Selbstdatenschutz:
Zur Benutzbarkeit von Security & Privacy-Boxen

Masterarbeit zur Erlangung des Master-Grades
Master of Science im Studiengang Medientechnologie
an der Fakultät für Informations-, Medien- und Elektrotechnik
der Technischen Hochschule Köln

vorgelegt von:	Rafael Tarek Bela Mäuer
Matrikel-Nr.:	111 307 23
Adresse:	Sudetenstraße 9
	64342 Seeheim-Jugenheim
	rafael.maeuer@smail.th-koeln.de
eingereicht bei:	Prof. Dr.-Ing. Luigi Lo Iacono
Zweitgutachter:	Prof. Dr. Andreas Heinemann

Köln, 16.12.2020

„If you are not paying for it, you're not the customer; you're the product being sold.“ — Andrew Lewis

Gender Erklärung

In dieser Arbeit wird aus Gründen der besseren Lesbarkeit das generische Maskulinum bei personenbezogenen Substantiven und Pronomen verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint. Es soll keine Benachteiligung implizieren, sondern dient lediglich der sprachlichen Vereinfachung.

Eidesstattliche Erklärung

Ich versichere, die von mir vorgelegte Arbeit selbstständig verfasst zu haben. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder nicht veröffentlichten Arbeiten anderer oder des Verfassers selbst entnommen sind, habe ich als entnommen kenntlich gemacht. Sämtliche Quellen und Hilfsmittel, die ich für die Arbeit benutzt habe, sind angegeben. Die Arbeit hat mit gleichem Inhalt bzw. in wesentlichen Teilen noch keiner anderen Prüfungsbehörde vorgelegen.

Darmstadt, 16.12.2020

Ort, Datum

Rechtsverbindliche Unterschrift

Zusammenfassung

Die wachsende Anzahl an vernetzten Geräten in der heutigen Zeit führt gerade im Privatbereich zu einem erhöhten Aufkommen sensibler und personenbezogener Daten. Damit steigt auch der Bedarf nach Schutzmaßnahmen wie Ad-Blocker und VPN-Dienste an, wobei Security & Privacy-Boxen eine Gesamtlösung anbieten. Für das Marktangebot fehlen allerdings systematische Tests, die Nutzer bei der Kaufentscheidung helfen können. Ein wichtiger Aspekt dabei ist die Umsetzung der Benutzbarkeit. Das Ziel dieser Arbeit ist daher die Untersuchung der Benutzbarkeit von Privacy-Boxen für Privat-Anwender.

Dazu wird folgende Forschungsfrage gestellt: „Wie ist die Usability von Privacy-Boxen zu bewerten, wenn Nutzer sich vor ungewollter Verwendung ihrer Daten sowie Eingriffen in die Privatsphäre schützen möchten?“. Um diese Frage wissenschaftlich zu beantworten, wird im ersten Schritt eine Marktanalyse für Privacy-Boxen durchgeführt, um aus deren Ergebnis eine repräsentative Vorauswahl an Geräten für eine Usability-Evaluation zu bestellen. Anhand einer Zielgruppenanalyse lassen sich für Privacy-Boxen relevante Nutzertypen ermitteln, mithilfe derer sich Geräte und Aufgaben für eine Untersuchung festlegen lassen.

Bei der Analyse des Stands der Forschung wird herausgearbeitet, dass bislang keine geeignete Methodik für eine Usability-Untersuchung von Privacy-Boxen zu existieren scheint. Deshalb wird die Entwicklung einer eigenen Methodik notwendig, um das Ziel der Arbeit durch Beantwortung der Forschungsfrage zu erreichen. Als Grundlage wird ein Modell entwickelt, welches Selbstdatenschutz-Ziele, -Eigenschaften und -Funktionen von Privacy-Boxen beschreibt. Auf Basis des Modells, der Geräte-Vorauswahl und der definierten Nutzertypen wird anschließend eine Evaluationsmethodik für Privacy-Boxen entwickelt.

Die analytische Methodik baut dabei auf existierenden Vorarbeiten, wie etablierten Evaluationsmethoden und Heuristiken auf. Neben Usability- und Privacy-Eigenschaften bei der Nutzung, wird zusätzlich die User Experience (UX) bei Inbetriebnahme von Privacy-Boxen untersucht. Es werden vier Geräte für zwei unterschiedliche Nutzertypen (*Bemühte Amateure* und *Techniker*) auf die zuvor genannten Eigenschaften hin untersucht. Ausgewertet werden die Ergebnisse anhand bereits etablierter sowie selbst definierter Bewertungs-Skalen, die damit eine anschließende Beantwortung der Forschungsfrage ermöglichen.

Anhand der Auswertung zeigt sich, dass die Bewertung der Usability von Privacy-Boxen beim Selbstdatenschutz abhängig vom jeweiligen Nutzertyp ist: den *Bemühten Amateuren* fällt es schwer, Selbstdatenschutz mit Privacy-Boxen zu realisieren. Das liegt allerdings weniger an der guten Usability, als am Mangel der angebotenen Privacy-Funktionen. *Techniker* hingegen profitieren von einer guten Usability und vielzähligen Selbstdatenschutz-Funktionen, allerdings nur bei Privacy-Boxen, deren Inbetriebnahme aufwändiger ist.

Die Ergebnisse zeigen die Relevanz der Betrachtung dieses Marktes: Es existiert ein Mangel an Privacy-Boxen mit vielfältigen Selbstdatenschutz-Funktionen für eine bestimmte Nutzergruppe. Dies betrifft die *Bemühten Amateure*, die sich vor Datenmissbrauch und Privatsphäre-Eingriffen schützen wollen, aber nur geringe Motivation dafür aufbringen. Die Usability wird damit ebenso als Entscheidungskriterium für erfolgreichen Selbstdatenschutz mit Privacy-Boxen identifiziert, wie auch die Anzahl der unterstützten Privacy-Funktionen.

Abstract

The growing number of connected devices today leads to an increased volume of sensitive and personal data, especially in the private sector. With it, the need for protective measures such as ad blockers and VPN services also increases, with Security & Privacy Boxes offering a total solution. However, there is a lack of systematic tests for the market offer, which can help users with their purchase decision. The goal of this work is therefore to investigate the usability of Privacy Boxes for private users.

For this purpose, the following research question is posed: „How is the usability of Privacy Boxes to be evaluated when users want to protect themselves from unwanted use of their data as well as intrusions into their privacy?“. In order to answer this question scientifically, the first step is a market analysis for Privacy Boxes. Based on the results of this analysis, a representative pre-selection of devices for a usability evaluation is ordered. With a target group analysis, relevant user types for Privacy Boxes can be determined. They can be used to define devices and tasks for an usability evaluation.

The analysis of the current state of research shows that no suitable methodology for a usability study of privacy boxes seems to exist so far. Therefore, the development of an own methodology becomes necessary to achieve the goal of the thesis by answering the research question. As foundation, a model describing privacy goals, features, and functions of Privacy Boxes is developed. An evaluation methodology for the usability of Privacy Boxes is then developed based on the model, the device pre-selection, and the defined user types.

The analytical methodology is based on existing prior work, such as established evaluation methods and heuristics. In addition to usability and privacy characteristics during use, the user experience (UX) during the initial setup of Privacy Boxes is analyzed as well. Four devices for two different user types (*Struggling Amateurs* and *Technicians*) are evaluated for the previously mentioned properties. The results are interpreted on the basis of already established and self-defined rating scales. This allows the research question to be answered in the end.

The analysis shows that the evaluation of Privacy Boxes' usability for self-data protection depends on the respective user type: the *Struggling Amateurs* find it difficult to implement self-data protection with Privacy Boxes. However, this is less due to good usability than to the lack of privacy features available. *Technicians*, on the other hand, benefit from good usability and numerous privacy functions, but only with Privacy Boxes that are more complex to set up.

The results show the relevance of investigating this market: There is a lack of Privacy Boxes with diverse self-data protection features for a specific user group. This concerns the *Struggling Amateurs* who want to protect themselves from data misuse and privacy intrusions, but have little motivation to do so. Usability is therefore identified as a decision criterion for successful self-data protection with Privacy Boxes, as is the number of privacy functions supported.

Inhaltsverzeichnis

Abkürzungen

Das Abkürzungsverzeichnis listet alle, in der vorliegenden Arbeit verwendeten, Abkürzungen alphabetisch auf, die nicht aus dem gewöhnlichen Sprachgebrauch ersichtlich sind.

ABT Ad Blocking Tools

ARPU Average Revenue per User

BDSG Bundesdatenschutzgesetz

BSI Bundesamt für Sicherheit in der Informationstechnik

BVerfG Bundesverfassungsgericht

CCPA California Consumer Privacy Act

DIY Do It Yourself

DSGVO Datenschutz-Grundverordnung

EFF Electronic Frontier Foundation

EoL End of Life

ePVO ePrivacy Verordnung

GIS Grundrecht auf informationelle Selbstbestimmung

HW Heuristic Walkthrough

IKS Informations- und Kommunikations-Sektor

IoT Internet of Things

LGPD Lei Geral de Proteção de Dados

MSI Mensch-System-Interaktion

NSA National Security Agency

OBA Online Behavioural Advertising

OOBE Out-of-Box Experience

P3P Platform for Privacy Preferences

PET Privacy Enhancing Technologies

PbD Privacy by Design

PD Personenbezogene Daten

TOM Technische und organisatorische Maßnahmen

TPT Tracking Prevention Tools

UI User Interface

UX User Experience

Glossar

Das Glossar enthält Definitionen[1] der technischen Begriffe, die entweder in Form von Abkürzungen auftreten, oder aus dem gewöhnlichen Sprachgebrauch nicht ersichtlich sind.

DHCP Das Dynamic Host Configuration Protocol (DHCP) beschreibt ein Verfahren, das Clients in einem Netzwerk automatisiert Konfigurationsdaten zuweist.

DNS Das Domain Name System (DNS) verknüpft sprechende URLs mit kryptischen IP-Adressen und zählt zu den wichtigsten Diensten IP-basierter Netzwerke. Als DynDNS (Dynamisches DNS) wird dieses Verfahren bei wechselnden IP-Adressen bezeichnet.

DoS Ein Denial of Service (DoS)-Angriff versucht durch eine gezielt herbeigeführte Überlastung die Nichtverfügbarkeit eines Internetservices herbeizuführen.

FTP Das File Transfer Protocol (FTP) ist ein Netzwerkprotokoll, mit dem sich Daten in einem IP-Netzwerk übertragen lassen.

HTTP Das Hypertext Transfer Protocol (HTTP) kommt in IP-basierten Netzen hauptsächlich für die Übertragung von Daten für Webseiten zwischen Server und Browser zum Einsatz.

IMAP Mit Hilfe des Internet Message Access Protocols (IMAP) ist der Zugriff auf E-Mails eines Mail-Servers möglich. Es erlaubt die Onlineverwaltung der E-Mails direkt auf dem Server und unterstützt Ordnerstrukturen.

IP-Adresse Geräte in einem auf dem Internetprotokoll basierenden Netzwerk erhalten eine IP-Adresse. Mithilfe dieser IP-Adresse sind die Geräte eindeutig identifizierbar.

IPS Ein Intrusion Prevention System (IPS) ist in der Lage, Angriffe auf Netzwerke oder Computersysteme zu erkennen und automatische Abwehrmaßnahmen zu ergreifen.

ISP Ein Internet Service Provider (ISP) ist ein Dienstleister der für Wartung, Verwaltung, Bereitstellung und Ausbau der Infrastruktur des Internets zuständig ist.

Malware Unter Malware, auch Malicious Software oder Schadsoftware, versteht man bösartige, schädliche Software, die nur für den Zweck erzeugt wird, um Schaden anzurichten. Dazu gehören Spyware, Viren, Würmer und Trojaner.

NGFW Bei Next Generation Firewalls (NGFW) handelt es sich um Sicherheitslösungen, die über die Protokoll- und Port-Inspektion klassischer Firewalls hinausgehen und Datenanalysen auf Anwendungsebene ermöglichen.

PFS Perfect Forward Secrecy (PFS) ist eine Methode für den Schlüsselaustausch kryptografischer Verfahren, das die nachträgliche Entschlüsselung durch Bekanntwerden des Hauptschlüssels verhindert.

1 Quellen: IP-Insider – Definitionen (ip-insider.de/specials/definitionen), Security-Insider – Definitionen (security-insider.de/specials/definitionen), SEO-Analyse – SEO-Lexikon (seo-analyse.com/seo-lexikon)

PGP Der Standard Pretty Good Privacy (PGP) nutzt private und öffentliche Schlüssel zum verschlüsseln und signieren von E-Mails. Er basiert auf dem sogenannten Web of Trust, einem auf Gegenseitigkeit aufbauendem Vertrauensmodell.

Phishing Phishing beschreibt den Versuch des Diebstahls von Kennungen und Passwörtern per Internet durch den Versand von gefälschten E-Mails oder SMS.

POP3 Das Post Office Protocol Version 3 (POP3) ist ein Kommunikationsprotokoll, mit dem sich E-Mails von einem Server auflisten, abholen und löschen lassen.

S/MIME Mit dem Standard Secure/Multipurpose Internet Mail Extensions (S/MIME) lassen sich E-Mails verschlüsseln und signieren. Die Technologie basiert auf asymmetrischer Verschlüsselung und verwendet X.509-Zertifikate als Vertrauensmodell.

SEO Search Engine Optimization (SEO) beschreibt Maßnahmen eine Webseite für Suchmaschinen zu optimieren, um in den Ergebnissen möglichst weit vorne zu stehen.

SMTP Das Simple Mail Transfer Protocol (SMTP) ist ein Protokoll zum Versenden von E-Mails in einem IP-Netz zwischen einem E-Mail-Client und einem Server.

SPI Bei Stateful Packet Inspection (SPI) handelt es sich um eine dynamische Paketfiltertechnik für Firewalls, die den Zustand einer Datenverbindung in die Überprüfung der Pakete mit einbezieht und so für eine höhere Sicherheit sorgt.

SSH Secure Shell (SSH) ist ein Protokoll, mit dem sich im IP-Netz über eine verschlüsselte Verbindung auf einen entfernten Rechner zugreifen lässt.

SSL Secure Sockets Layer (SSL) ist ein (veraltetes) Protokoll, mit dem sich Daten durch Verschlüsselung geschützt und sicher übertragen lassen.

TLS Transport Layer Security (TLS) ist der Nachfolger von SSL, mit dem sich Daten verschlüsselt zwischen authentifizierten Kommunikationspartnern über potenziell unsichere IP-Netze wie das Internet übertragen lassen.

TOR Das Tor-Netzwerk (TOR) nutzt das Prinzip des Onion-Routings, um die Verbindungs- und Transferdaten von Nutzern im Internet zu verschlüsseln.

UID Als Unique Identifier (UID) wird eine einzigartige, individuell erstellte Folge aus Buchstaben und Zahlen bezeichnet, anhand derer eine Identifikation möglich ist.

VPN Ein Virtual Private Network (VPN) ermöglicht eine verschlüsselte, zielgerichtete Übertragung von Daten in geschützten und in sich geschlossenen Netzwerken mit verschiedenen Endgeräten.

X.509 Standard für digitale Zertifikate (elektronischer Echtheitsnachweis), der von einer Zertifizierungsstelle ausgestellt wird, um Webseiten mit dem HTTPS-Protokoll oder E-Mails nach dem S/MIME-Standard zu verschlüsseln und zu signieren.

1 Einleitung

Mit dem Wachstum der digitalen Vernetzung und der erhöhten Nutzung von digitalen Diensten im alltäglichen Leben, ist die Menge der verwendeten personenbezogenen Daten in den letzten Jahren massiv angestiegen [138]. Dieser Trend wird durch die wachsende Anzahl an vernetzten Geräten pro Person aus den Bereichen *Internet of Things* (IoT), *Smart Home* und *Wearables* noch begünstigt. *Smart Speaker* im Wohnzimmer, *Smart Watches* am Handgelenk und *Smart Lamps* im Schlafzimmer seien hier als repräsentative Beispiele genannt. Durch die Vielzahl an vernetzten Geräten erhöht sich auch die Menge an digitalen Daten, die in einem Haushalt verarbeitet werden. Diese bestehen zumeist aus sensiblen Informationen über die Nutzer und ihr Verhalten.

Dass ein Interesse an der Sammlung und Auswertung von Nutzerdaten besteht, wird z.B. an der Überwachung durch staatliche Institutionen deutlich. Der „National Security Agency (NSA)"-Skandal, ausgelöst durch die Veröffentlichungen von Edward Snowden, zeigt, dass dies nicht nur auf Spekulationen beruht [12]. Die Einführung des Sozialkreditsystems in China, mit dem ein riesiges soziales Bewertungssystem der Bevölkerung realisiert werden soll, bestätigt dieses Interesse [114]. Durch die Entwicklung von Geschäftsmodellen, die auf der Sammlung und Verwertung von Nutzerdaten basieren, haben sich zudem einige große Plattformen wie z.B. *Google* und *Facebook*[2] etabliert, die zusätzlich ein großes kommerzielles Interesse an Nutzerdaten erkennen lassen.

1.1 Problemstellung

Ein Alltag ohne die Nutzung dieser Plattformen ist heute kaum noch vorstellbar. Die Sammlung und Verwertung von Nutzerdaten birgt jedoch Risiken und Gefahren. Als Beispiel sei der „Cambridge Analytica"-Skandal um Facebook genannt, dem nicht nur die Manipulation des US-Wahlsiegs von 2016, sondern auch des Brexit-Referendums vorgeworfen wird [94]. Neben gesellschaftlichen Einflüssen ist vor allem das Potenzial zur Beeinträchtigung von Privatheit und Selbstbestimmtheit einzelner Personen ein ernstzunehmendes Problem. Der Fall von Juli Briskman z.B. zeigt mögliche Auswirkungen dieser Problematik: Im Oktober 2017 begegnete sie beim Radfahren der Fahrzeugkolonne des US-Präsidenten Trump. Ein Foto ihres Grußes mit dem Mittelfinger ging auf den Sozialen Medien um die Welt. Der Arbeitgeber kündigte ihr daraufhin kurzerhand den Job und begründete dies mit Verletzung von Ethikrichtlinien des Unternehmens [11].

Zur Vermeidung solcher Gefahren muss Datenschutz richtig verstanden und angewendet werden. Einerseits gibt es mit Gesetzen zur Einhaltung und Durchsetzung von Datenschutz staatliche Maßnahmen, die Bürgern den Schutz ihrer Daten ermöglichen. Durch Einführung der DSGVO in der EU, des CCPA in Kalifornien oder des LGPD in Brasilien zeigt sich die Aktualität dieses Themas. Andererseits existieren technische Werkzeuge zum Schutz von Daten und Privatsphäre als Maßnahmen, welche Nutzer für sich selbst ergreifen müssen. Das immer größer werdende Angebot von Werkzeugen wie z.B. Ad-Blocker, Web-Filter und VPN-Dienste zeigt, dass das Bewusstsein für Datenschutz im Privat-Bereich ange-

2 Google LLC (google.de), Facebook Inc. (facebook.com)

kommen ist und sich dort etabliert [140]. Der jüngste Schritt in dieser Entwicklung geht mit sogenannten *Security & Privacy-Boxen* einher. Dabei handelt es sich um Hardware, die viele dieser technischen Schutzfunktionen in einem Gerät bündelt und sich z.B. in ein bestehendes Netzwerk integrieren lässt. Durch eine Filterung des gesamten Datenverkehrs wird so der Schutz aller damit verbundenen Netzwerkteilnehmer möglich. Das Angebot an Security & Privacy-Boxen ist bisher recht gering und reicht von Open Source „Do It Yourself (DIY)"-Projekten, über „Crowd Funding"-Kampagnen bis hin zu kommerziellen Lösungen.

1.2 Ziel der Arbeit

Ziel dieser Arbeit ist es, einen Überblick über das bestehende Angebot an Security & Privacy-Boxen (im Folgenden nur als „Privacy-Boxen" bezeichnet) zu geben, diese miteinander zu vergleichen und hinsichtlich Benutzbarkeit für den Endverbraucher zu untersuchen. Es gilt herauszufinden, wie verschiedene Hersteller die Usability von komplexen Konfigurations-Aufgaben bei Privacy-Boxen umgesetzt haben. Die Arbeit untersucht jedoch nicht, ob die versprochenen Security- und Privacy-Ziele der Geräte auch korrekt umgesetzt werden. Es geht also um die Entwicklung einer neuen Methodik zur Bewertung der Benutzbarkeit, jedoch nicht um die Bewertung des aktuellen Implementierungsstandes existierender Privacy-Boxen.

Bei der Formulierung der Ziele tauchen folgende Fragen auf: Wie gut ist die Benutzbarkeit von Privacy-Boxen umgesetzt? Wie sieht die Nutzer- bzw. Zielgruppe von Privacy-Boxen aus? Wie kommt der Nutzer mit der Bedienung klar, d.h. inwiefern wird er durch das User Interface (UI) bei Einrichtung und Verwendung des Geräts unterstützt?

Mögliche Ergebnisse, die bei der Untersuchung von Privacy-Boxen erwartet werden, sind neben grundlegenden Unterschieden in Leistungs- und Funktionsumfang vor allem Gegensätze in der intuitiven Benutzbarkeit der im Vergleich stehenden Produkte. Dabei werden vor allem Unterschiede bei der Einrichtung und der Verwaltung von Einstellungen zur Verbesserung des Selbstdatenschutzes erwartet. Es wird vermutet, dass in vielen Fällen das erforderliche Know-how des Endanwenders über das Grundwissen der Zielgruppe hinaus geht, um ein Gerät den Bedürfnissen entsprechend zu konfigurieren.

1.3 Methodisches Vorgehen

Zur Untersuchung dieser Fragestellungen ist es notwendig, zunächst ein tieferes Verständnis für die Themen Sicherheit und Privatheit zu entwickeln. Auf dieser Grundlage wird dann erarbeitet, welche Nutzerdaten besonders schützenswert sind und mit welchen technischen Lösungen dieser Schutz erreicht werden kann. Daraus ergibt sich wiederum ein Katalog an Möglichkeiten, mithilfe derer Selbstdatenschutz von Nutzern verbessert werden kann.

Darauf aufbauend lassen sich anschließend Anforderungen entwickeln, welche hinsichtlich Benutzbarkeit an Privacy-Boxen gestellt werden können. Diese Anforderungen werden später auf Usability-Ebene untersucht. Dabei kann z.B. der gesamte Lebenszyklus der Geräte betrachtet werden. Ebenso wird eine Untersuchung der Konfiguration vorhandener Funk-

tionen stattfinden, welche für die Verbesserung der Daten-Privatheit zur Verfügung stehen. Hierbei sollen typische Anwendungsszenarien eines Endanwenders untersucht werden.

Mithilfe einer Marktanalyse wird eine Übersicht der aktuell verfügbaren Privacy-Boxen erarbeitet. Angebote aus dem Profi-Segment werden dabei ausgelassen, da diese für die Zielgruppe nicht relevant sind. Es werden Produkte von kommerziellen Anbietern, „Crowd Funding"-Campagnen und DIY-Projekten vorgestellt. Dabei liegt der Fokus darauf, welche Geräte für eine Untersuchung hinsichtlich einer Verbesserung des Selbstdatenschutzes interessant sein könnten. Da sich der Funktionsumfang der verfügbaren Produkte teilweise stark unterscheidet, werden aus jeder „Kategorie" von Produkten mindestens ein bis zwei repräsentative Modelle bestellt. Dies soll sicherstellen, dass die Untersuchung auf Grundlage einer repräsentativen Auswahl von verfügbaren Geräten stattfinden kann.

Die Auswahl an bestellten Geräten wird anschließend hinsichtlich des Funktionsumfangs untersucht. Ziel ist die Bestimmung einer gemeinsamen Schnittmenge, um die Untersuchung auf einer normalisierten Grundlage durchführen zu können. Mithilfe von analytischen Methoden wird die Benutzbarkeit der Privacy-Boxen anhand von Usability-Methoden und Heuristiken untersucht und bewertet. Hierzu wird bei Aufbau, Einrichtung und Durchführung bestimmter Aufgaben die Umsetzung von Benutzbarkeit und „benutzbarer Privatheit" (engl. Usable Privacy) bei einer Auswahl von Privacy-Boxen untersucht.

1.4 Aufbau und Struktur der Arbeit

Um einen strukturellen Überblick über den Aufbau der vorliegenden Arbeit zu bekommen, werden im Folgenden die Kapitel methodisch kompakt zusammengefasst.

In Kapitel 2 (Grundlagen zu Datenschutz und Usability) wird eine erste Basis für Privacy-Boxen gelegt, indem Grundlagen zum Thema Datenschutz und Benutzbarkeit erarbeitet werden. Nach Definition der wichtigsten Begriffe wird der Nutzer als Urheber von Daten in den Mittelpunkt der Betrachtung gestellt. Es werden Probleme und Risiken aufgezeigt, welche bei der täglichen Nutzung digitaler Dienste entstehen können. Nach der Einführung in Digitale Grundrechte werden Maßnahmen vorgestellt, die zu deren Schutz beitragen. Eine anschließende Einführung in Usability-Grundlagen dient dem Verständnis für die spätere Untersuchung.

