Usability stumm geschaltet? Usable Security und Privacy in Videokonferenzsystemen

Mandy Balthasar
Universität der Bundeswehr München
Deutschland

Nina Gerber
Technische Universität Darmstadt
Darmstadt, Deutschland

Hartmut Schmitt
HK Business Solutions GmbH
Deutschland

ZUSAMMENFASSUNG

Unter Druck von außen durch die COVID-19-Pandemie erfuhren Unternehmen weltweit einen Aufschwung in der Nutzungsbilanz von Werkzeugen für computergestützte Gruppenarbeit. Die sogenannte *Computer Supported Cooperative Work (CSCW)* ermöglichte trotz Kontaktbeschränkungen die Arbeit in Gruppen durch digitale Informations- und Kommunikationstechnologien. Aufgrund einer Notlage schnell in den Arbeitsprozess integriert, wurden erst im Anschluss Schwächen im Bereich IT-Sicherheit und Datenschutz ersichtlich. Ebenso der hohen Integration verschiedener Werkzeuge in den Arbeitsalltag geschuldet sind Schwächen in der Usability. So bieten beispielsweise Videokonferenzsysteme Hürden bei der Bedienbarkeit, welche wiederum zu Lücken in der IT-Sicherheit bzw. dem Datenschutz von Unternehmen führen können. Doch welche Trends im Bereich Videokonferenzsysteme gibt es? Welche sicherheits- und privatheitsfördernde Empfehlungen werden für die Usability gegeben? Und wo liegen einzelne Defizite für *Usable Security & Privacy* von Videokonferenzsystemen? Dieser Beitrag soll erste Antworten auf diese Fragestellungen geben, welche in einem Workshop auf der Mensch und Computer 2021 gemeinsam mit den Teilnehmer:innen näher betrachtet werden.

KEYWORDS

Communications, CSCW, Enterprise, Privacy, Security, Usability, Video/Audio Conferencing

1 EINLEITUNG

Bis zum Ausbruch der COVID-19-Pandemie fristete das Homeoffice in vielen deutschen Unternehmen eher ein Schattendasein. Dies änderte sich schlagartig durch Maßnahmen wie Kontaktbeschränkungen und Bundesnotbremse. Fünfundvierzig Prozent der deutschen Berufstätigen arbeiteten, teils von heute auf morgen, ausschließlich oder teilweise im Homeoffice. [9] Insbesondere Videokonferenzlösungen erfuhren dadurch eine enorme Nachfrage.

Veröffentlicht durch die Gesellschaft für Informatik e.V. und die German UPA e.V. 2021 in E. Ludewig & T. Jackstädt (Hrsg.):
Mensch und Computer 2021 – Usability Professionals, 05.-08. September 2021, Ingolstadt

https://doi.org/10.18420/muc2021-up-448

Zahlreiche Beschäftigte wissen die Vorteile des Homeoffice zu schätzen, wie beispielsweise den Wegfall von Pendelzeiten oder ein Mehr an Flexibilität. Daneben entlastet die Arbeit im Homeoffice auch den Berufsverkehr. Da auch die Unternehmen profitieren, beispielsweise durch Einsparungen bei Dienstreisen oder durch das gemeinsame zeitlich versetzte Arbeiten an einem Arbeitsplatz, geht der BITKOM davon aus, dass die COVID-19-Pandemie der Auslöser eines tiefgreifenden und nachhaltigen Wandels in der Arbeitswelt sein wird. [9] Achtundfünfzig Prozent der Unternehmen wollen daher das Angebot zum Homeoffice auch nach der Pandemie aufrechterhalten oder ausweiten. [5]

