschläge, welche Berechtigungen entzogen werden können
  - Crowdsourcing-Ansätze [bspw. 7]
  - Lokal [bspw. 8]
  - Meist mit Eingriffen ins Betriebssystem verbunden

SYNTHESE DER ARBEITEN

# AUSWAHL VON APPS

- Idee: Nutzer sollen „schlechte“ Apps gar nicht erst installieren
- Verbesserte Visualisierung der Berechtigungen
  - Checkliste, was eine App mit den Berechtigungen machen darf [9]
  - Auswirkung durch persönliche/konkrete Beispiele [10]
  - Risiko (auf Basis der Berechtigungen) einer App darstellen
  - → Probanden wählen „sicherere“ App aus
- Leitfaden zur Auswahl einer App
  - Flyer, welcher erklärt, auf welche Punkte geachtet werden sollte
  - → Fundiertere, aber nicht immer bessere Entscheidung [11]

SYNTHESE DER ARBEITEN

# SECURITY AWARENESS DER NUTZER

- Nutzern fehlt das Wissen über die Existenz bestimmter Schutzmaßnahmen oder Verhaltensweisen [14 u.a.]
  - Selbst „erfahrene“ Nutzer kennen nicht alle Optionen
- Benutzbarkeit wichtig für die Akzeptanz [15]
  - Ablehnung, wenn sie im Alltag als störend empfunden werden [16]
- PC im Vergleich zum Smartphone sicherer [bspw. 15]
  - Gründe: Ausgereifte Technik, lange etabliert
  - Angst vor Verlust des Smartphones [17]

SYNTHESE DER ARBEITEN

# SECURITY AWARENESS DER NUTZER

- Auswahl von Apps
  - Basiert nicht auf Sicherheit und Privatsphäre [19]
  - Stattdessen: Empfehlung, Beliebtheit, Bewertungen und Werbeanzeigen [9]
  - Nutzer-Annahme: nur sichere und geprüfte Apps in den Stores → unbesorgtere Wahl [20]
  - Benötigte Berechtigungen meist kein Kriterium [13]
  - Anzahl an Berechtigungen kann zu Ablehnung führen, nicht deren Kritikalität [13]
  - → Nutzer verstehen das Berechtigungssystem (Android) nicht

SYNTHESE DER ARBEITEN

# SECURITY AWARENESS DER NUTZER

- Einflüsse und Zusammenhänge
  - Demographische Daten lassen keinen Rückschluss auf Security Awareness zu [21 u.a.]
  - Antivirensoftware installiert oder (mittleres) Interesse an Cybersicherheit
    - → höhere Security Awareness, sichereres Verhalten [21, 22]

SYNTHESE DER ARBEITEN

# AUFKLÄRUNG UND SCHULUNG DER NUTZER

- Auswirkungen von Berechtigungen
  - Bei (genauer) Anzeige der zu sendenden Daten möchten 60% diese Daten nicht versendet haben [23]
  - Abweichung von tatsächlichem und vorgestelltem Verhalten bzgl. Berechtigungen [6]
- Dedizierte Lern-Apps [4 und 24]
  - Können Wissen vermitteln, Animierung zum Weitermachen sinnig
- Nutzer zu sichererem Verhalten animieren
  - Gezielte Nachrichten führen selten zur Änderung des Verhaltens [26]
  - Video mit Hinweis über die möglichen Folgen animiert die Probanden eher [16]

# DISKUSSION DER ARBEITEN

Limitierungen und Forschungslücken

## DISKUSSION DER ARBEITEN

# LIMITIERUNGEN UND FORSCHUNGSLÜCKEN

- Eigenaussagen der Probanden
  - Genanntes Verhalten kann von tatsächlichem Verhalten abweichen [21]
  - Fragen können missverstanden werden [18]
  - Momentaufnahmen [10]
  - „Gestellte“ Situation [28]
- iOS kaum vertreten
  - Lediglich eine Arbeit beschäftigt sich explizit und exklusiv mit iOS-Nutzern [27]
  - Praktisches (bspw. Implementierungen) überwiegend für Android [bspw. 24 und 12]
    - Mehrzahl der Nutzer
    - Anpassungen am System dank Open-Source möglich

## DISKUSSION DER ARBEITEN

# LIMITIERUNGEN UND FORSCHUNGSLÜCKEN

- Nicht repräsentative Wahl der Probanden [bspw. 12]
  - Keine Generalisierung der Aussagen möglich
  - Durchführung zumeist an Hochschulen und Universitäten
    - Junge und gebildete Probanden
- Fehlende Alltagstauglichkeit der Entwicklungen/Vorschläge [bspw. 25]
  - Keine Anwendung/Umsetzung im realen Leben

# RESÜMEE

Beantwortung der Forschungsfragen, Limitierungen, und Ausblick

RESÜMEE

# BEANTWORTUNG DER FORSCHUNGSFRAGEN

- Welche Ansätze gibt es, um die Security Awareness zu erhöhen bzw. zu verbessern?
  - Nutzer entlasten durch Automatisierung
  - Apps, welche den Nutzer aufklären
  - Risiken aufzeigen und Möglichkeiten zur Vermeidung aufzeigen
- Mit welchen Methodiken wurde die Security Awareness gemessen?
  - Meist Fragebogen oder vergleichbare Mittel
    - Kein Standard vorhanden

RESÜMEE

# BEANTWORTUNG DER FORSCHUNGSFRAGEN

- Wie wird die Gültigkeit der Aussagen belegt?
  - Wirksamkeit einer App oder Idee: Nutzertest
  - Fragebögen und Interviews
- Welche typischen Limitierungen gibt es?
  - Anzahl und Wahl der Probanden
  - Selbstaussagen
  - Momentaufnahme
- Wie hat sich die Security Awareness über die Jahre verändert?
  - Antwort nicht trivial, da keine „Skala“ vorhanden
  - Nutzung von Displaysperre über die Jahre gestiegen (mögl. Anhaltspunkt)

RESÜMEE

# AUSBLICK / FORSCHUNGSAGENDA

- Daten während der Studie (zusätzlich) automatisiert erfassen
- Realistischeres Probandenprofil
  - Ggf. regionale Unterschiede erfassen
- Immer den Nutzer einbeziehen, wenn etwas für ihn entwickelt wird
- Vergleichbarkeit von Security Awareness ermöglichen
  - Rahmenwerk mit definierten Inhalten
  - Zahlenwerte oder ähnlich vergleichbares als Ergebnis

# VIELEN DANK FÜR DIE AUFMERKSAMKEIT.



**Philipp Goldberg, M. Sc.**
Zur Security Awareness bei Nutzern von Smartphones
pgoldberg.de | E-Mail: mail@pgoldberg.de

17. Deutscher IT-Sicherheitskongress
BSI

# LITERATURVERZEICHNIS


[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, „Die Lage der IT-Sicherheit in Deutschland 2014", S. 44, Dez. 2014.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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].

[9] 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.

[10] 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.

# LITERATURVERZEICHNIS


[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

# LITERATURVERZEICHNIS


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

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.