Kapitel 3 (Aktueller Forschungsstand / Related Work) befasst sich anhand der Betrachtung von themenverwandten Arbeiten mit dem aktuellen Forschungsstand. Es werden Arbeiten mit Bezug zu Online-Tracking, User-Profiling und Risiken durch IoT und Smart Home vorgestellt. Arbeiten aus den Themenbereichen Privatheit, Selbstdatenschutz und Usability schließen sich daran an.

In Kapitel 4 (Selbstdatenschutz mit Privacy-Boxen) wird die Problemstellung zusammengefasst und die Forschungsfragen werden formuliert. Darauf folgt die Vorstellung von Privacy-Boxen und die Erläuterung ihrer Funktionsweise. Es wird erklärt, mit welchen Mechanismen eine Verbesserung des Selbstdatenschutzes erreicht werden kann. Zu diesem Zweck werden konkrete Werkzeuge vorgestellt, mit denen Nutzer diesen Schutz erreichen können. Anschließend wird überprüft, welche der Werkzeuge mithilfe von Privacy-Boxen umgesetzt

werden können. Zuletzt folgt eine Marktübersicht, aus der eine repräsentative Vorauswahl an Privay-Boxen für die Untersuchung ausgewählt und bestellt wird.

Kapitel 5 (Evaluationsmethodik für Privacy-Boxen) befasst sich anschließend mit der Methodik, welche zur Untersuchung der Benutzbarkeit einer Auswahl von Privacy-Boxen dient. Zu Beginn wird ein Modell erstellt, das Funktionen von Privacy-Boxen mit ähnlichen Zielen in thematischen Bereichen gruppiert. Anhand des Modells lassen sich die Privacy-Funktionen mit den bereits definierten Selbstdatenschutz-Werkzeugen vergleichen. Anschließend folgt die Definition der Zielgruppe, wobei relevante Nutzertypen ermittelt werden. Mithilfe der Zielgruppe können die Geräte der Vorauswahl den Nutzertypen zugeordnet werden. Durch eine Gewichtung der Anwendungsbereiche von Privacy-Boxen, auf Grundlage häufiger Nutzeraktivitäten, können „interessante“ Geräte für einen Vergleich und typische Anwendungsszenarien für die Evaluation ermittelt werden. Damit lässt sich die Methodik für die Untersuchung von Privacy-Boxen unter Berücksichtigung von Usability- und Privacy-Heuristiken entwickeln.

In Kapitel 6 (Untersuchung von Privacy-Boxen und Ergebnisse) wird zunächst die anstehende Durchführung der Evaluation zusammengefasst und mit Test-Durchläufen optimiert. Anschließend folgt die Durchführung und Dokumentation der Untersuchung mithilfe der entwickelten Methodik an einer Auswahl von Privacy-Boxen. Danach werden die daraus gewonnenen Ergebnisse ausgewertet, interpretiert und diskutiert. Zum Schluss werden die Ergebnisse auf Gültigkeit überprüft und mit den Annahmen zu Beginn der Arbeit verglichen.

In Kapitel 7 (Fazit und Ausblick) wird nach einer kritischen Reflexion, über den Verlauf der Arbeit, ein Fazit gezogen. Ein abschließender Ausblick zeigt, welche Aspekte im Rahmen dieser Arbeit nicht betrachtet werden konnten, sich jedoch für Untersuchungen in zukünftigen Arbeiten eignen.

2 Grundlagen zu Datenschutz und Usability

In diesem Kapitel wird der Grundstein gelegt, auf dem anschließend die Fragestellung der Thesis aufbaut. Zuerst wird ein tieferes Verständnis für die Themen Sicherheit und Privatheit geschaffen, um dann entsprechende Begriffe wie Privatsphäre und Identität einführen zu können. Durch diesen thematischen Fokus wird deutlich, warum der Nutzer im Mittelpunkt der Betrachtung steht und welche Bedeutung der Datenschutz für ihn hat. Es werden Risiken und Gefahren für Nutzer aufgezeigt, welche durch die Sammlung und Monetarisierung von Daten entstehen können. Dies führt zum zentralen Thema Selbstdatenschutz hin, als Sammelbegriff für Möglichkeiten, die dem Nutzer zum Schutz seiner Daten zur Verfügung stehen. Anschließend wird das Thema Benutzbarkeit eingeführt, um auf die im weiteren Verlauf folgende Usability-Untersuchung von Privacy-Boxen vorzubereiten.

2.1 Begriffe und Definitionen

Im digitalen Zeitalter des 21. Jahrhunderts werden die Begriffe Sicherheit und Privatheit oft in einem Atemzug genannt. Dies lässt sich dadurch erklären, dass digitale Systeme mittlerweile eine wesentliche Grundlage für Wirtschaft und Gesellschaft der heutigen Zeit bilden. Beim Schutz dieser Systeme lag der Fokus der letzten Jahre vor allem auf der Sicherheit (IT-Sicherheit). Die Wirtschaftlichkeit von Cyber-Angriffen betraf vor allem das Finden von Schwachstellen eines Systems, z.B. um sensible Nutzerdaten zu erbeuten.

Durch die Entwicklung von Geschäftsmodellen, welche auf der „legalen“ Sammlung und Verwertung von sensiblen Nutzerdaten basieren, haben sich einige große Plattformen etabliert, ohne deren Nutzung ein Alltag heute kaum noch vorstellbar ist. Diese Daten-Verwertung birgt jedoch Potenzial die Privatheit und Selbstbestimmtheit von Nutzern zu beeinträchtigen. Daher rückt die Privatheit mittlerweile vermehrt in den Fokus, wenn es um den Schutz digitaler Systeme geht. Diese Entwicklung zeigt sich auch in der Bekanntmachung vom *Bundesministerium für Bildung und Forschung* (BMBF), in der zur Erforschung ökonomischer Aspekte von IT-Sicherheit und Privatheit aufgerufen wird [17]. Aus diesem Grund wird in dieser Arbeit das Thema „Privatheit“ stärker in den Fokus gerückt und im Folgenden noch detaillierter betrachtet.

Um Sicherheit und Privatheit als zentrale Themen dieser Arbeit gut zu begreifen, werden zu Beginn die Begriffe *privat* und *sicher* erst einmal definiert und näher beleuchtet. Darauf aufbauend werden anschließend die Themen *Privatsphäre*, *Identität*, *Anonymität* und *Pseudonym* als Grundlage für die folgenden Kapitel eingeführt.

2.1.1 Sicherheit und Privatheit

Das Wort *sicher* hat seinen Ursprung im Latein und kommt vom Begriff *sē-cūrus*, was so viel wie „sorglos“ oder „unbekümmert“ bedeutet[3]. Das darauf aufbauende Substantiv *Sicherheit* wird vom Duden als „Zustand des Sicherseins, Geschütztseins vor Gefahr oder Schaden“ und als „höchstmögliches Freisein von Gefährdung“ definiert[4]. Laut Bundes-

3 Securus, Übersetzung Latein-Deutsch – Langenscheidt (de.langenscheidt.com/latein-deutsch/securus)
4 Sicherheit, Bedeutung – Duden (duden.de/rechtschreibung/Sicherheit)

zentrale für politische Bildung ist Sicherheit sowohl ein individuelles als auch kollektives Grundbedürfnis, das sich als „Abwesenheit von Gefährdung, sowie Erhalt der psychischen und physischen Unversehrtheit“ definieren lässt [56].

Der Ursprung des Wortes *privat* liegt ebenfalls im Latein und leitet sich vom Begriff *prīvātus* ab, was übersetzt so viel wie „der Herrschaft beraubt“, „gesondert“ oder „für sich stehend“ bedeutet. Damit ist vor allem die Trennung von der öffentliche Sphäre gemeint, welche als staatliche Zugehörigkeit verstanden werden kann. Im heutigen Sprachgebrauch wird der Begriff *privat* zumeist als Gegenteil von *öffentlich* verwendet. Neben dieser räumlichen Bedeutung des Begriffs gibt es jedoch noch weitere Dimensionen, die z.B. auch Handlungen, Verhaltensweisen oder Informationen betreffen können [106, S. 16].

Dimensionen der Privatheit

Der Politologe Alan F. Westin beschreibt in seinem Werk *„Privacy and Freedom“* von 1967 vier Formen des Privaten. Sie bieten eine gute Übersicht über verschiedene Ausprägungen von *Privatheit* und helfen dabei, den Umfang des Begriffs besser zu verstehen [106, S. 17]:

- *Für-sich-Sein (Solitude)* beschreibt die Situation eines Individuums, bei dem es frei von der Wahrnehmung oder Beobachtung anderer ist.
- *Intimität (Intimacy)* gilt als Zustand, bei dem sich Beteiligte in gegenseitigem Vertrauen öffnen können. Der Kontext kann sowohl für Liebesbeziehungen, als auch für kleine Gruppen von Freunden oder Familienmitgliedern gelten.
- *Anonymität (Anonymity)* bezeichnet die Freiheit in der Öffentlichkeit nicht identifiziert, beobachtet oder kontrolliert zu werden.
- *Zurückhaltung (Reserve)* kann mit gesellschaftlichen Anstandsformen verglichen werden. Es geht um die geistige und körperliche Zurückhaltung gegenüber anderen.

Mit Hilfe dieser Übersicht lassen sich zwei Erkenntnisse festhalten. Erstens: es gibt unterschiedliche Intensitäten in der Ausprägung von Privatheit (im Verlauf der Aufzählung nimmt diese ab). Zweitens: es lassen sich unterschiedliche Dimensionen von Privatheit definieren, die sowohl räumlicher, interaktioneller als auch informativer Natur sein können.

Funktionen der Privatheit

Nachdem verschiedene Eigenschaften von Privatheit beschrieben wurden, wird im Folgenden auf die Funktionen von Privatheit eingegangen. Hierzu werden vier Beispiele aus dem Baustein *„Privatsphäre und Big Data“* der politisch und wirtschaftlich unabhängigen EU-Initiative *klicksafe*[5] vorgestellt [106, S. 17]:

- *Persönliche Autonomie* soll Manipulation, Dominanz oder Bloßstellung durch andere verhindern.
- *Emotionaler Ausgleich* ist wichtig um frei von sozialem Druck oder gesellschaftlichen Erwartungen zu sein und innere Ruhe zu finden.

5 Politisch und wirtschaftlich unabhängige Initiative für mehr Sicherheit im Internet (klicksafe.de)

- *Selbst-Evaluation* dient der Reflektion vom Alltag, dem Einordnen von Eindrücken und Erfahrungen sowie dem Ziehen von Schlüssen.
- *Geschützte Kommunikation* hilft sowohl beim vertraulichen Austausch im geschützten Raum, als auch bei der Differenzierung von Kommunikationspartnern und vermittelten Inhalten.

Anhand dieser Funktionen lässt sich erkennen, warum der Schutz von Privatheit wichtig ist und welche Gefahren hinter deren Verletzung lauern können. Der optimale Grad an Privatheit ist ein dynamischer Prozess, der je nach persönlicher Konstitution und Situation variiert. Er kann definiert werden als „das individuelle Bedürfnis nach sozialer Interaktion einerseits und dem nach Privatsphäre andererseits.“ [106, S. 17].

Die Privatsphäre

Das Modell der *Privatsphäre* kann mithilfe der verschiedenen Dimensionen von Privatheit erklärt werden. Dafür ist es notwendig die Privatsphäre als ein Konstrukt zu sehen, welches wie eine Zwiebel aus mehreren Schichten besteht (vgl. Abb. 1): Die äußerste Schicht stellt das geringste Maß an Privatheit dar, repräsentiert durch Gesellschaft, Staat und Wirtschaft. Die inneren Schichten entsprechen verschiedenen Intensitäten von Privatheit, die zur Mitte hin zunehmen. Es folgen Schichten für enge Freundschaften, häusliche Geborgenheit sowie Familie und intime Beziehungen. Die innerste Schicht repräsentiert das höchste Maß an Privatheit und damit Intimität.

Abbildung 1: Modell der Privatsphäre [106, S. 16]

Die Privatsphäre kann als eine Art geschützter Raum verstanden werden, in dem das Agieren unabhängig von der Beeinflussung anderer möglich ist. Sie gibt also jedem Individuum

die Möglichkeit, authentisch und selbstbestimmt die Person sein zu können, die sie sein möchte [106, S. 17]. Die Privatsphäre kann somit als eine Art Legitimation zur authentischen Selbstbestimmung verstanden werden.

Gemäß der *Allgemeinen Erklärung der Menschenrechte der Vereinten Nationen* ist die Privatsphäre sogar ein Menschenrecht, welches das Individuum vor unangemessenen Einmischungen schützen soll. Dieser Schutz beginnt bei neugierigen Nachbarn und soll auch bei Institutionen wie Unternehmen oder Regierungen gelten [87, S. 22]. Es geht um die Einflussnahme, also die Souveränität über Inhalt, Zeitpunkt und Kontext bei der Preisgabe von persönlichen Informationen entscheiden zu können [87, S. 17].

Da es in dieser Arbeit um Selbstdatenschutz geht, ist die *informationelle Dimension* der Privatsphäre von besonderem Interesse. Deshalb wird sie im weiteren Verlauf der Arbeit synonym mit Privatsphäre verwendet.

2.1.2 Identität und Anonymität

Um persönliche Daten, und damit die eigene Privatsphäre, schützen zu können, muss zuerst der Wert der Privatsphäre für das Menschsein – und damit die Identität einer Person – ermittelt werden. [106, S. 15]. Aus diesem Grund wird zunächst der Begriff *Identität* definiert, um im weiteren Verlauf mithilfe von *Anonymität* und *Pseudonym* auf deren Verbindung zu Privatheit zurück zu kommen.

Identität

Eine Definition im Duden[6] beschreibt *Identität* als „Echtheit einer Person oder Sache“ bzw. als „völlige Übereinstimmung mit dem was sie ist, oder als was sie bezeichnet wird“. Im digitalen Zeitalter muss bei der Definition von Identität jedoch berücksichtigt werden, dass zu der Summe an Dingen, die eine Person ausmacht, auch ihre Online-Aktivität dazugehört. Aus diesem Grund sollte bei der Identität eines Menschen von der *Vereinigung* gesprochen werden, die seiner *Präsenz in der Online- und Offline-Welt* gleicht [87, S. 22-23].

In der folgenden Aussage wird die Korrelation zwischen Identität und Privatsphäre noch einmal verdeutlicht, da der Begriff der Identität verwendet wird, um eine Gefährdung der Privatsphäre und damit der Sicherheit einer Person zu beschreiben: „In der digitalen Welt ist Identität der treffendere Begriff, um die Gefährdung der Privatsphäre zu begreifen. (...) Wer seine Privatsphäre schützen will, muss die Kontrolle über möglichst viele Bestandteile seiner Identität erlangen und bewahren.“ [87, S. 24].

Nach dieser Erkenntnis ergibt sich die wichtige Frage, welche Veränderungen sich seit der Einführung des Social Web[7] für die Identität ergeben haben? Eine notwendige Voraussetzung für das Erkennen von Risiken ist die Sensibilisierung für Situationen und Umstände der heutigen Zeit. Dazu gehört das Einschätzen von Gefahren für die persönliche Privatsphäre, und damit die Identität, die von hinterlassen Datenspuren im Internet ausgehen [106, S. 18 u. 20].

6 Identität, Bedeutung – Duden (duden.de/rechtschreibung/Identitaet)
7 Menge an sozialen Beziehungen und Netzwerken, die Menschen im Internet miteinander verbindet [70]

Anonymität und Pseudonym

Mit der Frage nach Schutz der persönlichen Identität ist es notwendig auch die Begriffe Anonymität und Pseudonymität zu definieren. *Anonymität* wird im Duden als „das Nichtbekanntsein, Nichtgenanntsein“ oder als „Namenlosigkeit“ definiert[8]. Darauf aufbauend beschreibt das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) Anonymität als Zustand eines Vorgangs, bei dem die Identität beteiligter Instanzen nicht mehr bestimmbar ist. Dies kann einen der folgenden Gründe haben [23]:

- Die Instanz ist den anderen beteiligten Instanzen nicht bekannt.
- Die Instanz tritt gegenüber den anderen beteiligten Instanzen nicht in Erscheinung.
- Die Instanz agiert innerhalb des anonymen Vorgangs ohne erkennbaren Namen.

In jedem der drei Fälle kann durch Anonymität die Identität einer Person geschützt werden. Nach §3 Abs. 6 Bundesdatenschutzgesetz (BDSG) ist Anonymisieren „(...) das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.“ [10].

Als *Pseudonym* hingegen wird ein angenommener, nicht dem wirklichen Namen entsprechender „Deckname“ bezeichnet[9]. Nach §3 Abs. 6a BDSG ist Pseudonymisieren „(...) das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.“ [10].

Mithilfe der Definition von Identität, Anonymität und Pseudonym, die teilweise sogar in Gesetzen eine rechtliche Grundlage besitzen, lässt sich nun besser begreifen, warum Nutzer im Mittelpunkt der Betrachtung stehen. Die Nachteile, welche ihnen durch die Preisgabe privater Informationen entstehen können, werden im nächsten Abschnitt näher beleuchtet.

2.2 Personenbezogene Daten

Personenbezogene Daten (PD) sind laut Datenschutz-Grundverordnung (DSGVO) „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“ [41]. Durch die digitale Form von PD sind preisgegebene Informationen nicht mehr flüchtig, sondern liegen beständig, langfristig verfügbar und für Suchmaschinen indexierbar vor. Sie lassen sich beliebig vervielfältigen, zusammensetzen und aus ihrem ursprünglichen Kontext lösen. Jeder Mensch braucht jedoch unterschiedliche soziale Rollen, die er in verschiedenen Kontexten ausleben kann.

Durch die fehlende soziale, räumliche und zeitliche Abgrenzung des Internets gehen die verschiedenen sozialen Kontexte der Daten verloren. Die Öffentlichkeit dieser aus dem Kontext gelösten und neu zusammenstell- und interpretierbaren Daten kann zu großen

8 Anonymität, Bedeutung – Duden (duden.de/rechtschreibung/Anonymitaet)
9 Pseudonym, Bedeutung – Duden (duden.de/rechtschreibung/Pseudonym)

Problemen führen. Das Wissen, welches mittels Algorithmen aus scheinbar harmlosen Angaben gewonnen werden kann, bedroht die Privatsphäre der Nutzer [106, S. 21]. Dies führt zu der Fragestellung: Wer hat ein Interesse an – freiwillig oder unfreiwillig – preisgegebenen privaten Informationen und zu welchem Zweck?

2.2.1 Interessen von Staat und Unternehmen

Auch wenn immer mehr Staaten und Länder Datenschutz-Verordnungen verabschieden wie die Datenschutz-Grundverordnung (DSGVO), den California Consumer Privacy Act (CCPA) und das Lei Geral de Proteção de Dados (LGPD), existiert ein zeitlicher Wettlauf zwischen Datensammlern und Datenschützern. Das Problem für dieses Dilemma soll in diesem Abschnitt näher betrachtet werden. Es muss zunächst klar werden, warum Regierungen und Unternehmen Interesse an den Daten von Bürgern haben, bevor darauf eingegangen wird, mit welchen Methoden diese gesammelt und verarbeitet werden können und welche Methoden zum Schutz davor existieren.

Staatliche Interessen

Regierungen, insbesondere Sicherheitsbehörden und Geheimdienste, haben ein großes Interesse an personenbezogenen Daten, denn Daten bedeuten Informationen und Wissen. Entsprechend verwendet, können sie Macht bedeuten und zur Kontrolle genutzt werden – ein Blick auf China und Russland reicht als Beweis schon aus [14]. Die Frage, die hier allerdings gestellt werden muss, lautet: Auf welcher rechtlichen Grundlage können Regierungen Daten ihrer Bürger sammeln und auswerten? Anhand einiger Gesetze wie z.B. der Vorratsdatenspeicherung, der Telekommunikations-Überwachungsverordnung (TKÜV), dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G-10-Gesetz) oder der Strafprozessordnung lassen sich auch in Deutschland deutliche Intentionen zur Überwachung der Bürger erkennen [102, S. 3-4].

Neben den offiziellen Möglichkeiten gibt es noch gesetzliche Grauzonen, in der Überwachungsprogramme wie *PRISM*, *Tempora* und *XKeyscore*[10], sowie umfangreiche staatliche Datenbanken eingesetzt werden, um Informationen über Bürger zu sammeln und zu speichern. Zusätzlich geben viele Unternehmen Polizei und Geheimdiensten Zugang zu sensiblen privaten Daten aus den Bereichen Finanzen, Mobilfunk, Mobilität, Kommunikations-Dienste und Soziale Netzwerke [122]. Diese Grauzone existiert, da Gesetze immer den Entwicklungen der realen Welt hinterherhinken, egal wie bemüht und erfolgreich Beamte und Aufsichtsbehörden versuchen, den Schutz von Bürgern durchzusetzen [87, S. 16].

Kommerzielle Interessen

Viele Firmen verkaufen Produkte und Services mithilfe von Werbung und Angeboten, die auf Basis von Daten auf den Kunden zugeschnitten sind. Unternehmen stellen kostenlose digitale Angebote bereit, welche durch Werbung oder Datenhandel finanziert werden. Es zeichnet sich ein Paradigmenwechsel zu einer „Data-Driven Economy“ ab, da Unternehmen im Informations- und Kommunikations-Sektor (IKS) verstärkt auf das Sammeln

10 Überwachungsprogramme von NSA (PRISM) und britischem Geheimdienst (Tempora) [90]; „Allsehendes Internet-Auge“ der NSA mit weltweitem Zugriff auf Netzwerkkommunikation (XKeyscore) [163]

personenbezogener Daten setzen, um ihre Services und Produkte perfekt auf den Kunden abstimmen zu können [102, S. 3].

In diesem recht neuen Sektor für Digitale Werbung, in dem pro Jahr mittlerweile Milliarden an US-Dollar umgesetzt werden, haben sich eine Vielzahl an Unternehmen darauf spezialisiert, Profit aus dem Weiterverkauf von Daten und den daraus berechneten Analysen zu erzielen [55]. Einige der größten Unternehmen, die als „Datensammler“ agieren, sind Facebook, *Alphabet* (Holding von Google) und *Palantir* sowie *Oracle*, *Acxiom* und *Segment*[11]. Gerade letztere drei besitzen Tochterunternehmen oder Kooperationspartner, die sich auf Datensammlung und -verwertung spezialisiert haben, oder aus anderen Bereichen wie Immobilienmarkt oder Anbietern für Consent-Management[12] Nutzerdaten abrufen können [148, S. 12-21].

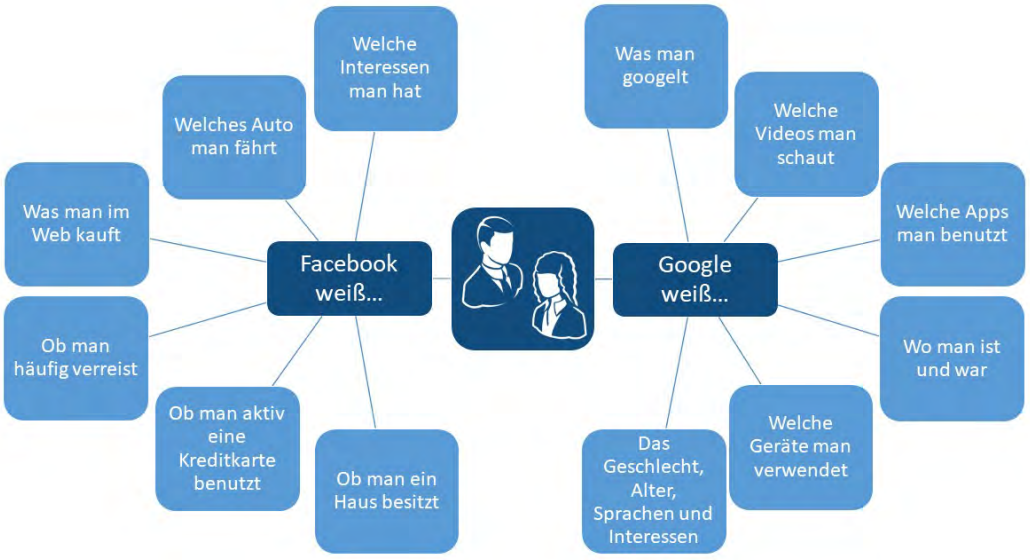


Abbildung 2: Wer weiß was über mich? (modifiziert nach [165])

Abb. 2 zeigt sehr deutlich, dass alleine Facebook und Google bereits ausreichen, um den Großteil an Informationen über einen Nutzer zu bestimmen, die seine Identität ausmachen. Die Methoden, mit denen diese Nutzerdaten im großen Stil gesammelt und in Profit umgewandelt werden, sollen im nächsten Abschnitt vorgestellt werden.