1.1 Geänderte Arbeitsumgebung = neue Gefährdungslage

Nicht nur für Homeoffice und hybride Arbeitsmodelle, auch für die Cyber-Gefährdungslage war die COVID-19-Pandemie ein enormer Treiber. Damit der Geschäftsbetrieb aufrecht erhalten werden konnte, wurden viele Maßnahmen spontan umgesetzt, wie die Nutzung von Plattformen für Meetings per Video oder Audio. Mögliche Auswirkungen auf IT-Sicherheit und Datenschutz wurden dabei zunächst hintangestellt. [2] Zudem wurde durch Kontaktbeschränkungen die Einsatzfähigkeit von Fachpersonal für IT-Security drastisch erschwert, ebenso die Durchsetzbarkeit von IT-Sicherheits- und Datenschutzrichtlinien. In der Folge gab es durch den Wechsel von 18,8 Millionen Berufstätigen ins Homeoffice deutlich mehr Angriffsmöglichkeiten als zuvor. Dies galt insbesondere, wenn Beschäftigte auf private Endgeräte zurückgreifen mussten. Der BITKOM beziffert den durch Cyberangriffe entstandenen Gesamtschaden auf über 100 Milliarden EUR pro Jahr. [1] Mehr als ein Viertel der während der Pandemie betroffenen Unternehmen bewertete die entstandenen Schäden als existenzbedrohend. [3]

Vor diesem Hintergrund ist es wichtiger denn je, den Nutzer:innen Lösungen anzubieten, mit denen sie ihre Sicherheits- und Datenschutzziele (bzw. die des Unternehmens) möglichst einfach, ohne Hindernisse, erreichen können. Für mobiles Arbeiten, so BSI-Präsident Arne Schönbohm, bedarf es einer Balance zwischen benutzerfreundlichen Zugriffen auf Unternehmensdaten und dem Schutz der IT-Infrastruktur. [2] Insbesondere dort, wo die Nutzer:innen ihrer Arbeit nachgehen, muss der Weg des geringsten Widerstands immer auch der sicherste Weg sein. [20]

1.2 Usable Security & Privacy in Videokonferenzsystemen

Der Begriff *Usable Security & Privacy* steht für inter- und transdisziplinäre Methoden, um sicherheits- und privatheitsfördernde Maßnahmen so auszugestalten, dass deren Benutzer und Entwickler bei ihren sicherheits- bzw. datenschutzrelevanten Zielen und Vorhaben bestmöglich unterstützt werden. [21] Deshalb ist die IT-Sicherheit und der Datenschutz in interaktiven Systemen auch von Usability- und User-Experience-Professionals (UUX-Professionals) abhängig, welche meist maßgeblich das Design der Produkte gestalten. In diesem Beitrag beschreiben wir in *Kapitel 2* zunächst kurz den Markt und aktuelle Trends bei Videokonferenzsystemen. In *Kapitel 3* und *Kapitel 4* gehen wir auf Empfehlungen für die Sicherheit und den Datenschutz von Videokonferenzsystemen ein, die von Behörden wie dem BSI veröffentlicht wurden. Zudem erläutern wir, welche Eigenschaften oder Merkmale von Videokonferenzsystemen sicherheits- und datenschutzrelevant sind und stellen anhand konkreter Beispiele dar, welche Usabilityschwächen selbst die Produkte der Marktführer aufweisen. In *Kapitel 5* erläutern wir das Konzept und den Ablauf unseres Workshops, und stellen anschließend den *Arbeitskreis Usable Security & Privacy* der *German UPA* vor.

2 VIDEOKONFERENZEN – TOOLS UND TRENDS

Der weltweite Markt für Videokonferenzsysteme wird von drei Produkten dominiert, welche im Jahr 2020 auf insgesamt rund 80 Prozent Marktanteil kamen – *Microsoft Teams*, *Cisco Webex* und *Zoom*. [12] Dabei geht der Funktionsumfang von Microsoft Teams jedoch weit über ein reines Videokonferenzsystem hinaus. Mit über 40 Prozent Marktanteil ist es das am häufigsten verwendete Kollaborations- und Kommunikationstool. [17] Zoom hingegegen mauserte sich während der COVID-19-Pandemie zum führenden Videokonferenzdienst. Das Unternehmen konnte die Anzahl seiner Nutzer:innen während der ersten Welle der Pandemie bereits verdreißigfachen und die Anzahl der Unternehmenskunden innerhalb eines Jahres vervierfachen. [15] Neben den genannten großen Akteuren gibt es auch einige erfolgreiche Videokonferenzsysteme, welche branchenspezifische Erfolge feiern können. So beispielsweise im Bildungsbereich das Open-Source-Webkonferenzsystem *BigBlueButton*, welches von den Bildungsministerien mehrerer deutscher Bundesländer auf eigenen Servern gehostet und für Bildungseinrichtungen bereitgestellt wird. [14]

