Verbundprojekt:

Erfahrbarer Datenschutz und IT-Sicherheit in Smarthome-Anwendungen

– UsableSec@Home –

Teilvorhaben: Usable Security in Smart Homes: Motivation, Kompetenz, Entscheidungen

GEFÖRDERT VOM

Schlussbericht
- Ruhr-Universität Bochum -

Hinweis: Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16SV8505 im Rahmen des Programms „Mensch-Technik-Interaktion für digitale Souveränität“ gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

TYP	Schlussbericht
TITEL	Erfahrbarer Datenschutz und IT-Sicherheit in Smarthome-Anwendungen – UsableSec@Home Teilprojekt: Usable Security in Smart Homes: Motivation, Kompetenz, Entscheidungen
INHALT	Schlussbericht und Liste der Veröffentlichungen des Projektpartners Ruhr-Universität zum Verbund-projekt UsableSec@Home
DATUM	24.04.2024
FÖRDERKENNZEICHEN	16SV8505
AUTOR*INNEN	Prof. Dr. Malte Elson, Nele Borgert

Inhalt

1 ALLGEMEINE INFORMATIONEN 4

1.1 AUFGABENSTELLUNG 4

1.2 VORAUSSETZUNG 6

1.3 PLANUNG UND ABLAUF DES VORHABENS 7

1.4 WISSENSCHAFTLICHER UND TECHNISCHER STAND 7

1.5 ZUSAMMENARBEIT MIT ANDEREN STELLEN 10

2 EINGEHENDE DARSTELLUNG 11

2.1 VERWENDUNG DER ZUWENDUNG UND ERZIELTE ERGEBNISSE 11

2.1.1 Gesamtüberblick über die Ergebnisse 11

2.1.2 Beteiligung an den Arbeitspaketen 12

2.2 WICHTIGSTE POSITIONEN DES ZAHLENMÄßIGEN NACHWEISES 16

2.3 NOTWENDIGKEIT UND ANGEMESSENHEIT DER GELEISTETEN ARBEIT 16

2.4 VORAUSSICHTLICHER NUTZEN 17

2.5 FORTSCHRITT 17

2.6 LISTE DER VERÖFFENTLICHUNGEN 18

3 ANHANG 20

3.1 LITERATUR 20

1 Allgemeine Informationen

Zuwendungsempfänger	Ruhr-Universität Bochum
Verbundprojekt	UsableSec@Home
Teilprojekt	UsableSec@Home - RUB
Förderkennzeichen	16SV8505
Vorhabenbezeichnung	Verbundprojekt Erfahrbarer Datenschutz und IT-Sicherheit in Smarthome-Anwendungen – UsableSec@Home; Teilvorhaben: Usable Security in Smart Homes: Motivation, Kompetenz, Entscheidungen
Laufzeit	01.05.2020 – 31.10.2023
Berichtszeitraum	01.05.2020 – 31.10.2023

Dieser Abschlussbericht enthält die Beschreibung der geleisteten Arbeiten und Ergebnisse der Ruhr-Universität im Rahmen des BMBF-Verbundprojektes „UsableSec@Home“. Der Bericht umfasst den Projektzeitraum vom 01.05.2020 – 31.10.2023. Für Detailinformationen wird auf die Projektdokumentationen und die Veröffentlichungen verwiesen.

1.1 Aufgabenstellung

Bereits heute werden in vielen Haushalten Smarthome-Geräte genutzt; dieser Trend wird sich in den nächsten Jahren fortsetzen und sogar deutlich verstärken, wie eine Studie des Bitkom e.V. zeigt [Bitkom, 2022]. In Heimnetzen kommen oft sehr unterschiedliche Geräte wie z.B. smarte Lampen, intelligente Türschlösser, digital steuerbare Heizungen, Smart-TVs, IP-Kameras und intelligente Küchengeräte zum Einsatz. Diese Geräte sind meist in einem Heimnetz verbunden und können über Smartphones, aber auch mit Sprachsteuerung kontrolliert werden. Häufig ist auch ein Zugriff über das Internet möglich.

Neben den Chancen dieser Technologien bestehen aber auch Risiken, welche die Informationssicherheit und den Datenschutz im eigenen Heim betreffen, ein Bereich, der im Allgemeinen als sehr geschützt angesehen wird. Besonders durch die Vielzahl unterschiedlicher Geräte, die wiederum oft von verschiedenen Herstellern stammen, ist für Nutzer*innen unklar, welchen Sicherheits- und Datenschutzstandards diese Geräte genügen. Sind die Geräte sicherheitstechnisch auf dem aktuellen Stand? Werden geltende Datenschutzanforderungen eingehalten und falls ja, worin bestehen diese? Was bedeutet es für das eigene Smarthome, wenn dort unsichere Geräte integriert wer-den? Kann die unsichere Konfiguration des eigenen Netzes in Kombination mit Sicherheitslücken in den Smarthome-Geräten zur Kompromittierung

des Heimnetzes führen? Trotz dieser für die allermeisten Nutzer*innen ungeklärten Fragen werden Smarthome-Geräte ohne größere Bedenken genutzt. Dabei unterschätzen Nutzer*innen in der Regel einerseits, welchen Wert die vermeintlich banalen Daten, die bei der Heimnutzung solcher Geräte anfallen, für Dritte haben. Andererseits wird auch das Risiko der Kompromittierung der Sicherheit des Heimnetzes unterschätzt (etwa die Wahrscheinlichkeit eines Abflusses der Daten). Hinzu kommt, dass Hersteller auch nicht routinemäßig über etwaige Risiken bei der Nutzung aufklären. In Kombination führt dies zu einem impliziten (oder auch expliziten) Vertrauen darin, dass geltende Datenschutzstandards eingehalten und Daten, wenn überhaupt, nur im Interesse des Anwenders verarbeitet werden.

Ziel des UsableSec@Home-Projektes war es daher, das Thema „Informationssicherheit und Datenschutz in Smarthome-Anwendungen“ umfassend aus einer nutzer*innenzentrierten Sicht zu betrachten, wobei insbesondere eine Smarthome-App umgesetzt werden sollte, die Nutzer*innen dabei unterstützt, diese Problematik besser zu verstehen und ggf. ihr Handeln anzupassen. Mit der Entwicklung einer App für die Steuerung eines Smarthomes wurden auf Basis von psychologischen Erkenntnissen neue Interaktionsformen für verbesserte Usability und User Experience geschaffen, die die Digitale Souveränität fördern. Neue methodische Ansätze halfen Privacy und Security schon im Mensch-zentrierten Designprozess zu berücksichtigen. Exemplarisch wurde dies in einem Demonstrator realisiert.

Um das Smarthome System erfahrbar zu machen, sollte eine **Augmented Reality** (AR) Anwendung entwickelt werden, wie in Abbildung 1 skizzenhaft dargestellt, um die Datenübertragung zwischen den Smarthome-Komponenten sowie die Reichweite und Wirkung von Sensoren (Kameras, Mikrofone, Bewegungssensoren) und Aktuatoren (Türöffner) sichtbar zu machen. Dies dient vor allem der Visualisierung der Privacy-Einstellungen in Multiuser-Szenarien. Dabei sollten auch unsichere Übertragungswege oder Angriffspunkte verständlich visualisiert werden.

Dies sollte mithilfe eines Simulationssystems für Smarthomes erreicht werden, das mit einer 3D-Visualisierung verbunden ist. Neben der Augmented Reality Version sollte auch eine herkömmliche Web- oder Desktopanwendung entstehen, um eine hohe Reichweite zu erzielen. Die Simulation greift auf eine Datenbank zurück, in der die Eigenschaften unterschiedlicher Smarthome-Geräte erfasst sind.

Die Simulation sollte die aktuelle Sicherheitskonfiguration des App-gesteuerten Smarthome-Systems (inkl. der Vernetzung und der eingesetzten Verschlüsselung/Authentisierung) verständlich darstellen. Nutzer*innen können dann in dieser Simulation Änderungen der Sicherheitseinstellungen des Smarthome-Systems vornehmen, z.B. Passwörter ändern oder auf einen unsicheren Werkzustand zurücksetzen, Berechtigungseinstellungen zum Zugriff auf Kamera oder Zentrale vornehmen, einen remote-Zugriff zulassen; die Simulation zeigt dann die Konsequenzen der vorgenommenen Sicherheitseinstellungen in verständlicher und nachvollziehbarer Form.

Um die Motivation der Nutzung zu erhöhen, waren auch Konzept wie Playful Interaction und Gamification vorgesehen, damit Nutzer*innen in unterschiedlichen Rollen spielerisch in verschiedenen Missionen Sicherheitseinstellungen und deren Konsequenzen ausprobieren und erfahren können. Dies soll das Interesse an gängigen Sicherheitskonzepten wie Verschlüsselung, Authentisierung und Autorisierung wecken und die Kompetenz der Nutzer*innen im Sinne der Digitalen Souveränität fördern.