2.2.2 Tracking und Data-Mining

Um zu verstehen, wie aus Nutzerdaten Profit generiert werden kann, ist es sinnvoll, zuerst den Begriff *Big Data* einzuführen und zu erklären wie *Cookies* oder *Fingerprinting*-Methoden funktionieren. Darauf aufbauend können die Methoden *Tracking*, *Scoring* und *Profiling* erläutert werden. Dies schafft eine Grundlage, anhand derer im weiteren Verlauf der Wert eines Nutzers bestimmt und nachvollzogen werden kann.

11 Alphabet Inc. (abc.xyz), Palantir Tech. Inc. (palantir.com), Oracle Corporation (oracle.com), Acxiom Deutschland GmbH (www.acxiom.de), Segment.io Inc. (segment.com)
12 Immobilien Scout GmbH (immobilienscout24.de), LiveRamp Holdings, Inc. (liveramp.com)

Big Data

Durch die Verwendung elektronischer Dienste im alltäglichen Leben hinterlassen Nutzer große Mengen an Daten in ihrer digitalen Umgebung, welche als *Datenspuren* bezeichnet werden. Als repräsentative Beispiele können EC-Zahlungen, Telefonate über Mobilfunk, Buchungen von Reisen oder das Surfen im Internet genannt werden [120]. Viele Firmen haben ein finanzielles Interesse daran entwickelt, die vermehrte Sammlung und Speicherung von Datenspuren kommerziell zu verwerten und ihr Kerngeschäft darauf aufgebaut.

Die Anhäufung dieser Daten-Mengen, die nur noch maschinell analysier- und auswertbar sind, werden unter dem Sammelbegriff *Big Data* zusammengefasst [106, S. 21]. Durch geschickte Analysen mithilfe von Algorithmen können aus der Masse an Daten, die im Einzelnen vielleicht nutzlos erscheinen, im Zusammenhang wertvolle Informationen wie Trends oder globale Zusammenhänge erkannt werden.

Durch die automatische Erfassung und Aktualität der Daten, sowie fortschrittliche Algorithmen, sind so Rückschlüsse in einer gewaltigen Dimension möglich. Die Unternehmen *dm*, *OTTO* und *TomTom*[13] nutzen Big Data z.B. zur Mitarbeitereinsatzplanung, zur Verbesserung der Absatzprognose und zum Flottenmanagement in Echtzeit [16].

Tracking und Tracing

Das Verfolgen des Verhaltens einer Person anhand bestimmter Eigenschaften wird *Tracking* oder *Tracing* genannt. Tracking im Internet bedeutet daher die Beobachtung des Surf-, Nutzungs- und Konsumverhaltens von Personen [106, S. 22]. Erfolg Tracking über einen längeren Zeitraum oder über verschiedene Orte hinweg, so wird auch von *Tracing*[14] gesprochen. Der Ablauf von Nutzeraktivitäten ist zeitlich und/oder räumlich versetzt und wird zu Auswertungszwecken zurückverfolgt und rekonstruiert.

Dass Online-Tracking bereits eine etablierte Praxis ist, wird deutlich, wenn der Besuch einer Website im Durchschnitt 56 Tracking-Vorgänge auslöst, von denen 40% zu Werbezwecken genutzt werden [106, S. 22]. Im Rahmen der Cliqz-Studie *„Tracking the Trackers“* wurde ermittelt, dass bei 200.000 Nutzern innerhalb einer siebentägigen Untersuchung im Durchschnitt 95% aller Seitenaufrufe eine Anfrage an einen potentiellen Tracker erzeugen [177, S. 124]. Durch Beobachtung des Surf-Verhaltens (Surf-Historie) von Nutzern können zudem einzigartige Fingerabdrücke erzeugt werden, wie die Studie *„Why Johnny Can't Browse in Peace“* zeigt. Bei einer Untersuchung mit 370.000 Nutzern wurde festgestellt, dass 70% aller Nutzer nach dem Besuch von nur vier Webseiten mit einer Wahrscheinlichkeit von 97% identifiziert werden können [137, S. 1].

Mithilfe der durch Tracking gesammelten Daten ist es anschließend möglich, das detaillierte Profil eines Nutzers zu erstellen, welches Einblicke in sein Privatleben ermöglicht. Durch die zusätzliche Verbindung mit Tracking-Daten aus der Offline-Welt (z.B. durch Nutzung von Kreditkarten, Kundenkarten oder Bonusprogrammen) kann die Qualität der Personen-Zuordnung nochmal deutlich verbessert werden, was den Wert von Analysen und Vorhersagen steigert. Dieser Wert ist natürlich von Menge und Qualität der Rohdaten

13 dm-drogerie markt GmbH (dm.de), Otto GmbH (otto.de), TomTom Int. BV. (tomtom.com)
14 Tracing, Bedeutung – Duden (duden.de/rechtschreibung/Tracing)

abhängig, die einem Individuum zugeordnet werden können [106, S. 22-23]. Auf Grundlage dieser Analysen und Vorhersagen kann dann mithilfe von Online-Auktionen, die in Sekunden-Bruchteilen im Hintergrund ablaufen (Real-Time Bidding) entschieden werden, welche Werbung der Nutzer zu sehen bekommt [148, S. 28].

Scoring

Als *Scoring* wird die zahlenmäßige Bewertung der Eigenschaft einer Person bezeichnet, die auf mathematisch-statistischer Analyse von Erfahrungswerten basiert. Hierbei wird die Analyse der Vergangenheit benutzt, um zukünftiges Verhalten vorherzusagen. Scoring basiert dabei auf der Annahme, dass das Verhalten von Nutzern basierend auf vergleichbaren Merkmalen anderer Personen vorhergesagt werden kann. Als Grundlage für die Berechnung von Scores können z.B. Daten verwendet werden, die mithilfe von Tracking gesammelt und gespeichert wurden [106, S. 23].

Scoring dient oft als Grundlage zur Berechnung von Risiko-Einschätzungen z.B. für Arbeitsleistungen, kriminelles Verhalten oder den Gesundheitszustand von Personen. Ein sehr bekanntes Beispiel ist die *Schufa*[15], welche mithilfe von Scores die Kreditwürdigkeit von Personen berechnet. Ein Szenario, welches sich durch die Verbreitung von Scoring abzeichnet, ist die Erstellung von individuellen kundenspezifischen Preisen auf Grundlage von berechneten Scores. Ein Beispiel, wo dieses Verfahren schon angewendet wird, ist der Versicherer *Axa Global Direct*[16], der nach eigenen Angaben individuelle Kunden-Prämien durch eine Auswertung von ca. 50 verschiedenen Variablen berechnet [106, S. 23].

Profiling

Der nächste logische Schritt, der auf Tracking und Scoring eines Nutzers folgt, ist die Erstellung eines digitalen Nutzer-Profils durch Klassifizierung und Bewertung von persönlichen Eigenschaften. Aus diesen Profilen lassen sich sensible Informationen wie politische oder religiöse Einstellung, Gesundheit, Sexualität, Gefühle und Stimmungen ableiten. Für Organisationen und Unternehmen, die im Besitz solcher Profile sind, ergeben sich daraus Möglichkeiten zur Manipulation und Diskriminierung von Nutzern bis hin zu sozialer Kontrolle und Überwachung. Für Nutzer bedeutet dies eine massive Einschränkungen in ihrer Entscheidungs- und Handlungsfreiheit [106, S. 24].

Die Profil-Erstellung wird von manchen Nutzern sogar selbst noch optimiert, indem sie freiwillig wertvolle Informationen wie z.B. Fitness- und Vital-Daten von Smart Watches oder Fitness-Trackern preisgeben. Aber auch von Nutzern, die selbst nicht online aktiv sind, können mithilfe der Datenpreisgabe von Freunden und Bekannten Profile erstellt werden. Dies geschieht z.B. bei Facebook auch wenn die Person die Plattform gar nicht selbst nutzt und kein Facebook-Konto besitzt [106, S. 21]. Mithilfe von Adressbuch-Daten bereits registrierter Nutzer werden für alle nicht registrierten Nutzer „Schattenprofile“ angelegt. Meldet sich eine Person doch noch bei Facebook an, wird das bereits existierende Schattenprofil mit dem Nutzer-Profil zusammengeführt [65].

15 SCHUFA Holding AG (schufa.de/schufa)
16 AXA Konzern AG (www.axa.de/wir-ueber-uns)

Cookies

Die von Nutzern generierten Datenspuren bestehen größtenteils aus Informationen, welche bei der Online-Nutzung digitaler Dienste entstehen. Das Sammeln von Daten beim Besuch von Webseiten geschieht durch die Verwendung von *Browser-Cookies*. „Cookies sind Datenpakete, die zwischen Computerprogrammen ausgetauscht werden. Allgemein werden mit dem Begriff meist HTTP-Cookies bezeichnet, mit deren Hilfe Websites Nutzerdaten lokal und serverseitig speichern, um einzelne Funktionen und Webanwendungen wie Onlineshops, soziale Netzwerke und Foren nutzerfreundlicher gestalten zu können.“ [96].

Der Web-Browser speichert Cookies in Form von kleinen Dateien auf dem Computer, sobald ein Nutzer zum ersten Mal eine Seite im Internet aufruft. Sie beinhalten eine zufällig generierte einzigartige Kennung (UID), mit dem das benutzte Gerät identifiziert werden kann. Des Weiteren können Domainname der Webseite, Nutzersprache und -präferenzen, Uhrzeit, Formulardaten, Navigationsverlauf und andere Meta-Daten abgespeichert werden. Eine Website erkennt so anhand des Cookies, welcher Nutzer sie gerade besucht und kann sich dadurch in gewissem Rahmen an dessen Bedürfnisse anpassen [96].

Es lassen sich generell zwei Arten von Cookies unterscheiden:

- *First-Party-Cookies* kommen vom Seitenbetreiber selbst, sind für die Funktion der Webseite notwendig und verbessern das Nutzererlebnis.
- *Third-Party-Cookies* kommen von Dritten (Werbetreibende) und werden dazu verwendet das Surfverhalten von Nutzern aufzuzeichnen.

Cookies haben ein Ablaufdatum, welches so gesetzt werden kann, dass sie nach dem Besuch einer Webseite automatisch gelöscht werden (z.B. bei Webseiten für Online-Banking). In vielen Fällen wird das Verfallsdatum von Cookies jedoch auf ein Datum weit in der Zukunft gesetzt. So lassen sich bei Wiederkehr des Nutzers die bereits gespeicherten Informationen verwenden und weitere Informationen sammeln. Dies geschieht oft über einen langen Zeitraum hinweg und manchmal sogar webseitenübergreifend, bis der Cookie abläuft oder manuell gelöscht wird [96].

Fingerprinting und Super-Cookies

Neben Cookies gibt es noch eine Reihe von alternativen Tracking-Methoden. Es kann hierbei zwischen Verfahren unterschieden werden, die in Web-Browsern zum Einsatz kommen und Lösungen, die speziell für mobile Anwendungen auf Smartphones konzipiert sind.

Letztere Variante bietet nur sehr eingeschränkte Tracking-Möglichkeiten, da die gewonnenen Informationen nicht in anderen Apps genutzt werden können. Wird jedoch auf die gerätespezifischen Werbe-IDs zurückgegriffen, die sowohl unter Android als auch iOS zur Verfügung stehen, so lassen sich gesammelte Daten anwendungsübergreifend auf einzelne Nutzer zurückführen. Diese Werbe-UIDs lassen sich jedoch vom Nutzer zurücksetzen, sodass zukünftige Daten dem Gerät nicht mehr zugeordnet werden können. Zusätzlich können Nutzer ihre Einwilligung über die Nutzung von UIDs zu Werbezwecken generell entziehen (Opt-out) [25, S. 21-22].

Bei browserbasierten Technologien ist *Fingerprinting* (Fingerabdruck-Berechnung) eine gängige Methode, um ein Gerät anhand einer bestimmten Kombination von Hard- und Software-Merkmalen wiederzuerkennen. Dabei kann zwischen Browser- und Canvas-Fingerprinting unterschieden werden. Der Fingerabdruck des Browsers wird anhand von HTTP-Header-Attributen bestimmt und lässt so Rückschlüsse auf das genutzte Betriebssystem, die Browser-Version, Uhrzeit, Sprache und weitere Informationen wie Bildschirmauflösung, installierte Schriftarten und Browser-Plugins zu. Beim Canvas-Fingerprinting wird ein *HTML5-Canvas-Element*[17] genutzt, um JavaScript-Attribute wie Kanten-, Schriftglättung oder die Version von Grafikkarte und -Treiber zu bestimmen. Durch die Vielzahl an möglichen Attributen ist dieser Fingerabdruck in den meisten Fällen einzigartig und lässt damit auch eine eindeutige Identifikation des Nutzers zu [25, S. 13-15].

Eine weitere Variante des browserbasierten Trackings ist der Einsatz von Flash-Cookies. Hierbei handelt es sich, wie bei Cookies auch, um kleine Dateien, die auf dem genutzten Gerät abgespeichert werden. Sie können dann mithilfe des *Adobe Flash Player*[18] ausgelesen und beschrieben werden. Da diese Flash-Cookies kein Ablaufdatum haben, beim Löschen des Browser-Cache erhalten bleiben und sich nicht über Datenschutzeinstellungen des Browsers ablehnen lassen, werden sie auch als *Super-Cookies* bezeichnet [25, S. 19].

Nachdem Methoden zum Sammeln, Auswerten und Klassifizieren von Nutzerdaten, sowie dazu notwendige technische Grundlagen erklärt wurden, wird im Anschluss gezeigt, warum sich dieser Aufwand lohnt und welche Probleme für Nutzer daraus entstehen können.

2.2.3 Probleme, Risiken und Gefahren

„Wenn Sie für etwas nichts bezahlen, sind Sie nicht der Kunde. Sie sind das Produkt, das verkauft wird.“ Diesen Satz schrieb der Nutzer *blue_beetle* (Andrew Lewis) 2010 im Online-Blog *MetaFilter*, der als Meme bekannt wurde und sich seitdem weit im Internet verbreitet hat [112]. Es zeigt, dass sich langsam ein Bewusstsein dafür formt, das Nutzer kostenloser Angebote im Internet mit ihren Daten bezahlen. Mit dem folgenden Abschnitt soll ein Bewusstsein für den Wert bzw. Preis eines Nutzers geschaffen werden, um die Notwendigkeit von Selbstdatenschutz deutlich zu machen.

Der Wert des Nutzers

Die meisten Menschen ahnen, dass sie einen Preis zahlen, wenn sie beliebten kostenlosen Diensten wie Facebook, *Twitter* oder *Instagram*[19] beitreten. Sie geben ihre persönlichen Informationen an diese Plattformen und viele andere Werbenetzwerke preis. Obwohl das Misstrauen gegenüber den genannten Diensten wächst, werden die meisten Dienste jedoch weiter genutzt – oft aus Bequemlichkeit [87, S. 32-33].

In der Studie *„Der Preis des Kostenlosen“* aus dem Jahr 2016 von Peter Buxmann, Professor für Wirtschaftsinformatik an der *TU Darmstadt*, wurden etwa 1.000 Teilnehmer befragt, was ihnen ihre Daten wert seien. Zusätzlich wurde gefragt wie hoch die Akzeptanz

17 Das Canvas-Element ist eine Fläche auf der mittels JavaScript gezeichnet werden kann [25, S. 14]
18 Adobe Flash Player (get.adobe.com/de/flashplayer) – wird am 31. Dezember 2020 eingestellt
19 Twitter Inc. (twitter.com), Instagram (instagram.com)

für Geschäftsmodelle sei, die vordergründig kostenlos erscheinen, aber eigentlich mit Nutzerdaten Geld verdienen [24]. Das Ergebnis zeigte deutlich: je älter die Befragten, desto skeptischer sind sie im Bezug auf die genannten Geschäftsmodelle. Abb. 3 zeigt, dass bis zu 40% der Befragten über 60 Jahre um ihre Privatsphäre besorgt sind, wohingegen jüngere Generationen weniger Bedenken haben. Nur noch etwa 20% der Befragten im Alter zwischen 14 und 29 Jahren machen sich Gedanken über ihre Daten.

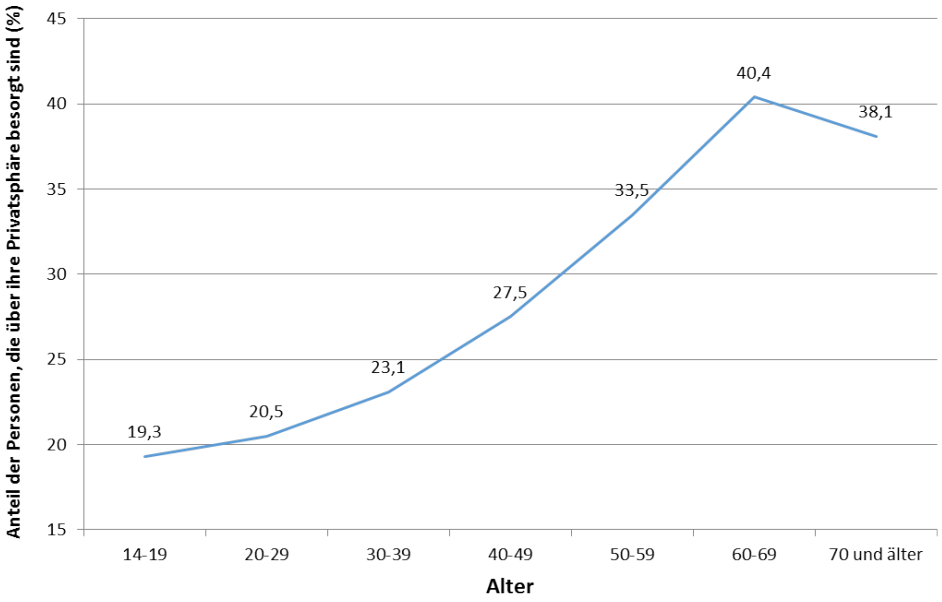


Abbildung 3: Bedenken über Privatsphäre nach Alter (modifiziert nach [24])

Um den tatsächlichen Wert eines Nutzers zu bestimmen, gibt es verschiedene Ansätze:

Eine erste Schätzung kann sich anhand der Strafe von Unternehmen für den unerlaubten Upload von Adressbüchern auf Firmen-Server orientieren. US-Anwälte veranschlagten Strafen in Höhe von 60 Cent bis drei US-Dollar für jeden einzelnen Kontakt [142]. Dies entspräche dem Wert, den Anbieter für die Anwerbung eines Nutzers zur weiteren Monetarisierung seiner Daten bezahlen würden.

Eine andere Möglichkeit ist die Berechnung der Kopfprämie „Average Revenue per User“ (ARPU), welche sich mithilfe des Quotienten von Unternehmensumsatz und Nutzeranzahl bestimmen lässt. Dieser Wert lag 2017 für das Unternehmen Google weltweit bei 137 US-Dollar für den durchschnittlichen Umsatz pro Nutzer [66].

Eine dritte Möglichkeit besteht darin, den Wert jedes einzelnen Nutzers in Relation zur finanziellen Bewertung des jeweiligen Unternehmens zu setzten. Facebook kam bei dieser Bewertung 2014 auf einen Wert von 141 US-Dollar pro Kopf [162]. Je nach Methode und Unternehmen variiert dieser Wert also zwischen einigen Cent und hunderten US-Dollar pro Nutzer [87, S. 46-47].

Ein etwas anderer Ansatz liegt darin, den Wert eines Nutzers anhand der durch ihn generierten Werbe-Einnahmen zu berechnen. Laut Higinio Maycotte, ehemaliger CEO des Dienstleisters *Umbel* (mittlerweile *MVPindex*[20]), der Datenanalysen im Bereich Entertain-

20 U-MVPindex, LLC (mvpindex.com)

ment und Sport verkauft, ist jeder Nutzer rund 30 US-Dollar pro Monat auf einem einzigen Werbenetzwerk wert. Da beim Verrichten täglicher Geschäfte jeder Nutzer von etwa 75-100 verschiedenen Werbenetzwerken getrackt wird, ergibt sich daraus ein Wert von durchschnittlich 87,5 US-Dollar für einen einzelnen Nutzer pro Tag [87, S. 54-55].

Anhand dieser Beispiele lässt sich deutlich erkennen, wie lukrativ das Geschäft mit Nutzerdaten ist. Umso wichtiger ist es jedoch, dass immer mehr Menschen ein Bewusstsein für den Wert der eigenen (digitalen) Identität entwickeln und diese auch schützen [87, S. 51].

Das Privacy-Paradox

Als *Privacy-Paradox* wird das Phänomen beschrieben, dass Nutzer den Schutz ihrer Privatsphäre zwar generell für wichtig halten, dies aber nicht unbedingt auf ihr Handeln übertragen. In der Studie *„Sicherheitsbewusstsein bei der Nutzung von Apps“* von *mediaTest digital* kam 2013 heraus, dass 70% der Nutzer Datenschutz als wichtig erachten. Sogar 85% der Teilnehmer würden von der Nutzung einer App aufgrund von Angst vor Datenmissbrauch oder -verlust absehen. Allerdings gaben 51% der Befragten an, trotz Datenschutzbedenken nicht auf *WhatsApp*[21] oder Facebook verzichten zu wollen [81].

Mehr als 90% der Deutschen nutzen z.B. noch Google als Suchmaschine obwohl die Kritik an den Datenschutzpraktiken des Unternehmens bekannt sind. Mögliche Erklärungen für das Phänomen sind [106, S. 18]:

- Starke Gewöhnung an den Komfort der digitalen Dienste und Geräte.
- Fehlerhafte Selbsteinschätzung digital sozialisierter Gruppen.
- Mangelndes Bewusstsein gegenüber den Folgen der digitalen Datenpreisgabe.
- Mangelndes Wissen über vorhandene Schutztechniken.

Eine Gewöhnung an den Komfort von digitalen Diensten und Geräten ist nachvollziehbar und wurde schon in Abschnitt 2.2.3 (Der Wert des Nutzers) erwähnt. Zur fehlerhaften Selbsteinschätzung digital sozialisierter Gruppen kann das beliebte Argument „Ich habe doch nichts zu verbergen“ genutzt werden. Diese Aussage geht oft mit der Annahme einher, auch nichts befürchten zu müssen. Diese Annahme kann jedoch als Irrtum entlarvt werden: Es kann jedem schaden, wenn bestimmte private Informationen öffentlich werden. Die Verarbeitung, Verknüpfung und Bewertung von Daten ergibt immer neue Informationen, weshalb auch kein objektives Bild einer Person auf Grundlage gesammelter Daten entsteht. Dieses Bild entspricht nicht zwingend dem Bild, wie sich die Person selbst sieht oder wie sie vielleicht gesehen werden möchte [106, S. 19].

Nach dem Aufzeigen des Werts von Nutzerdaten und der Darstellung des Privacy-Paradox als Diskrepanz zwischen Bewusstsein und Handlungsbereitschaft von Nutzern werden nachfolgend einige Probleme und Risiken genannt, die daraus entstehen können. Im weiteren Verlauf wird anschließend auf digitale Grundrechte und Schutz-Optionen eingegangen.

21 Whatsapp Inc. (whatsapp.com)

Manipulation

Ein Problem, dem Nutzer als Folge der digitalen Datenpreisgabe ausgesetzt sein können, ist die Manipulation durch „Behavioral Targeting“ und „Persuasion Profiling“.

Behavioral Targeting kann mit „verhaltensbezogener Anzeige von Werbung im Internet“ übersetzt werden und wird auch *Online Behavioural Advertising* (OBA) genannt. Die Manipulation von Nutzern geschieht durch gezielte Werbefeldzüge von Unternehmen, die sich am Verhalten des Einzelnen ausrichten. Konkret bedeutet das: Sucht ein Nutzer eine Weile lang nach etwas Bestimmten, so wird ihm an anderer Stelle das gesuchte Produkt in Form von Werbung angezeigt. *Amazon*[22] kann z.B. als Pionier von Behavioral Targeting genannt werden. Nutzer werden dabei automatisch in zwei Zielgruppen aufgeteilt: die „lohnenswerten“ Nutzer, welche empfänglich für Werbung sind und die nötige Kaufkraft besitzen, und die „wertlosen“ Nutzer, denen entweder finanzielle Mittel oder die Bereitschaft fehlen etwas zu kaufen [87, S. 108-109].

Beim *Persuasion Profiling* geht es darum, mithilfe von Tracking die Stimmung oder Laune von Nutzern zu analysieren. Das Ziel dabei ist es, durch Analyse der Psyche Schwachstellen zu finden und diese auszunutzen. Von Verhaltensforschern wurde herausgefunden, dass sich z.B. das Kaufverhalten bei Personen unter Trunkenheit oder Depression verändert [18]. Das Hineindenken in eine Person ermöglicht in diesem Zustand unter Umständen auch die Beeinflussung ihres Handelns und damit das Umgehen rationaler Entscheidungen. Diese Art der Beeinflussung, kann als emotionale Cyberattacke bezeichnet werden und richtet laut Steven Weber, Leiter des *Center for Longterm Cybersecurity* in Berkely, genauso viel Schaden an wie der Diebstahl von Datensätzen [87, S. 119-120].

