

7. Usable Security und Privacy Workshop

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

Svenja Polst
svenja.polst@iese.fraunhofer.de
Fraunhofer IESE

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

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

ZUSAMMENFASSUNG

Auch die mittlerweile siebte Ausgabe des wissenschaftlichen Workshops "Usable Security und Privacy" auf der Mensch und Computer 2021 wird aktuelle Forschungs- und Praxisbeiträge präsentiert und anschließend mit allen Teilnehmer:innen diskutiert. Zwei Beiträge befassen sich dieses Jahr mit dem Thema Privatsphäre, zwei mit dem Thema Sicherheit. Mit dem Workshop wird ein etabliertes Forum fortgeführt und weiterentwickelt, in dem sich Expert:innen aus unterschiedlichen Domänen, z. B. dem Usability- und Security-Engineering, transdisziplinär austauschen können.

CCS CONCEPTS

• Security and privacy → Social aspects of security and privacy; Usability in security and privacy.

KEYWORDS

Usable Security, Usable Privacy

1 INTRODUCTION

Die Digitalisierung hat durch die Corona-Pandemie nochmals einen Schub erfahren. In nahezu allen Wirtschaftszweigen haben Unternehmen ihre Prozesse digitalisiert, um die Arbeitsfähigkeit während der Corona-Pandemie sicherzustellen und um besser auf künftige Krisen vorbereitet zu sein. Nach einer Bitkom-Umfrage [2] nutzen rund 80 % der Unternehmen heute Videokonferenzen und digitale Kollaborationstools, über 60 % setzen auf digitale Dokumente und digitale Signaturen. 70 % der Firmen haben Homeoffice eingeführt oder planen dies aktuell.

Doch es gibt auch Digitalisierungshemmnisse: Als die zwei größten Hürden bei der Digitalisierung werden von den Unternehmen die Anforderungen an den Datenschutz (69 %) und die technische Sicherheit (58 %) wahrgenommen [2]. Und nicht nur für die Digitalisierung, auch für die Cyber-Gefährdungslage war Corona ein Treiber [4]. Da schnell Lösungen hermussten, wurden viele Maßnahmen – Wechsel der Beschäftigten ins Homeoffice, Bring-your-own-Device, Einrichtung von Videokonferenzen – sehr spontan umgesetzt. IT- und Datensicherheit spielten dabei oft nur eine untergeordnete Rolle. In der Folge gab es durch Corona deutlich mehr

Angriffsmöglichkeiten, zugleich war die Verfügbarkeit und Einsatzfähigkeit von IT-Security-Fachpersonal durch die Beschränkungen erschwert [5].

Vor diesem Hintergrund – verschärfte Gefährdungslage bei gleichzeitig gestiegenen Anforderungen an Datenschutz und Sicherheit – besteht eine der wesentlichen Herausforderungen darin, eine gute Balance zwischen Sicherheit und Benutzerfreundlichkeit herzustellen. Denn insbesondere dort, wo die Nutzer:innen ihrer Arbeit nachgehen müssen, muss der Weg des geringsten Widerstands immer auch der sicherste Weg sein [3]. 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. privatsphärefördernden 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. 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 [9]. 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 Privatsphäreinstellungen vornehmen zu können. Somit wird Nutzer:innen mit geringem technischem Verständnis oder eingeschränkten Sehfähigkeiten der Zugang dazu erschwert. Auch andere Methoden und Werkzeuge zum Selbstschutz 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.

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

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

Mensch und Computer 2021, Workshopband, Workshop on 7. Usable Security und Privacy Workshop

© Copyright held by the owner/author(s).

<https://doi.org/10.18420/muc2021-mci-ws14-124>

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.

