8. Usable Security und Privacy Workshop

Luigi Lo Iacono
luigi.lo_iacono@h-brs.de
Hochschule Bonn-Rhein-Sieg

Hartmut Schmitt
hartmut.schmitt@hk-bs.de
HK Business Solutions GmbH

Svenja Polst
hallo@svenja-polst.de
unabhängig

Andreas Heinemann
andreas.heinemann@h-da.de
Hochschule Darmstadt

ZUSAMMENFASSUNG

Ziel der achten Auflage des wissenschaftlichen Workshops "Usable Security and Privacy" auf der Mensch und Computer 2022 ist es, aktuelle Forschungs- und Praxisbeiträge zu präsentieren und anschließend mit den Teilnehmenden zu diskutieren. Der Workshop soll ein etabliertes Forum fortführen und weiterentwickeln, in dem sich Experten aus verschiedenen Bereichen, z. B. Usability und Security Engineering, transdisziplinär austauschen können.

KEYWORDS

Usable Security, Usable Privacy

1 THEMA UND INHALT

Deutschland kommt bei der Digitalisierung nur langsam voran und liegt nur knapp über dem EU-Durchschnitt [4]. Daher hat die Bundesregierung mit ihrer 2021 beschlossenen Datenstrategie das Ziel ausgegeben, Deutschland zum Vorreiter bei Innovationen zu machen [11]. Insgesamt wurden rund 240 Maßnahmen beschlossen, die in vier Handlungsfeldern gebündelt sind [10]. Als grundlegende Voraussetzung für nachhaltige und erfolgreiche Digitalisierung wird in allen Handlungsfeldern und Maßnahmen *Sicherheit* berücksichtigt. *Datenschutz* wurde als wichtige Herausforderung erkannt und findet sich ebenso wie die *nutzerfreundliche Gestaltung* von digitalen Angeboten und Diensten in zahlreichen Maßnahmen wieder. Dieser Ansatz ist auch in Übereinstimmung mit den Zielen der Regierung Scholz, die sich beispielsweise dafür einsetzt, die Digitalisierung der Verwaltung konsequent aus der Nutzungsperspektive heraus zu denken und interdisziplinäre Problemlösungen zu entwickeln [12].

Der Ansatz, diese drei wichtigen Grundlagen der Digitalisierung – Sicherheit, Datenschutz und Usability – zusammen zu denken und miteinander in Einklang zu bringen, wird als *Usable Security* bzw. *Usable Privacy* bezeichnet. Besonders wichtig ist Usable Security und Privacy bei der Digitalisierung der Arbeitswelt. Überall dort, wo die Nutzer:innen ihrer Arbeit nachgehen müssen, muss der einfachste Weg durch eine Anwendung auch der sicherste sein [1]. Angemessene Sicherheits- und Datenschutztechnologien, die von den Benutzer:innen verstanden sowie effektiv, effizient und zufriedenstellend genutzt werden können, sind grundlegende Faktoren für einen effektiven Schutz von Privat- und Unternehmensdaten.

Die Usability von sicherheits- bzw. privatheitsfördernden Verfahren ist somit eine Schlüsseleigenschaft, die die individuellen Anforderungen aller beteiligter Gruppen von Benutzer:innen sowohl in Entwicklungsprozessen als auch im produktiven Einsatz berücksichtigen muss. *Usable Security* bezeichnet den inter- und transdisziplinären Ansatz, sicherheitsfördernde Verfahren für digitale Produkte und Dienstleistungen so auszugestalten, dass Benutzer:innen bei ihren sicherheitsrelevanten Zielen und Vorhaben bestmöglich unterstützt werden. Hierdurch werden z. B. auch Lai:innen und technikferne Anwender:innen in die Lage versetzt, Sicherheitselemente und deren Notwendigkeit zumindest grundlegend zu verstehen und die Elemente in der dafür vorgesehenen Weise zu verwenden. *Usable Privacy* verfolgt äquivalente Ziele und fokussiert dabei auf Technologien zur Förderung der Privatheit in digitalen Systemen und Plattformen.