Diskriminierung

Ein anderes Risiko, welches durch Preisgabe von Daten entstehen kann, ist soziale Diskriminierung. Diese entsteht z.B. durch den Zugang, den Mitarbeiter oder Vorgesetzte zu den Privatleben anderer bekommen. So haben Arbeitgeber mittlerweile rund um die Uhr Zugriff auf Informationen aus dem Privatleben ihrer aktuellen oder zukünftigen Mitarbeiter. Darauf basierend können sie Entscheidungen treffen, die vielleicht Anstellung, Gehaltsverhandlung oder auch Kündigung betreffen können [87, S. 58-60].

Dass diese Vorgehensweise bereits seit einigen Jahren praktiziert wird, zeigt eine Studie von Microsoft, die im Jahr 2010 unter dem Titel *„Online Reputation in a Connected World“* veröffentlicht wurde. Hier gaben bereits 70% der befragten Personalvermittler aus den USA und 16% aus Deutschland an, dass sie Kandidaten bei der Bewerbung aufgrund von online gefundenen Daten abgelehnt hatten [21, S. 5].

Diese Art von Diskriminierung ist nur ein Beispiel für Nachteile, die aus einer beliebigen Kombination von Informationen verschiedener Quellen des digitalen Privatlebens entstehen können. Für Menschen mit Erbkrankheiten, die unter Depressionen leiden oder sich in einer Schwangerschaft befinden, lassen sich ähnliche Szenarien finden [87, S. 115-117].

22 Amazon.com, Inc. (amazon.de)

Reputationsverlust

Die Online-Spuren, welche Nutzer im Verlauf der Jahre hinterlassen, können schnell von fremden Personen verfälscht werden – unbeabsichtigt oder mit Vorsatz. Das Resultat ist jedoch gleich: das Bild der Online-Identität einer Person kann dadurch verzerrt werden. Das Internet bietet somit eine einfache Möglichkeit anderen zu schaden, die Behebung dieses Schadens ist jedoch schwierig und zeitaufwändig. Es ist ein komplizierter Prozess Informationen wieder zu entfernen, wenn sie einmal online sind.

Als konkretes Beispiel, bei dem eine Verzerrung der Online-Identität zu Reputationsschäden geführt hat, kann die Klage von Bettina Wulff gegen Google aus dem Jahr 2012 genannt werden. Sie forderte den Konzern auf, Einträge und Suchvervollständigungen bei denen sie mit Begriffen wie „Escort“ oder „Prostituierte“ in Verbindung gebracht wurde, zu löschen. Auch nachdem sie Gerüchte über ein Vorleben im Rotlichtmilleu „eidesstattlich“ abgestritten hatte, blieb der Schaden ihres Rufs, welcher eigentlich auf ihren Gatten Christian Wulff abgezielt hatte, bestehen [113].

Dieses Beispiel zeigt, dass die Identität im Netz und damit die Reputation einer Person nicht mehr zwangsweise in der eigenen Hand liegt. Anders gesagt liegen die Parameter, welche die eigene Identität bestimmen, nicht mehr unter der alleinigen Kontrolle [87, S. 88]. Die Relevanz der Problematik wird zusätzlich durch Reputationsmanagement deutlich, welches sich in den letzten Jahren zu einer boomenden Branche entwickelt hat [139].

Seit Mai 2014 dürfen Einzelpersonen gemäß dem Urteil des Europäischen Gerichtshofs bei Suchmaschinen wie Google die Entfernung bestimmter Suchergebnisse beantragen [75]. Im Falle von hasserfüllten und belästigenden Online-Kommentaren gibt es seit 2017 mit dem Netzwerkdurchsetzungsgesetz (NetzDG) sogar eine gesetzliche Grundlage, um die Entfernung negativer Kommentare auf Social-Media-Plattformen durchzusetzen [132].

Identitätsdiebstahl

Eine etwas kompliziertere Angelegenheit als „nur“ der Verlust von Reputation ist der Diebstahl einer ganzen Identität. Der für die betroffene Person entstehende Schaden betrifft nicht nur die finanzielle Situation, sondern sowohl Ruf als auch Leben des Opfers können langfristig geschädigt und zerstört werden. Damit ist Identitätsdiebstahl gegenüber Reputationsverlust noch eine Steigerung was den verursachten Schaden betrifft [87, S. 89].

Beim Identitätsdiebstahl wird die Identität einer Person von Unbekannten gekapert und übernommen. Das bedeutet im Regelfall, dass Datensätze mit Zugang zu privaten Accounts in die Hände von Dritten gelangen. Angreifer können dann mit den Accounts im Namen des Opfers agieren und in ihrem eigenen Interesse handeln. Bis das Opfer den Diebstahl bemerkt und die Kontrolle zurückerlangt hat, können die Angreifer bereits irreparablen Schaden angerichtet haben.

Als konkretes Beispiel kann der Fall von Jürgen Beer genannt werden, dessen Verkäuferprofil im Mai 2020 gehackt wurde. Der Name seines Amazon-Shops wurde geändert, ebenso das Sortiment und die Kontoverbindung. Was blieb war sein Name im Impressum eines Shops, über den vier Tage lang fiktive Artikel verkauft wurden. So lange dauerte es, bis

die Betrüger aus dem System verbannt wurden. Um von Amazon jedoch wahrgenommen zu werden, war er gezwungen dem Kundensupport mit Suizid zu drohen [133].

Millionen von Menschen auf der Welt wird jedes Jahr die Identität gestohlen – immer häufiger auch online. Die Übernahme passiert häufig auf Grundlage von gestohlenen Datensätzen durch Sicherheitspannen und Hackerangriffe. Die schockierende Erfahrung, einem Identitätsdieb zum Opfer zu fallen, kann als vergleichbar mit einem Einbruch in die Intimsphäre beschrieben werden. Nach einer Bestandsaufnahme gilt es Schadensminimierung zu betreiben. Das ist jedoch nicht einfach, denn welche Details aus dem Privatleben entwendet wurden und wo bereits Kopien davon kursieren, ist oft nicht nachvollziehbar [87, S. 94-95].

Durch das Aufzeigen konkreter Probleme und Risiken für Nutzer mittels Überwachung, Manipulation, Diskriminierung, Reputationsverlust und Identitätsdiebstahl wird der Wert von Nutzerdaten noch einmal verdeutlicht. Es dient auch der Motivation, um entsprechende Maßnahmen zu untersuchen, mithilfe derer ein Schutz vor diesen Gefahren möglich ist. Daher wird das Thema „Selbstdatenschutz“ Inhalt des nächsten Abschnitts sein.

2.3 Selbstdatenschutz

Um das zentrale Thema „Selbstdatenschutz“ vorzubereiten, wird zu Beginn des Kapitels zunächst die Entwicklung der Gesetzeslage beleuchtet. Darauf folgend werden Datenschutzprinzipien vorgestellt, um einen Überblick über organisatorische Maßnahmen zum Schutz von Nutzerdaten zu bekommen. Anschließend wird auf digitale Grundrechte eingegangen und es werden technische Schutzmaßnahmen zur digitalen Selbstverteidigung vorgestellt. Zuletzt wird der Begriff „Selbstdatenschutz“ definiert und eingeführt.

2.3.1 Entwicklung der Datenschutzgesetze

Als Grundlage und Einstieg in das Thema Datenschutz folgt eine kurze Beschreibung der Entwicklung von Datenschutzgesetzen. Mit einem Blick auf die aktuelle Gesetzeslage werden sowohl Relevanz als auch Präsenz der Thematik anschließend verdeutlicht.

Im Jahr 1983 wurde das Grundrecht auf informationelle Selbstbestimmung (GIS) vom Bundesverfassungsgericht in einem Volkszählungs-Urteil als „Allgemeines Persönlichkeitsrecht“ herausgearbeitet. Es gibt jedem Bürger die Freiheit darüber entscheiden zu können, welche personenbezogenen Daten (PD) preisgegeben werden dürfen und wer sie verwenden darf. Bereits vor 30 Jahren erkannte das Bundesverfassungsgericht die Gefahr, welche bei der Erstellung von Persönlichkeits-Profilen auf Grundlage gesammelter Daten entsteht, wenn die Betroffenen keine Kontrolle darüber haben [97].

Das GIS gewährt jedem Nutzer das Privileg selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Es schützt die individuelle Entfaltungsmöglichkeit des Einzelnen, der je nach Kontext und Situation entscheiden und kontrollieren können muss, welche Daten über ihn preisgegeben werden. Jeder Nutzer erhält mit dem GIS ein Abwehrrecht gegen rechtswidrige Eingriffe: Es verpflichtet den Staat, die digitalen Grundrechte der Nutzer zu wahren und zu schützen. Wo die Ressourcen des

Staates allerdings nicht ausreichen, um die informationelle Selbstbestimmung zu gewährleisten, besteht ein rechtmäßiges Interesse von Bürgern, ihre Privatheit durch den Einsatz geeigneter technischer Werkzeuge selbst zu schützen[23].

Neben dem GIS gilt das Bundesdatenschutzgesetz (BDSG) als das zentrale Gesetz im deutschen Datenschutzrecht. Es enthält Anweisungen, wie PD verarbeitet werden dürfen. Die erste Fassung wurde 1977 im Bundesgesetzblatt als „Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung“ veröffentlicht. Schon in dieser ersten Fassung werden „Aufgaben und Gegenstand des Datenschutzes“, als auch Begriffe wie „Speichern“, „Übermitteln“, „Verändern“ und „Löschen“ definiert. Des Weiteren werden die Zulässigkeit der Datenverarbeitung und Rechte des Betroffenen festgelegt und das Datengeheimnis sowie technische und organisatorische Maßnahmen (TOM) formuliert [13, S. 201-203].

Die zuletzt gültige (alte) Fassung des BDSG von 2003 diente vor allem der Umsetzung der EU-Richtlinie von 1995 (*Richtlinie 95/46/EG*[24]). Im Kern ging es um die Etablierung von Gesetzen zum Austausch PD innerhalb der EU-Mitgliedsstaaten. Die koordinierte Einführung neuer Telekommunikationsgesetze sollte die verstärkte wissenschaftliche und technische Zusammenarbeit erleichtern und eine Einschränkung durch unterschiedliche Datenschutz-Niveaus der einzelnen Mitgliedsstaaten verhindern [60, S. 31].

Durch Inkrafttreten der DSGVO wurde 2018 eine neue Fassung des BDSG eingeführt. Hierarchisch gesehen steht die DSGVO an oberster Stelle, da sie die EU-übergreifende rechtliche Grundlage bildet. Sie wird durch das BDSG lediglich ergänzt – in Bereichen in denen dies zulässig ist. Ausnahmen dieser Vormachtstellung bilden bereichsspezifische Datenschutzgesetze wie das Telekommunikationsgesetz (TKG), das Telemediengesetz (TMG) oder die Telekommunikations-Überwachungsverordnung (TKÜV). Unterhalb dieser Gesetzes-Ebene gelten in Deutschland für jedes Bundesland individuelle Landesdatenschutzgesetze (LDSG). Auch die Kirche hat für ihre Institutionen ein eigenes Gesetz über den kirchlichen Datenschutz (KDG) erlassen [1].

Die EU-Richtlinie von 1995 wurde mit der EU-Richtlinie von 1997 (*Richtlinie 97/66/EG*[25]) in spezielle Vorschriften für den Telekommunikationssektor umgesetzt. Beide EU-Richtlinien dienten als Basis für die EU-Richtlinie von 2002 (*Richtlinie 2002/58/EG – Datenschutzrichtlinie für elektronische Kommunikation*[26]), welche die EU-Richtlinie von 1997 ablöste. Als sogenannte „e-Datenschutz-Richtlinie“ hatte sie den Schutz von Grundrechten und vertraulicher Kommunikation zum Ziel. Insbesondere ging es auch um die Anpassung von Anforderungen an den Schutz PD und der Privatsphäre von Nutzern, durch neue elektronische Dienste im IKS [58, S. 37].

23 Die Grundrechte von BVerfG (Abwehrrecht und Schutzpflicht) und GIS besagen: Es muss gewährleistet sein, dass der Einzelne in der Lage ist, seine Daten gegenüber Dritten zu schützen [102, S. 5 u. 32]
24 Richtlinie des Europäischen Parlaments und des Rates vom 24.10.1995 „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ [60]
25 Richtlinie des Europäischen Parlaments und des Rates vom 15.12.1997 „über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation“ [61]
26 Richtlinie des Europäischen Parlaments und des Rates vom 12.07.2002 „über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation“ [58]

Die EU-Richtlinie von 2002 erhielt einige Jahre später mit der EU-Richtlinie von 2009 (*Richtlinie 2009/136/EG*[27]) eine wichtige Ergänzung. Diese sogenannte „Cookie-Richtlinie" schreibt vor, dass Webseiten den Nutzer vor der Speicherung von Cookies informieren und sein Einverständnis dazu einholen müssen. Dies wurde damit begründet, dass die Notwendigkeit der Speicherung von legitimen Gründen (wie funktionale Cookies) bis hin zum unberechtigten Eindringen in die Privatsphäre von Nutzern (z.B. mittels Spähsoftware oder Viren) reichen kann [59, S. 20].

Aus der beschriebenen Entwicklung von Richtlinien und Gesetzen der vergangenen 30 Jahre lässt sich zusammenfassen, dass sowohl das GIS als auch das BDSG die wichtigsten rechtlichen Grundlagen für die Anwendung von Datenschutz in Deutschland gebildet haben. Durch die Einführung der DSGVO wurden sie von einer höheren, EU-weiten Gesetzes-Instanz abgelöst und finden nur noch ergänzend in ihrem Wirkungsbereich Anwendung.

Aktuelle Gesetzeslage

Der jüngste Vorschlag des Europäischen Parlaments von 2017 sieht eine EU-Verordnung (*Verordnung über Privatsphäre und elektronische Kommunikation*[28]) zur Aufhebung der EU-Richtlinie von 2002 vor. Dieser Vorschlag – auch als *ePrivacy Verordnung* (ePVO) bekannt – soll das Vertrauen in digitale Dienste und deren Sicherheit erhöhen, die DSGVO präzisieren und ergänzen [62, S. 3]. Er kann als Grundstein für eine verbindliche Regelungen auf EU-Ebene zur Normierung des Umgangs mit PD in Online-Medien gesehen werden [73].

Die Vorschriften der ePVO sollen das Vertrauen der Nutzer in elektronische Kommunikationswege erhöhen und die Rahmenbedingungen für digitale Unternehmen in den EU-Ländern vereinheitlichen. Die Handlungsempfehlungen für Unternehmen beziehen sich auf den elektronischen Kommunikationsweg, auf strengere Cookie-Bestimmungen sowie auf datenschutzfreundliche Voreinstellungen in Webbrowsern. Für Privatpersonen wird ein Entscheidungsspielraum geschaffen, der den Umgang mit PD erleichtert und deren Schutz gegenüber Dritten stärkt [73].

Der aktuelle Entwurf der ePVO sorgte im Vorfeld bereits für starke Kritik. Vor allem Unternehmen aus der digitalen Werbebranche sahen sich durch deren Umsetzung in ihrer Existenz bedroht [74]. Eine Studie des *Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdienste* (WIK) aus 2017 zeigt, dass diese Bedenken nicht unberechtigt sind: Auf Grundlage einer Einschätzung der Europäischen Kommission, dass lediglich 11% der Nutzer eine Einwilligung zu Cookies erteilen, wird eine Reduktion des gesamten digitalen Werbebudgets von einem Drittel angenommen [88, S. I]. Aufgrund zeitlicher Verzögerungen durch Stellungnahmen von EU-Mitgliedsstaaten wird die ePVO vermutlich nicht mehr 2020 in Kraft treten, sondern eher ab 2022 anwendbar sein [74].

Neben dem Vorschlag der ePVO sorgte ein Urteil des Bundesverfassungsgerichts (BVerfG) vom 27. Mai 2020 zuletzt für Aufsehen. Das BVerfG erklärte § 113 des TKG und meh-

27 Richtlinie des Europäischen Parlaments und des Rates vom 25.11.2009 „(...) über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (...)" [59]

28 Vorschlag für eine Verordnung „über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG [62]

rere Fachgesetze des Bundes zur Bestandsdatenauskunft als verfassungswidrig [27, S. 3]. Behörden dürfen im Kampf gegen Straftäter und Terroristen Daten von Handy- und Internetnutzern (wie z.B. Name des Anschlussinhabers oder IP-Adressen) abfragen. Als Begründung des Urteils nannte das BVerfG Verletzungen des GIS sowie der Wahrung des Telekommunikationsgeheimnisses der Inhaber von Telefon- und Internetanschlüssen. Das TKG und entsprechende Vorschriften in anderen Gesetzen müssen nun bis spätestens Ende 2021 überarbeitet werden [28].

Ein anderes Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 betrifft das „Privacy-Shield"-Abkommen, welches 2016 zwischen den USA und der Europäischen Kommission getroffen wurde. Das Abkommen wurde entwickelt, um Unternehmen auf beiden Seiten des Atlantiks einen Mechanismus zur Verfügung zu stellen, mit dem sie die Datenschutzanforderungen bei der Übermittlung PD aus der Europäischen Union und der Schweiz in die Vereinigten Staaten zur Unterstützung des transatlantischen Handels erfüllen können. Mit dem neuen Rechtsentscheid des EuGH wurde die Angemessenheit des Schutzes durch das „Privacy-Shield" für ungültig erklärt [3].

Die Begründung des EuGH lautet, dass die US-Gesetzgebung nicht dem Schutzniveau der DSGVO entspricht und der Einsatz von Überwachungsprogrammen (wie PRISM oder UPSTREAM[29]) nicht auf das zwingend erforderliche Maß beschränkt ist [63, S. 48]. Die Auswirkungen dieses Urteils, dass erst einmal keine Nutzerdaten aus der EU mehr in die USA übertragen und dort verarbeitet werden dürfen, werden sich in den nächsten Monaten zeigen. Die Liste der betroffenen Dienste ist lang: viele der bekannten Unternehmen wie Facebook, Twitter, Google, *Pinterest*, *Spotify*[30] etc. haben ihren Firmensitz in den Vereinigten Staaten von Amerika [157].

Durch diese jüngsten Entwicklungen und Rechtsentscheide wird deutlich, dass die gesetzliche Grundlage rund um das Thema Datenschutz nicht ruht und sich stetig weiterentwickelt. Es zeigen sich vermehrt Auswirkungen, welche durch die Einführung der DSGVO verursacht wurden, wie sich am Beispiel des „Privacy-Shield"-Abkommens zeigen lässt. Nicht zuletzt verdeutlicht die geplante Einführung der ePVO und die Kritik aus der davon betroffenen Unternehmensbranche die Brisanz der Thematik im Bereich Digitale Werbung und Datenschutz.

2.3.2 Digitale Grundrechte und Prinzipien

Die Grundlagen zum Datenschutz werden anhand von Datenschutzprinzipien aus der *Norm ISO/IEC 29100* noch weiter vertieft. Darauf folgt die Vorstellung des Digitalen Grundrechtekatalogs von Shane Green, ein Pionier in der Bewegung zur persönlichen Daten-Bevollmächtigung, der sich für die Etablierung von Online-Datenschutz und -Kontrolle als Menschenrecht einsetzt [77]. Dieser Grundrechtekatalog wird anschließend diskutiert, um die Notwendigkeit von digitaler Selbstverteidigung deutlich zu machen und auf den Einsatz von entsprechenden Maßnahmen vorzubereiten.

29 Programme der NSA für vorgelagerte (UPSTREAM) und nachgelagerte (PRISM) Überwachung [54]
30 Pinterest Ltd. (pinterest.de), Spotify AB (spotify.com)

Datenschutzprinzipien

Neben den rechtlichen Grundlagen für die Anwendung von Datenschutz gibt es eine Reihe von Prinzipien, die von unterschiedlichen Ländern und internationalen Organisationen entwickelt wurden. Diese Datenschutzprinzipien werden in der Norm *EN ISO/IEC 29100* zusammengefasst, um die Entwicklung und Verwirklichung von Grundsätzen und Steuerungsmaßnahmen für den Datenschutz anzuleiten. Trotz der Unterschiede in den sozialen, kulturellen, rechtlichen und wirtschaftlichen Faktoren, welche die Anwendung dieser Prinzipien in einigen Kontexten einschränken können, wird in der Norm die Anwendung der folgenden definierten Prinzipien empfohlen [48, S. 24]:

1. Einwilligung und Wahlfreiheit
2. Zulässigkeit des Zwecks und Zweckbestimmung
3. Beschränkung der Erhebung
4. Datensparsamkeit
5. Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung
6. Genauigkeit und Qualität
7. Offenheit, Transparenz und Benachrichtigung
8. Persönliche Teilnahme und Zugang
9. Verantwortlichkeit
10. Informationssicherheit
11. Einhaltung der Datenschutzpflichten

Um die Bedeutung der aufgezählten Datenschutzprinzipien zu verstehen, wird jeder der genannten Punkte im Folgenden erläutert [48, S. 24-30]:

Die Beachtung des *Prinzips von Einwilligung und Wahlfreiheit* (Prinzip 1) bedeutet zum einen, der betroffenen Person die Wahl zu überlassen, ob sie der Verarbeitung ihrer personenbezogenen Daten (PD) zustimmt oder nicht. Zum anderen bedeutet es die Einholung ihrer Einwilligung zur Erhebung oder anderweitigen Verarbeitung dieser Daten und der rechtzeitigen Unterrichtung des Vorhabens mit Offenheit und Transparenz.

Das *Prinzip der Zulässigkeit von Zweck und Zweckbestimmung* (Prinzip 2) bedeutet die Sicherstellung der Übereinstimmung vom Zweck der Verarbeitung mit dem geltenden Recht und gegebenenfalls die Bereitstellung ausreichender Erklärungen für die Notwendigkeit der Verarbeitung in einer klaren und den Umständen angepassten Sprache.

Beim *Prinzip der Beschränkung der Erhebung* (Prinzip 3) geht es um den Grundsatz, die Erhebung von PD auf ein Maß zu beschränken, das sich im Rahmen des geltenden Rechts bewegt und für den angegebenen Zweck unbedingt erforderlich ist.

Für das *Prinzip der Datensparsamkeit* (Prinzip 4) wird auf dem vorherigen Prinzip aufgebaut, indem es bei der Konzeption und Implementierung von Systemen vorschreibt, die Verarbeitung von PD strikt zu minimieren.

Die Anwendung des *Prinzips der Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung* (Prinzip 5) bedeutet, dass die Nutzung von PD auf die von der verantwortlichen

Stelle vor der Erhebung angegebenen Zwecke beschränkt wird, die Aufbewahrung nur so lange erfolgt, wie zur Erfüllung der angegebenen Zwecke erforderlich ist und sie anschließend sicher vernichtet oder anonymisiert gespeichert werden.

Das *Prinzip der Genauigkeit und Qualität* (Prinzip 6) bedeutet die Sicherstellung der Richtigkeit, Vollständigkeit und Aktualität von PD, durch die Einrichtung von Kontrollmechanismen bei deren Erhebung und Änderung.

Die Beachtung des *Prinzips der Offenheit, Transparenz und Benachrichtigung* (Prinzip 7) beschreibt die Bereitstellung eindeutiger und leicht zugänglicher Richtlinien, Verfahren und Praktiken der verantwortlichen Stelle in Bezug auf die Verarbeitung der PD. Zusätzlich müssen Wahlmöglichkeiten offengelegt werden, wie die Verarbeitung beschränkt und PD berichtigt bzw. entfernt werden können.

Beim *Prinzip der persönlichen Teilnahme und des Zugangs* (Prinzip 8) geht es darum, betroffenen Personen die Möglichkeit zu geben, auf ihre PD zuzugreifen um diese zu überprüfen und ggf. ändern, berichtigen oder löschen zu lassen.

Das *Prinzip der Verantwortlichkeit* (Prinzip 9) beschreibt die Sorgfaltspflicht bei der Verarbeitung von PD. Dazu zählen angemessene Schulungen von Personal, die Einrichtung effizienter interner Beschwerde- und Abhilfeverfahren oder das Informieren von betroffenen Personen über Datenschutzverletzungen, die zu erheblichen Schäden führen können.

Im *Prinzip der Informationssicherheit* (Prinzip 10) wird der Schutz von PD von verantwortlichen Stellen durch geeignete Kontrollen auf operativer, funktionaler und strategischer Ebene gefordert. Das Ziel ist die Integrität, Vertraulichkeit und Verfügbarkeit der PD sicherzustellen und sie während ihres gesamten Lebenszyklus vor Risiken wie unbefugtem Zugang, Zerstörung, Verwendung, Änderung, Offenlegung oder Verlust zu schützen.

Die Beachtung des letzten *Prinzips zur Einhaltung der Datenschutzpflichten* (Prinzip 11) schreibt die Existenz geeigneter interner Kontrollen und unabhängiger Aufsichtsmechanismen vor, welche die Einhaltung der einschlägigen Datenschutzgesetze und ihrer Richtlinien und Verfahren zur Sicherheit und zum Schutz von PD sicherstellen.