Ethische, legale und soziale Implikationen (ELSI) waren in dem vorgeschlagenen Projekt durchgängig zu betrachten, zumal Informationssicherheit und Datenschutz für das Vertrauen und die Nutzer*innenakzeptanz in Smarthome-Systemen zunehmend eine herausragende Rolle spielen. Nutzer*innenvertrauen gewinnt bei der Vermarktung von Produkten an Bedeutung und auch der Datenschutz entwickelt sich nach Inkrafttreten und Wirksamwerden der europäischen Datenschutz-Grundverordnung (EU DS-GVO) immer mehr vom ursprünglichen „Wettbewerbsnachteil“ zum Verkaufsargument. Dies ist insbesondere eine Chance für Produkte europäischer Hersteller, die sich durch Privacy by Design künftig von anderen Herstellern differenzieren könnten.

Das Projekt sollte zudem die Thematik aus lern- und motivationspsychologischer Hinsicht betrachten. Hierbei sollte u.a. untersucht werden, ob und inwieweit die gewählten Darstellungsformen das Verhalten von Nutzer*innen beeinflussen. Hierfür sollten entsprechende Nutzer*innenstudien durchgeführt werden.

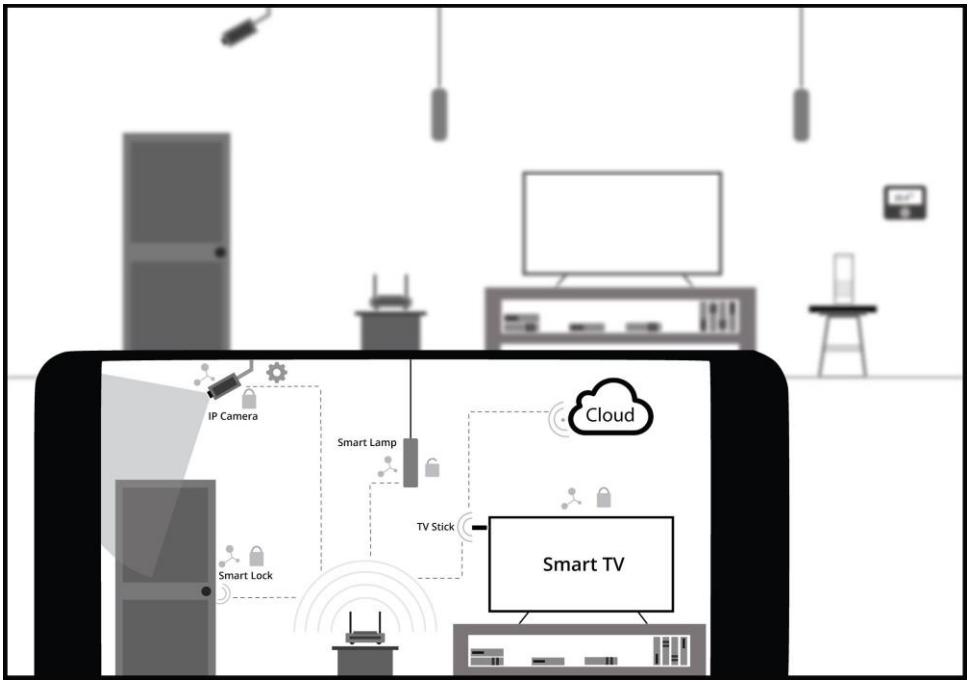

Abbildung 1: Visualisierung der Smarthome-Komponenten und der Datenflüsse in der AR (als Magic Mirror).

1.2 Voraussetzung

Voraussetzung für das UsableSec@Home-Vorhaben war neben der Förderung durch das BMBF im Rahmen des Programmes „Mensch-Technik-Interaktion für digitale Souveränität“ das Konsortium.

Eine weitere wichtige Voraussetzung war zudem die Expertise der Arbeitsgruppe „Mensch-Technik-Interaktion“ der Ruhr-Universität Bochum in der interdisziplinären Verzahnung von Technologie und den Fachbereichen der Psychologie, vor allem in Bezug auf Lern-, Motivations- und Kognitionspsychologie. Aufgrund der Vorarbeiten konnten relevante theoretische und

methodologische Fragestellungen aufgeworfen sowie bisheriger Forschungspraktiken, d. h. Erhebungsinstrumente, der HCI-Community systematisch weiterentwickelt werden. Diese gelten maßgeblich als Voraussetzung einer fundierte Forschungssynthese, indem sie nicht nur die Vergleichbarkeit, sondern auch die Reproduzierbarkeit und Validität der metawissenschaftlichen Interpretationen verbessern. Auch konnte so die entwickelte App zur Sicherheits- und Datenschutzadministration für Nutzer*innen in ihrem Wirkungsumfang überprüft werden.

1.3 Planung und Ablauf des Vorhabens

Wir haben uns bei der Planung des Teilvorhabens im Wesentlichen am Arbeitsplan aus der Teilvorhabenbeschreibung orientiert. Hierbei ging es nach einer Bestandsaufnahme der Thematik um die Konzeption verschiedener motivationspsychologischer Ansätze der AR-Anwendung zur Administration der Informationssicherheit im Smarthome und letztendlich zu ihrer Evaluation. Für die Operationalisierung der Evaluation wurden zudem Studien konzipiert und durchgeführt.

Der Ablauf dieses Vorhabens wurde stark durch die COVID-19-Pandemie beeinflusst. Insbesondere wurde dieses Projekt während der ganzen Zeit der COVID-19-Pandemie durchgeführt, was zu einer Verzögerung der Arbeiten geführt hat, indem beispielweise die Studien zwischenzeitlich nicht in Präsenz durchgeführt werden konnten und es ferner schwierig war, geeignetes Personal rechtzeitig zu bekommen. Dies konnte aber teilweise aufgeholt bzw. durch eine kostenneutrale Verlängerung des Projektes um sechs Monate (01.05.2023 – 31.10.2023) dann schließlich ausgeglichen werden – alle geplanten Tätigkeiten konnten so erfolgreich zu Ende geführt werden, insbesondere auch die Durchführung und Auswertung der Nutzer*innenstudien.

1.4 Wissenschaftlicher und technischer Stand

Im Folgenden wird der wissenschaftliche und technische Stand beschrieben, wie er sich **zur Beantragungszeit** des UsableSec@Home-Projektes darstellte (November 2019). Hierbei werden im Wesentlichen nur noch einmal jene Aspekte erwähnt, die sich auf die Thematik des Datenschutzes und der Informationssicherheit in Smarthome-Systemen beziehen, vor dem Hintergrund des Einsatzes von Methoden der Mensch-Technik-Interaktion:

Benutzbarkeit in Smarthome-Systemen: Momentan entsteht eine Vielfalt von Technologien für "Smarthomes". Dabei interagieren zahlreiche Geräte im Haushalt über lokale Netze miteinander und sind auch über Schnittstellen von außen ansprechbar. Mit zunehmender Verbreitung dieser Smarthome-Systeme und zunehmender Abhängigkeit der Nutzer*innen von mobilen Geräten für den Umgang mit vertraulichen Informationen gibt es immer mehr Forschungsarbeiten zur Entwicklung eines nutzbaren Sicherheitsrahmens für Smarthomes. Um das Potenzial der Visualisierung des Systemzustands zu erkunden und das Nutzer*innenverständnis zu verbessern, verwenden Vermeulen et. al. Beamer, um die Umgebung mit einer grafischen Darstellung zu überlagern. Wenn eine Aktion vom System ausgeführt wird, wird eine Animation angezeigt, um die Verknüpfungen zwischen dieser Aktion und den verschiedenen Geräten oder Sensoren in der Umgebung transparent zu machen. Die

Studie belegt, dass solche Methoden helfen können, intelligente Umgebungen besser zu verstehen und zu steuern [Vermeulen et. al., 2009].

Mit dem Aufkommen der Smarthome-Technologie können Menschen verschiedene Geräte mit verschiedensten Techniken steuern und handhaben. Mit Augmented Reality (AR) lassen sich jetzt schon Smarthome-Geräte steuern. AR bietet eine virtuelle Ansicht der Smarthome-Geräte, die eine reale Umgebung erzeugt. Sorgalla et. al. entwickelten einen neuartigen Ansatz zur Steuerung einer Smarthome-Umgebung mittels AR mit Gestenerkennung. Ihre Studie zeigt, dass 3D-Modelle von Smarthome-Geräten ein visuelles Feedback geben, wenn eine Interaktion auftritt. Der AR-Ansatz reduziert die obligatorischen Gesten und ist einfach zu konfigurieren [Sorgalla et. al., 2018].