Betrachtet man die aktuellen Nutzungsstatistiken genauer, so fällt auf, dass nicht nur die Anzahl an Videokonferenzen steigt, sondern auch die Anzahl an Teilnehmer:innen. Sowohl bei virtuellen Meetings als auch bei Web-Seminaren hat sich die Anzahl der Teilnehmer:innen ungefähr verdoppelt. [19] Zudem verändert sich die Gruppe der Nutzer:innen. War das Videokonferenzsystem Zoom zu Beginn beispielsweise für den Einsatz im Unternehmenskontext angedacht, so entwickelte sich zunehmend auch der Einsatz im Verbrauchermarkt. [15]

Aktuelle Technologie-Trends spielen auch in Videokonferenzsystemen eine nicht zu unterschätzende Rolle. So beispielsweise der gezielte Einsatz von Künstlicher Intelligenz in der Meeting-Assistenz, als Dolmetscher oder autonomer Moderator. Aber auch der Einsatz von Mitteln zur Erweiterungen der Realitätswahrnehmung wie Augmented bzw. Virtual Reality werden genutzt, um möglichst realistische Online-Meetings zu kreieren. [16]

Durch den erhöhten Einsatz von Videokonferenzsystemen und den dadurch entstandenen Fokus, konnten bei vielen Anbietern dieser Systeme Sicherheitslücken und Datenschutzverletzungen aufgedeckt werden, welche zum Teil zeitnah geschlossen wurden. Die aus der Aufdeckung vorhandener Defizite entstandene Diskussion konnte den Aufstieg von Videokonferenzsystemen bisher jedoch nicht bremsen. [13]

> *Wenn man sich künftig zwischen mehr Sicherheit oder mehr Bequemlichkeit für die Nutzer entscheiden müsse, werde die Sicherheit den Vorrang bekommen.*
> Eric Yuan (CEO bei Zoom) [22]

Ob diese Rechnung tatsächlich aufgehen kann, wird sich erst noch zeigen müssen, denn dieser vermeintlichen Entscheidung gegenüber steht:

> *If it's not usable, it's not secure.*
> Jared Spool [18].

Aktuell gibt es zahlreiche Vergleichstest für Videokonferenzsysteme sowie Empfehlungen, worauf bei der Auswahl zu achten ist. Die Aspekte *Benutzerfreundlichkeit*, *IT-Sicherheit* und *Datenschutz* werden dabei häufig einbezogen, im Vordergrund stehen jedoch Fragen zum Funktionsumfang (z. B. Teilen des Bildschirms, gemeinsames Arbeiten u.ä.) sowie andere weitere Aspekte (z. B. unterstützende Plattformen, mögliche Anzahl an Teilnehmer:innen oder Lizenzkosten).

3 EMPFEHLUNGEN FÜR SECURITY UND PRIVACY

Zahlreiche Behörden, Verbände und Datenschutzexperten haben im Laufe der COVID-19-Pandemie Empfehlungen veröffentlicht, welche es Unternehmen ermöglichen sollen, eine datenschutzkonforme Ausgestaltung und Nutzung von Videokonferenzsystemen für ihre Mitarbeiter:innen zu verwirklichen. [4], [8] Diese Hilfestellungen, in Form von Empfehlungen, bieten meist eine sehr gute Orientierung für ganz unterschiedliche Aspekte von Videokonferenzsystemen. So werden beispielsweise Funktionen wie eine Ende-zu-Ende-Verschlüsselung oder die Aufzeichnung von Konferenzen erläutert sowie auf Aspekte wie Anbieter bzw. Serverstandorte, kommerzielle Interessen der Anbieter oder Zweit- und Drittnutzung von Daten, Bezug genommen.

Am ausführlichsten wurden relevante Bedrohungen und Schwachstellen von Videokonferenzsystemen vom *Bundesamt für Sicherheit in der Informationstechnik (BSI)* in seinem *Kompendium Videokonferenzsysteme* spezifiziert. [6] Von besonderem Interesse für das Themenfeld *Usable Security & Privacy* ist darin insbesondere das Kapitel *5.2.6 Fehlerhafte Bedienung und Nutzung*. Darin wird beschrieben, wie aufgrund der Vielzahl von Funktionen, die für Anwender:innen nicht immer überschaubar und beherrschbar sind, die Gefahr einer fehlerhaften Bedienung, Nutzung und Konfiguration entsteht, welche sogar einen unbeabsichtigten Datenabfluss zur Folge haben kann.