Die vorgestellte Norm enthält ein allgemeines Rahmenwerk für den Schutz PD in Systemen des IKS zur Anwendung in organisatorischen, technischen und verfahrenstechnischen Bereichen. Es soll bei Entwicklung und Einführung von Systemen und innovativen Lösungen helfen, den Schutz von PD durch den Einsatz bewährter Vorgehensweisen zu verbessern [48, S. 7]. Im Anschluss daran wird ein digitaler Grundrechtekatalog vorgestellt, welcher den Übergang von Datenschutz zu Selbstdatenschutz einleitet. Es wird anschließend überprüft, welche der vorgestellten Datenschutz-Prinzipien darin bereits berücksichtigt werden.

Digitaler Grundrechtekatalog

Im März 2012 leitete Shane Green auf der Konferenz SXSW[31] in Austin Texas eine Sitzung zum Thema *„We the People: Creating a Consumer's Bill of Rights“* mit Datenschutzexper-

31 South by Southwest Conference & Festivals (sxsw.com/about)

ten, Werbe- und Internetverantwortlichen [78]. Unter dem Titel *„A Digital Bill of Rights by the people, for the people“* entstand ein digitaler Grundrechtekatalog. Die Kernpunkte sind nach fast 10 Jahren immer noch gültig und beschreiben die grundlegenden Aspekte für die Anwendung von Selbstdatenschutz. Aus diesem Grund wird nachfolgend die deutsche Übersetzung aus dem Buch *„Mich kriegt ihr nicht!: Die wichtigsten Schritte zur digitalen Selbstverteidigung“* von Steffan Heuer vorgestellt (wörtlich zitiert aus [87, S. 53-54]):

> *Präambel*
>
> Dieses Digitale Grundgesetz gilt für die Unantastbarkeit des digitalen Ich. Das digitale Ich sollte vor dem Gesetz und von der Gesellschaft gleichberechtigt mit dem physischen Ich behandelt werden.
>
> *Rechte*
>
> 1. **Recht auf Transparenz:** Ich habe das Recht zu wissen, wer meine Daten sammelt, verwendet, teilt oder vermarktet und wie es geschieht. Ich habe das Recht zu wissen, wie meine Daten geschützt und gesichert werden. Ich habe das Recht, den Wert meiner Daten zu erfahren.
> 2. **Recht auf Privatsphäre:** Ich habe das Recht auf Schutz meiner Privatsphäre als Voreinstellung.
> 3. **Recht auf Auswahl und Kontrolle:** Ich habe das Recht, die Erlaubnis zu geben, meine Daten zu sammeln, zu nutzen, zu teilen oder zu vermarkten, und sie wieder zu entziehen. Ich habe das Recht, meine Daten zu sehen, auf sie zuzugreifen, sie zu korrigieren, zu bearbeiten, zu überprüfen, zu exportieren und zu löschen. Ich habe das Recht, sie zu besitzen und/oder die ‚Goldene Kopie‘ meiner Daten frei zu nutzen. Ich habe das Recht, das Produkt oder die App zu kaufen und nicht ‚das Produkt zu sein‘.
> 4. **Recht auf Sicherheit:** Ich habe das Recht zu erwarten, dass meine Daten sicher gelagert und transportiert werden.
> 5. **Recht auf Identität:** Ich habe das Recht, je nach Kontext verschiedene digitale Persönlichkeiten zu benutzen. Ich habe das Recht auf Anonymität.
> 6. **Recht auf minimale Verwendung:** Ich habe das Recht zu verlangen, dass meine Daten nur für den angegebenen Zweck und Kontext gesammelt, genutzt, geteilt oder vermarktet werden. Ich habe das Recht, vergessen zu werden, nachdem meine Daten ihren Zweck erfüllt haben.

Der Kernpunkt, auf dem der gesamte Grundrechte-Katalog aufbaut, wird in der Präambel verdeutlicht: Die Gleichsetzung von digitaler und physischer Identität zum Zweck der Gleichberechtigung vor Gesetz und Gesellschaft. Es wird von der „Unantastbarkeit des digitalen Ichs“ gesprochen, was als Parallele zu einem der wichtigsten Grundrechte des Menschen – die Unantastbarkeit der Menschenwürde – gesehen werden kann [68]. Dies macht deutlich, dass der Stellenwert des digitalen Selbst dem des physischen entsprechen sollte. Im Folgenden werden Parallelen zwischen dem digitalen Grundrechtekatalog und

bereits vorgestellten Themen gesucht, um die Relevanz für diese Arbeit auf Grundlage gefundener Schnittmengen zu überprüfen und eventuelle inhaltliche Lücken zu finden und zu schließen.

Im *Recht auf Transparenz* (Grundrecht 1) lassen sich deutliche Schnittmengen zu den in Abschnitt 2.2.2 (Tracking und Data-Mining) bereits genannten Punkten „Sammeln, Verwenden und Vermarkten von Daten“ wiederfinden. Ebenso wurde der Punkt „Der Wert des Nutzers“ bereits in Abschnitt 2.2.3 (Probleme, Risiken und Gefahren) genannt. Insgesamt ist eine deutliche Überschneidung mit Datenschutzprinzip 7 (Offenheit, Transparenz und Benachrichtigung) festzustellen und der Punkt „Schutz und Sicherung von Daten“ taucht bereits in Datenschutzprinzip 10 (Informationssicherheit) auf.

Das *Recht auf Privatsphäre* (Grundrecht 2) spiegelt sich deutlich in Abschnitt 2.1.1 (Sicherheit und Privatheit) unter dem Punkt „Die Privatsphäre“ wieder.

Mit dem *Recht auf Auswahl und Kontrolle* (Grundrecht 3) wird ein Punkt aufgegriffen, der sich in Datenschutzprinzip 1 (Prinzip von Einwilligung und Wahlfreiheit) und Datenschutzprinzip 8 (Persönliche Teilnahme und Zugang) wiederspiegelt. Die Möglichkeit von Korrektur, Einsicht und Bearbeitung von Daten wurde zusätzlich in Abschnitt 2.2.3 (Probleme, Risiken und Gefahren) beim Punkt „Reputationsverlust“ schon angeschnitten. Ein weiterer neuer Aspekt der hinzukommt, ist der Begriff der „Goldenen Kopie“, welcher den unverfälschten Master der digitalen Identität beschreibt und mit Datenschutzprinzip 6 (Genauigkeit und Qualität) in Verbindung gebracht werden kann.

Das *Recht auf Sicherheit* (Grundrecht 4) deckt sich weitestgehende mit Datenschutzprinzip 10 (Informationssicherheit) und betrifft vor allem Transport und Speicherung von Daten, was im nächsten Abschnitt noch etwas genauer betrachtet wird.

Mit dem *Recht auf Identität* (Grundrecht 5) kann eine deutliche Parallele zu Abschnitt 2.1.2 (Identität und Anonymität) gefunden werden, wo der Begriff „Identität“ detailliert eingeführt und beleuchtet wurde.

Mit Nennung vom *Recht auf minimale Verwendung* (Grundrecht 6) wird ein Punkt aufgeführt, der von Datenschutzprinzip 3 (Beschränkung der Erhebung) und Datenschutzprinzip 4 (Datensparsamkeit) bereits abgedeckt wird. Der Begriff der „Datensparsamkeit“ wird im weiteren Verlauf noch stärker in den Fokus rücken.

Insgesamt ist bereits eine sehr hohe thematische Deckung dieser Arbeit mit dem digitalen Grundrechtekatalog zu erkennen. Die bislang weniger thematisierten Punkte werden im weiteren Verlauf der Arbeit noch intensiver behandelt. Nachdem in den vorherigen Abschnitten auf Funktionen und Gefahren von Tracking und Data-Mining sowie rechtliche Grundlagen eingegangen wurde, ist es an der Zeit Maßnahmen vorzustellen, mit denen sich Nutzer schützen können.

2.3.3 Sieben V der digitalen Selbstverteidigung

Neben den rechtlichen und organisatorischen Maßnahmen, die sich aus den digitalen Grundrechten ergeben, existieren auch technische Maßnahmen, die Nutzer eigenständig ergreifen können, um sich vor dem unberechtigten Zugriff auf ihre Daten durch Dritte zu schützen. Steffan Heuer beschreibt in seinem Buch drei operative Schritte zur digitalen Selbstverteidigung, die alle mit „V“ beginnen. Bei diesen drei Punkten handelt es sich jeweils um aktive Schutzmaßnahmen. Ein vierter Punkt, welcher auch als „Notfall-V“ bezeichnet wird, beschreibt passive Maßnahmen zur digitalen Selbstverteidigung [87, S. 225-226]:

1. **Verweigern** persönlicher Informationen gegenüber Datensammlern.
2. **Verschleiern** der Identität durch Pseudonyme und Anonymität.
3. **Verschlüsseln** von privaten Daten und Kommunikation.
4. **Verbannen** von digitalen Diensten und Technologien.

Mit *Verweigern* wird das Erschweren und Verhindern von Tracking und Profiling durch den Einsatz von Werkzeugen wie Ad Blocking Tools (ABT) oder Tracking Prevention Tools (TPT) gemeint. Beim *Verschleiern* geht es um das Verwischen digitaler Datenspuren durch die Nutzung von Pseudonymen, VPN-Diensten und Anonymitäts-Werkzeugen. *Verschlüsseln* hingegen bedeutet, dass private Informationen vor Dritten geschützt werden, sowohl bei der Übertragung als auch bei der Speicherung. Das *Verbannen* beschreibt zuletzt den Einsatz von reaktiven Maßnahmen durch das Aussortieren „kritischer“ Dienste und Daten sowie den Umstieg auf datenschutzfreundliche Alternativen.

Diese vier Schritte befassen sich mit dem eigentlichen Prozess der digitalen Selbstverteidigung. Sie lassen sich jedoch um drei weitere „V“ ergänzen, welche im Vorfeld zur Sensibilisierung oder im Nachgang zur Schadensbegrenzung angewendet werden können:

5. **Vorbereiten** auf mögliche Schwachstellen und den Wert von Daten.
6. **Vorbeugen** von Gefahren durch proaktive Schutzmaßnahmen.
7. **Vermindern** von Schäden an Reputation und Identität.

Mit *Vorbereiten* ist das Schaffen eines Bewusstseins für den Wert von Nutzerdaten und potentielle Gefahren gemeint. *Vorbeugen* beschreibt den Einsatz proaktiver Schutzmaßnahmen und das Reflektieren vor dem Teilen von persönlichen Daten. Als *Vermindern* wird die Beschränkung bereits eingetretener Schadensfälle für die Privatsphäre bezeichnet. Dabei können *Vorbereiten* und *Vorbeugen* als präventive und *Vermindern* als reaktive Maßnahmen eingestuft werden.

Durch Einordnen aller genannten Maßnahmen in die Reihenfolge ihrer Anwendung, ergeben sich *Sieben V der digitalen Selbstverteidigung*. Diese können durch die Gruppierung in präventive, operative und reaktive (Notfall-) Maßnahmen wie folgt dargestellt werden:

I) Präventive Maßnahmen: Vorbereiten, Vorbeugen

II) Operative Maßnahmen: Verweigern, Verschleiern, Verschlüsseln

III) Reaktive und Notfall-Maßnahmen: Verbannen, Vermindern

Im späteren Verlauf der Arbeit wird jede dieser sieben Kategorien durch die Vorstellung von Beispiel-Maßnahmen noch konkretisiert. Dies ist notwendig um zu verstehen, welche Selbstdatenschutz-Funktionen mithilfe von Privacy-Boxen überhaupt realisiert werden können (siehe „Werkzeuge zum Selbstdatenschutz“ in Abschnitt 4.2).

Die Anwendung der vorgestellten Maßnahmen zur digitalen Selbstverteidigung kann mit dem Begriff „Selbstdatenschutz“ beschrieben werden: „Unter *Selbstdatenschutz* versteht man die durch den Einzelnen zum Schutz seiner Datenschutzgrundrechte ergriffenen technischen, organisatorischen und rechtlichen Maßnahmen.“ [36]. Diese Definition des sächsischen Datenschutzbeauftragten von 2012 macht nochmal deutlich, dass neben rechtlichen und organisatorischen Maßnahmen auch technische Maßnahmen den Selbstdatenschutz ausmachen. Zusätzlich kann zwischen aktiven und passiven Schutzmaßnahmen unterschieden werden.

Aktive Maßnahmen beschreiben die Nutzung von datenschutzunterstützenden Techniken wie die Abwehr von Tracking und der Einsatz von Anomymisierung oder Verschlüsselung. Passive Maßnahmen hingegen betreffen vor allem die „Datensparsamkeit“, also die Vermeidung der Preisgabe von personenbezogenen Daten [102, S. 4]. Bei den als *Sieben V der digitalen Selbstverteidigung* beschriebenen Maßnahmen können die operativen Maßnahmen als *aktiv* eingeordnet werden. Alle anderen Maßnahmen gelten als *passiv*, da sie zur Vor- oder Nachbereitung genutzt werden.

Nutzer können durch den Einsatz von Selbstdatenschutz-Techniken ihren Unmut über die allumfängliche Überwachung ihres Verhaltens ausdrücken. Selbstdatenschutz erhöht einerseits den Aufwand für die Überwacher erheblich und signalisiert andererseits unmissverständlich, dass ein Nutzer nicht mit der Überwachung seiner Aktivitäten einverstanden ist [84, S. 148]. Selbstdatenschutz kann dabei als Werkzeug zur Notwehr interpretiert bzw. als „eine Waffe der Schwachen im Kampf gegen die Überwachung durch übermächtige Staaten und Internetkonzerne“ [84, S. 152] beschrieben werden. Konkrete Beispiele für solche Werkzeuge werden in Abschnitt 4.2 (Werkzeuge zum Selbstdatenschutz) vorgestellt.

Zu Beginn wurden Grundlagen für Sicherheit und Privatheit mit Begriffsdefinitionen gelegt und der Wert von Nutzer und Daten anhand von Risiken und Gefahren verdeutlicht. Anschließend wurden mit rechtlichen, organisatorischen und technischen Maßnahmen zur digitalen Selbstverteidigung relevante Bereiche vorgestellt, mithilfe derer Datenschutz und Selbstdatenschutz angewendet werden kann. Somit verbleibt die Benutzbarkeit als letztes Thema des Grundlagen-Kapitels und stellt den Inhalt des nächsten Abschnitts dar.

2.4 Benutzbarkeit

Da die vorliegende Arbeit insbesondere die Benutzbarkeit von Privacy-Boxen untersucht, ist es notwendig, an dieser Stelle die wichtigsten Begriffe einzuführen, die mit Benutzbarkeit im Zusammenhang stehen. Im Anschluss daran werden bewährte Prinzipien (Heuristiken) vorgestellt, anhand derer sich das spätere Konzept der Untersuchung bedienen kann. Abschließend wird das Thema *Nutzerzentrierte Privatheit* als Schnittstelle zwischen den Themenbereichen Privatheit und Benutzbarkeit eingeführt.

2.4.1 Ergonomie und Gebrauchstauglichkeit

Zu Beginn werden Grundlagen-Begriffe wie *Ergonomie*, *Benutzerfreundlichkeit* und *Gebrauchstauglichkeit* definiert, bevor mittels Heuristiken auf deren Verwendung eingegangen werden kann. Dazu wird überwiegend auf die Normen der Familie *DIN EN ISO 9241* zurückgegriffen, die wichtige Grundlagen zur Ergonomie der *Mensch-System-Interaktion* (MSI) beschreiben.

Ergonomie

Der Begriff *Ergonomie* kommt vom englischen Wort „ergonomics“ und setzt sich aus den griechischen Wörtern „érgon“ (Arbeit) und „nomía“ (Sachkunde) zusammen[32]. Es bedeutet zusammengesetzt soviel wie „Lehre der Arbeit“. Der Begriff wurde erstmals vom polnischen Professor Wojciech Jastrzębowski im Jahr 1857 in seinem Buch *„An outline of ergonomics (...)“* geprägt. In der Übersetzung von Sowa und Laurig (1982) wird Ergonomie definiert als „(...) wissenschaftlicher Ansatz, um mit geringster Mühe und größter Zufriedenheit reichlichst Früchte zu erhalten für das eigene und allgemeine Wohl.“ [128, S. 1].

Etwas detaillierter wird Ergonomie in der Norm *DIN EN ISO 6385* beschrieben als „wissenschaftliche Disziplin, die sich mit dem Verständnis der Wechselwirkungen zwischen Menschen und anderen Elementen eines Systems befasst, und der Berufszweig, der Theorie, Grundsätze, Daten und Verfahren auf die Gestaltung von Arbeitssystemen anwendet, mit dem Ziel, das Wohlbefinden des Menschen und die Leistung des Gesamtsystems zu optimieren“ [45, S. 7]. Es geht bei Ergonomie also um die Optimierung von Wohlbefinden und Leistung bei der Interaktion zwischen Menschen und Arbeitssystemen (MSI).

Benutzerfreundlichkeit

Der entscheidende Faktor der bestimmt, ob ein System genutzt wird oder nicht, lag in der Vergangenheit überwiegend in der Art und der Anzahl der zur Verfügung stehenden Funktionen eines technischen Systems. Durch die Weiterentwicklung technischer Systeme und einer zunehmenden „Multifunktionalität“, stieg auch die Komplexität bei der Bedienung an, was zu der Frage nach der Benutzerfreundlichkeit eines Systems führte [147, S. 19].

Benutzerfreundlichkeit ist mittlerweile ein Merkmal für Softwarequalität und beschreibt die Eigenschaft eines Produkts auf die Anforderungen des Nutzers zugeschnitten zu sein. Im Bezug auf Software kann Benutzerfreundlichkeit wie folgt definiert werden: „Das Softwareprodukt soll sich den Bedürfnissen der jeweiligen Benutzerkategorie entsprechend verhalten,

32 Ergonomie, Bedeutung – Duden (duden.de/rechtschreibung/Ergonomie)

der Vorbildung und Intention der Benutzer angemessene Ausdrucks- und Interaktionsformen vorsehen und leicht handhabbar sein.“ [110].

Neben der komfortablen Nutzung eines technischen Systems durch Benutzerfreundlichkeit, wird heute zusätzlich noch die Unterstützung des Nutzers beim Erreichen seiner Ziele gefordert. Hierfür reicht der Begriff „Benutzerfreundlichkeit“ nicht mehr aus und macht den Begriff der „Gebrauchstauglichkeit“ notwendig.

Gebrauchstauglichkeit

Die *Gebrauchstauglichkeit* (engl. *Usability*) beschreibt das „Anpassen von System, Aufgabe und Nutzer aus der Perspektive einer vom Nutzer wahrgenommenen Qualität der Zielerfüllung“ [117, S. 6]. Usability kann also als Qualitäts-Aspekt eines technischen Systems gesehen werden, welcher die Gestaltung nach den Erkenntnissen der Ergonomie zum Ziel hat [117, S. 5]. Da sich der Begriff „Usability“ im deutschen Sprachgebrauch bereits etabliert hat, wird er in folgenden Verlauf synonym mit „Gebrauchstauglichkeit“ verwendet.

Eine wichtige Definition von Usability wird in Teil 11 der Norm *DIN EN ISO 9241* beschrieben: „Die Gebrauchstauglichkeit ist das Ausmaß, in dem ein System, ein Produkt oder eine Dienstleistung durch bestimmte Benutzer in einem bestimmten Nutzungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen“ [46, S. 15]. Es geht somit um das Erreichen von Zielen bei der Benutzung eines Systems in einem bestimmten Kontext unter Einhaltung der Qualitätsmerkmale Effektivität[33], Effizienz[34] und Zufriedenstellung[35].

Usability ist im Gegensatz zu Ergonomie jedoch keine eigene Disziplin, sondern beschreibt die Qualität eines technischen Systems. Sie kann als ein Ziel bei der Gestaltung technischer Systeme, nach den Erkenntnissen der Ergonomie, verstanden werden [147, S. 19].

Nach Einführung von Ergonomie, Benutzerfreundlichkeit und Usability wird das Ziel der anstehenden Untersuchung von Privacy-Boxen etwas klarer: Es gilt herauszufinden, in welchem Maß Privacy-Boxen den Nutzer effektiv, effizient und zufriedenstellend bei der Anwendung von Selbstdatenschutz unterstützen können. Daher werden im nächsten Abschnitt zuerst einige Konzepte und Heuristiken für die Anwendung von Usability vorgestellt.

2.4.2 Konzepte und Heuristiken der Usability

In diesem Abschnitt wird zunächst das Verständnis von Usability anhand eines Konzepts von Gebrauchstauglichkeit in einem bestimmten Nutzungskontext vertieft. Darauf folgend werden Interaktionsprinzipien als wichtige Basis der MSI vorgestellt, bevor das Konzept der *User Experience* im Verhältnis zur Usability eingeführt wird. Abschließend wird mit den Themen *Usability Engineering* und *Usability Evaluation* die Grundlage für die Untersuchung von Privacy-Boxen konkretisiert.

33 „Genauigkeit und Vollständigkeit, mit denen Benutzer bestimmte Ziele erreichen“ [46, S. 11]
34 „Eingesetzte Ressourcen im Verhältnis zu den erreichten Ergebnissen“ [46, S. 11]
35 „Ausmaß der Übereinstimmung der physischen, kognitiven und emotionalen Reaktionen des Benutzers, die aus der Benutzung eines Systems, eines Produkts oder einer Dienstleistung resultieren, mit den Benutzererfordernissen und Benutzererwartungen“ [46, S. 11]

Konzept der Gebrauchstauglichkeit

Teil 11 der Norm *DIN EN ISO 9241* ist ein wichtiges Dokument, um ein Verständnis für das Konzept von Usability und deren Anwendung auf interaktive Systeme zu entwickeln. Sie beinhaltet ein Konzept, welches Gebrauchstauglichkeit als Ergebnis der Nutzung eines Systems (oder eines Produkts oder einer Dienstleistung) in einem bestimmten Nutzungskontext darstellt (vgl. Abb. 4).

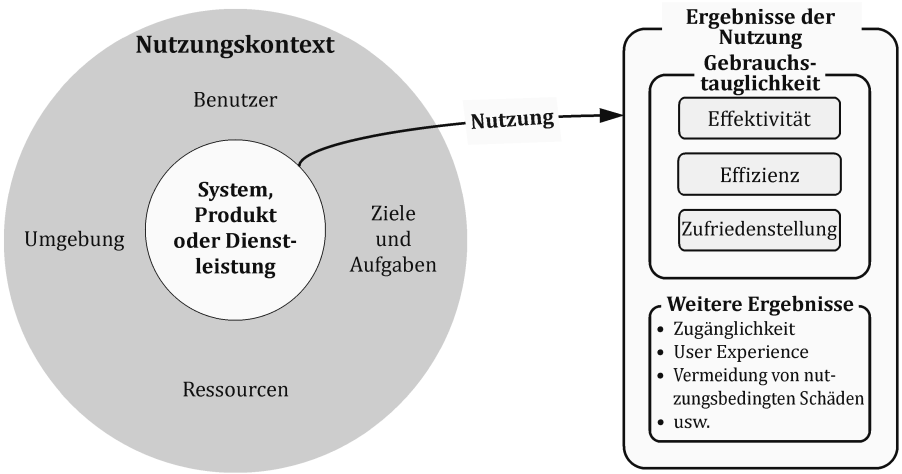


Abbildung 4: Gebrauchstauglichkeit in einem Nutzungskontext [46, S. 15]

Wie Abb. 4 zeigt, stehen System, Produkt oder Dienstleistung im Zentrum und stellen so den Betrachtungsgegenstand dar. Dieser ist innerhalb des Nutzungskontexts dargestellt, welcher aus Benutzern, Zielen und Aufgaben, Ressourcen und der Umgebung besteht. Die Gebrauchstauglichkeit wird als ein Ergebnis der Nutzung des Betrachtungsgegenstands abgebildet und setzt sich aus Effektivität, Effizienz und Zufriedenstellung zusammen. Als weitere Ergebnisse der Nutzung werden Barrierefreiheit, User Experience und Vermeidung nutzungsbedingter Schäden aufgezählt [46, S. 15].

Das Ausmaß, in dem Gebrauchstauglichkeit erreicht wird, ist dabei vor allem vom jeweiligen Nutzungskontext abhängig und kann sich in Abhägigkeit davon signifikant unterscheiden. Gebrauchstauglichkeit wird üblicherweise in Bezug auf den Nutzungskontext, also für bestimmte Benutzergruppen, Aufgaben und bestimmte Umgebungen, gestaltet oder evaluiert [46, S. 15-16].