IT-Sicherheit und Datenschutz in Smarthome-Systemen: Im Zuge des Fortschritts im Bereich IoT haben Sicherheitsexperten Bedenken in Bezug auf IoT und Smarthome-Systeme festgestellt. Dies beinhaltet Datenschutzrisiken sowie unsichere und unzuverlässige Geräte. Im Kontext von Smarthome-Systemen sind verschiedene Sicherheitsprobleme diskutiert worden. Beispielsweise erlangte das Mirai-Botnet u.a. über Standardpassworteinstellungen Zugriff auf mehr als 3 Millionen IoT-Geräte. Des Weiteren zeigten Sicherheitsanalysen, dass das SmartThing-Framework von Samsung verschiedene Sicherheitslücken aufwies wie z.B. das Durchsickern von vertraulichen Informationen, die Überprivilegierung von Anwendungen und die Möglichkeit, Informationen zu fälschen [Fernandes et al., 2016]. Zudem entdeckten IT-Sicherheitsforscher Schwachstellen in der kryptographischen Implementierung und im Softwareupdate-Mechanismus von Philips-Hue-Lampen; die Ausnutzbarkeit der Lücken demonstrierten die Forscher anhand eines Wurms, der sich von einer Lampe zur anderen verbreiten konnte [Ronen et al., 2017].

Im BMBF-Verbundprojekt SecureSmartHomeApp haben die Universität Bremen und die neusta mobile solutions GmbH systematisch Bedrohungen in App-gesteuerten Smarthome-Systemen untersucht. Hierbei lag der Schwerpunkt der Untersuchungen auf der Sicherheitsanalyse zwischen App und Smarthome-Zentrale bzw. App und Cloud . In diesem Rahmen entstand auch eine Referenzsicherheitsarchitektur [Müller, 2017]. Des Weiteren wurde ein Schema zur Klassifikation von Smarthome-Systemen bzgl. der IT-Sicherheit entwickelt.

Zeng et. al. untersuchten die Sicherheits- und Datenschutzbedenken der Endbenutzer*innen, die das Smarthome von heute einrichten und mit ihm interagieren [Zeng et. al., 2017]. Ihre Studie hat gezeigt, dass es für Benutzer*innen ohne technisches Verständnis der Technologie schwierig ist, fundierte Sicherheitsentscheidungen zu treffen, wenn gemeinsame Elemente des Bedrohungsmodells und Strategien zur Schadensbegrenzung fehlen. Darüber hinaus deuten die Ergebnisse darauf hin, dass zufällige Nutzer*innen von Smarthome-Systemen weniger technisch versiert sind oder weniger über potenzielle Sicherheits- und Datenschutzprobleme informiert sind.

Mit dem Inkrafttreten der DS-GVO im Jahr 2016 und deren Wirksamwerden in 2018 wurde das europäische Datenschutzrecht einer umfassenden Neuordnung unterzogen. Zwar entsprechen die wesentlichen Grundprinzipien einer jeden Datenverarbeitung nach wie vor der EU-Datenschutzrichtlinie aus 1995, dennoch stellt die DS-GVO aufgrund verschiedener neuer, an die technologische Entwicklung angepasste rechtliche Änderungen eine Herausforderung für Unternehmen dar. Die DS-GVO selbst ist technologieneutral formuliert, sodass sie nicht auf bestimmte Produkte oder Dienste abstellt. Dementsprechend gibt es keine Smarthome-spezifischen rechtlichen Vorgaben. Eine Herausforderung für Hersteller und Anbieter von

Smarthome-Lösungen ist deshalb, die für sie anwendbaren Rechtsvorgaben zu ermitteln und in ihren Produkten umzusetzen. Dass verschiedene Unternehmen hierbei schon an den einfachsten Anforderungen scheitern, zeigt das Thema der oftmals fehlerhaften Datenschutzerklärungen, die mit der Abmahnproblematik verbunden sind [Baumgartner und Sitte, 2018]. Ein Smarthome-System besitzt jedoch eine weitaus höhere Komplexität als z.B. die bloße Datenerhebung in einem Anmeldeformular auf einer Website o.Ä. Seit dem Wirksamwerden der DS-GVO im Mai 2018 wurden die datenschutzrechtlichen Rahmenbedingungen für derlei Systeme nicht vollumfänglich erforscht, sondern immer nur Teilbetrachtungen vorgenommen, z.B. die Videoaufzeichnung betreffend [Lachenmann, 2017] oder für Sonderfälle wie dem Datenschutz im Smart Office [Braun, 2018]. Damit wird jedoch verkannt, dass sich die datenschutzrechtlichen Gefährdungen im Smarthome gerade durch die Vernetzung zahlloser Einzelgeräte ergeben, die personenbezogene Daten in alle Richtungen übermitteln, damit bei Nutzer*innen für Intransparenz sorgen und so die informationelle Selbstbestimmung gefährden. Eine datenschutzrechtliche Betrachtung, die alle bisherigen Erkenntnisse und Komponenten miteinander verknüpft und weiterentwickelt, würde mithin weithin über den gegenwärtigen Stand von Wissenschaft und Technik hinausreichen.

Gamification zur Erhöhung der Motivation: Gamification wurde definiert als die Verwendung von Game-Design-Elementen in nicht-spielbezogenen Kontexten wie Bildung und Gesundheit [Deterding et. al., 2011]. Forscher, die Gamification implementiert und untersucht haben, haben dokumentiert, dass das Spielen von Videospielen Vorteile mit sich bringt, die die kognitiven Fähigkeiten (Aufmerksamkeit, Fokus und Reaktionszeit), die Motivation sowie den emotionalen und sozialen Nutzen verbessern [Granic et. al., 2014]. Suknot et al. schlugen vor, das Bildungserlebnis durch Gamification zu verbessern, um den Benutzer*innen die Sicherheit bei verschiedenen Arten von Bedrohungen im Zusammenhang mit dem Internet bewusster zu machen. Ihr Spiel umfasst Datenschutzthemen wie Smartphone, soziale Netzwerke, E-Mail und allgemeine Internetnutzung [Suknot et. al., 2014].

Security und Privacy by Design: Softwareentwicklungsprozesse können um Aspekte der IT-Sicherheit erweitert werden; hier spricht man dann von einem Security Development Lifecycle (SDL). Verbreitet ist in diesem Zusammenhang insbesondere der SDL von Microsoft [Howard und Lipner, 2006]; Konzepte des Microsoft SDL flossen in den Standard ISO/IEC 27034:2011 [ISO, 2011]. Ein wesentlicher Bestandteil eines SDL ist die architekturelle Risikoanalyse von Software (z.B. Threat Modeling), bei dem Sicherheitsschwächen von Anwendungen bereits in der Design-Phase systematisch ermittelt und behoben werden (Security by Design-Ansatz). Analog bedeutet Privacy by Design, Datenschutzanforderungen bereits in das Design von Anwendungen einzubauen [Danezis et al., 2015]. Auch hier lassen sich Entwicklungsprozesse entsprechend anpassen, indem beispielsweise in der Design-Phase Rollen- und Berechtigungen sowie organisatorische Kontrollregeln definiert und letztendlich in der Softwarearchitektur verankert werden.

Spätestens seit Inkrafttreten der DS-GVO sind Privacy by Design, und in einem etwas geringerem Maße auch Security by Design, de facto-Standards in Systemtechnik und System Engineering. Grundlegende Prinzipien wie Proaktivität und Prävention von Privacy-Maßnahmen, ihre Einbettung in die Systemarchitektur ohne die Einschränkung von Funktionalität sowie ihre Sichtbarkeit und Transparenz werden im Design von Smarthome-Geräten implementiert. Eine effektive Umsetzung dieser Maßnahmen im Sinne einer Usable Privacy und Usable Security kann jedoch nur erfolgen, wenn Kenntnisse, Einstellungen, und

Verhaltenskontingenzen von Nutzer*innen im Designprozess berücksichtigt werden [Zheng et al., 2018].

So ist die lernpsychologische Überlegenheit von visuellen Repräsentationen, insbesondere animierte Darstellungen, für das Verständnis komplexer technischer oder mechanischer Prozesse in unterschiedlichen Domänen belegt. Diese Vorteile sind beobachtbar in der unmittelbaren Nachvollziehbarkeit von dargestellten Informationen, nachhaltigen Behaltensleistung sowie effektiveren Umsetzung von Informationen in die Praxis [Klerkx et al., 2014]. Die Prinzipien psychologisch informierter Visualisierungstechniken werden mit Erfolg bereits im Design der Funktionalität von Smarthome-Systemen verwendet, bspw. für die Überwachung ihrer elektrischen Integrität [Kumar et al., 2009], der Interaktion von Sensoren in Smarthomes [Thomas und Crandall, 2011] oder der Simulation ganzer Smarthome-Umgebungen, um Innenausstattung und Installation planbar zu machen [Lazovik et al., 2009]. Bislang wenig Anwendung findet diese Forschung, um Privacy- und Security-Design nutzbarer zu machen, obwohl die hohe Informationsdichte bedingt u.a. durch Interkonnektivität von Geräten unterschiedlicher Hersteller (mit unterschiedlichen Interfaces) in Smarthomes die Nachvollziehbarkeit und nachhaltiges Lernen im Umgang mit Technologien erschwert.

