

Instrumente zur aktiven und sicheren Verbraucherteilhabe an öffentlichen Online-Diensten

Esther Ruiz Ben¹, Anne Jellinghaus², Britta Hesse³, Margit Scholl⁴, Sebastian Möller⁵

Abstract: Das Projekt „Instrumente zur aktiven und sicheren Verbraucherteilhabe an Online Public Services“ (IVTOPS) analysiert die Verbraucherakzeptanz von öffentlichen Online-Diensten am Beispiel von Nutzerkonten in Berlin und Brandenburg, um geeignete Instrumente zur Überwindung von Akzeptanzbarrieren bzw. Informations- und digitalen Kompetenzasymmetrien bezüglich Datensicherheit und Datenschutz bei der Nutzung von öffentlichen Online-Diensten zu schaffen und zu testen.

Keywords: Öffentliche Online-Dienste, Datensicherheit und -schutz, Usable Privacy and Security, Digital Divide.

1 Projektziele

Die Digitalisierung von Public Services ist für Verbraucher*innen eine große Herausforderung. In einer sich immer stärker diversifizierenden Angebots- und Anbietervielfalt von digitalen öffentlichen Diensten benötigen Verbraucher*innen Orientierung, um Nutzungsentscheidungen treffen zu können. Speziell Datensicherheit und -schutz spielen dabei eine ebenso wesentliche Rolle wie Informationen und digitale Kompetenzen, die zur inklusiven Teilhabe in der Nutzung von digitalen Public Services beitragen. Wie die Ergebnisse des jährlich durchgeführten eGovernment MONITOR⁶ zeigen, erweist sich unter anderem die Angst vor Datendiebstahl als wesentliche Barriere für die Nutzung von E-Government Online-Angeboten bzw. digitalen Public Services. Auch wenn diese Angst der Verbraucher*innen als Akzeptanzbarriere für die Nutzung von digitalen Public Services bekannt ist, wurde die Ursache dieser Akzeptanzbarriere bzw. den Informations- und Kompetenzstand der Verbraucher*innen bezüglich Datenschutz und -sicherheit kaum analysiert.

1 TH Wildau, Wirtschaft, Informatik Recht, Technische Hochschule Wildau Hochschulring 1, 15745 Wildau, ruiz_ben@th-wildau.de

2 TH Wildau, Wirtschaft, Informatik Recht, Technische Hochschule Wildau Hochschulring 1, 15745 Wildau, anne.jellinghaus@th-wildau.de

3 TU Berlin, Institut für Softwaretechnik und Theoretische Informatik, Quality and Usability Lab, TU-Hochhaus Ernst-Reuter-Platz 7, 10587 Berlin, britta.hesse@tu-berlin.de

4 TH Wildau, Wirtschaft, Informatik Recht, Technische Hochschule Wildau Hochschulring 1, 15745 Wildau, margit.scholl@th-wildau.de

5 TU Berlin, Institut für Softwaretechnik und Theoretische Informatik, Quality and Usability Lab, TU-Hochhaus Ernst-Reuter-Platz 7, 10587 Berlin, sebastian.moeller@tu-berlin.de

6 <https://initiated21.de/publikationen/egovernment-monitor-2019/> (Zugriff: 20.04.2022)

Instrumente zur Lösung von diesen Akzeptanzproblemen bei öffentlichen Online-Diensten wurden bisher nicht umgesetzt. Heuwing and Maletz [HM19] erklären, dass partizipative Entwicklungsmethoden in der Gestaltung von öffentlichen Online-Diensten nicht etabliert sind. Diese Autor*innen haben partizipative Ansätze für die Umsetzungsempfehlungen von öffentlichen Online-Diensten in Ländern und Kommunen verwendet. Usable Security Aspekte werden dabei jedoch nicht genutzt.

Das laufende Projekt IVTOPS⁷ analysiert die Verbraucherakzeptanz von öffentlichen Online-Diensten am Beispiel von Nutzerkonten in Berlin und Brandenburg, um geeignete Instrumente zur Überwindung von Akzeptanzbarrieren bzw. Informationsdefiziten und digitalen Kompetenzasymmetrien bezüglich Datensicherheit und -schutz bei der Nutzung von öffentlichen Online-Diensten zu schaffen und zu testen.