Interaktionsprinzipien

Um ein hohes Maß an Gebrauchstauglichkeit bei der Interaktion zwischen Mensch und System zu erreichen, existieren Interaktionsprinzipien, die beschreiben, wie die MSI umgesetzt werden sollte. Die Grundlagen dafür wurden bereits 1978 in dem Paper *„User-Perceived Quality of Interactive Systems“* vorgestellt [44, S. 271]. In Teil 110 der Norm *DIN EN ISO 9241*, die Prinzipien der Interaktionsgestaltung für die Ergonomie der MSI beschreibt, werden folgende sieben Interaktionsprinzipien[36] vorgestellt (wörtlich zitiert aus [49, S. 11]):

36 Die „Grundsätze der Dialoggestaltung“ aus der Norm von 2008 werden in der Norm von 2020 als „Interaktionsprinzipien“ vorgestellt. Die Prinzipien stimmen inhaltlich mit den Grundsätzen überein, bis auf Punkt 7: der Grundsatz der „Individualisierbarkeit“ wird vom Prinzip der „Benutzerbindung“ abgelöst

1. **Aufgabenangemessenheit:** Ein interaktives System ist aufgabenangemessen, wenn es die Benutzer bei der Erledigung ihrer Aufgaben unterstützt, d. h., wenn die Bedienfunktionen und die Benutzer-System-Interaktionen auf den charakteristischen Eigenschaften der Aufgabe basieren (und nicht auf der zur Erfüllung der Aufgabe gewählten Technologie).
2. **Selbstbeschreibungsfähigkeit:** Wo immer erforderlich für den Benutzer, bietet das interaktive System angemessene Information an, die die Fähigkeiten des Systems und seine Nutzung unmittelbar offensichtlich machen, ohne dass hierzu unnötige Benutzer-System-Interaktionen erforderlich werden.
3. **Erwartungskonformität:** Das Verhalten des interaktiven Systems ist vorhersehbar, basierend auf dem Nutzungskontext und allgemein anerkannten Konventionen in diesem Kontext.
4. **Erlernbarkeit:** Das interaktive System unterstützt die Entdeckung seiner Fähigkeiten und deren Verwendung, erlaubt das Explorieren („Ausprobieren“) des interaktiven Systems, minimiert den Lernaufwand und bietet Unterstützung, wenn Lernen erforderlich ist.
5. **Steuerbarkeit:** Das interaktive System erlaubt es dem Benutzer, die Kontrolle über die Benutzungsschnittstelle und die Interaktionen zu behalten, einschließlich der Geschwindigkeit, Abfolge und Individualisierung der Benutzer-System-Interaktion.
6. **Robustheit gegen Benutzungsfehler:** Das interaktive System unterstützt den Benutzer beim Vermeiden von Fehlern, toleriert Benutzungsfehler im Falle von erkennbaren Fehlern und unterstützt den Benutzer bei der Fehlerbehebung.
7. **Benutzerbindung:** Das interaktive System stellt Funktionen und Informationen auf einladende und motivierende Weise dar und fördert so eine kontinuierliche Interaktion mit dem System.

Um die Interaktionsprinzipien besser zu verstehen, werden ein paar konkrete Beispiele von Anwendungsszenarien für jedes Prinzip gegeben:

- Die *Aufgabenangemessenheit* (Prinzip 1) ist gewährleistet, wenn in einer Notsituation nur für die Lösung relevante Informationen angezeigt werden.
- Für die *Selbstbeschreibungsfähigkeit* (Prinzip 2) kann bei einem Eingabefeld das erwartete Format einer Nutzereingabe eingeblendet werden.
- *Erwartungskonformität* (Prinzip 3) ist gegeben, wenn anwendungsspezifische Kurzbefehle systemübergreifend funktionieren (z.B. unter Windows, macOS und Linux).
- *Erlernbarkeit* (Prinzip 4) kann durch Einblendung von Kurzbefehlen neben anwendungsspezifischen Interaktionselementen erreicht werden.
- Die *Steuerbarkeit* (Prinzip 5) eines Systems wird ermöglicht, indem die Möglichkeit einer „Rückgängig-Funktion“ angeboten wird.
- Die *Robustheit gegen Benutzungsfehler* (Prinzip 6) kann durch Korrekturvorschläge bei Eingabefehlern von Nutzern erreicht werden.

- Die *Benutzerbindung* (Prinzip 7) kann durch die Anzeige eines Systemstatus mit einem Hinweis für „Weitere Informationen“ gefördert werden.

Auch wenn alle Prinzipien bei Analyse, Gestaltung und Bewertung eines Systems berücksichtigt werden müssen, so können sie abhängig von Nutzungskontext in ihrer Wichtigkeit variieren, was Kompromisse bei deren Einhaltung erforderlich machen kann [49, S. 13].

User Experience (UX)

Da die Usability lediglich den Prozess während der MSI beschreibt, die Interaktion zwischen Mensch und System[37] aber schon früher beginnt und später noch fortbesteht, gibt es den Begriff der *User Experience* (UX). Sie beschreibt den vollständigen Prozess der MSI vom Zustand vor, während und nach der Nutzung eines Systems (vgl. Abb. 5).

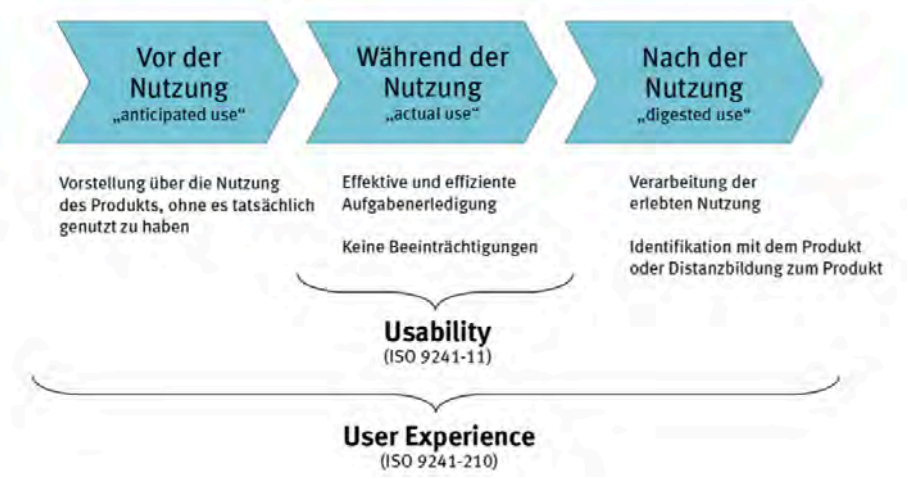


Abbildung 5: Vergleich von Usability und User Experience [99]

Abb. 5 veranschaulicht die Abgrenzung zwischen Usability und UX. Sie zeigt, dass neben „effektiver und effizienter Aufgabenerledigung“ noch zusätzlich die „Vorstellung über Nutzung des Systems (ohne es tatsächlich genutzt zu haben)“, sowie die „Verarbeitung der erlebten Nutzung“ zur UX dazu gehören. Wenn ein Nutzer den Prozess der UX durchlaufen hat, kann es bei ihm zu einer „Identifikation mit dem System“ oder zu einer „Distanzierung von dem System“ kommen. Anders gesagt ist UX der entscheidende Faktor, welcher den Erfolg eines Systems bestimmt.

Die UX wird in Teil 210 der Norm *DIN EN ISO 9241*, die menschzentrierte Gestaltung interaktiver Systeme beschreibt, wie folgt definiert: User Experience (auch *Benutzererlebnis*) sind die „Wahrnehmungen und Reaktionen[38] einer Person, die aus der tatsächlichen und/oder der erwarteten Benutzung eines Systems, eines Produkts oder einer Dienstleistung resultieren“ [47, S. 11].

Des Weiteren wird als Anmerkung zum Begriff folgendes konkretisiert: „User Experience ist eine Folge des Markenbilds, der Darstellung, Funktionalität, Systemleistung, des interaktiven Verhaltens und der Unterstützungsmöglichkeiten eines Systems, eines Produkts

37 System steht im folgenden Verlauf auch stellvertretend für Produkt oder Dienstleistung
38 „Die Wahrnehmungen und Reaktionen der Benutzer umfassen sämtliche Emotionen, Vorstellungen, Vorlieben, Wahrnehmungen, Wohlbefinden oder Unbehagen, Verhaltensweisen und Leistungen, die sich vor, während und nach der Nutzung ergeben.“ [47, S. 11]

oder einer Dienstleistung. Sie ergibt sich auch aus dem psychischen und physischen Zustand des Benutzers aufgrund seiner Erfahrungen, Einstellungen, Fertigkeiten, Möglichkeiten und seiner Persönlichkeit sowie des Nutzungskontextes.“ [47, S. 11].

Die UX beschreibt also das ganzheitliche *Benutzererlebnis*, welches aus dem Zusammenspiel von Leistung, Funktion und Darstellung eines Systems mit der Persönlichkeit, den Fertigkeiten und Erfahrungen eines Nutzers entsteht. Im Gegensatz zur Usability liegt der Fokus der UX weniger auf der Optimierung des Systems selbst, als auf der Optimierung von emotionalen Faktoren, die vor, während oder nach der Benutzung entstehen.

2.4.3 Usability Engineering und -Evaluation

Nachdem Usability und UX als Güte- und Erfolgskriterien von Systemen eingeführt wurden, wird im folgenden Abschnitt darauf eingegangen, wie sie bei deren Entwicklung berücksichtigt werden können und welche Möglichkeiten es gibt, ihre Wirksamkeit bei der späteren Nutzung zu überprüfen.

Usability Engineering

Um eine optimale Usability zu gewährleisten, müssen bei der Entwicklung neuer, technischer Systeme entsprechende Kriterien berücksichtigt werden. Das „klassische“ Engineering (z.B. Software-Engineering) wird dabei um ergonomische Perspektiven ergänzt. Dieser Prozess, der methodische Weg zur Erzeugung von Usability, wird *Usability Engineering* genannt [117, S. 18]. Er läuft parallel und eng verzahnt zur technischen Entwicklung ab und erfordert eine enge Kooperation zwischen Entwicklern, Designern und Usability-Experten. Es ist zusätzlich sinnvoll, Vertreter der Zielgruppe in den Prozess zu integrieren, um deren Anforderungen zu erfassen und Aufgaben, Bedürfnisse und Probleme ausreichend berücksichtigen zu können [147, S. 87].

Alle gängigen Modelle des Usability Engineerings sind als iterativer Prozess konzipiert, der nach Bedarf mehrfach durchlaufen werden kann. Teil 210 der Norm *DIN EN ISO 9241* beinhaltet ein Beispiel, welches sich gut eignet, um diesen Prozess anschaulich zu erklären (vgl. Abb. 6). Folgende sechs Punkte gehören demnach zum Usabilty-Engineering dazu, wobei der erste und letzte Punkt als Beginn und Abschluss gelten und die Punkte zwei bis fünf den Iterationskreislauf darstellen [47, S. 21]:

1. **Planen des menschenzentrierten Gestaltungsprozesses**

   (Durch Konzeption, Analyse, Gestaltung, Implementierung, Prüfung und Wartung als Projekt-Phase)

2. **Verstehen und Festlegen des Nutzungskontexts**

   (Mit Profilen von Benutzergruppen, Zustands-Szenarien oder Personas)

3. **Festlegen der Nutzungsanforderungen**

   (Durch Identifizieren von Benutzererfordernissen, abgeleiteten Nutzungsanforderungen oder anwendbaren Gestaltungsregeln)

4. **Erarbeiten von Gestaltungslösungen**

   (Mithilfe von Nutzungsszenarien und Prototypen mit verschiedener Realitätstreue)

5. **Evaluieren der Gestaltung**
   (Mittels Prüfbericht zur Usability, Feldbericht oder Bericht zu Nutzerbefragungen)
6. **Gestaltungslösung erfüllt die Nutzungsanforderungen**
   (Durch Abschluss der entsprechenden Projekt-Phase)

Die Iterationsschleife kann so oft wiederholt werden, bis die Gestaltungslösung die Nutzungsanforderungen erfüllt und – falls Evaluierungsergebnisse Bedarf dafür aufzeigen – auch wieder bei einem beliebigen Zwischenschritt einsteigen. Abb. 6 zeigt das genannte Beispiel als wechselseitige Abhängigkeit menschenzentrierter Gestaltungsaktivitäten:

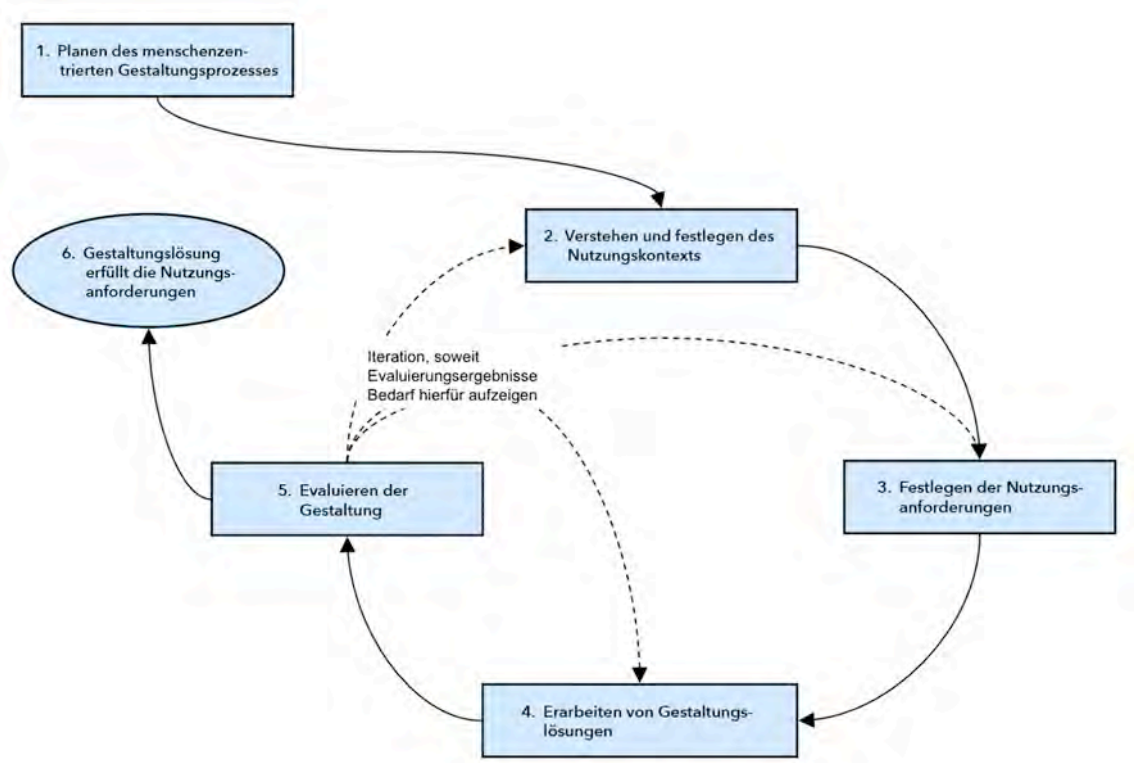


Abbildung 6: Iterationskreislauf des Usability Engineerings (modifiziert nach [47, S. 21])

Usability Evaluation

Die *Usability Evaluation* ist nicht nur ein wichtiger Bestandteil des Usability Engineerings, sondern kann auch unabhängig davon zur Überprüfung der Usability eines Systems angewendet werden. Der Zweck der Evaluation muss bei der Wahl einer passenden Methode jedoch berücksichtigt werden. Hierbei kann zwischen summativer, formativer und komperativer Evaluation unterschieden werden [130, S. 224], [147, S. 120]:

- Die *summative* (abschließende) Evaluation findet einmalig am Ende des Entwicklungsprozesses statt und führt häufig zu einer globalen Bewertung, ohne dass konkrete Anhaltspunkte für eine Verbesserung ermittelt werden.
- Die *formative* (gestaltende) Evaluation hingegen ist eine den Entwicklungsprozess begleitende Bewertung, die konstruktive Verbesserungsmöglichkeiten aufzeigen soll. Diese können im weiteren Entwicklungsprozess bereits berücksichtigt werden.

- Die *komperative* (vergleichende) Evaluation vergleicht die Usability verschiedener Lösungsvarianten miteinander. Damit vergleichbare Daten erhoben werden können, müssen die Rahmenbedingungen der Evaluation möglichst identisch gewählt werden. Geht es bei der komperativen Evaluation um ein selbst entwickeltes Produkt, wird auch von *kompetetiver* Evaluation gesprochen.

Dabei können die zur Verfügung stehenden Methoden in zwei Gruppen eingeteilt werden: analytische und empirische Verfahren. Durch die Vorstellung einiger Evaluationsmethoden wird der Unterschied zwischen analytischer und empirischer Vorgehensweise kurz dargestellt. Gleichzeitig wird ein Methoden-Katalog erarbeitet, aus dem später eine geeignete Methodik für die anstehende Untersuchung von Privacy-Boxen ausgewählt werden kann:

Analytische Evaluation (expertenorientiert)

Bei *analytischen* Methoden wird die Beurteilung von Usability-Experten vorgenommen, welche versuchen sich in die Situation der Nutzer hineinzuversetzen. Die Beurteilung erfolgt dabei anhand von Richtlinien und Erfahrungen in der entsprechenden Anwendungsdomäne.

- **Cognitive Walkthrough:** Durch das Hineinversetzen in die Rolle eines Nutzers und dem Durchspielen eines typischen Handlungsablaufs achten ein oder mehrere Usability-Experten auf eine verständliche Interaktion mit einem System und überprüfen das erwartete Verhalten [130, S. 234].

- **Heuristische Evaluation:** Die Benutzerschnittstelle eines Systems wird von einem oder mehreren Usability-Experten anhand einer Liste von Heuristiken auf mögliche Usability-Probleme überprüft, wobei die Effizienz der Methode mit der Anzahl an Experten steigt [130, S. 232].

- **Guideline Review:** Das Verfahren ähnelt der Heuristischen Evaluation, jedoch erfolgt die Bewertung nicht anhand von allgemeinen Heuristiken, sondern mithilfe konkreter Gestaltungsvorschriften aus der Ergonomie. Deren Erfüllung wird vom Experten, ähnlich einer Checkliste, nacheinander überprüft [108, S. 39].

- **GOMS-Modell:** Mit Goals, Operators, Methods and Selection Rules (GOMS) kann die Zeit berechnet werden, welche ein Nutzer benötigt, um ein gewisses Ziel zu erreichen. Dies geschieht anhand der Zerlegung jeder Interaktion in ihre elementaren Schritte und der Zuweisung eines empirisch ermittelten Zeitwerts [130, S. 238].

Empirische Evaluation (anwenderorientiert)

Bei *empirischen* Methoden werden die Informationen über die Beobachtung und Befragung von tatsächlichen Anwendern durch Tests oder Fragebögen gewonnen.

- **Hallway Test:** Einfachster Test und geringste formelle Evaluationsmethode. Zufällige Personen z.B. der Arbeitskollege auf dem Gang (Hallway), werden spontan zur Benutzbarkeit eines Systems befragt. Es handelt sich um eine gut geeignete Methode für schnelles Feedback und zum Aufdecken grober Usability-Probleme [130, S. 226].

- **Usability Walkthrough:** Auch *Pluralistic Walkthrough* wird in Form von Workshops mit Nutzern und Usability-Experten gemeinsam durchgeführt. Jeder Teilnehmer versucht individuelle Lösungen für mehrere Aufgaben zu finden, die dann mit allen Teilnehmern diskutiert werden. Ein Usability-Experte moderiert und versucht konstruktiv zwischen den Teilnehmern zu vermitteln [130, S. 228].
- **Usability Befragung:** Quantitative Methode auf Grundlage von standardisierten Fragebögen. Nutzern werden verschiedene Fragen zu Usability-Aspekten gestellt, welche auf einer numerischen Skala beantwortet werden müssen. Durch statistische Auswertung wird der Vergleich mit Normdaten oder anderen Tests möglich [130, S. 236].
- **A/B-Test:** Durch Unterteilung der Teilnehmer in zwei Untergruppen können zwei Varianten einer Lösung (A und B) miteinander verglichen werden. Mittels Befragung und Vergleich der Konversionsrate (ein Quotient, der die Wirksamkeit einer Lösung darstellt) wird ermittelt, welche Variante erfolgreicher war [130, S. 240].
- **Formaler Usability-Test:** Methode zur objektiven und nachvollziehbaren Überprüfung der Usability. Um einen Großteil der Usability-Probleme aufzudecken, werden Teilnehmern realistische Aufgaben gestellt, um unter Beobachtung herauszufinden, wie gut sie diese mit der zu testenden Benutzerschnittstelle lösen können. Aufgaben und Test-Szenario werden zur Reproduzierbarkeit schriftlich ausgearbeitet und festgehalten [130, S. 230].

Jede Evaluationsmethode hat einen eigenen Ansatz zur Bewertung der Usability, mit jeweils unterschiedlichen Stärken und Schwächen. Aus diesem Grund können sich die Ergebnisse in ihrer Effizienz und Aussagekraft stark unterscheiden:

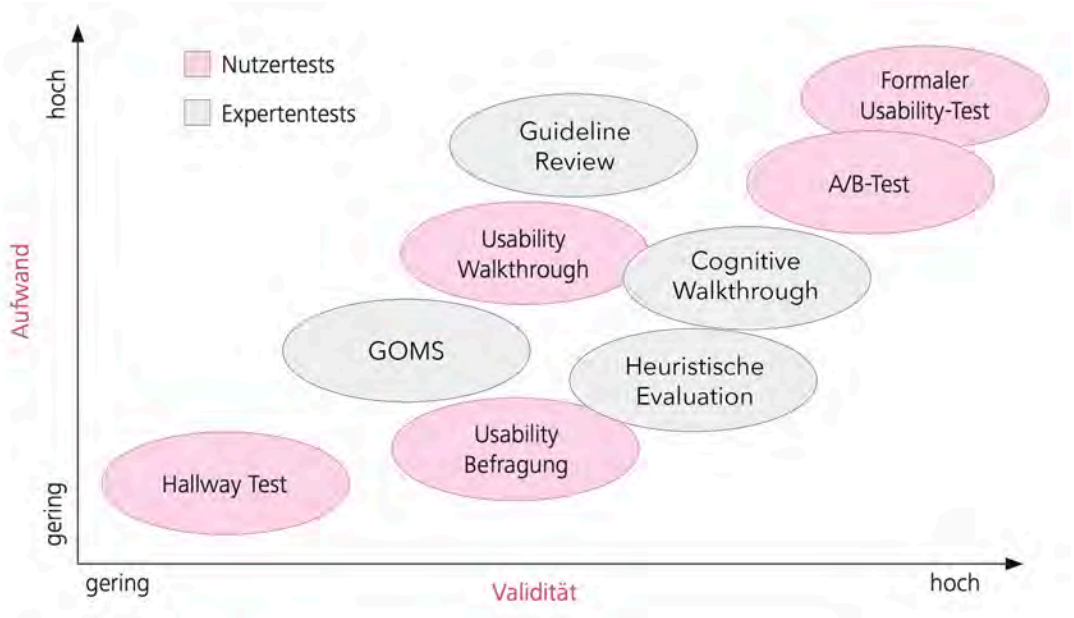


Abbildung 7: Aufwand vs. Validität von Evaluationsmethoden (korrigiert[39] nach [130, S. 225])

39 Beim Vergleich von Evaluationsmethoden in Abschnitt 5.4.3 fiel auf, dass Werte aus [130, S. 225] in der Grafik falsch dargestellt werden. Daher wird hier eine korrigierte Variante gezeigt, die der zugrundeliegenden Bewertung entspricht und zusätzlich um die Methode „Guideline Review“ erweitert wurde.

Abb. 7 veranschaulicht in welchem Verhältnis von *Aufwand der Methode* zu *Validität der Ergebnisse* die bereits vorgestellten Usability-Evaluationsmethoden im Vergleich zueinander abschneiden. Es wird deutlich, dass mit der Mehrheit der analytischen Methoden, bei mittlerem Aufwand auch nur eine mittlere bis mittelhohe Validität (Gültigkeit) erreicht werden kann. Empirische Methoden hingegen ermöglichen bei deutlich größerem Aufwand auch eine Validität im hohen Bereich.

Neben Aufwand und Validität sind Objektivität (Unbeeinflusstheit) und Reliabilität (Zuverlässigkeit) weitere wichtige Gütekriterien von Usability-Evaluationsmethoden. Sie entscheiden darüber, ob Resultate unabhängig sind von Rahmenbedingungen oder Experten und ob sie unter den gleichen Bedingungen wiederholt zu den selben Resultaten führen [130, S. 224].

2.4.4 Usable Privacy und Privacy by Design

Nachdem Grundlagen zu Privacy, Security und Usability erläutert wurden, ist es notwendig den Zusammenhang aller drei Themengebiete herzustellen und deren Relevanz für diese Arbeit zu verdeutlichen. Dies geschieht auf Grundlage der Begriffe *Usable Privacy* und *Privacy by Design*, welche den Grundlagenteil abschließen und thematisch zum aktuellen Forschungsstand überleiten.

Benutzbare und nutzerzentrierte Privatheit

Die Gefahren, welche durch die Verletzung der Privatheit von Nutzerdaten entstehen können, wurden in Abschnitt 2.2.3 (Probleme, Risiken und Gefahren) bereits beschrieben. Sie machen Selbstdatenschutz-Praktiken notwendig, um Sicherheit und Privatheit der Nutzer bei der MSI zu verbessern. In Abschnitt 2.3.3 (Sieben V der digitalen Selbstverteidigung) wurden Maßnahmen vorgestellt, mithilfe derer sich Nutzer vor diesen Gefahren schützen können. Wie in Abschnitt 2.4.2 (Konzepte und Heuristiken der Usability) erläutert wurde, sind Usability und UX entscheidend für den Erfolg eines Systems. Um den Erfolg von Selbstdatenschutz-Werkzeugen also zu gewährleisten, muss bei deren Entwurf Wert auf eine gute Usability und UX gelegt werden. Diese Anforderung an ein System kann mit dem Begriff *Benutzbare Privatheit* (engl. *Usable Privacy*) beschrieben werden.