1.5 Zusammenarbeit mit anderen Stellen

In dem Verbundprojekt UsableSec@Home arbeitete die Ruhr-Universität eng mit allen Konsortialpartnern zusammen. Insbesondere hat die Ruhr-Universität mit der die Universität Bremen vor allem im Bereich der Durchführung von Nutzer*innenstudien zusammengearbeitet, um motivationspsychologische Aspekte zu untersuchen. Mit neusta mobile solutions GmbH wurden unterschiedliche nutzer*innenzentrierte Interventionsdesigns für die AR-Anwendung entwickelt. Auch mit der Certavo GmbH und dem VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V. – DKE CERT@VDE & Cybersecurity wurde sich über die gesamte Projektlaufzeit zur Abstimmung der interdisziplinären Perspektiven regelmäßig beraten. Die Kooperation wird beispielsweise deutlich in gemeinsamen Publikationen oder auch Experti*innen-Workshops, die zur inhaltlichen Validierung psychologischen Messinstrumente dienten. Darüber hinaus haben wir mit der Leibniz Universität Hannover, dem Horst-Görtz-Institut für IT-Sicherheit in Bochum und dem Lehrstuhl Human-Centred Security der Informatikfakultät der Ruhr-Universität Bochum zur Schnittstelle menschlicher Aspekte von Cybersecurity und Privatsphäre von Smart Homes kooperiert. Auch die Universität Bern wirkt nun bei der Verwertung der Ergebnisse mit.

2 Eingehende Darstellung

2.1 Verwendung der Zuwendung und erzielte Ergebnisse

Zunächst stellen wir die Ergebnisse unseres Teilvorhabens im Gesamtüberblick dar. Anschließend beschreiben wir die Ergebnisse bzgl. der Arbeitspakete, an denen die Ruhr-Universität Bochum beteiligt war, im Einzelnen.

2.1.1 Gesamtüberblick über die Ergebnisse

Im Rahmen des UsableSec@Home-Projekts stand die Erforschung von Nutzer*innen-zentrierten Zugängen im Zentrum, Informationssicherheit und Datenschutz besser zu verstehen und entsprechende Verhaltensweisen zu unterstützen. Das Projekt verfolgte das Ziel, die digitale Souveränität der Nutzer*innen zu stärken.

Im Forschungsprojekt haben wir umfangreiche Untersuchungen und Entwicklungen zur Verbesserung der Informationssicherheit und des Datenschutzes in Smart-Home-Systemen durchgeführt. Die zentralen Ergebnisse des Projekts umfassen auch die Identifizierung der psychologischen Faktoren, die das Sicherheitsverhalten der Nutzer*innen beeinflussen, insbesondere die Cybersecurity-Selbstwirksamkeit. Diese stellt die Überzeugung der Nutzeri*nnen dar, mit den unterschiedlichen Aspekten der IT-Sicherheits- und Privatsphäre-Anforderungen ihrer Systeme umgehen zu können.

Durch ein systematisches Literaturreview, welches 168 empirische Publikationen des letzten Jahrzehnts umspannt, und eigenen originalen Studien konnten wir die umfassende Bedeutung der Selbstwirksamkeit im Kontext der Smart-Home-Sicherheit herausarbeiten und darauf basierend Handlungsempfehlungen für die Gestaltung nutzer*innenfreundlicher Sicherheitsschnittstellen entwickeln. Diese Schnittstellen sollten so gestaltet sein, dass sie die Nutzer*innen in die Lage versetzen, Konfigurationen an den Endgeräten eigenständig und sicher vorzunehmen. Diese innovativen Ansätze, die auch im Rahmen von Gamification-Techniken und der Self-Determination Theory erforscht wurden, dienen fundamental der Förderung der individuellen Motivation zur Auseinandersetzung mit komplexen Sicherheitsthemen.

Ein weiteres Kernergebnis des Projekts ist die Entwicklung und Validierung einer kontextspezifischen Skala zur Messung der Cybersecurity-Selbstwirksamkeit in Smart Homes (CySESH). Diese Skala wurde in fünf Studien mit über 1200 Teilnehmenden erprobt und zeigte eine hohe Zuverlässigkeit und Validität. Die Ergebnisse dieser Studien tragen dazu bei, die Forschung in der Mensch-Computer-Interaktion durch zukunftsweisende Messmethoden voranzutreiben sowie differenzierte Nutzer*innengruppen zu identifizieren, um darauf aufbauend spezifischere Sicherheitslösungen beispielsweise in Konfigurations-Wizards entwickeln zu können.

Durch unser Projekt haben wir auch tiefere Einblicke in das Phänomen Overtrust gewonnen, das auftritt, wenn Nutzer*innen ein übermäßiges Vertrauen in die Sicherheits- und Datenschutzfunktionen ihrer Smarthome-Systeme setzen. Diese Erkenntnisse tragen wesentlich dazu bei, die Bedingungen zu verstehen, unter denen Overtrust entsteht und wie die

Interface-Gestaltung von z. B. der im Projekt entwickelten VR-Smarthome-App dies mitigierend beeinflussen kann.

Unsere Forschungsergebnisse bieten somit eine fundamentale Basis für die Entwicklung und den Einsatz motivierender und zielgruppenspezifischer digitaler Anwendungen zur Förderung des Verständnisses von Informationssicherheit und Datenschutz und leisten einen wichtigen Beitrag zur Stärkung der digitalen Autonomie und Sicherheit von Endverbraucher*innen.

2.1.2 Beteiligung an den Arbeitspaketen

Im Folgenden werden die einzelnen Arbeitspakete zusammen mit einer kurzen Beschreibung der geleisteten Arbeiten aufgelistet. Die Gliederung orientiert sich an Vorhabenbeschreibung für das UsableSec@Home-Projekt.

Arbeitspaket 2: Analyse

In diesem Arbeitspaket wurde wie geplant ein Überblick der Literatur zu Kenntnissen, Erwartungen und Ansprüchen von Nutzer*innen an die Informationssicherheit ihrer Smarthome-Systeme gewonnen. Dabei liegt ein besonderer Schwerpunkt auf der Motivation von Nutzer*innen, Sicherheitsfeatures ihrer Systeme zu nutzen bzw. sich überhaupt mit der Sicherheit auseinanderzusetzen und ggf. Konfigurationen vorzunehmen.

AP 2.3: Psychologische Betrachtung der Motivation von Nutzern bzgl. Datenschutz und Informationssicherheit

Aufwand: 5 Personenmonate

Cybersecurity-Selbstwirksamkeit ist die Überzeugung, dass die eigenen Fähigkeiten (hier bezogen auf IT-Sicherheit und Privatsphäre) effektiv sein können. Es ist laut meta-wissenschaftlichen Erkenntnissen das einzige Human Factors Konstrukt, dass individuelles Sicherheitsverhalten reliable und maßgeblich mitbestimmt. Damit Nutzer*innen selbstwirksam und daher motiviert sind, sich überhaupt mit der Konfiguration ihrer Geräte auseinanderzusetzen, müssen Interfaces der Systeme für die Selbstwirksamkeit ein angemessenes Komplexitätsmaß haben (bspw. Fachbegriffe, Darstellungen, Eindeutigkeit der Konsequenzen von Konfigurationsänderungen).

Im Rahmen dieses Arbeitspaketes führten wir ein systematisches Review durch, das die empirische Literatur des letzten Jahrzehnts zum Thema Cybersecurity Self-Efficacy synthetisiert (mit N = 174 Originalstudien). Darüber hinaus betrachteten wir auch Handlungsanweisungen für Nutzer*innen und Designer*innen von Systemen, die auf dieser Literatur basieren. Die Ergebnisse wurden in den Proceedings der internationalen A* Konferenz „CHI: Conference on Human Factors in Computing Systems (CHI ’24)“ veröffentlicht [Paper: https://doi.org/10.1145/3613904.3642432].

AP 3: Konzeption

Auf Basis der Self-Determination Theory wurden verschiedene Szenarien untersucht, um die Motivation von Nutzer*innen zu erhöhen, die sich mit komplexen Sicherheitsthemen in Smarthome-Geräten auseinandersetzen. Neben der Cybersecurity-Selbstwirksamkeit, die für

die motivationalen Bedürfnisse Kompetenz und Autonomie steht, wird hier noch Ergebniserwartung als Einflussfaktor und das dritte Bedürfnis der sozialen Eingebundenheit mitbetrachtet. In diesem Zusammenhang untersuchten wir das Konstrukt Overtrust.