Viele Lösungen zum Schutz der Privatsphäre erreichen geltende Usability-Standards bislang nicht. Eine im Januar 2021 publizierte Studie zum benutzerfreundlichen Datenschutz in cloudbasierten Office-Lösungen hat klaffende Lücken in den bereitgestellten Funktionen und Daten der Privacy Dashboards festgestellt [14]. Diese bilden die Betroffenenrechte aktuell nur unzureichend ab, was sich z. B. durch eine Beschränkung auf die anbieterspezifischen Datenverarbeitungen, lücken- oder fehlerhafte Datenübersichten und Datenexport sowie inkonsistentes bzw. unerwartetes Verhalten (z. B. "privater" Kalendereintrag für Administratoren einsehbar) äußert. In einem weiteren Beispiel aus dem privaten Umfeld erfordern Sprachassistenten wie Amazon Alexa den Wechsel zu einem anderen Interface, um umfassende Privatsphäreeinstellungen vornehmen zu können. Somit wird Nutzer:innen mit geringem technischem Verständnis oder eingeschränkten Sehfähigkeiten der Zugang dazu erschwert. Auch andere Methoden und Werkzeuge zum Selbstdatenschutz erfordern in der Regel ein hohes technisches Verständnis der Anwender:innen. Den Bedarf an guten Lösungen zeigt auch eine aktuelle Studie des Arbeitskreises "Usable Security & Privacy" der German UPA auf: Seitdem die Europäische Datenschutzgrundverordnung gilt, müssen sich zwei Drittel der Usability Professionals öfter als zuvor mit der Umsetzung von Betroffenenrechten (z. B. Auskunftsrecht, Recht auf Vergessenwerden) beschäftigen.

Die Verunsicherung zeigt sich beispielsweise bei der Umsetzung der ePrivacy-Richtlinie ("Cookie-Richtlinie"), die zuletzt 2009 geändert wurde. In den letzten Jahren hat sich eine Praxis bei der Gestaltung und technischen Umsetzung von Cookie-Bannern etabliert, die sowohl datenschutzrechtlich [15] als auch aus Usability-Sicht [3] – Stichworte Nudging und Dark Patterns – umstritten ist. Durch sogenannte PIMS (Personal Information Management Systems) soll nun eine zentrale Einwilligungsverwaltung durch eine technische und datenschutzfreundliche Gestaltung ermöglicht werden [2]; Rechtsgrundlage ist § 26 des am 1. Dezember 2021 in Kraft getretenen TTDSG. Allerdings sind auch diese PIMS umstritten, da das Auslesen einer neuen zentralen Einwilligungsverwaltung, auf die z. B. Browser und

Veröffentlicht durch die Gesellschaft für Informatik e.V.
in K. Marky, U. Grünefeld & T. Kosch (Hrsg.):
Mensch und Computer 2022 – Workshopband, 04.-07. September 2022, Darmstadt

https://doi.org/10.18420/muc2022-mci-ws01-101

Plugins (bzw. deren Hersteller) zugreifen können, zu ganz neuen, gravierenden Datenschutzproblemen führen kann [9].

2 ZIELE UND INHALTE DES WORKSHOPS

Der Workshop "Usable Security und Privacy" ist seit 2015 Teil der Konferenz "Mensch und Computer". Ziel der achten Auflage ist es, dieses etablierte Forum, in dem sich Expert:innen aus Wissenschaft und Praxis zum Thema nutzerfreundliche Technologien zur Gewährleistung von Informationssicherheit und Privatsphäre austauschen können, zu festigen und weiterzuentwickeln. Zugleich soll der Workshop die Diskussion für ein breiteres Fachpublikum öffnen.

Interessent:innen können Forschungs- und Entwicklungsarbeiten - auch in noch frühen Stadien - in deutscher oder englischer Sprache einreichen. Mögliche Beitragstypen sind:

- neue Vorgehensweisen oder Werkzeuge,
- gestalterische Studien, z. B. UI-Gestaltung, Persuasive Design,
- Berichte praktischer Umsetzung (erfolgreiche Beispiele, untaugliche Ansätze),
- Systemdemonstrationen,
- praxiserprobte Methoden, Best Practices,
- kritische Reflexionen (Herausforderungen, Fallstricke),
- Replikationsstudien,
- theoretische/zukunftsweisende Arbeiten,
- laufende Forschungs- und Entwicklungsprojekte,
- Betrachtungen besonderer Benutzergruppen (z. B. Kinder, Senior:innen, Arbeitnehmer:innen, Softwareentwickler:innen, Administrator:innen).

Thematisch möchte der Workshop ein möglichst breites Spektrum abdecken. Einige aktuelle Beispiele sind:

- neuartige Interaktionsformen und Benutzeroberflächen, z. B. Voice User Interfaces,
- konkrete UI-Gestaltung, z. B. bei Video-Konferenzsystemen,
- konkrete Anwendungen/Erfahrungen aus der Praxis,
- Erfahrungen aus den ersten vier Jahren DSGVO-Anwendung,
- Security Awareness vs. Usable Security.