Ein besonderes Gefahrenpotenzial für eine fehlerhafte Bedienung besteht, laut BSI, vor allem bei der Vernetzung eines Videokonferenzsystems mit weiteren Diensten, da hier die Komplexität des Gesamtsystems für die Nutzer:innen oft nicht mehr überschaubar ist. Als beispielhaftes Szenario kann der unberechtigte Zugriff von Teilnehmer:innen auf eine Dateiablage mit vertraulichen Daten genannt werden. Neben spezifischen Gefährdungen verweist das Kompendium Videokonferenzsysteme des BSI auch auf allgemeingültige, elementare Gefährdungen, welche im *IT-Grundschutz-Kompendium* definiert sind und auch für Videokonferenzsysteme gelten (z. B. die fehlerhafte Nutzung oder Administration von Enderäten und Systemen). [7] Die Kompendien des BSI spezifizieren detailliert die sich aus unterschiedlichen Gefährdungen ergebenden Anforderungen an Anwendungen und deren zentrale Komponenten, an Endgeräte und Clients und an das Netzwerk sowie an die Planung und den Betrieb. Analog zum IT-Grundschutz-Kompendium sind die Anforderungen im Kompendium Videokonferenzsysteme ebenfalls in Basis- und Standardanforderungen abgestuft – also in Anforderungen, welche umgesetzt werden müssen bzw. sollten – sowie in Anforderungen für einen erhöhten Schutzbedarf. Zudem gibt das speziell auf Videokonferenzsysteme zugeschnittene Kompendium konkrete Umsetzungsempfehlungen und beschreibt anhand von Beispielkonzepten, wie die Sicherheitsanforderungen und -maßnahmen in unterschiedlichen Nutzungsszenarien berücksichtigt werden können.

4 BEISPIELE DER USABILITY VON SECURITY- UND PRIVACY-FUNKTIONEN

Im folgenden Abschnitt soll beispielhaft aufgezeigt werden, welche Schwächen die Usability in Funktionen hat, die für IT-Sicherheit und Datenschutz besonders relevant sind. Zu diesem Zweck werden die Einrichtung der Ende-zu-Ende-Verschlüsselung in Zoom sowie die Verwaltung der Privatsphäre-Einstellungen in dem Onlinedienst *Discord* beschrieben.

4.1 Aktivierung der Ende-zu-Ende-Verschlüsselung in Zoom

Ein Beispiel für mangelhafte Usability stellt die Aktivierung der Ende-zu-Ende-Verschlüsselung in der Videokonferenzsoftware Zoom dar. Die Ende-zu-Ende-Verschlüsselung ist bei Zoom keine vorhandene Voreinstellung, sondern muss proaktiv von den Nutzer:innen angestoßen werden. Um Meetings mit Ende-zu-Ende-Verschlüsselung in der Software planen zu können, muss diese Funktion zunächst im eigenen Profil auf der Zoom-Website aktiviert werden (siehe Abbildung 1). Dabei wird man darüber informiert, dass eine Nutzung der Ende-zu-Ende-Verschlüsselung mit einer Einschränkung der Funktionalität erkauft werden muss – beispielsweise ist dann das Einwählen per Telefon nicht mehr möglich und es können keine Funktionen, wie Breakout Rooms oder Umfragen, mehr für die Online-Meetings genutzt werden.

Wer bereit ist, zum Schutz der Privatsphäre auf zum Teil grundlegende Funktionalitäten zu verzichten, muss nach Aktivierung der Ende-zu-Ende-Verschlüsselung auf der Website weitere Maßnahmen ergreifen. Beim Erstellen bzw. Planen eines neuen Meetings in der App muss so unter dem Punkt *Verschlüsselung* eine Ende-zu-Ende-Verschlüsselung gesondert ausgewählt (siehe Abbildung

Abbildung 1: Aktivierung der Verschlüsselung [11].