AP 3.5: Vorstudien und Konzeption verschiedener Gamification-Ansätze zum Erlernen von Sicherheits- und Datenschutzkonzepten in App-gesteuerten Smarthome-Systemen

Aufwand: 1.5 Personenmonate

Eine Studie zum wahrgenommenen Spannungsverhältnis zwischen der spielerischen Nutzbarkeit von Smarthome-Systemen (Convenience-Leistung) und den inhärenten Einschränkungen bzw. Aufwandes für die Gewährleistung von Sicherheitsmechanismen wurde im Rahmen eines Forschungspraktikums durchgeführt und ausgewertet. Die Ergebnisse wurden den Verbundpartnern präsentiert und deuteten u.a. auf relevante Kauffaktoren hin, wie die physische Repräsentation [Präregistrierung: https://doi.org/10.17605/OSF.IO/PVZC5; OSF Project Page: https://osf.io/pgcns/].

AP 3.6: Entwicklung von Datenschutz- und IT-Sicherheitskonzepten für App-gesteuerte Smarthome-Systeme

Aufwand: 2 Personenmonate

Um ebenso negative Auswirkungen der Motivation von Nutzer*innen zu vermeiden, ist es notwendig Overtrust als Variable in die Verhaltenserklärungen einzubeziehen. Overtrust beschreibt einen zu hoch kalibrierten Vertrauenszustand der Nutzer*innen in die Cybersecurity- und Privatheits-Features des Smarthome-Systems. Dieser Befund hat sich bereits in anderen Mensch-Roboter-Interaktionen bewährt. Die Kausalität dieses erhöhten Vertrauens liegt vor allem in der Fehleinschätzung des Risikos und des Werts der privaten Daten. Diese Fehleinschätzungen wurden in zwei Studien untersucht. Ziel war die Versuchsmaterialien auf Verständlichkeit und Angemessenheit zu testen [OSF Project Page: https://osf.io/uqj8v/].

AP 3.7: Vorstudie und Konzeption einer App zur Konfiguration von Datenschutz- und Sicherheitseinstellungen für Smarthome-Systeme

Aufwand: 2 Personenmonate

Im Zusammenhang mit Cybersecurity-Selbstwirksamkeit wurden psychologische Modelle entwickelt, die notwendige und hinreichende Bedingungen für das Sicherheitsverhalten von Nutzer*innen abbilden. Dazu gehört der Zusammenhang zwischen dem gezeigten oder auch unterlassenen Sicherheitsverhalten und dem latenten Konstrukt der Outcome Expectancies (Ergebniserwartungen). Ergebniserwartungen können sowohl soziale, kognitive und physische Konsequenzen von Nutzer*innenverhalten umfassen. Sie beziehen sich also auf die Folgen der Verhaltensausführung (z. B. Gruppenkonformität, Sorgen um die IT-Sicherheit, verlorene Daten), während Selbstwirksamkeit die geglaubte Fähigkeit ist, besagtes Verhalten auszuführen. Im Rahmen einer Abschlussarbeit wurde eine Skala zur Messung von Ergebniserwartungen im Kontext der IT-Sicherheit in Bezug auf Smart Home Geräte entwickelt und in einer Studie validiert [Präregistrierung: https://doi.org/10.17605/OSF.IO/2B6XC; OSF

Project Page: https://osf.io/w3vef/?view_only=]. Die Items basieren auf qualitativen Befunden vorhergehender Studien im Teilvorhaben.

Arbeitspaket 4: Iterative Entwicklung der Smarthome App

In diesem Arbeitspaket wurden die bisherigen Erkenntnisse aus 2.3 und 3.6 vertiefend bearbeitet. Overtrust in risikohafte Privacy-Features wurde unter dem Aspekt des Einflusses von Anthropomorphismus untersucht und die im Review identifizierten, nicht standardisierten Messmethoden von Cybersecurity Selbstwirksamkeit wurden vergleichend analysiert. Dies dient auch vor allem der Differenzierungsfähigkeit verschiedener Nutzer*innengruppen.

AP 4.2: Entwicklung eines Wizards zur Erstellung und Zuordnung der Rollen

AP 4.2.2: Datenschutzrechtliche- und psychologische Aspekte der Gestaltung des Wizards

Aufwand: 3 Personenmonate

Im Rahmen einer Abschlussarbeit wurde sich mit der Thematik der physischen Repräsentation, d. h. dem Einfluss von Anthropomorphismus, auseinandergesetzt. Die Fragestellung der Studie bezog verschiedene kognitive Heuristiken (machine heuristic und die individuelle Neigung zum Anthropomorphisieren) als Moderatoren für das Zustimmen zu riskanten Smart Home Nutzungsbedingungen - im Sinne niedriger Privatheit - mit ein [Präregistrierung: https://doi.org/10.17605/OSF.IO/DQGE4; OSF Project Page: https://osf.io/6ugwn/?view_only=].

AP 4.5: Kontinuierliche Betrachtung der rechtlichen und psychologischen Aspekte sowie Messung der User Experience

Aufwand: 3 Personenmonate

Auch die Qualität bisheriger Operationalisierungen von Cybersecurity-Selbstwirksamkeit wurde in einer Studie im Rahmen einer Abschlussarbeit geprüft; insbesondere hinsichtlich der konvergenten Validität und auch verschiedener Reliabilitäts- und zusätzlichen Validitätsmerkmalen. Diese Analyse von sieben Selbstwirksamkeitsskalen offenbarte erhebliche Abweichungen von testtheoretischen best-practices, Schwächen in der Itemschwierigkeit und der konvergenten Validität, was eine dringende Überarbeitung der bisherigen Skalen indizierte [Präregistrierung: https://osf.io/bsu6j?view_only=013939779554426a86cd39f11234decb; OSF Project Page: https://osf.io/6nrv8/?view_only=013939779554426a86cd39f11234decb].

Arbeitspaket 5: Iterative Entwicklung der Simulation

Ergebnis dieses Arbeitspaketes war die Entwicklung und Validierung einer Cybersecurity Selbstwirksamkeits-Skala für Smart Home Kontexte, um die als relevant definierten Dimensionen empirisch erfassen und evaluieren zu können.

AP 5.5: Kontinuierliche Betrachtung der rechtlichen und psychologischen Aspekte, sowie Messung der User Experience

AP 5.5.2 Betrachtung der psychologischen Aspekte mit Messung der User Experience

Aufwand: 6 Personenmonate

Die Sicherheit und der Datenschutz in Smart Homes sind von zentraler Bedeutung, jedoch wird die Effektivität von Maßnahmen zur Förderung sicherer Benutzer*innenverhaltensweisen durch das Fehlen validierter Instrumente zur Messung relevanter psychologischer Konstrukte eingeschränkt.

Wir entwickelten und validierten die Skala „Cybersecurity Self-Efficacy in Smart Homes“ (CySESH), ein eindimensionales Messinstrument mit 12 Items. Über fünf Studien mit N = 1247 Teilnehmenden haben wir drei Pilotstudien zur Entwicklung der Items durchgeführt. Die Ergebnisse zeigen eine ausgezeichnete Zuverlässigkeit und konvergente Validität. Die CySESH-Skala bietet Potenzial, zukünftige Forschung im Bereich Mensch-Computer-Interaktion zu Cybersicherheit voranzutreiben, sowie Nutzer*nnen-Differenzierung und politische Implikationen des Verbraucher*innenschutzes. Die Ergebnisse wurden in den Proceedings der internationalen A* Konferenz „CHI: Conference on Human Factors in Computing Systems (CHI ’23)“ veröffentlicht [Paper: https://doi.org/10.1145/3544548.3580860].

Arbeitspaket 6: Evaluation

In diesem Arbeitspaket haben wir sowohl die medien- und kognitionspsychologischen Erkenntnisse zur Datenschutzkonfiguration als auch die Einflussfaktoren zur Stärkung der Selbstwirksamkeit von Nutzer*innen sowie zur Kalibrierung ihres Vertrauens vertieft.

AP 6.1 Studie zur App zur Konfiguration von Datenschutz- und IT-Sicherheitseinstellungen von Smarthome-Systemen

Aufwand: 2 Personenmonat

Die Vorarbeiten aus dem Arbeitspaket 3.6 wurden hier weiterentwickelt. Die erarbeiteten Ergebnisse dienen nun der Verwertung für ein Vignetten-basiertes Studiendesign, welches behavioral die subjektive Einschätzung des Werts der eigenen Daten erhebt. Die Studie diskutiert die dichotomen Annahmen gegenwärtigen Theorien und modelliert übergreifende Vorhersagen zum Sicherheitsverhalten von Smarthome Nutzer*innen in Bezug auf ihren Datenschutz [der Registered Report ist under review bei der Fachzeitschrift Media Psychology; OSF Project Page: https://osf.io/uqj8v/].