Der Schwerpunkt dieses Workshops liegt auf Usable Security und Privacy. Der Workshop findet in enger Abstimmung mit der Fachgruppe "Usable Safety & Security" im Fachbereich Mensch-Computer-Interaktion (MCI) der Gesellschaft für Informatik (GI) statt, die federführend den "9. Workshop Mensch-Maschine-Interaktion in sicherheitskritischen Systemen" organisiert. Einreichungen aus dem Umfeld von Usable Safety verweisen wir auch auf diesen Workshop.

Die angenommenen Beiträge werden in Vorträgen vorgestellt und mit dem gesamten Auditorium diskutiert. Zudem wurde wie in den vergangenen Jahren angeboten, die schriftlichen Einreichungen zu publizieren.

Das Ergebnis des Workshops ist eine dokumentierte Sammlung von neuen Entwicklungen und Forschungsergebnissen im Bereich Usable Security und Privacy im Workshopband der Mensch und Computer 2022.

3 PROGRAMMKOMITEE

Das Programmkomitee des Workshops übernahm die fachliche und inhaltliche Begutachtung der Einreichungen und unterstützte die Verbreitung des Call for Papers zum Workshop. Die Mitglieder des Programmkomitees sind anerkannte Expert:innen auf dem Gebiet der Usable Security und Privacy aus Wissenschaft und Praxis:

- Florian Alt (Universität der Bundeswehr München, DE)
- Denis Feth (Fraunhofer IESE, DE)
- Peter Gorski (infodas, DE)
- Timo Jakobi (Universität Siegen, DE)
- Marian Magraf (FU Berlin, DE)
- Tilo Mentler (Hochschule Trier, DE)
- Christian Reuter (TU Darmstadt, DE)
- Jan Tolsdorf (Hochschule Bonn-Rhein-Sieg, DE)
- Stephan Wiefling (Hochschule Bonn-Rhein-Sieg, DE)

Alle eingereichten Beiträge wurden durch die Mitglieder des Programmkomitees in einem Double-Blind-Peer-Review-Verfahren begutachtet. Jede Einreichung wurde von drei Gutachtern bewertet. Auswahlkriterien für die Annahme waren die Relevanz, Originalität und wissenschaftliche Qualität des Beitrags, eine klare Beschreibung des Lösungsansatzes und ein überzeugender Beleg für dessen Nützlichkeit. In diesem Jahr wurden die Autoren dabei erstmals mit einem Shepherding-Prozess unterstützt, in dem den Autoren jeweils ein Mitglied des Organisationsteams für Rückfragen zu den Reviewkommentaren zur Verfügung stand.

4 AKZEPTIERTE BEITRÄGE UND KEYNOTE

Das Workshop-Programm besteht im Wesentlichen aus einer eingeladenen Keynote und den angenommenen Beiträgen.

In seiner Keynote geht Denis Feth auf die benutzerfreundliche Umsetzung von Datensouveränität in sogenannten digitalen Ökosystemen ein. Dies sind komplexe sozio-technische Systeme, in denen meist eine Vielzahl von Unternehmen und Menschen miteinander kooperieren. Die Verarbeitung sensibler Daten ist eine Voraussetzung für das Funktionieren dieser Systeme, Usability und positive UX für deren Akzeptanz.

Von den eingereichten Beiträgen wurden fünf Arbeiten für das Programm des Workshops akzeptiert, die im Folgenden kurz vorgestellt werden. Die vollständigen Papiere sind im Workshopband der Mensch und Computer 2022 enthalten.

In der Arbeit "The Implementation of Protective Measures and Communication of Cybersecurity Alerts in Germany - A Representative Survey of the Population" [5] untersuchen die Autoren Kaufhold et. al mittels einer repräsentativen Umfrage unter deutschen Bürger:innen, wie diese die Bedrohungslage durch Cyberangriffe sowie mögliche Schutzmaßnahmen in Deutschland einschätzen. Daneben wurden die Bürger:innen nach ihren Informationsbedarfen und präferierten Kommunikationskanälen im Kontext der Cybersicherheit befragt. Demnach fühlen sich große Teile der Bevölkerung nicht ausreichend informiert und wenden im privaten Kontext vor allem Sicherheitsmaßnamen an, die vom Anbieter oder Hersteller erzwungen werden, z.B. eine Zweifaktor-Authentisierung. Weiterhin ist das Vertrauen gegenüber den deutschen Sicherheitsbehörden eher gering und Einrichtungen wie die Computer Emergency Response Teams (CERTs) der Bundesländer sind weitgehend unbekannt. Es ist festzuhalten, dass in diesem Zusammenhang noch erheblicher Nachholbedarf hinsichtlich der Aufklärung der deutschen Bevölkerung besteht.