2) werden. Im Gegensatz zur Website wird sie hier jedoch nicht mehr als *End-to-End-Verschlüsselung* bezeichnet, sondern als *Durchgehende Verschlüsselung*. Obwohl die Wortwahl den Grundgedanken hinter der Ende-zu-Ende-Verschlüsselung widerspiegelt – die Verschlüsselung erfolgt durchgehend zwischen den beteiligten Gesprächspartnern und damit erfolgt keine Entschlüsselung *auf dem Weg* zu den Zoom-Servern – wird dies nur für technisch versierte Nutzer:innen eindeutig sein. Wird dann die entscheidende Frage nach einer *erweiterten* oder einer *durchgehenden Verschlüsselung* gestellt, könnte der Ausdruck *erweitert* eine mindestens gleichwertige, wenn nicht sogar höhere Sicherheit suggerieren, als dies der Begriff einer *durchgehenden* Verschlüsselung verspricht.

Abbildung 2: Einstellung der Verschlüsselung für Meetings [11].

Innerhalb eines Meetings wird die Art der Verschlüsselung über ein kleines Icon in der linken oberen Ecke angezeigt (siehe Abbildung 3). Ist das Meeting Ende-zu-Ende-verschlüsselt, wird ein Schloss innerhalb eines grünen Schildes angezeigt, ansonsten ein Haken. Das Symbol ist schnell zu übersehen und ebenso schwierig zu deuten. Nutzer:innen, welche lediglich am Meeting teilnehmen und dieses eben nicht selbst erstellt und eingerichtet haben, werden kaum auf die Art der Verschlüsselung aufmerksam gemacht.

Abbildung 3: Anzeige der Verschlüsselungsart im Meeting, a) Ende-zu-Ende-Verschlüsselung, b) Einfache Verschlüsselung [11].

Klickt man auf ein Icon, öffnet sich ein Kasten, in welchem die Verschlüsselungsart (erneut als *erweitert* oder *durchgehend* bezeichnet) als Text dargestellt wird. Zudem gibt es die Möglichkeit, die Verbindung zu *Verifizieren*, indem man auf das entsprechende Wort klickt. Hierfür wird ein aus mehreren Blöcken bestehender Zahlencode angezeigt (siehe Abbildung 4). Ist dieser bei allen teilnehmenden Nutzer:innen identisch, gilt die Verbindung als verifiziert, dies bedeutet, niemand hat sich in einer sogenannten *Man-in-the-middle-Attacke* zwischengeschaltet, um die Ende-zu-Ende-Verschlüsselung der Videokonferenz zu umgehen.

Das gegenseitige Vorlesen und Vergleichen eines Codes durch zahlreiche Teilnehmer:innen kann im Rahmen eines Online-Meetings

Abbildung 4: Verifikation über Sicherheitscode [11].

einiges an Aufwand bedeuten. Hinzukommt, dass den Nutzer:innen keinerlei weiterführende Informationen über die Funktionsweise der Verschlüsselung oder den Zweck bzw. die Relevanz der Verifizierung an die Hand gegeben werden. Insgesamt birgt die Implementierung der Ende-zu-Ende-Verschlüsselung aus Usability-Sicht einiges an Verbesserungspotential.

4.2 Verwaltung der Privatsphäre-Einstellungen in Discord

Inwiefern eigene Daten im Rahmen von Online-Meetings erfasst und ausgewertet werden, lässt sich bei vielen Programmen und Diensten in den Privatsphäre-Einstellungen steuern. Ruft man diese im Videokonferenzsystem Discord auf (unter den Punkten *Benutzereinstellungen -> Privatsphäre & Sicherheit*) bietet sich zuerst die Einstellungsmöglichkeit, wie Discord mit empfangenen Direktnachrichten umgehen soll (siehe Abbildung 5). Hier sticht als Erstes eine ungewöhnliche, wenig technische Formulierung ins Auge: die Optionen umfassen *Die Welt ist böse*, *Meine Freunde sind nett* und *Nicht überprüfen*. Intuitiv könnte davon ausgegangen werden, dass die erste Option, (*Die Welt ist böse*), die passende für Nutzer:innen ist, welchen der Schutz ihrer Daten am Herzen liegt und der digitalen Welt eher misstrauisch gegenüberstehen, während bei der zweiten Option (*Meine Freunde sind nett*) eher Vertrauen ausdrückt wird. Tatsächlich ist es aber genau umgekehrt, ein *Die Welt ist böse* ermächtigt Discord dazu, alle empfangenen Direktnachrichten zu lesen (und auf anstößige Inhalte zu überprüfen), während *Meine Freunde sind nett* zumindest verhindert, dass zusätzlich auch empfangene Nachrichten von Freunden durchsucht werden. Die offene dritte Auswahlmöglichkeiten (*Nicht überprüfen*) ist hingegeben die datenschutzfreundlichste, da sie das automatische Mitlesen von empfangenen Nachrichten komplett unterbindet.