2 Methodologie

Es werden qualitative und quantitative Methoden angewandt, die sukzessiv die Entwicklung der verschiedenen Methodeninstrumente unterstützen. In der explorativen Phase wurde mit Hilfe einer Dokumentenanalyse der Stand der Entwicklung und Nutzung von Servicekonten bzw. eIDAS in Berlin und Brandenburg sowie von Messinstrumenten für die Akzeptanzanalyse eruiert. Basierend auf diesen Ergebnissen wird die Akzeptanz von Servicekonten aus der Perspektive des Digital Divide in der Analysephase mit qualitativen (Experteninterviews) und quantitativen (Umfrage bei Nutzer*innen von Servicekonten bzw. eIDAS in Berlin und Brandenburg) Methoden genau analysiert. Aus den Erkenntnissen dieser Analysen werden Usable Security-Instrumente für eIDAS bzw. Servicekonten partizipativ (Fokusgruppen und Design Thinking) entwickelt und evaluiert. Die Abb. 1 zeigt eine Zusammenfassung der angewandten Methodologie:



Abb. 1: IVTOPS-Methodologie

⁷ Das diesem Poster zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz unter dem Förderkennzeichen 28V1403A20 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autor*innen.

3 Usable Privacy und Security Instrumente

Zusammen mit Verbraucher*innen werden „Usable Privacy und Security Instrumente“ (Privacy Enhancing Technologies – PETs [AS17], [Be20], [SD18], [SB15]) zur Überwindung von Informationsdefiziten und digitalen Kompetenzasymmetrien bezüglich Datensicherheit und Datenschutz bei der Nutzung von öffentlichen Online-Diensten entwickelt. Dazu werden Design-Thinking-Workshops mit Verbraucher*innen organisiert, um Usable Privacy und Security Instrumente als Prototypen partizipativ zu entwickeln. Die gemeinsam partizipativ entwickelten Prototypen werden in Fokusgruppen danach diskutiert bzw. getestet.

Wir gehen davon aus, dass ein partizipatives Design (z. B. Fokusgruppen und Design-Thinking-Methoden) von Usable Security Instrumenten notwendig ist, um mögliche Intransparenzen von „Security Nudges“ zu vermeiden [Fu20].

4 Vorläufige Ergebnisse

Die vorläufigen Ergebnisse der Akzeptanzuntersuchung zeigen u. a., dass öffentliche Online-Dienste und speziell Nutzerkonten wenig bekannt sind und kaum genutzt werden. Auch wenn die Mehrheit der Befragten den Zugang zu diesen Diensten als unproblematisch einschätzt, fühlen sich viele unsicher hinsichtlich der Selbstbestimmung über ihre persönlichen Daten sowie bezüglich der Verarbeitung ihrer Daten in den Nutzerkonten. Hinsichtlich der Benutzerfreundlichkeit der Nutzerkonten wird die Registrierung von der Mehrheit der Befragten als umständlich gewertet. Bei dem Design der „Usable Security Prototypen“ werden wir u. a. diese Aspekte als Grundlage verwenden.

Literaturverzeichnisses

- [AS17] Acquisti, M.; Sleeper, Y.; Wang, S.; Wilson, I.; Adjerid, R.; Balebako, L.; Brandimarte, L. F.; Cranor, S.; Komanduri, P. G.; Leon, N. Sadeh; Schaub, F.: Nudges for privacy and security. In: *ACM Computer Surv.*: 50: 3: 1–41, 2017
- [Be20] Bertino, E.: Privacy enhancing techniques for security. In (S. E. Woo, L. Tay, & R. W. Proctor Hrsg.): *Big data in psychological research* (411–424). American Psychological Association, 2020
- [Fu20] Fuhrberg, R.: Verhaltensökonomie in der Verwaltungskommunikation – Der Staat als Entscheidungsarchitekt. In: K. Kocks et al. *Öffentliche Verwaltung – Verwaltung in der Öffentlichkeit*. Berlin: Springer, 2020
- [HM19] Heuwing, B.; Maletz, C.: Bürger-Services nutzerzentriert gestalten. Mit Digitalisierungslaboren Verwaltung und Bürger zusammenbringen. In: S. Hess; H. Fischer (Hrsg.): *Mensch und Computer 2019 – Usability Professionals*, 08.-11. September 2019, Hamburg.
- [SD18] Sunyaev, A.; Dehling, T.; Schmidt-Kraepelin, M.: Verbraucherorientierter Datenschutz: Identifizierung von Verbraucherarchetypen zur effektiven Kommunikation von Datenschutzpraktiken. In (Bala, C.; Schuldzinski, W. Hrsg.), *Jenseits des Otto Normalverbrauchers: Verbraucherpolitik in Zeiten des „unmanageable consumer“* (S. 163-179). Düsseldorf: Kompetenzzentrum Verbraucherforschung NRW. https://doi.org/10.15501/978-3-86336-920-0_8 (20.06.2020), 2018
- [SB15] Schaub, F.; Balebako, R.; Durity, A. L.; Cranor, L. F.: A design space for effective privacy notices. In: *Eleventh symposium on usable privacy and security (SOUPS 2015)*, 1–17. Ottawa: USENIX Association. <https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub> (Zugriff: 20.04.2022), 2015