Kühn et al. schlagen in ihrem Beitrag "The Notion of Relevance in Cybersecurity" [7] eine neuartige Kategorisierung von IT-Sicherheitswerkzeugen vor und leiten entsprechende Begriffe der Relevanz ab. Angemessene Cybersicherheit erfordert zeitnahe und relevante Informationen. Manuelles Zusammenzutragen

dieser Informationen ist sehr zeitaufwendig und Automatisierungsansätze bieten hierbei die Möglichkeit Abhilfe zu schaffen, benötigen jedoch entsprechende Relevanzkonzepte.

In der Arbeit "PassGlobe: Ein Shoulder-Surfing resistentes Authentifizierungsverfahren für Virtual Reality Head-Mounted Displays" [8] gehen Länge et al. auf die Nutzung virtueller Erlebniswelten ein und befassen sich mit der nutzerfreundlichen Authentifizierung in derartigen Umgebungen, die technisch durch Head-Mounted-Displays realisiert werden. Da diese Geräte auch im Beisein anderer Personen verwendet werden und die Bewegungen bei der Authentifizierung nicht verborgen werden können, sind auch die von der passwortbasierten Authentifizierung bekannten Shoulder-Surfing-Angriffe in diesen Umgebungen ein relevantes Risiko. Die Autor:innen schlagen in ihrer Arbeit ein graphisches Authentifizierungsverfahren names PassGlobe vor, das resistent gegen diese Angriffsklasse sein soll. Bestimmte Punkte auf einer Weltkarte dienen als Passwörter. Die Weltkarte mit den Punkten wird auf eine Kugel projiziert und bei jeder Authentifizierung in eine zufällige Ausgangsposition rotiert. Darüber hinaus wird die Kugel nach jeder Eingabe zufällig gedreht. Die Autor:innen planen noch eine empirische Evaluierung von PassGlobe.

Stöver et al. [13] untersuchten, ob Cookie-Einwilligungserklärungen benutzerfreundlich gestaltet werden können mittels sog. Consent Management Platforms (CMP). Solche Plattformen werden von Websitebetreibern genutzt, in der Erwartung, damit Einwilligungserklärungen erzeugen zu können, die der DSGVO entsprechen. Die Ergebnisse haben sie in ihrer Publikation "Website operators are not the enemy either - Analyzing options for creating cookie consent notices without dark patterns" festgehalten.

Kqiku et al. [6] präsentieren in ihrem Beitrag "Exploration of a Mobile Design for a Privacy Assistant to Help Users in Sharing Content in Online Social Networks" einen Ansatz zum Schutz der Privatheit in sozialen Netzen. Ein Assistent unterstützt die Benutzer:in bei der Bestimmung der Empfänger:innen einer Nachricht. Der Empfängerkreis wird in Abhängigkeit von der Sensitivität des Nachrichteninhalts bestimmt. Eine für mobile Geräte konzipierte Benutzeroberfläche stellt sowohl die Nachirichtensensitivität mittels einer Ampelfarbskala als auch den Empfängerkreis mittels einer Radarnetzstruktur visuell dar. Eine Usability-Studie mit zehn Probanden lieferte erste Hinweise auf die gute Verständlichkeit des Ansatzes (SUS-Score von 70,75).

5 ORGANISATION UND DURCHFÜHRUNG

Die Durchführung des Workshops erfolgt durch die vier folgenden Organisator:innen:

- Luigi Lo Iacono (Hochschule Bonn-Rhein-Sieg)
- Hartmut Schmitt (HK Business Solutions GmbH)
- Svenja Polst (unabhängig)
- Andreas Heinemann (Hochschule Darmstadt)

in Zusammenarbeit mit dem Arbeitskreis Usable Security & Security der German UPA und dem Projekt "D'accord – Adaptive Datenschutz-Cockpits in digitalen Ökosystemen".

DANKSAGUNG

Die Organisator:innen möchten nochmals allen Autor:innen danken, die den Workshop mit ihren Einreichungen bereichert haben. Außerdem gebührt den Mitglieder:innen des Programmkomitees ein herzlicher Dank, die die Einreichungen mit konstruktiven und ausführlichen Gutachten bewertet haben. Diese Arbeit wurde vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des Projekts "D'accord – Adaptive Datenschutz-Cockpits in digitalen Ökosystemen" unterstützt.