Weiter unten im Einstellungsmenü des Videokonferenzsystems, befindet sich die Option *Daten verwenden, um Discord zu verbessern*, über welche man der Erhebung und Analyse der eigenen Nutzungsdaten zustimmen oder widersprechen kann. Die Einstellung selbst ist an dieser Stelle recht eindeutig dargestellt und die Datenerfassung kann über einen einfachen Klick deaktiviert werden. Auf

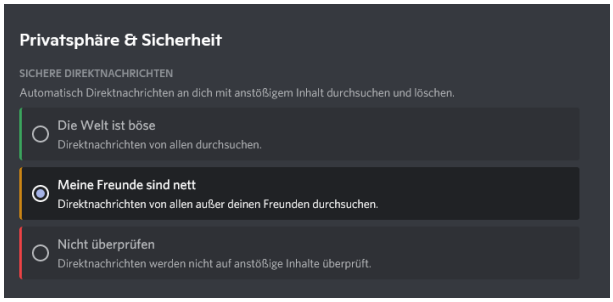

Abbildung 5: Einstellungsoptionen für die Durchsuchung empfangener Direktnachrichten [10].

diesen Klick folgt jedoch das in Abbildung 7 dargestellte Pop-Up-Fenster, welches aus Usability-Sicht gleich mehrere Schwachpunkte aufweist:

(1) Nutzer:innen werden gefragt, ob man *einige* Nutzungsstatistiken deaktivieren möchte, ohne dass erklärt wird, welche Statistiken dies betrifft bzw. welche nicht und wie dadurch nicht deaktivierte Statistiken alternativ deaktiviert werden könnten.

(2) Nutzer:innen werden darauf hingewiesen, dass jene Einstellung auch bewirke, dass alte Daten anonymisiert werden, ohne dass erklärt wird, welche Konsequenzen dies für die Nutzer:innen hat.

(3) Der Hinweis, dass Discord durch die Einstellung *dümmer* werde, kann ein schlechtes Gewissen bei den Nutzer:innen erzeugen, welche gerade durch ihre auf Datenschutz bedachten Einstellungen die Verdummung der Plattform in Kauf nehmen und sie so zu einer weniger privatsphärefreundlichen Entscheidung motivieren.

Auch der prägnante rot hinterlegte *Ja, ich will das!*-Button suggeriert im Vergleich zu dem farblich an den Hintergrund angepassten *Nein, bitte nicht!*-Button ein in Kauf nehmen von Nachteilen in Online-Meetings als Tauschmittel für mehr Privatsphäre. Aus Usability-Sicht wäre an dieser Stelle eine neutrale Darstellung der Optionen oder gar eine Bestärkung der Nutzer:innen in privatsphärefreundliche Optionen wünschenswert.

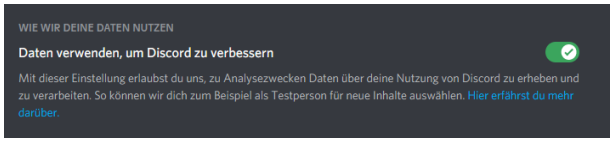

Abbildung 6: Einstellungsoption für die Erfassung und Analyse von Nutzungsdaten [10].

5 WORKSHOP

Auf die Nutzer:innen von Software für Videokonferenzen zukommende Einstellungen und Funktionen, um für sich und andere eine geschützte Meetingatmosphäre zu schaffen, sind in Bezug auf technische Systeme häufig nicht selbsterklärend. Im Workshop wird aufgrund der oben aufgezeigten Beispiele für Hürden in der Bedienbarkeit ein gemeinsames Bewusstsein für UUX-Professionals und interessierte Teilnehmer:innen geschaffen. Dadurch sollen zwei gesteckte Ziele erreicht werden: Zum einen sollen die Teilnehmer:innen des Workshops in die Lage versetzt werden sowohl für