2 ZIELE UND INHALTE DES WORKSHOPS

Ziel des 7. Usable Security und Privacy Workshops ist es, das etablierte Forum zu festigen und weiterzuentwickeln, in dem sich Expert:innen aus Wissenschaft und Praxis zum Thema benutzerfreundlicher Technologien zur Gewährleistung der Informationssicherheit und Privatheit austauschen können. Zugleich soll durch den Workshop die Diskussion für ein breiteres Fachpublikum geöffnet werden. 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 drei Jahren DSGVO,
- 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 “8. 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 soll wie in den vergangenen Jahren angeboten werden, die schriftlichen Einreichungen zu publizieren.

Neben den Publikationen sollen für den 7. Usable Security und Privacy Workshop auf der Mensch und Computer 2021 auch interaktive Beiträge eingereicht werden können. Die Art des Beitrages

ist relativ offen, soll sich aber deutlich von einem Vortrag unterscheiden. Denkbar sind kurze, moderierte Gruppenarbeitsphasen aber auch Übungen mit neuartigen Werkzeugen. Für diese Beitragsart soll eine kurze Beschreibung des Themas und des geplanten Formats eingereicht werden.

Das Ergebnis des Workshops ist eine dokumentierte Sammlung von neuen Entwicklungen und Forschungsergebnissen im Bereich Usable Security und Privacy in den Proceedings der „Mensch und Computer 2021“ sowie – für den zweiten Teil – ein intensiver Wissensaustausch zwischen den Teilnehmer:innen auf Basis der Interaktion am Workshoptag, der ebenfalls in geeigneter Form dokumentiert und veröffentlicht wird.

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:

- Yasemin Acar (Leibniz Universität Hannover, DE)
- Florian Alt (Universität der Bundeswehr München, DE)
- Jens Bender (BSI, DE)
- Zinaida Benenson (FAU Erlangen-Nürnberg, DE)
- Alexander de Luca (Google, DE)
- Markus Dürmuth (Ruhr-Universität Bochum, DE)
- Denis Feth (Fraunhofer IESE, DE)
- Simone Fischer-Hübner (Karlstad University, SE)
- Peter Gorski (infodas, DE)
- Marit Hansen (ULD Schleswig-Holstein, DE)
- Timo Jakobi (Universität Siegen, DE)
- Marian Magraf (FU Berlin, DE)
- Tilo Mentler (Hochschule Trier, DE)
- Sebastian Möller (TU Berlin, DE)
- Delphine Reinhardt (Universität Göttingen, DE)
- Christian Reuter (TU Darmstadt, DE)
- Matthew Smith (Universität Bonn, DE)
- Gunnar Stevens (Universität Siegen, DE)
- Jan Tolsdorf (Hochschule Bonn-Rhein-Sieg, DE)
- Stephan Wiefing (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.

4 AKZEPTIERTE BEITRÄGE

Von den eingereichten Beiträgen wurden vier Arbeiten für das Programm des Workshops akzeptiert, die im Folgenden kurz vorgestellt werden. Die vollständigen Papiere sind im Workshopband der Mensch und Computer 2021 enthalten.

In der Arbeit “Privacy Needs Reflection: Conceptual Design Rationales for Privacy-Preserving Explanation User Interfaces” [8]

gehen Sörries et al. auf Datenschutzherausforderungen beim Machine Learning im Medizinbereich ein. Anhand eines realen Anwendungsfalls aus dem Gesundheitswesen wird vorgestellt, wie Bedürfnisse der relevanten Stakeholder im Designprozess berücksichtigt und erfolgversprechende Ansätze, z. B. Differential Privacy, integriert werden können.

Schmitt et al. [6] präsentieren in ihrem Beitrag “Willingness to Pay for the Protection of Different Data Types” Studienergebnisse zum monetären Wert, den Verbraucher ihrer Privatsphäre bzw. verschiedenen Datenkategorien beimessen. Das herkömmliche Notice-and-Choice-Prinzip von Datenschutzrichtlinien bietet den Verbrauchern keine ausreichende Kontrolle über ihre persönliche Datenschutzpräferenzen. Die Studienergebnisse ermöglichen einen Einblick, welche Datenkategorien von den Nutzern als wie wertvoll wahrgenommen werden.