LITERATUR

[1] Computerweekly. 2020. Coronavirus shines spotlight on cyber security. :https://www.computerweekly.com/news/252486216/Coronavirus-shines-spotlight-on-cyber-security Abgerufen am 22.02.2021.
[2] Datenethikkommission der Bundesregierung. 2019. Gutachten der Datenethikkommission. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf
[3] datenschutz notizen. 2021. Neue Nudging-Nuancen bei Cookie-Bannern. https://www.datenschutz-notizen.de/neue-nudging-nuancen-bei-cookie-bannern-3031373/
[4] Europäische Kommission. 2021. Deutschland im digitalen Vergleich in der EU auf Platz elf. https://germany.representation.ec.europa.eu/news/deutschland-im-digitalen-vergleich-der-eu-auf-platz-elf-2021-11-12_de
[5] M.-A. Kaufhold, J. Bäumler, and C. Reuter. 2022. The Implementation of Protective Measures and Communication of Cybersecurity Alerts in Germany - A Representative Survey of the Population. In *Proceedings of the Mensch und Computer 2022, 8. Usable Security und Privacy Workshop.* https://doi.org/10.18420/muc2022-mci-ws01-228
[6] L. Kqiku, J. Dieterle, and D. Reinhardt. 2022. Exploration of a Mobile Design for a Privacy Assistant to Help Users in Sharing Content in Online Social Networks. In *Proceedings of the Mensch und Computer 2022, 8. Usable Security und Privacy Workshop.* https://doi.org/10.18420/muc2022-mci-ws01-461
[7] P. Kühn, J. Bäumler, M.-A. Kaufhold, M. Wendelborn, and C. Reuter. 2022. The Notion of Relevance in Cybersecurity: A Categorization of Security Tools and Deduction of Relevance Notions. In *Proceedings of the Mensch und Computer 2022, 8. Usable Security und Privacy Workshop.* https://doi.org/10.18420/muc2022-mci-ws01-220
[8] T. Länge, P. Matheis, R. Düzgün, P. Mayer, and M. Volkamer. 2022. PassGlobe: Ein Shoulder-Surfing resistentes Authentifizierungsverfahren für Virtual Reality Head-Mounted Displays. In *Proceedings of the Mensch und Computer 2022, 8. Usable Security und Privacy Workshop.* https://doi.org/10.18420/muc2022-mci-ws01-462
[9] Malte Engeler. 2021. Stellungnahme – Ausschussdrucksache 19(9)1056 – 20. April 2021. https://www.bundestag.de/resource/blob/836166/e95c01bdb37ed9f6c08ef027cd902e47/19-9-1056_Stellungnahme_SV_Dr-_Engeler_oeATTDSG_21-04-2021-data.pdf
[10] Presse- und Informationsamt der Bundesregierung. 2021. Bundesregierung beschließt Datenstrategie. https://www.bundesregierung.de/breg-de/themen/digitalisierung/datenstrategie-beschlossen-1842786
[11] Presse- und Informationsamt der Bundesregierung. 2021. Digitalisierung gestalten. https://www.bundesregierung.de/breg-de/service/publikationen/digitalisierung-gestalten-1605002
[12] SPD, Bündnis 90/Die Grünen, and FDP. 2021. MEHR FORTSCHRITT WAGEN. BÜNDNIS FÜR FREIHEIT, GERECHTIGKEIT UND NACHHALTIGKEIT. https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800 Abgerufen am 9. Januar 2022.
[13] A. Stöver, N. Gerber, C. Cornel, M. Henz, K. Marky, V. Zimmermann, and J. Vogt. 2022. Website operators are not the enemy either - Analyzing options for creating cookie consent notices without dark patterns. In *Proceedings of the Mensch und Computer 2022, 8. Usable Security und Privacy Workshop.* https://doi.org/10.18420/muc2022-mci-ws01-458
[14] J. Tolsdorf, F. Dehling, and D. Feth. 2021. Benutzerfreundlicher Datenschutz in Cloud-basierten Office-Paketen. *Datenschutz und Datensicherheit - DuD* 45, 1 (Jan. 2021), 33–39. https://doi.org/10.1007/s11623-020-1386-x
[15] Verwaltungsgerichtsbarkeit Hessen. 2021. Cookie-Dienst. https://verwaltungsgerichtsbarkeit.hessen.de/presse/website-der-hochschule-rheinmain