Abbildung 7: Pop-up-Fenster, das zur (Nicht-)Bestätigung der Deaktivierung auffordert [10].

sich selbst, als auch für ihr Umfeld, einen kritischen Blick auf Videokonferenzsysteme zu richten und gleichzeitig proaktiv vorhandene Einstellungsmöglichkeiten zu nutzen. Zum anderen soll das Interesse von UUX-Professionals an der menschzentrierten Ausgestaltung von sicherheits- und privatheitsfördernden Funktionen in Videokonferenzsystemen geweckt werden, um die Nutzer:innen solcher Systeme zu unterstützen eine bestmöglich geschützte Meetingatmosphäre zu generieren.

Schlussendlich muss es für Nutzer:innen sowie Unternehmen problemlos möglich sein, souverän mit Videokonferenzsystemen umgehen zu können, indem die bereitgestellten Einstellungen und Funktionen für Sicherheit und Datenschutz nicht als Barrieren fungieren.

Teilnehmer:innen am Workshop können sich mit Mitgliedern des *Arbeitskreises Usable Security & Privacy* zu den Aspekten sicherheits- und/oder privatheitsfördernde Verfahren in Videokonferenzsystemen austauschen und gemeinsam eine kreative Gestaltungsmöglichkeit skizzieren. Im Vordergrund stehen dabei die Nutzer:innen, mit welchen mittels Transparenz, Verständlichkeit und Bedienbarkeit eine virtuelle Umgebung kreiert wird, die ihren tatsächlichen Bedürfnissen an Sicherheit und Privatsphäre in Online-Meetings entspricht. Andererseits soll die gesammelte Erfahrung der UUX-Professionals und der Workshop-Teilnehmer:innen genutzt werden, um deren Ideen in erste Gestaltungsansätze zu überführen und so die wichtigste Perspektive, die der Nutzer:innen, zu ergänzen. Die Ideen und Gestaltungsansätze können wiederum Nutzer:innen zurückgespielt und damit einer Rückkopplung und Evaluation zugeführt werden.

6 VORSTELLUNG DES ARBEITSKREISES

Der *Arbeitskreis Usable Security & Privacy* beschäftigt sich seit 2015 mit Ansätzen und Konzepten, welche sicherheits- und/oder privatheitsfördernde Verfahren für Software und interaktive Produkte stärker an den Zielen und Aufgaben der Nutzer:innen ausrichten und welche dafür sorgen, dass Funktionsweisen von Sicherheitselementen auch für Nichtexpert:innen verständlich gemacht werden. Ziel des Arbeitskreises ist es dabei, sowohl bei UUX-Professionals als auch bei Nutzer:innen im privaten und beruflichen Umfeld ein verstärktes Bewusstsein für das Themengebiet *Usable Security & Privacy* zu schaffen.

Um die Arbeit der UUX-Professionals zu unterstützen, wird das inter- und tranzdisziplinär ausgerichtete Fachwissen aus wissenschaftlicher Forschung und beruflicher Praxis zusammengeführt und damit eine Brücke zwischen der Arbeit von UUX-Professionals und anderen Disziplinen, wie dem Security Engineering, geschlagen.

ACKNOWLEDGMENTS

Die Autor:innen dieses Textes danken den übrigen Mitglieder:innen des *Arbeitskreises Usable Security & Privacy* für bereichernden Ideenaustausch, das wertschätzende Korrektiv und die eingebrachten Ressourcen. Aber auch für ihr Interesse, die produktive Zusammenarbeit und ein bereicherndes Miteinander.

Teile dieser Forschungsarbeit wurden vom *Bundesministerium für Bildung und Forschung (BMBF)* und vom *Hessischen Ministerium für Wissenschaft und Kunst (HMWK)* im Rahmen ihrer gemeinsamen Förderung für das *Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE* unterstützt. Weitere Teile dieser Arbeit sind im Rahmen des *Forschungsprojekts TrUSD* entstanden, das mit Mitteln des BMBF im Rahmen des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit *Selbstbestimmt und sicher in der digitalen Welt* gefördert wird (16KIS0896K).