Der verwandte Begriff *Usable Security* wurde bereits 1975 von den renommierten Wissenschaftlern des *Massachusetts Institute of Technology* (MIT) Saltzer und Schroeder in ihrem Paper *„The protection of information in computer systems“* geprägt. Sie betonen die Bedeutung von der Gestaltung benutzerfreundlicher Schnittstellen zwischen Mensch und Computer, damit Schutzmechanismen routiniert und korrekt angewendet werden: „It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.“ [146, S. 1283]. Dieser Grundsatz ist in gleichen Maßen für Systeme aus den Bereichen Sicherheit und Privatheit gültig.

Die Forderung nach benutzbaren Software-Lösungen führt dazu, dass Nutzer bei deren Entwicklung vermehrt in den Mittelpunkt rücken. Das Ziel dabei ist die Benutzbarkeit der Systeme zu verbessern, indem ein Verständnis über Kenntnisse und Fähigkeiten der Nutzer gewonnen wird [83]. Der Begriff für diesen Trend wurde bereits 1996 von den Forschern Zur-

ko und Simon vom *Open Group Research Institute* geprägt: In dem Paper *„User-Centered Security“* führen sie den Begriff *Nutzerzentrierte Sicherheit* ein, „(...) um auf Sicherheitsmodelle, Mechanismen, Systeme und Software zu verweisen, deren primäre Motivation oder Ziel die Benutzerfreundlichkeit ist“ [181, S. 1]. Wird dieses Konzept auf Systeme mit Fokus auf Privatheit übertragen, kann von *Nutzerzentrierter Privatheit* gesprochen werden.

Privatheit als Standard und Voreinstellung

Die Frage, ob sich analog zur *nutzerzentrierten Sicherheit* auch ein Trend zur *nutzerzentrierten Privatheit* entwickelt, lässt sich beispielhaft anhand von DSGVO Artikel 25 *„Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“* beantworten [40]:

DSGVO Artikel 25 Absatz 1 behandelt den Teil *Datenschutz durch Technikgestaltung* und kann auch mithilfe des englischen Begriffs *Privacy by Design* beschrieben werden. Er besagt, dass bei der Entwicklung von Systemen die Verantwortlichen in der Pflicht sind, geeignete TOMs für Datenschutz zu definieren. Mit deren Umsetzung müssen sie zusätzlich sicherstellen, dass die Datenschutzgrundsätze wirksam umgesetzt werden, sodass die Rechte betroffener Personen geschützt sind.

DSGVO Artikel 25 Absatz 2 beschreibt *datenschutzfreundliche Voreinstellungen*, die sich wiederum mit dem englischen Begriff *Privacy by Default* gleichsetzen lassen. Er besagt, dass Verantwortliche mithilfe definierter TOMs sicherstellen müssen, dass nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Zweck erforderlich ist. Dabei sind vor allem die Menge der erhobenen Daten, der Umfang ihrer Verarbeitung, ihre Speicherfrist und die Zugänglichkeit gemeint.

Zusammengefasst kann Artikel 25 der DSGVO wie folgt interpretiert werden: Datenschutz muss bereits bei der Entwicklung eines Systems berücksichtigt und implementiert werden, sodass die Standard-Einstellungen zum Schutz der Privatsphäre des Nutzers beitragen. Als TOMs können hierbei die *Werkzeuge zum Selbstdatenschutz* aus Abschnitt 4.2 sowie *Digitale Grundrechte und Prinzipien* aus Abschnitt 2.3.2 verstanden werden. Die Datenschutzgrundsätze werden in DSGVO Artikel 5 (Grundsätze für die Verarbeitung personenbezogener Daten) wie folgt definiert (wörtlich zitiert aus [42]):

> Personenbezogene Daten müssen
>
> a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (...)
>
> b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; (...)
>
> c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (”Datenminimierung”);
>
> d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; (...)

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; (...)

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet (...)

Die Pflicht zur Einhaltung von datenschutzfreundlichen Voreinstellungen bedeutet demnach, dass die Datenschutzeinstellungen bei einem Produkt oder Dienst, ohne Zutun des Nutzers, auf einem Niveau voreingestellt sein müssen, die den Datenschutzgrundsätzen entsprechen. Privacy by Default zielt darauf ab, den Selbstdatenschutz der betroffenen Person und damit ihre Souveränität zu stärken [166, S. 185].

Ann Cavoukian, kanadische Datenschüzterin und ehemalige Datenschutzbeauftragte der kanadischen Provinz Ontario, hat bereits 2010 sieben Grundprinzipien für Privacy by Design formuliert. Diese sind in Abb. 8 in Form von kleinen Zahnrädern dergestellt. Sie greifen alle gemeinsam in ein zentrales, größeres Zahnrad mit dem Titel „Privacy by Design“, als würden sie es antreiben. Die kreisförmige Anordnung wird zusätzlich von drei Pfeilen umrundet, die mit der Bezeichnung „Physikalischer Systemaufbau“, „Informations- und Kommunikationstechnik“ und „Verantwortungsbewusste Geschäftspraktiken“ die Anwendungsbereiche der jeweils benachbarten Grundprinzipien verdeutlichen.

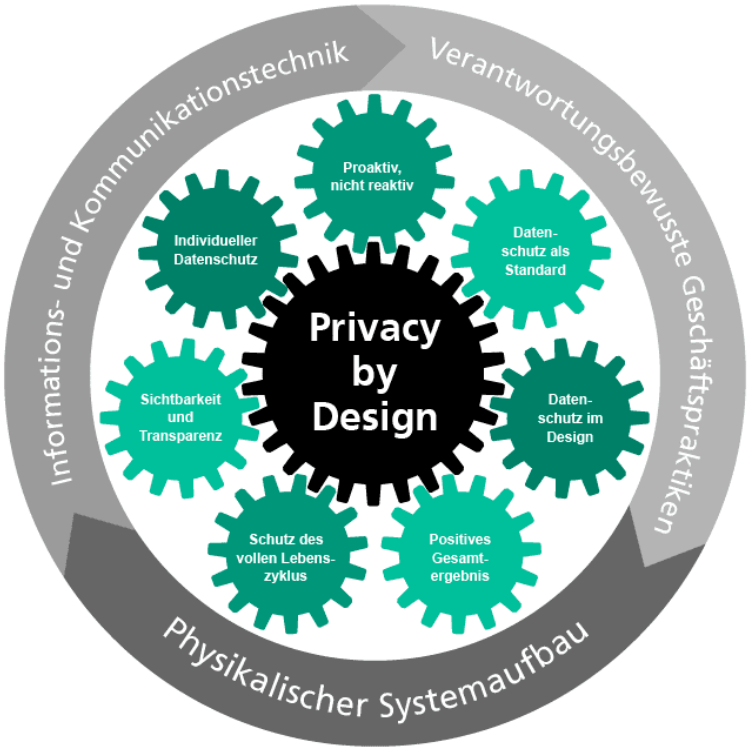


Abbildung 8: Privacy by Design – Die sieben Grundprinzipen [107]

Die in Abb. 8 dargestellten Grundprinzipien des Privacy by Design (PbD) werden im Folgenden anhand der offiziellen deutschen Übersetzung des *Fraunhofer Instituts für Optronik, Systemtechnik und Bildauswertung* (IOSB) aus Karlsruhe vorgestellt [107]:

1. **Proaktiv, nicht reaktiv:** Der PbD-Ansatz sieht Ereignisse voraus, welche in die Privatsphäre vordringen und verhindert sie, bevor sie geschehen können.

2. **Datenschutz als Standard:** PbD soll den größtmöglichen Schutz der Privatsphäre bringen, indem sichergestellt wird, dass personenbezogene Daten automatisch in jedem System und bei allen Geschäftspraktiken geschützt werden.

3. **Datenschutz im Design:** Datenschutz wird zu einer wesentlichen Komponente der Kernfunktionalität eines Systems, ohne dabei Abstriche bei der Funktionalität zu verursachen.

4. **Positives Gesamtergebnis:** Durch PbD wird die Vortäuschung falscher Gegensätze wie Datenschutz vs. Sicherheit vermieden. PbD zeigt, dass es möglich ist, beides zugleich zu erreichen.

5. **Schutz des vollen Lebenszyklus:** Durch starke Sicherheitsmaßnahmen von Anfang bis Ende wird erreicht, dass alle Daten sicher gespeichert und am Ende des Lebenszyklus sicher und rechtzeitig vernichtet werden.

6. **Sichtbarkeit und Transparenz:** PbD sorgt durch Unterwerfung einer unabhängigen Prüfung dafür, dass die einzelnen Komponenten und Verfahren eines Systems sichtbar und transparent bleiben, und zwar gleichermaßen für Nutzer und Anbieter.

7. **Individueller Datenschutz:** PbD erfordert von System-Entwicklern und -Betreibern, dass strenge datenschutzfreundliche Voreinstellungen und angemessene Benachrichtigungen angeboten, sowie benutzerfreundliche Optionen und nutzerzentrierte Gestaltung umgesetzt werden.

Auch wenn diese Grundprinzipien PbD sehr detailliert beschreiben, fehlt doch eine Aussage zu den konkreten Möglichkeiten der Umsetzung von geeigneten TOMs. Diese Problematik wird auch im nächsten Kapitel wieder auftauchen, wo mithilfe der Diskussion themenverwandter Arbeiten (*Related Work*) zunächst der aktuelle Forschungsstand aufgezeigt wird.

3 Aktueller Forschungsstand / Related Work

Die Analyse von Related Work ist hilfreich um herauszufinden, inwiefern sich diese Arbeit von themenverwandte Arbeiten abgrenzen, oder auf ihnen aufbauen kann. Dies lässt sich daran erkennen, ob bisherige Ansätze fortgeführt werden können oder ob neue Ansätze erarbeitet werden müssen. Neben diversen Testberichten[40] verschiedener Technik-Magazine zu Privacy-Boxen aus den Jahren 2016-17 scheint der aktuelle Stand der Forschung zu diesem Thema[41] noch nicht viel her zu geben. Deshalb werden in diesem Kapitel themenverwandte Arbeiten (*Related Work*) mit größtmöglichen Schnittmengen zu dieser Arbeit vorgestellt. Die betrachteten Arbeiten lassen sich in vier große Themenbereiche mit direktem Bezug einteilen: 1. Tracking und Profiling, 2. Datenschutz im Internet of Things und Smart Home, 3. Privacy und (Selbst-)Datenschutz sowie 4. Usability und Usable Privacy.

3.1 Tracking und Profiling

Da durch Tracking und Profiling erst die Notwendigkeit für den Einsatz von Selbstdatenschutz-Maßnahmen entsteht, wird im Folgenden auf Arbeiten eingegangen, die sich mit diesem Thema befassen. Es werden Arbeiten vorgestellt, welche die Nutzerwahrnehmung von Werbung und Tracking, Methoden für Profiling und Behavioral Targeting, den Einsatz von Blocker-Erweiterungen und verhaltensbasiertes Tracking untersuchen.

3.1.1 Nutzerwahrnehmung von Sharing, Werbung und Tracking

Im Rahmen des Papers *„User Perceptions of Sharing, Advertising, and Tracking“* von Chanchary et al. (2015) wurde eine Online-Nutzerstudie mit 368 Teilnehmern durchgeführt, um das Verständnis von Nutzern für Online Behavioural Advertising (OBA) und Tracking Prevention Tools (TPT) zu untersuchen. Ziel war es, die Bereitschaft von Nutzern zu ermitteln, ihre Daten für Werbeunternehmen auf unterschiedlichen Plattformen preiszugeben. Dabei wurden unterschiedliche Arten von Webseiten aus den Bereichen Online-Banking, Online-Shopping, Soziale Netzwerke und Suchmaschinen untersucht [29, S. 53].

Es gab 24 unterschiedliche Typen von persönlichen Daten, die in der Untersuchung abgefragt wurden: von sehr sensiblen Informationen (Sozialversicherungsnummer, Bankdaten, Einkommen und Kreditwürdigkeit) über demografische Daten (Alter, Geschlecht, Größe und Gewicht) bis hin zu persönlichen Informationen (Name, sexuelle und politische Ausrichtung, Bildungsstand und Hobbies) wurden auch technische Details (Betriebssystem, Browser und IP-Adresse) abgefragt [29, S. 56].

Das Ergebnis zeigte, dass die Hälfte der Teilnehmer (55%) gut über OBA informiert war und die Mehrheit (>80%) zumindest einige Maßnahmen zum Schutz ihrer Privatsphäre bereits angewendet hatte. Das allgemeine Bewusstsein über Tracking und den Schutz durch TPT war allerdings sehr gering (27%). Jedoch zeigten die Teilnehmer klare Präferenzen über die Art von Daten, welche sie bereit waren zu teilen. Diese Aussagen waren größten-

40 Golem – Privacy-Boxen im Test: Trügerische Privatheit [69], PC Magazin – Privacy-Boxen im Test: Trutzbox, Eblocker und Co. [150], PC-WELT – Sicherheitsboxen im Test: Schutz oder Augenwischerei? [6]
41 Ergebnis von Suchanfragen bei ResearchGate, ACM Digital Library, IEEE Xplore, SpringerLink und Microsoft Academic zu dem Begriff „Privacy-Box“ und ähnlichen Suchbegriffen (Stand 05.10.2020)

teils konsistent, die Art der Webseite zeigte jedoch keinen signifikanten Einfluss auf die Entscheidung der Benutzer [29, S. 56-57].

Die Nutzer zeigten die geringste Bereitschaft zur Offenlegung von Informationen wie Kreditkarte, Sozialversicherungsnummer, Telefonnummer, Privatadresse und Kreditwürdigkeit (10–17% Bereitschaft), wohingegen Land, Geschlecht, Hobbies, Betriebssystem und Browser (55–38% Bereitschaft) als weniger schützenswerte Informationen eingestuft wurden [29, S. 56]. Zur Befragung der Nützlichkeit gaben nur 37% der Befragten an, dass sie Ad Blocking Tools (ABT) für brauchbar halten, jedoch 55% fanden TPT sinnvoll. 72% der Befragten bevorzugten den Einsatz von TPT vor ABT [29, S. 59].

Es wird deutlich, dass Nutzern die Methodik von OBA (siehe „Manipulation“ in Abschnitt 2.2.3) größtenteils bewusst ist. Sie haben zudem recht klare Vorstellung davon, welche persönlichen Daten sie preisgeben wollen und welche nicht. Zum Schutz vor ungewollter Datenpreisgabe wird der Einsatz von TPT zwar als sinnvoller eingestuft als der von ABT, jedoch hat nur ein kleiner Teil der Nutzer das Bewusstsein oder die Kenntnis über deren korrekte Anwendung (siehe „Verwenden von Blocker-Software“ in Abschnitt 4.2.2).

3.1.2 User-Profiling und Behavioral Targeting

Zum Thema Profiling und OBA beschreiben Trusov et al. in ihrem Paper *„Crumbs of the Cookie: User Profiling in Customer-Base Analysis and Behavioral Targeting“* von 2015 einen Modellierungsansatz, der aus Daten des Online-Surfens individuelle Nutzerprofile generieren kann. Diese Methode ermöglicht es Online-Unternehmen Profilvorhersagen über Nutzer zu treffen, auch wenn nur begrenzte Informationen zur Verfügung stehen. Der Ansatz lässt sich durch Parallelisierung gut skalieren, wodurch auch große Mengen an Aufzeichnungen über Nutzer-Aktivitäten verarbeitet werden können [170, S. 1].

In der Arbeit wird anhand einer empirischen Studie gezeigt, dass Nutzer-Profile von großen Werbenetzwerken zu verzerrten Ergebnissen führen können, wenn sie einzig auf Basis der internen Datenansammlungen erstellt wurden. Des Weiteren wurde festgestellt, dass Verhaltensprofile von Nutzern, die auf Grundlage kleinerer Datensätze (z.B. von Suchmaschinen) erstellt wurden, von höherer Qualität sind, als die der großen Werbenetzwerke. Der vorgestellte Ansatz funktioniert, im Gegensatz zu denen großer Online-Unternehmen, besonders effektiv mit Daten, die aus einem kurzen Zeitraum stammen [170, S. 1].

Neben der Ableitung von Nutzer-Eigenschaften und -Interessen auf Grundlage von Textinhalten aus Sozialen Netzwerken, sind auch visuelle Inhalte von Bedeutung. Dies zeigt ein neuer Ansatz über die Profil-Erstellung anhand von nutzergenerierten visuellen Inhalten. In dem Paper *„A Picture Tells a Thousand Words – About You! User Interest Profiling from User Generated Visual Content“* von You et al. (2016) wird davon ausgegangen, dass Bilder, die von Nutzern in sozialen Netzwerken geteilt werden, ein Spiegelbild der Themen sind, für die sie sich interessieren [176, S. 1].

Mit dem vorgeschlagenen Ansatz ist es möglich, aus Bildern die von Nutzern gepostet wurden, Rückschlüsse auf ihre persönlichen Interessen und Eigenschaften zu erhalten. Un-

ter Zuhilfenahme von neuronalen Netzwerken, die mithilfe von Bildern aus 748 Pinterest-Fotoalben trainiert wurden, ließen sich durch experimentelle Auswertung vielversprechende Ergebnisse erzielen [176, S. 15].

Aus diesen Ergebnissen ist erkennbar, dass unter der Preisgabe einer geringen Menge an Informationen bereits detaillierte Profile von Nutzern erzeugt werden können. Es lässt sich zudem erkennen, dass die Gefahr einer verzerrten Online-Darstellung (siehe „Reputationsverlust“ in Abschnitt 2.2.3), real ist und schnell eintreten kann. Zuletzt wird klar, dass diese Gefahr eher durch die Preisgabe von Informationen an große Werbenetzwerke und soziale Medien entsteht, als durch die Nutzung von datenschutzkritischen Suchmaschinen.

3.1.3 Einsatz von Blocking-Erweiterungen gegen Tracking

Um den Praxis-Einsatz von Blocking-Erweiterungen, deren Effektivität gegen Tracking und die Entscheidungskriterien von Nutzern verstehen zu können, wurden von Mathur et al. zwei Online-Umfragen durchgeführt, in der sowohl Benutzer als auch Nicht-Benutzer von Blocking-Erweiterungen befragt wurden. In dem Paper *„Characterizing the Use of Browser-Based Blocking Extensions To Prevent Online Tracking“* von 2018 werden drei Haupterkenntnisse aus den Umfragen vorgestellt [125, S. 103]:

1. Sowohl Benutzer als auch Nicht-Benutzer von Blocking-Erweiterungen verfügen über ein grundlegendes Verständnis von Online-Tracking. Jedoch sind ihre mentalen Modelle von Online-Tracking zumeist auf den Einsatz von Blocking-Erweiterungen begrenzt.

2. Jede Art von Blocking-Erweiterung hat einen spezifischen primären Nutzen. Es wird zwischen Ad-Blockern, Tracking-Blockern und Content-Blockern unterschieden. Letztere versuchen als Multifunktions-Werkzeuge sowohl Werbung als auch Tracker zu blockieren.

3. Nutzer berichten, dass Blocking-Erweiterungen nur selten eine Website in ihrer Funktionalität einschränken. Geschieht dies doch, so deaktivieren Nutzer die Erweiterung abhängig davon, ob sie der Webseite vertrauen und wie wichtig der Inhalt ist, auf den sie zugreifen wollen.

Auf Grundlage dieser Ergebnisse wird empfohlen, anstatt Nutzern die Pflicht zum Ergreifen von Maßnahmen zu überlassen, Software zu entwickeln, die den Nutzern schon per Voreinstellung den notwendigen Schutz bietet. Als Beispiel wird der Privat-Modus bestimmter Browser (*Firefox* und *Safari*[42]) genannt, der bereits Schutz vor Tracking per Voreinstellung implementiert hat. Zusätzlich wird die Verbesserung von Blocking-Tools gefordert, sodass Funktionseinschränkungen von Websites verhindert werden können, indem zwischen notwendigem Code und Tracking-Code unterschieden wird [125, S. 111-112].

In den Empfehlungen und Forderungen zum Einsatz von Blocking-Erweiterungen können sowohl Parallelen zu PbD (siehe „Privatheit als Standard und Voreinstellung“ in Ab-

42 Mozilla Firefox (mozilla.org/firefox), Apple Safari (apple.com/safari)

schnitt 2.4.4) als auch der Verwendung von Privacy-Browsern (siehe „Nutzung verschiedener Browser“ in Abschnitt 4.2.2) gefunden werden.

3.1.4 Verhaltensbasiertes Tracking

Die bisher beschriebenen Tracking-Methoden haben eine Gemeinsamkeit: sie können auf der Nutzer-Seite (Client) erkannt werden. Daraus ergibt sich die Möglichkeit, mit den entsprechenden Maßnahmen eingreifen zu können, um das Tracking zu erschweren oder zu verhindern. Verhaltensbasiertes Tracking dagegen stellt eine durchaus größere Bedrohung für die Privatsphäre von Nutzern dar, da es auf der Client-Seite nicht erkannt und somit nur schwer verhindert werden kann.

Herrmann et al. präsentieren in *„Behavior-Based Tracking of Internet Users with Semi-Supervised Learning“* von 2016 eine Technik die es erlaubt Benutzeraktivitäten, trotz wechselnder IP-Adressen, über lange Zeiträume hinweg zu beobachten. Im Gegensatz zu vorherigen Arbeiten, die auf große Mengen „kategorisierter“ Datensätze angewiesen waren, funktioniert dieser Ansatz mit halb-überwachtem maschinellem Lernen. Durch die Nutzung von „unkategorisierten“ Datensätzen wird die Stabilität der Algorithmen erhöht, was die Genauigkeit bestehender Tracking-Technologien verbessert [86, S. 1].

Die Evaluation wurde mit einem realistischen Datensatz (DNS-Verkehr von mehr als 3.800 Nutzern) durchgeführt. Unter Verwendung des Daten-Verkehrs von einer Woche ließen sich im Durchschnitt 87% der Sitzungen, mit „überraschend“ geringem Aufwand, den richtigen Nutzern zuordnen. 55% der Nutzer wurden dabei jedes Mal korrekt wiedererkannt. Es zeigt, dass „unkategorisierte“ Nutzersitzungen eines Zeitraums von einer Woche für verhaltensbasiertes Tracking ausreichen [86, S. 4].

Die Arbeit *„Tracked Without a Trace: Linking Sessions of Users by Unsupervised Learning of Patterns in Their DNS Traffic“* (2016) des selben Forschungs-Teams geht noch einen Schritt weiter. Es wird gezeigt, dass der Aufwand von überwachten Lerntechniken vermieden werden kann. Dafür wird ein Algorithmus vorgestellt, der ohne die schwer zu erhaltenden „kategorisierten“ Schulungssitzungen auskommt. Die Untersuchung wurde mit demselben Datensatz durchgeführt (DNS-Abfragen von 3.800 Nutzern), sowie einem simulierten Beobachter (Tracker) und einem simulierten ISP, der jedem Benutzer pro Tag eine neue IP-Adresse zuweist [105, S. 1].

Bei 73% aller hochaktiver Nutzer (Aktivität an 40 von 56 Tagen) ließen sich die Sitzungen verknüpfen, bei 13% funktionierte die Rekonstruktion perfekt. Bei kürzeren Zeiträumen (Aktivität an vier von sieben Tagen) war die Rückverfolgung noch effektiver: sie funktionierte bei 75% der Sitzungen, bei 40% der Nutzer mit perfekter Übereinstimmung. Aufgrund dieser Ergebnisse werden Befürchtungen geäußert, dass Werbe-Netzwerke und Analytik-Anbieter das verhaltensbasierte Tracking als Ergänzung zu ihren bisherigen Tracking-Bemühungen einsetzen werden. [105, S. 11].

Anhand dieser beiden Beispiele wird deutlich, dass neben dem Tracking auf Client-Seite durch das Tracking auf Server- oder ISP-Seite zusätzliche Gefahren für die Privatsphäre

von Nutzern entstehen. Umso wichtiger ist der Einsatz eines vertrauenswürdigen und sicheren (verschlüsselten) DNS-Anbieters (siehe „Sichere DNS und VPN-Dienste nutzen“ in Abschnitt 4.2.2).