AP 6.2: Studie zur AR-basierten Simulation von Smarthome-Systemen

Aufwand: 2 Personenmonate

Die Evaluation verschiedener Manipulationen, näher beschrieben in Arbeitspaket 6.3, hat bereits mit zwei Abschlussarbeiten innerhalb einer auch noch weiter fortlaufen multi-lab Studie stattgefunden. Eine Abschlussarbeit konzentrierte sich auf den Einfluss von wahrgenommenem und tatsächlich gelerntem IT-Sicherheits- und Datenschutzwissen. Die andere Abschlussarbeit machte einen Wirksamkeitsvergleich der Interventionen verteilt auf fünf Experimentalgruppen.

AP 6.3: Studie zu den Serious Games-/Gamification-Ansätzen

Aufwand: 2 Personenmonate

Spielerische App-Elemente bauen beständig auf Erkenntnissen der Lern- und Motivationspsychologie auf. Prominente Theorien aus diesem Fachbereich sind unter anderem die in diesem Projekt untersuchten Modelle der Social Cognitive Theory (mit Focus auf Selbstwirksamkeit) und der Self-Determination Theory (hier mit Schwerpunkt auf Overtrust). Neben dem Erkunden der AR-App durch verschiedene Aufgaben mit Sicherheitsbezug (als

mastery experience codiert), wurden unterschiedliche Darstellungsvariationen entwickelt: eine Intervention beinhaltete Charakteristika von visueller Persuasion, eine andere setzt vicarious experiences durch eingespielte Lösungsverhaltensweisen um und die letzte Intervention manipuliert Vertrauen durch eine Veränderung der Warnsymbole, um Risikounsicherheit zu verursachen.

Die in Arbeitspaket 6.2 beschriebene multi-lab Studie (geplantes N = 550) untersucht vor allem die psychologischen Konsequenzen dieser verschiedenen AR-App-Ansätze. An der Studie sind sowohl die Ruhr-Universität, die Universität Bremen als auch die Universität Bern im Rahmen der Verwertung des Projektes beteiligt. Die Präregistrierung der übergreifenden Studie ist auf OSF dokumentiert: https://osf.io/aqtv6/?view_only=561a4462f405443a8c125daabfa82fb0.

Arbeitspaket 7: Zusammenarbeit mit dem Netzwerk "Digitale Souveränität"

AP 7.1 Erschließung von weiteren Nutzergruppen und Stakeholdern

Aufwand: 2 Personenmonate

Im Rahmen dieses Arbeitspaketes haben wir um auch Arbeits- und Ingenieurspsycholog*innen zu erreichen, die sich mit Trainingskonzepten zu Usable Security in unterschiedlichen Arbeitskontexten auseinandersetzen, die Ergebnisse nicht nur in HCI fachspezifischen Outlets publiziert, sondern auch auf psychologischen Konferenzen präsentiert. Auch haben wir regelmäßig an den Veranstaltungen des Digital Autonomy Hub (Begleitprojekt) teilgenommen. Darüber hinaus haben wir Informationen über das UsableSec@Home-Projekt für die Webseite des Digital Autonomy Hub (https://digitalautonomy.net/) bereitgestellt und inhaltlich zum Policy Brief zum Thema „Digitale Selbstbestimmung und Nachhaltigkeit" beigetragen.

2.2 Wichtigste Positionen des zahlenmäßigen Nachweises

Im Wesentlichen besteht der zahlenmäßige Nachweis aus den Personalkosten. Diese Kosten entsprechen den Aufwänden aus den zuvor genannten Arbeitspaketen.

2.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Ziel des UsableSec@Home-Projektes war es, auf Basis von Methoden der Mensch-Technik-Interaktion beruhende Anwendungen zu entwickeln, die nachweislich dazu beitragen, das Verständnis der Sicherheits- und Datenschutzthematik im Smarthome zu erhöhen und Nutzer*innen zu motivieren, entsprechend in diesem Umfeld zu agieren. Hierbei wurde eine AR-Anwendung entwickelt, die entsprechende Kriterien der Usability und der User Experience erfüllen sollte. Zudem haben wir in einen breitgefächerten Datensatz zu Methoden der Cybersecurity Selbstwirksamkeitsforschung mit N = 173 Studien erarbeitet und darauf aufbauend eine Skala zur Messung von Cybersecurity Selbstwirksamkeit in Smarthome Kontexten entwickelt und validiert (N = 1247). Mithilfe des Unity-Frameworks war es außerdem möglich, eine solche Anwendung umzusetzen, die an der Universität Bremen und der Ruhr-Universität Bremen in Studien mit mehr als aktuell 230 Proband*innen evaluiert wurde. Auch kann die Anwendung nach Projektende weiterentwickelt und in anderen, ähnlich gearteten

Projekten eingesetzt werden. Aufgrund unseres Projektergebnisses waren damit die geleisteten Arbeiten notwendig und angemessen.

2.4 Voraussichtlicher Nutzen

Oft ist für Nutzer*innen intransparent, welche Daten in ihrem Smarthome über welche Kommunikationsschnittstelle wohin fließen und wie sicherheits- bzw. datenschutzkritisch diese tatsächlich sind. Die von uns entwickelte AR-basierte Konfigurationsapp bietet nun die Möglichkeit, diese Datenflüsse „sichtbar“ zu machen, so dass Nutzer*innen fundiertere Risikoeinschätzungen bzgl. der Sicherheit und des Datenschutzes ihrer Daten machen können.

Unsere in diesem Projekt durchgeführten Studien belegen zudem, dass die AR-Anwendung tatsächlich das Verständnis des Sicherheits- und Datenschutzrisikos in Smarthomes erhöht, ohne dass die Nutzung der AR-Anwendung zu aufwendig ist. Bei Weiterentwicklung und Anschluss an echte Daten (beispielsweise bereitgestellt aus einer Datenbank mit Informationen über Smarthome-Geräte) könnte diese Anwendung vielen Nutzer*innen als mobile App zur Verfügung gestellt werden. Ein typischer Multiplikator für die Verbreitung dieser App könnten Verbraucher*innenschutzorganisationen oder IT-Sicherheitsbehörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) sein.

Auch die theoretischen und methodischen Ergebnisse aus dem systematischen Literaturreview zu Cybersecurity Self-Efficacy haben einen weitreichenden Nutzen für Wissenschaftler*inne, Praktiker*innen und politischen Entscheidungsträger*innen. Sie deuten auf fundamentale Limitationen bezüglich replizierbarer wissenschaftlicher Evidenz zu psychologischen Faktoren von Usable Security und deren bisheriger Validität in metawissenschaftlichen Interpretationen (insbesondere angewandter Interventionen) hin.

Die sichtbare Relevanz des Themas Selbstwirksamkeit in der HCI-Community verläuft sich in heterogenen und nicht validierten Messinstrumenten. Die von uns entwickelte und validierte Skala zur Messung von Cybersecurity Self-Efficacy in Smart Homes (CySESH) stellt Akteur*innen im Bereich Usable Security eine fundierte Alternative zur Verfügung. Die Skala kann sowohl zur Wirksamkeitsforschung von Interventionen genutzt werden, als auch zur differenziellen Gestaltung von Interfaces je nach Ausprägung der Nutzer*innen. Nicht zuletzt können auch prävalente Nutzer*innenprofile mit erhöhtem Risikopotential durch gezielte Verbraucher*innenschutzrichtlinien in ihrer digitalen Souveränität unterstützt werden.

2.5 Fortschritt

Die im UsableSec@Home-Projekt entwickelte AR-Anwendung wird dazu beitragen, dass Nutzer*innen das Thema „Informationssicherheit und Datenschutz“ in ihrem Heimnetz besser verstehen können und durch die Verwendung von modernen Interaktionsformen wie AR motiviert werden, sich tiefer mit der doch oft etwas ermüdenden Thematik zu beschäftigen. Unseres Wissens ist es die erste Anwendung, die auf Basis von Augmented Reality Datenflüsse in Smarthome-Netzen transparent macht. Die AR-Anwendung und ihre Konzepte [Bahrini et al., 2023] stehen zur Verfügung und können in Folgeprojekten oder Verwertungsschritten beispielsweise durch Verbraucher*innenschutzorganisationen genutzt werden.

Ebenso kann die im Projekt entwickelte und validierte Skala zur Erhebung von Cybersecurity Selbstwirksamkeit in Smathome Kontexten (CySESH) in diversen Anwendungskontexten genutzt werden. Dies ermöglicht Interessierten eine wissenschaftlich fundierte Möglichkeit Sachverhalte bedeutungsvoll einschätzen und anpassen zu können. Die CySESH-Skala wurde von uns auf verschiedenen Veranstaltungen zu Disseminationszwecken vorgestellt:

- 13th Fachgruppentagung der AOW- und Ingenieurspsychologie, September 14, 2023, Kassel, Germany
- BMBF-Abschlusstreffen „Mensch-Technik-Interaktion für digitale Souveränität", April 27, 2023, Hamburg, Germany
- CHI Conference on Human Factors in Computing Systems (CHI ’23), April 26, 2023, Hamburg, Germany
- 52th Deutsche Gesellschaft für Psychologie Congress, September 12, 2022, Hildesheim, Germany
- Forschungstage der Wirtschaftspsychologie, April 14, 2022, Bochum, Germany

Darüber hinaus wurden bei allen Studien die Prinzipien des Open Science Ansatzes verfolgt (siehe OSF Project Page Links in diesem Bericht). Somit stehen alle sich aus den Studien ergebenden Datensatze und Auswertungsmanuskripte auf OSF der Öffentlichkeit zur Verfügung. Die veröffentlichten Full-Paper sind ebenfalls vollständig öffentlich zugänglich.