In ihrer Arbeit “Evaluation der interaktiven NoPhish Präsenzschulung” [1] werfen Berens et al. einen neuen Blick auf die Effektivität von Security-Awareness-Maßnahmen im Kontext von Phishing-Angriffen. Da die bisherige Forschung den Effekt meist unmittelbar nach der Durchführung der Maßnahme misst, wurde im Rahmen einer Studie untersucht, wie lange der Effekt einer Präsenzschulung anhält und wann sinnvollerweise eine Auffrischungsmaßnahme durchgeführt werden sollte.

Steinegger & Zinßer [7] gehen in dem Beitrag “Erfahrungen bei der UX-getriebenen Entwicklung Privatsphäre-schonender Anwaltssoftware” auf das besondere Spannungsverhältnis von Benutzbarkeit und Sicherheit bei Anwälten und Kanzleien ein, insbesondere die Sicherheitsvorbehalte gegenüber Cloud-Software. Anhand eines Praxisbeispiels zeigen sie, wie Sicherheit und Datenschutz in einen UX-getriebenen agilen Entwicklungsprozess integriert und mit der entwickelten Software die zentralen Prozesse einer Kanzlei bzw. eines Steuerberatungsbüros unterstützt werden können.

5 ORGANISATION UND DURCHFÜHRUNG

Die Durchführung des Workshops erfolgt durch die vier folgenden Organisatoren:

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

in Zusammenarbeit mit dem Arbeitskreis Usable Security & Security der German UPA und dem Projekt “TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen”.

DANKSAGUNG

Die Organisatoren 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 unterstützt vom Bundesministerium für Bildung und Forschung (BMBF) im Projekt “TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen”.

LITERATUR

- [1] B. Berens, L. Aldag, and M. Volkamer. 2021. Evaluation der interaktiven NoPhish Präsenzschulung. In *Proceedings of the Mensch und Computer 2021 Workshop on «7. Usable Security und Privacy Workshop»*. <https://doi.org/10.18420/muc2021-mci-ws14-394>
- [2] Bitkom. 2020. Corona treibt Digitalisierung voran – aber nicht alle Unternehmen können mithalten. <https://www.bitkom.org/Presse/Presseinformation/Corona-treibt-Digitalisierung-voran-aber-nicht-alle-Unternehmen-koennen-mithalten> Abgerufen am 22.02.2021.
- [3] 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.
- [4] Bundesamt für Sicherheit in der Informationstechnik. 2020. BSI-Lagebericht: Corona verschärft Cyber-Gefährdungslage. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/Lagebericht_201010.html Abgerufen am 22.02.2021.
- [5] Bundesamt für Sicherheit in der Informationstechnik. 2020. Die Lage der IT-Sicherheit in Deutschland. <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf> Abgerufen am 22.02.2021.
- [6] V. Schmitt, M. Poikela, and S. Möller. 2021. Willingness to Pay for the Protection of Different Data Types. In *Proceedings of the Mensch und Computer 2021 Workshop on «7. Usable Security und Privacy Workshop»*. <https://doi.org/10.18420/muc2021-mci-ws14-390>
- [7] R. H. Steinegger and A. Zinßer. 2021. Erfahrungen bei der UX-getriebenen Entwicklung Privatsphäre-schonender Anwaltssoftware. In *Proceedings of the Mensch und Computer 2021 Workshop on «7. Usable Security und Privacy Workshop»*. <https://doi.org/10.18420/muc2021-mci-ws14-395>
- [8] P. Sörries, C. Müller-Birn, K. Glinka, F. Boenisch, M. Margraf, S. Sayegh-Jodehl, and M. Rose. 2021. Privacy needs Reflection: Conceptual Design Rationales for Privacy-Preserving Explanation User Interfaces. In *Proceedings of the Mensch und Computer 2021 Workshop on «7. Usable Security und Privacy Workshop»*. <https://doi.org/10.18420/muc2021-mci-ws14-389>
- [9] 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>