LITERATUR

[1] Michael Barth and Niklas Hellemann et al.. 2020. Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt: Studienbericht 2020. https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI). 2021. BSI-Wirtschaftsumfrage: Home-Office vergrößert Angriffsfläche für Cyber-Kriminelle. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210415_HO-Umfrage.html

[3] Bundesamt für Sicherheit in der Informationstechnik (BSI). 2021. IT-Sicherheit im Home-Office: Unter besonderer Berücksichtigung der COVID-19-Pandemie. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html

[4] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK). 2020. Orientierungshilfe Videokonferenzsysteme. https://www.tlfdi.de/fileadmin/tlfdi/gesetze/orientierungshilfen/oh-videokonferenzsysteme_final.pdf

[5] Daniel Erdsiek and Sabine Elbert. 2020. Unternehmen wollen auch nach der Krise an Homeoffice festhalten. https://www.zew.de/presse/pressearchiv/unternehmen-wollen-auch-nach-der-krise-an-homeoffice-festhalten

[6] Bundesamt für Sicherheit in der Informationstechnik (BSI). 2020. Kompendium Videokonferenzsysteme: KoViKo - Version 1.0.1. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/Videokonferenzsysteme/videokonferenzsysteme_node.html

[7] Bundesamt für Sicherheit in der Informationstechnik (BSI). 2021. IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

[8] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD). 2020. Datenschutz: Plötzlich Videokonferenzen – und nun? https://www.datenschutzzentrum.de/uploads/it/ULD-Ploetzlich-Videokonferenzen.pdf

[9] Adél Holdampf-Wendel and Bastian Pauly. 2020. Homeoffice in Zeiten der Corona-Pandemie. https://www.bitkom.org/Themen/Corona/Homeoffice-in-Zeiten-der-Corona-Pandemie

[10] Discord Inc. 2021. Onlinedienst für Instant Messaging, Chat, Sprachkonferenzen und Videokonferenzen. https://discord.com/

[11] Zoom Video Communications Inc. 2021. Software für Videokonferenzen, Version 5.4.3, 58891.1115, 2021. http://zoom.us/

[12] Jakob Jung. 2020. Microsoft, Cisco und Zoom dominieren Videokonferenzen. https://www.zdnet.de/88388436/microsoft-cisco-und-zoom-dominieren-

videokonferenzen/
[13] Michael Kroker. 2020. Videokonferenz-Boom: Nutzerzahl von Zoom legt dank Corona-Schub im März um 110 Prozent zu. https://blog.wiwo.de/look-at-it/2020/05/11/videokonferenz-boom-nutzerzahl-von-zoom-legt-dank-corona-schub-im-maerz-um-110-prozent-zu/
[14] Michael Mierke. 2020. Videokonferenz-Tools im Überblick. https://www.heise.de/tipps-tricks/Videokonferenz-Tools-im-Ueberblick-4688243.html
[15] Zeit Online. 2020. Corona-Boom lässt Videokonferenz-Dienst Zoom träumen. https://www.zeit.de/news/2020-06/03/corona-boom-laesst-videokonferenz-dienst-zoom-von-mehr-traeumen
[16] Maximilian Reichlin. 2020. Videokonferenz Software Test: 20 Tools im Vergleich. https://trusted.de/videokonferenzen
[17] Jill Sayer. 2020. Die vier beliebtesten Videokonferenztools im Vergleich. https://www.fido-buerosysteme.de/Videokonferenzsoftware
[18] Jared Spool. 2018. If it's not usable, it's not secure. https://twitter.com/jmspool/status/1050452179360854017
[19] Mark Strassmann. 2020. Wie Covid-19 Videokonferenzen beeinflusst. https://www.it-zoom.de/mobile-business/e/wie-covid-19-videokonferenzen-beeinflusst-26814/
[20] Aaron Tan. 2020. Coronavirus shines spotlight on cyber security. https://www.computerweekly.com/news/252486216/Coronavirus-shines-spotlight-on-cyber-security
[21] Wikipedia. 2021. Usable Security & Privacy. https://de.wikipedia.org/wiki/Usable_Security_%26_Privacy
[22] Süddeutsche Zeitung. 2020. Corona-Boom lässt Videokonferenz-Dienst Zoom träumen. https://www.sueddeutsche.de/service/internet-corona-boom-laesst-videokonferenz-dienst-zoom-traeumen-dpa.urn-newsml-dpa-com-20090101-200603-99-287399