2.6 Liste der Veröffentlichungen

Wissenschaftliche Publikation, Vorträge und Poster:

1. Nele Borgert, Luisa Jansen, Imke Böse, Jennifer Friedauer, M. Angela Sasse, and Malte Elson. 2024. Self-Efficacy and Security Behavior: Results from a Systematic Review of Research Methods. In Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI ’24), May 11–16, 2024, Honolulu, HI, USA. ACM, New York, NY, USA, 32 pages. https://doi.org/10.1145/3613904.3642432
2. Nele Borgert, Oliver D. Reithmaier, Luisa Jansen, Larina Hillemann, Ian Hussey, and Malte Elson. 2023. Home Is Where the Smart Is: Development and Validation of the Cybersecurity Self-Efficacy in Smart Homes (CySESH) Scale. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI ’23), April 23–28, 2023, Hamburg, Germany. ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3544548.3580860
3. Mehrdad Bahrini, Karsten Sohr, Rainer Malaka, Dennis-Kenji Kipker, Nele Borgert, Malte Elson, Hendrik Reichmann. Erfahrbarer Datenschutz und IT-Sicherheit in Smart Home-Anwendungen. Datenschutz und Datensicherheit 45 (2021).
4. Borgert, N., Reithmaier, O.D., Jansen, L., Hillemann, L., Hussey, I., & Elson, M. (2023, September 14). Home Is Where the Smart Is: Development and Validation of the Cybersecurity Self-Efficacy in Smart Homes (CySESH) Scale [Research Talk]. 13th Fachgruppentagung der AOW- und Ingenieurspsychologie, Kassel, Germany.

5. Borgert, N., Böse, I., Jansen, L., Friedauer, J., Sasse, M. A., & Elson, M. (2022, October 1). Same Same, but Different: Lack of Standardization in Measurement of Cybersecurity Self-Efficacy [Symposium – Individual Contribution]. Quo Vadis Digital Democracy, Bonn, Germany.
6. Borgert, N., Böse, I., Jansen, L., Friedauer, J., Sasse, M. A., & Elson, M. (2022, September 15). Same Same, but Different: Lack of Standardization in Measurement of Cybersecurity Self-Efficacy [Symposium – Individual Contribution]. 52th Deutsche Gesellschaft für Psychologie Congress, Hildesheim, Germany.
7. Reithmaier, O.D., Borgert, N., Hillemann, L., Jansen, L., & Elson, M. (2022, September 12). Home is where the Smart is: Development and Validation of the Cyber Security in Smart Homes (CySESH) Scale [Research Talk]. 52th Deutsche Gesellschaft für Psychologie Congress, Hildesheim, Germany.
8. Borgert, N., Friedauer, J., Böse, I., Sasse, M. A., & Elson, M. (2021, September 10). The Study of Cybersecurity Self-Efficacy: A Systematic Literature Review of Methodology [Poster Presentation]. 12th Media Psychology Conference, Aachen, Germany.
9. Borgert, N., Friedauer, J., Böse, I., Sasse, M. A., & Elson, M. (2021, August 9). The Study of Cybersecurity Self-Efficacy: A Systematic Literature Review of Methodology [Poster Paper]. USENIX Symposium on Usable Privacy and Security (SOUPS) 2021, Vancouver, B.C., Canada.

Masterarbeiten:

1. Friederike Vorwerk. Breaking the Trust Barrier: A Manipulation of Trust for Increased Privacy in Smart Homes, 2024.
2. Larina Aylin Hillemann. Development of a scale to measure Cybersecurity Self-Efficacy in Smart Homes, 2022.

Bachelorarbeiten:

1. Rayan Mitkov. Exploring the Educational Benefits: A Comparative Study of Perceived and Tested Knowledge as well as Security Attitudes in a Smart Home Setting, 2024.
2. Amelie Hannah Marie Groeger. Die Erstellung eines Fragebogens zur Messung der Ergebniserwartungen im Kontext der IT-Sicherheit in Bezug auf Smarthome Geräte, 2022.
3. Leonie van Well. Das Internet als externes Gedächtnis: Wie Google und Co. Die menschliche Informationsbeschaffung beeinflussen, 2022.
4. Yvonne Kaltenstadler. Overtrust in Smart Home Sicherheit: Einfluss von Anthropomorphismus in Abhängigkeit kognitiver Heuristiken, 2022.
5. Luisa Anna Jansen. The Measurement of Self-Efficacy in Information Security Research: A mixed Methods Evaluation of Popular Scales, 2021.

3 Anhang

3.1 Literatur

[Bahrini et al., 2021] Mehrdad Bahrini, Karsten Sohr, Rainer Malaka, Dennis-Kenji Kipker, Nele Borgert, Malte Elson, Hendrik Reichmann. Erfahrbarer Datenschutz und IT-Sicherheit in Smart Home-Anwendungen. Datenschutz und Datensicherheit 45 (2021).

[Bahrini et al., 2023] Mehrdad Bahrini, Thomas Münder, Karsten Sohr und Rainer Malaka. Verständliche Informationssicherheit in Smarthome-Netzen. Datenschutz und Datensicherheit 47, 350–353 (2023). https://doi.org/10.1007/s11623-023-1775-z

[Baumgartner und Sitte, 2018] Ulrich Baumgartner/Konstantin Sitte - Abmahnungen von DS-GVO-Verstößen, ZD 2018, 555 ff.

[Bitkom, 2022] bitkom. Das intelligente Zuhause: Smart Home 2022. Ein Bitkom-Studienbericht. Oktober 2022. Zugreifbar unter: https://www.bitkom.org/Bitkom/Publikationen/Das-intelligente-Zuhause-Smart-Home-2022

[Braun, 2018] Steffen Braun: Datenschutz im Smart Office - Gestaltung von Energiemanagementsystem für vernetzte Gebäudeautomation, ZD 2018, 71 ff.

[Danezis et al., 2015] George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, Stefan Schiffner: Privacy and Data Protection by Design - from policy to engineering. CoRR abs/1501.03726 (2015)

[Deterding et. al., 2011] Sebastian Deterding, Dan Dixon, Rilla Khaled, and Lennart Nacke. 2011. From game design elements to gamefulness: defining "gamification". In Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments (MindTrek '11). ACM, New York, NY, USA, 9-15.

[Fernandes et al., 2016] E. Fernandes, J. Jung, A. Prakash Security Analysis of Emerging Smart Home Applications. In Proceedings of 37th IEEE Symposium on Security and Privacy, May 2016.

[Granic et. al., 2014] Granic, I., Lobel, A., & Engels, R. C. M. E. (2014). The benefits of playing video games. American Psychology 69(1), 66-78.

[Howard und Lipner, 2006] Michael Howard and Steve Lipner. 2006. The Security Development Lifecycle. Microsoft Press, Redmond, WA, USA.

[ISO, 2011] International Organization for Standardization. ISO/IEC 27034:2011+ Information technology — Security techniques — Application security, 2011.

[Klerkx et al., 2014] Joris Klerkx, Katrien Verbert und Erik Duval. 2014. Enhancing Learning with Visualization Techniques. In Handbook of Research on Educational Communications and Technology, Springer, New York, NY.

[Kumar et al., 2009] Pushpa Kumar, Nary Subramanian, and Kang Zhang. 2009. SaViT: Technique for Visualization of Digital Home Safety. In Proceedings of the Eighth IEEE/ACIS International Conference on Computer and Information Science, 1120-1125. IEEE.

[Lachenmann, 2017] Neue Anforderungen an die Videoüberwachung - Kritische Betrachtung der Neuregelungen zur Videoüberwachung in DS-GVO und BDSG-neu, ZD 2017, 407 ff.

[Lazovik et al., 2009] Elena Lazovik, Piet den Dulk, Martijn de Groote, Alexander Lazovik, and Marco Aiello. 2009. Services Inside the Smart Home: A Simulation and Visualization Tool. In Service-Oriented Computing, Springer, Berlin, Heidelberg.

[Müller, 2017] Daniel Müller: Reference Security Guide for App-Controlled Smart Home Systems, Masterarbeit, Universität Bremen, 2017.

[Ronen et al., 2017] E. Ronen, A. Shamir, A. O. Weingarten, C. O'Flynn. IoT Goes Nuclear: Creating a ZigBee Chain Reaction, 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, May 2017, pp. 195-212.

[Sorgalla et al., 2018] Sorgalla, J.; Fleck, J. and Sachweh, S. (2018). ARGI: Augmented Reality for Gesture-based Interaction in Variable Smart Environments.In Proceedings of the 13th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications - Volume 2: HUCAPP, ISBN 978-989-758-288-2, pages 102-107.

[Suknot et al., 2014] April Suknot, Timothy Chavez, Nathan Rackley, and Patrick Gage Kelley. 2014. Immaculacy: a game of privacy. In Proceedings of the first ACM SIGCHI annual symposium on Computer-human interaction in play (CHI PLAY '14). ACM, New York, NY, USA, 383-386.

[Thomas und Crandall, 2011] Brian L. Thomas and Aaron S. Crandall. 2011. A demonstration of PyViz, a flexible smart home visualization tool. In Proceedings of the 2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 304-306. IEEE.

[Vermeulen et al., 2009] Jo Vermeulen, Jonathan Slenders, Kris Luyten, and Karin Coninx. 2009. I Bet You Look Good on the Wall: Making the Invisible Computer Visible. In Proc. of the European Conference on Ambient Intelligence (AmI '09). Springer-Verlag, Berlin, Heidelberg, 196-205.

[Zeng et al., 2017] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security & privacy concerns with smart homes. In Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security (SOUPS'17). USENIX Association, Berkeley, CA, USA, 65-80.

[Zeng et al., 2018] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. Use Perceptions of Smart Home IoT Privacy. In Proceedings of the ACM on Human-Computer Interaction - CSCW Archive, Volume 2, Article No. 200.

Verbundprojekt:

Erfahrbarer Datenschutz und IT-Sicherheit in Smarthome-Anwendungen

– UsableSec@Home –

Teilvorhaben: Usable Security in Smart Homes: Motivation, Kompetenz, Entscheidungen

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Kurzbericht
- Ruhr-Universität Bochum -

Hinweis: Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16SV8505 im Rahmen des Programms „Mensch-Technik-Interaktion für digitale Souveränität“ gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Bereits heute werden in vielen Haushalten Smarthome-Geräte genutzt; dieser Trend wird sich in den nächsten Jahren fortsetzen und sogar deutlich verstärken. In Heimnetzen kommen oft sehr unterschiedliche Geräte wie z.B. smarte Lampen, intelligente Türschlösser, digital steuerbare Heizungen, Smart-TVs, IP-Kameras und intelligente Küchengeräte zum Einsatz. Neben den Chancen dieser Technologien bestehen aber auch Risiken, welche die Informationssicherheit und den Datenschutz im eigenen Heim betreffen, ein Bereich, der im Allgemeinen als sehr geschützt angesehen wird. Besonders durch die Vielzahl unterschiedlicher Geräte, die wiederum oft von verschiedenen Herstellern stammen, ist für Nutzer*innen unklar, welchen Sicherheits- und Datenschutzstandards diese Geräte genügen.

Ziel des UsableSec@Home-Projektes war es daher, das Thema „Informationssicherheit und Datenschutz in Smarthome-Anwendungen“ umfassend aus einer nutzer*innenzentrierten Sicht zu betrachten, wobei insbesondere eine Smarthome-App umgesetzt werden sollte, die Nutzer*innen dabei unterstützt, diese Problematik besser zu verstehen und ggf. ihr Handeln anzupassen. Mit der Entwicklung einer App für die Steuerung eines Smarthomes wurden auf Basis von psychologischen Erkenntnissen neue Interaktionsformen für verbesserte Usability und User Experience geschaffen, die die Digitale Souveränität fördern. Neue methodische Ansätze halfen Privacy und Security schon im Mensch-zentrierten Designprozess zu berücksichtigen.

Im Rahmen des UsableSec@Home-Projekts stand die Erforschung von Nutzer*innen-zentrierten Zugängen im Zentrum, Informationssicherheit und Datenschutz besser zu verstehen und entsprechende Verhaltensweisen zu unterstützen. Das Projekt verfolgte das Ziel, die digitale Souveränität der Nutzer*innen zu stärken.

Im Forschungsprojekt haben wir umfangreiche Untersuchungen und Entwicklungen zur Verbesserung der Informationssicherheit und des Datenschutzes in Smart-Home-Systemen durchgeführt. Die zentralen Ergebnisse des Projekts umfassen auch die Identifizierung der psychologischen Faktoren, die das Sicherheitsverhalten der Nutzer*innen beeinflussen, insbesondere die Cybersecurity-Selbstwirksamkeit. Diese stellt die Überzeugung der Nutzeri*nnen dar, mit den unterschiedlichen Aspekten der IT-Sicherheits- und Privatsphäre-Anforderungen ihrer Systeme umgehen zu können.

Durch ein systematisches Literaturreview, welches 168 empirische Publikationen des letzten Jahrzehnts umspannt, und eigenen originalen Studien konnten wir die umfassende Bedeutung der Selbstwirksamkeit im Kontext der Smart-Home-Sicherheit herausarbeiten und darauf basierend Handlungsempfehlungen für die Gestaltung nutzer*innenfreundlicher Sicherheitsschnittstellen entwickeln. Diese Schnittstellen sollten so gestaltet sein, dass sie die Nutzer*innen in die Lage versetzen, Konfigurationen an den Endgeräten eigenständig und sicher vorzunehmen. Diese innovativen Ansätze, die auch im Rahmen von Gamification-Techniken und der Self-Determination Theory erforscht wurden, dienen fundamental der Förderung der individuellen Motivation zur Auseinandersetzung mit komplexen Sicherheitsthemen.

Ein weiteres Kernergebnis des Projekts ist die Entwicklung und Validierung einer kontextspezifischen Skala zur Messung der Cybersecurity-Selbstwirksamkeit in Smart Homes (CySESH). Diese Skala wurde in fünf Studien mit über 1200 Teilnehmenden erprobt und zeigte eine hohe Zuverlässigkeit und Validität. Die Ergebnisse dieser Studien tragen dazu bei, die

Forschung in der Mensch-Computer-Interaktion durch zukunftsweisende Messmethoden voranzutreiben sowie differenzierte Nutzer*innengruppen zu identifizieren, um darauf aufbauend spezifischere Sicherheitslösungen beispielsweise in Konfigurations-Wizards entwickeln zu können.

Durch unser Projekt haben wir auch tiefere Einblicke in das Phänomen Overtrust gewonnen, das auftritt, wenn Nutzer*innen ein übermäßiges Vertrauen in die Sicherheits- und Datenschutzfunktionen ihrer Smarthome-Systeme setzen. Diese Erkenntnisse tragen wesentlich dazu bei, die Bedingungen zu verstehen, unter denen Overtrust entsteht und wie die Interface-Gestaltung von z. B. der im Projekt entwickelten VR-Smarthome-App dies mitigierend beeinflussen kann.

Unsere Forschungsergebnisse bieten somit eine fundamentale Basis für die Entwicklung und den Einsatz motivierender und zielgruppenspezifischer digitaler Anwendungen zur Förderung des Verständnisses von Informationssicherheit und Datenschutz und leisten einen wichtigen Beitrag zur Stärkung der digitalen Autonomie und Sicherheit von Endverbraucher*innen.

Die im UsableSec@Home-Projekt entwickelte AR-Anwendung wird dazu beitragen, dass Nutzer*innen das Thema „Informationssicherheit und Datenschutz“ in ihrem Heimnetz besser verstehen können und durch die Verwendung von modernen Interaktionsformen wie AR motiviert werden, sich tiefer mit der doch oft etwas ermüdenden Thematik zu beschäftigen. Unseres Wissens ist es die erste Anwendung, die auf Basis von Augmented Reality Datenflüsse in Smarthome-Netzen transparent macht. Die AR-Anwendung und ihre Konzepte [Bahrini et al., 2023] stehen zur Verfügung und können in Folgeprojekten oder Verwertungsschritten beispielsweise durch Verbraucher*innenschutzorganisationen genutzt werden.

Ebenso kann die im Projekt entwickelte und validierte Skala zur Erhebung von Cybersecurity Selbstwirksamkeit in Smathome Kontexten (CySESH) in diversen Anwendungskontexten genutzt werden. Dies ermöglicht Interessierten eine wissenschaftlich fundierte Möglichkeit Sachverhalte bedeutungsvoll einschätzen und anpassen zu können. Die CySESH-Skala wurde von uns auf verschiedenen Veranstaltungen zu Disseminationszwecken vorgestellt.

Darüber hinaus wurden bei allen Studien die Prinzipien des Open Science Ansatzes verfolgt (siehe OSF Project Page Links in diesem Bericht). Somit stehen alle sich aus den Studien ergebenden Datensatze und Auswertungsmanuskripte auf OSF der Öffentlichkeit zur Verfügung. Die veröffentlichten Full-Paper sind ebenfalls vollständig öffentlich zugänglich.