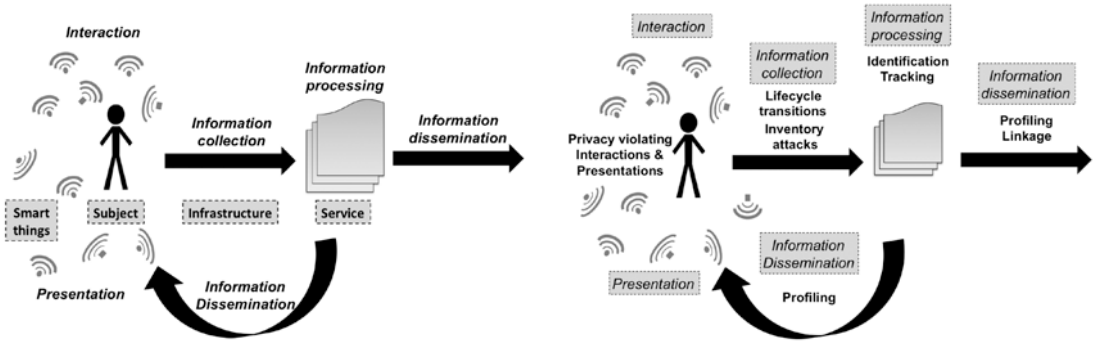
3.2 Internet of Things und Smart Home

Das Internet der Dinge (IoT) breitet sich im häuslichen Umfeld immer weiter aus. Die Nutzer verwandeln ihr Zuhause in ein intelligentes Heim, in dem Heizung, Licht und Schlösser mit dem Internet verbunden sind und über Sprache oder andere Automationen gesteuert werden können. Sicherheitsexperten haben Bedenken in Bezug auf IoT und Smart Homes festgestellt: neben anfälligen und unzuverlässigen Geräten existieren auch Risiken für die Privatsphäre der Nutzer [178, S. 65].

Bislang gibt es jedoch wenige Lösungen, die einen Schutz in diesem Bereich anbieten. Der Einsatz von Privacy-Boxen gewinnt hier an Relevanz, da sie durch den Wirkungsbereich auf Netzwerkebene einen Schutz für solche Geräte bieten können. Im Folgenden werden deshalb Arbeiten zu Sicherheit und Datenschutz bei Smart Homes und IoT, sowie der Wahrnehmung von Nutzern zu diesen Themen, vorgestellt.

3.2.1 Datenschutz im Internet of Things

Das IoT wird von Ziegeldorf et al. im Paper *„Privacy in the Internet of Things: Threats and Challenges“* von 2014 als die Weiterentwicklung des Internets beschrieben. Das Ziel, die reale Welt mit neuen Diensten abzudecken, um das Alltagsleben der Menschen zu verbessern und Gebäude, Städte und Verkehrsmittel intelligenter zu machen, bringt aber auch Bedrohungen der Privatsphäre mit sich. Die durch das IoT vermehrte, allgegenwärtige Datenerfassung – zum Erreichen dieser Fortschritte – ermöglicht auch ein omnipräsentes Tracking und Profiling [180, S. 1].



(a) IoT Referenz-Modell [180, S. 2] (b) IoT Gefahren-Modell [180, S. 6]

Abbildung 9: IoT Referenz- und Gefahren-Modell

Ziegeldorf et al. analysieren Datenschutzprobleme im Zusammenhang mit IoT anhand der Entwicklung von Merkmalen, Trends und ihren Auswirkungen auf Datenschutz. In Abb. 9a wird das vorgestellte IoT Referenz-Modell gezeigt. Smart Things, Nutzer, Infrastruktur und Services bilden die vier Grundelemente. Daran ausgerichtet können fünf Informationsflüsse stattfinden: Interaktion, Datensammlung, Informationsverarbeitung, Informationsverbrei-

tung und Darstellung. In Abb. 9b verwandelt sich das Referenz-Modell zum Gefahren-Modell durch Hinzufügen von Angriffs-Szenarien [180, S. 2 u. 6]:

Profiling wird dabei als die schwerwiegendste Bedrohung eingestuft, die aufgrund der feingranularen, allgegenwärtigen Datensammlung durch IoT verschärft wird. Zusätzliche Bedrohungen wie Nutzer-Identifizierung oder -Verfolgung tragen einen wichtigen Teil dazu bei. Weitere Datenschutzverletzungen gehen von der Interaktions-Gestaltung und der dafür notwendigen Nutzer-Schnittstelle von IoT-Geräten aus. Zusätzliche Bedrohungen können von Lebenszyklus (Löschung und Weiterverkauf), zentraler Verwaltung (unauthorisierte Auflistung) und Interoperabilität (Weitergabe von Daten an andere Systeme) von IoT-Hardware ausgehen (vgl. Abb. 9b) [180, S. 8-10].

Die Untersuchung wird mit folgenden Empfehlungen für die Entwicklung eines datenschutzbewussten IoT abgeschlossen: Aufgrund der ständigen technischen Weiterentwicklung bleibt der Schutz der Privatsphäre eine ständige Herausforderung, welcher mit entsprechender Weitsicht begegnet werden muss. Ein erfolgreiches Ergebnis erfordert zudem das koordinierte Vorgehen bei der Bereitstellung technischer Lösungen unter Berücksichtigung der entsprechenden rechtlichen Rahmenbedingungen [180, S. 11].

Aus der vorgestellten Arbeit wird deutlich, welche Risiken durch die Verwendung ungeschützter IoT-Geräte ausgehen kann (siehe „Profiling“ in Abschnitt 2.2.2) und wie wichtig die entsprechende Berücksichtigung von Datenschutz bereits bei der Entwicklung ist (siehe „Privatheit als Standard und Voreinstellung“ in Abschnitt 2.4.4).

3.2.2 Sicherheit und Datenschutz bei Smart Homes

Eine spezielle Form des IoT beschreibt die Interaktion zwischen verschiedenen Geräten in einem Haushalt als „Smart Home“-Architektur. Diese ermöglicht Nutzern sowohl die Steuerung aller damit verbundenen IoT-Geräte, als auch die logische Verknüpfung der Geräte untereinander. Die Anfälligkeit einer solchen Architektur für Sicherheits- und Datenschutzfragen wird in dem Paper *„Security and Privacy Issues for an IoT based Smart Home“* von Geneiatakis at al. von 2017 behandelt [67, S. 1292].

In der Arbeit wird beschrieben, dass IoT-Architekturen eine wichtige Komponente des zukünftigen Internets darstellen, indem die Lücke zwischen physischer und virtueller Welt geschlossen wird. Das Smart Home, als eine wichtige Kategorie von IoT-Umgebungen, bietet durch die Automation von Alltags-Aufgaben zwar Vorteile für die Nutzer, setzt sie jedoch auch neuen Gefahren aus. Aufgrund der begrenzten Rechenleistung von ubiquitären Geräten und der Notwendigkeit von heterogenen Netzwerkarchitekturen vergrößert sich die Angriffsfläche vieler bereitgestellter Dienste durch mangelhafte oder fehlende Datenschutzfunktionen [67, S. 1297].

Des Weiteren wird in der Arbeit ein Angriffs-Modell für „Smart Home“-Geräte vorgestellt, das unter Berücksichtigung von IoT-Standardkomponenten analysiert werden kann. Erste Ergebnisse zeigen, dass eine bestehende „Smart Home“-/IoT-Infrastruktur unter bestimmten Umständen anfällig für Attacken wie Lauschangriffe, Identitätsdiebstahl, DoS

oder Ausnutzung von Software-Schwachstellen ist. Solche Angriffe sind möglich, wenn sich Angreifer Zugang zum zugrunde liegenden Netzwerk verschaffen, oder wenn Geräte mit Werks-Einstellungen (z.B. Standard-Zugangsdaten) betrieben werden [67, S. 1296-1297]. Als mögliche Lösung für diese Probleme wird vorgeschlagen, den Nutzer zu einer korrekten Konfiguration der Geräte zu zwingen und die Funktionalität von Diensten sonst zu verweigern: IoT-Dienste, Fernzugriffe und Port-Freigaben könnten so nur aktiviert werden, wenn bereits ein sicheres Passwort vergeben wurde [67, S. 1296].

Um die Erwartungen, Handlungen und Einstellungen von „Smart Home"-Nutzern über Sicherheit und Datenschutz zu untersuchen, führten Zeng et al. halbstrukturierte Interviews durch, deren Ergebnisse 2017 in der Arbeit *„End User Security & Privacy Concerns with Smart Homes"* veröffentlicht wurden. Es wurden dabei 15 Personen befragt, die in Smart Homes lebten, davon zwölf „Smart Home"-Administratoren und drei weitere Bewohner, um mehr über ihre mentalen Modelle und die Existenz von Sicherheits- und Datenschutzbedenken zu verstehen [178, S. 65]. Dabei wurden folgende grundlegende Erkenntnisse gewonnen [178, S. 74-75]:

1. Unvollständige mentale Modelle führen zu Problemen bei der Wahrnehmung von Bedrohungen und dem notwendigen Sicherheitsverhalten.
2. Die „Smart Home"-Teilnehmer befassen sich mehr mit Fragen zur physischen Sicherheit als mit Fragen zu Privatsphäre und Datenschutz.
3. Es existiert ein gefährliches Ungleichgewicht zwischen Bewusstsein und Macht von „Smart Home"-Administratoren und anderen „Smart Home"-Bewohnern.

Auf Grundlage dieser Ergebnisse werden folgende Lösungen vorgeschlagen [178, S. 75-76]:

- Durch eine Verfeinerung der mentalen Modelle (über verwendete Technologien) kann eine Verbesserung beim Erkennen von Bedrohungen erreicht werden. Nutzer können so bewusste Entscheidungen über Datenschutz- oder Sicherheitsrisiken treffen.
- „Smart Home"-Plattformen müssen für mehrere Nutzer konzipiert werden. Dadurch werden potenzielle Risiken vermieden, die durch den Missbrauch von Wissens- und Macht-Diskrepanzen zwischen den einzelnen Nutzern entstehen können.
- Es müssen Anleitungen für Nutzer mit geringer technischer Expertise zur Verfügung stehen, damit sie fundierte Entscheidungen darüber treffen können, welche Produkte strengere Sicherheits- und Datenschutz-Anforderungen haben.
- Da Heuristiken viele Sicherheits- und Datenschutzprobleme im Bereich von Smart Home nicht abdecken, müssen „Best Practices" von Sicherheitsexperten im Kontext von Smart Home entwickelt und Nutzern auf effiziente Weise vermittelt werden.
- Die Entscheidung zwischen „Sicherheit und Privatsphäre" oder „Funktionalität und Bequemlichkeit" zwingt Nutzer oft zur Resignation, weshalb „Smart Home"-Systeme so konzipiert werden müssen, dass ein geeigneter Kompromiss zur Verfügung steht.

Es wird deutlich, dass in den Bereichen Smart Home und IoT das Schaffen eines Bewusstseins für potentielle Schwachstellen (siehe „Erkennen von Schwachstellen und Gefahren“ in Abschnitt 4.2.1), der Einsatz von sicheren Passwörtern (siehe „Erstellen und Verwenden sicherer Passwörter“ in Abschnitt 4.2.1) sowie die Verwendung sicherer DNS-Anbieter (siehe „Sichere DNS und VPN-Dienste nutzen“ in Abschnitt 4.2.2) zum Schutz von Sicherheit und Privatsphäre der Nutzer beitragen können.

Ebenso ist die Erarbeitung einer zufriedenstellenden Voreinstellung für Sicherheit und Privatsphäre auf Seite der Hersteller notwendig (siehe „Privatheit als Standard und Voreinstellung“ in Abschnitt 2.4.4). Es wird zudem deutlich, dass im Kontext „Smart Home“ verschiedene Nutzergruppen existieren. Die Geräte müssen für diese konzipiert werden, da von der unterschiedlicher Nutzer-Expertise sonst Gefahr für andere Teilnehmer (Manipulation oder Überwachung) ausgehen kann.

3.2.3 Nutzerwahrnehmung von Datenschutz bei Smart Home und IoT

Im Rahmen der Arbeit *„User Perceptions of Smart Home IoT Privacy“* von Zheng et al. wurde 2018 die Nutzerwahrnehmung von Datenschutz bei „Smart Home IoT“-Geräten anhand der Befragung von elf „Smart Home“-Besitzern untersucht. Es wurde nach Gründen für den Kauf von IoT-Geräten, der Wahrnehmung von Datenschutzrisiken im Smart Home und Maßnahmen zum Schutz der Privatsphäre gefragt [179, S. 200:1]. Dabei wurden die folgenden vier wiederkehrenden Punkte festgestellt [179, S. 200:2-3]:

1. Der Wunsch nach Bequemlichkeit und Vernetzung gilt weiterhin als eine primäre Rechtfertigung für den Verzicht auf Privatsphäre.

2. Die Akzeptanz der Datenpreisgabe an externe Institutionen ist abhängig von dem empfundenen Vorteil für die Nutzer: Hersteller genießen die höchste, Werbetreibende und Regierungen mittlere und ISPs die geringste Akzeptanz bei den Nutzern.

3. Markenbekanntheit und Ruf sind ausschlaggebende Faktoren bei der Kaufentscheidung für IoT-Geräte. Nutzer überprüfen jedoch nicht, ob versprochene Schutzmechanismen auch wirklich vorhanden sind.

4. Nutzern fehlt das Bewusstsein für Privatsphäre-Risiken, die von Geräten ausgehen, welche weder Audio noch Video aufzeichnen, jedoch Daten über Schlafgewohnheiten und Hausnutzung preisgeben können (z.B. vernetzte Glühbirnen und Thermostate).

Diese Ergebnisse werden als Motivation gesehen, Empfehlungen für Gerätedesigner, Forscher und Industrie zu entwickeln, um die Datenschutzfunktionen der Geräte besser an die Erwartungen und Vorlieben der Besitzer von Smart Homes anzupassen: Die erste Empfehlung betrifft die Nutzung visueller Indikatoren oder mobiler Apps für die Darstellung von Informationen auf Geräten, die über kein Display verfügen. Des Weiteren wird eine zentrale Verwaltung von Privatsphäre und Sicherheit für alle im Smart Home befindlichen Geräte vorgeschlagen. Eine weitere Idee ist der Einsatz von vorgeschlagenen Standardeinstellungen, die durch Crowd-Sourcing für verschiedene Situationen gesammelt werden. Zuletzt

wird ein Zertifizierungsprogramm mit festgelegten Industriestandards vorgeschlagen, welches gute Datenschutzpraktiken für Gerätehersteller vorgibt [179, S. 200:14-17].

Aus dieser Arbeit geht erneut hervor, dass Nutzern häufig das Bewusstsein für Privatsphäre-Risiken bei der Verwendung vernetzter Geräten fehlt (siehe „Erkennen von Schwachstellen und Gefahren“ in Abschnitt 4.2.1). Zusätzlich überwiegt der Wunsch nach Bequemlichkeit zumeist die Bereitschaft Selbstdatenschutz-Maßnahmen zu ergreifen. Zuletzt entscheiden Faktoren wie Image oder Bekanntheit über das Vertrauen in externe Institutionen und die Bereitschaft persönliche Daten mit ihnen zu teilen.

3.3 Privacy und (Selbst-)Datenschutz

Die Themen Privatsphäre und Datenschutz werden bereits von einer Vielzahl an Literatur und wissenschaftlichen Arbeiten behandelt, deshalb wird die Auswahl in diesem Abschnitt auf besonders relevante und aktuelle Arbeiten reduziert. Darunter fallen das *P3P-Projekt*, die *Privacy Design Strategies* und weitere Arbeiten zum Bewusstsein von Privatheitsrisiken, der Einstellung von Nutzern gegenüber Datenpreisgabe und Schwierigkeiten bei der Einbettung von Privatsphäre-unterstützenden Technologien.

3.3.1 Konzepte für den Datenschutz

Schon seit geraumer Zeit machen sich Internetnutzer zunehmend Sorgen darüber, welche persönlichen Informationen von ihnen preisgegeben werden, wenn sie sich online bewegen und wo diese schlussendlich landen. Die meisten Nutzer finden es schwierig und zeitaufwändig Datenschutzrichtlinien zu lesen, zu verstehen oder herauszufinden wie die Preisgabe persönlicher Informationen vermindert werden kann. Das Projekt *Platform for Privacy Preferences* (P3P) ging dieses Problem, mit einem computerlesbaren Standardformat für Datenschutzrichtlinien und einem Protokoll, mit dem Web-Browser diese automatisch lesen und verarbeiten können, an [33, S. 3].

Das P3P-Projekt wurde von Lorrie Cranor, Professorin für Sicherheit und Privacy an der *Carnegie Mellon University* in Pittsburgh und Gründerin des *Symposium On Usable Privacy and Security* (SOUPS), geleitet. Es wurde vom *World Wide Web Consortium* (W3C) entwickelt und im April 2002 als Standard empfohlen. Aufgrund der geringen Unterstützung des Standards durch populäre Browser und Webseiten wurde die Entwicklung 2018 als veraltet bzw. überholt erklärt und eingestellt. Lediglich der *Internet Explorer*[43] und 6% der 10.000 meist genutzten Webseiten hatten den Standard implementiert [171].

Das ursprüngliche Konzept von P3P sieht vor, dass Nutzer ihre persönlichen Datenschutzeinstellungen im einem P3P-fähigen Web-Browser konfigurieren können. Beim Aufruf von P3P-konformen Webseiten kann mithilfe der maschinenlesbaren Datenschutzrichtlinien abgeglichen werden, ob die Implementierung der Webseite den Einstellungen des Nutzers entspricht. Darauf basierend können Warnungen angezeigt werden, falls Webseiten nicht den Präferenzen des Nutzers entsprechen oder Zusammenfassungen der Datenschutzrichtlinien bereitgestellt werden [33, S. 4].

43 Internet Explorer (microsoft.com/de-de/download/internet-explorer.aspx)

Im Gegensatz zu Anonymitätstools, welche die Übertragung von persönlich identifizierbaren Informationen verhindern, war der Anspruch des P3P-Projekts, die Entwicklung von Werkzeugen zu ermöglichen, mithilfe derer fundierte Entscheidungen über die Preisgabe persönlicher Informationen getroffen werden können. Diese Instrumenten sollten dann Hand in Hand mit Anonymitätssoftware oder Werbe-Filtern eingesetzt werden können, um die Übertragung persönlicher Informationen in bestimmten Situationen tatsächlich verhindern zu können [33, S. 3-4].

In der Arbeit *„Engineering Privacy by Design“* (2011) schlagen Gürses et al. einen anderen Ansatz vor. Es geht darum, das Konzept von Privacy by Design (PbD) als Leitlinie für die Übersetzung komplexer sozialer, rechtlicher und ethischer Bedenken in Systemanforderungen zu verwenden. Dies soll dabei helfen, das schwierige Problem der Gestaltung und Umsetzung von Datenschutzanforderungen in Systemen zu lösen. Da die Prinzipien von PbD jedoch sehr vage bleiben und Fragen bezüglich der Implementierung offen lassen, wird die Umsetzung von Datenschutz durch *Datenminimierung* als erster konkreter Schritt untersucht. Anhand von zwei Fallstudien wird gezeigt, dass die Auslegung der PbD-Prinzipien spezielles technisches Fachwissen, kontextbezogene Analysen und eine Abwägung der vielseitigen Sicherheits- und Datenschutzinteressen erfordert [79, S. 1].

In *„Privacy Design Strategies“* (2014) greift Jaap-Henk Hoepman die Arbeit von Gürses et al. auf und verwendet zusätzlich die Norm *DIN EN ISO/IEC 29100* (siehe „Datenschutzprinzipien“ in Abschnitt 2.3.2). Er entwickelt daraus acht Datenschutzstrategien, welche IT-Architekten dabei helfen, PbD bereits früh im Lebenszyklus der Software-Entwicklung, also während der Konzeptentwicklung und Analyse, anzuwenden. Dabei wird zwischen datenorientierten Strategien (*Minimieren*, *Verbergen*, *Trennen*, *Aggregieren*) und prozessorientierten Strategien (*Informieren*, *Kontrollieren*, *Durchsetzen* und *Demonstrieren*) unterschieden [89, S. 452-456]. In Tabelle 1 wird gezeigt, welche Strategien sich bei welchen Datenschutzprinzipien – vollständig oder nur teilweise – anwenden lassen:

	Zweckbeschränkung	Datenminimierung	Datenqualität	Transparenz	Rechte des Betroffenen	Recht auf Vergessen	Angemessener Schutz	Datenübertragbarkeit	Missbrauch-Meldungen	(Prüfbare) Einhaltung
Minimieren	○	+								
Verbergen		+					○			
Trennen	○						○			
Aggregieren	○	+								
Informieren				+	+				+	
Kontrollieren			○		+			+		
Durchsetzen	+		+			+	+			○
Demonstrieren										+

Legende: + = Deckt das Prinzip weitgehend ab. ○ = Deckt das Prinzip teilweise ab.

Tabelle 1: Anwendbarkeit von Strategien zu Prinzipien beim Datenschutz (übers. n. [89, S. 456])

Gürses et al. untersuchen vier Jahre nach ihrer vorherigen Arbeit die Entwicklung der angestoßenen Diskussion über Datenminimierung und Privacy Engineering in *„Engineering Privacy by Design Reloaded“* (2015). Es stellt sich heraus, dass die Metapher „Datenminimierung“ zur Anwendung von Datenschutz nicht ausreicht, da trotz Minimierung der Datenflüsse noch sensible Nutzerdaten erfasst und in Systemen gespeichert werden. Nach einer Untersuchung bestehender Systementwürfe zur Wahrung von Privatsphäre wird deutlich, dass unter dem Begriff „Datenminimierung“ eine ganze Familie von Entwurfsprinzipien zusammengefasst wird. Es verbirgt sich eine Reihe von Entwurfsstrategien dahinter, die Experten bei der Entwicklung von Systemen zur Wahrung der Privatsphäre intuitiv anwenden: dazu gehören Einschränkungen des Informationsflusses, sowie die Minimierung der Sammlung, Offenlegung, Verlinkbarkeit, Replikation, Speicherung und Zentralität von Daten [80, S. 1-2].

Nach der Zusammenfassung dieser Arbeiten lässt sich schlussfolgern, dass auch gute Konzepte für die Anwendung von Datenschutz an fehlenden Umsetzungspflichten scheitern können (wie das P3P-Projekt). Des Weiteren wird deutlich, dass PbD ein guter Ansatz für die Realisierung von Datenschutz ist (siehe „Privatheit als Standard und Voreinstellung“ in Abschnitt 2.4.4), jedoch nicht konkret genug, um bei der Entwicklung von Systemen angewendet werden zu können. Aus diesem Grund besteht ein hoher Bedarf an Entwurfsstrategien, mit denen Datenschutzprinzipien umgesetzt werden können.

3.3.2 Privatheits- und Privatsphärekompetenz

Die als *Privacy-Paradox* bereits vorgestellten Unterschiede von Einstellung und Verhalten der Internetnutzer zum Online-Datenschutz, wurden in empirischen Forschungen bereits aufgedeckt. Trepte et al. schlagen in ihrer Arbeit *„Do People Know About Privacy and Data Protection Strategies? Towards the ‘Online Privacy Literacy Scale’ (OPLIS)“* (2015) eine umfassende Skala zur Messung der Datenschutzkompetenz und deren Umsetzung in künftiger Forschung und Politikgestaltung vor. Eine Skala für den Online-Datenschutz (OPLIS) wird auf der Grundlage bisheriger Literatur zum Datenschutz und einer Vielzahl von Aspekten erarbeitet, die für den Online-Datenschutz relevant sind. Die Skala umfasst folgende fünf Dimensionen der Online-Privatsphäre-Kompetenz [169, S. 333]:

1. Wissen über Praktiken von Organisationen, Institutionen und Online-Diensten
2. Wissen über technische Aspekte der Online-Privatsphäre und des -Datenschutzes
3. Wissen über Gesetze und rechtliche Aspekte des Datenschutzes in Deutschland
4. Wissen über europäische Richtlinien zum Schutz von Privatsphäre und Daten
5. Wissen über Nutzerstrategien zur individuellen Regulierung des Datenschutzes

Die Berechnung der Skala findet auf Grundlage eines Fragebogens zu oben genannten Dimensionen statt. Das Ziel von OPLIS ist herauszufinden, ob sich das paradoxe Verhalten der Nutzer durch mangelndes Wissen über: 1. individuelle Strategien zur Kontrolle der Online-Privatsphäre, 2. rechtliche und technische Aspekte oder 3. institutionelle Praktiken erklären lässt. Die Ergebnisse früherer Forschungen zeigen ein erschreckendes Bild.

Internet-Nutzer wissen nicht, wie sie ihre persönlichen Daten schützen oder ihre individuelle Privatsphäre effizient regeln können; außerdem gibt es wenig Informationen über Geschäftspraktiken, Gesetze und Vorschriften, die den Datenschutz betreffen [169, S. 362].

Philipp K. Masur schlägt in *„Mehr als Bewusstsein für Privatheitsrisiken“* (2018) vor, dass Online-Privatheitskompetenz nicht nur als Wissenskonstrukt, sondern allgemeiner als eine Kombination aus Wissen und besonderen Fähig- und Fertigkeiten bestehen muss. Er nimmt Bezug auf OPLIS und sieht in einer Rekonzeptualisierung vor, dass neben faktischem Wissen über ökonomische, technische und rechtliche Aspekte der Online-Privatheit auch privatheitsbezogene Reflexions- und Kritikfähigkeit sowie konkrete Privatheits- und Datenschutzfertigkeiten dazugehören müssen (vgl. Abb. 10) [124, S. 2].

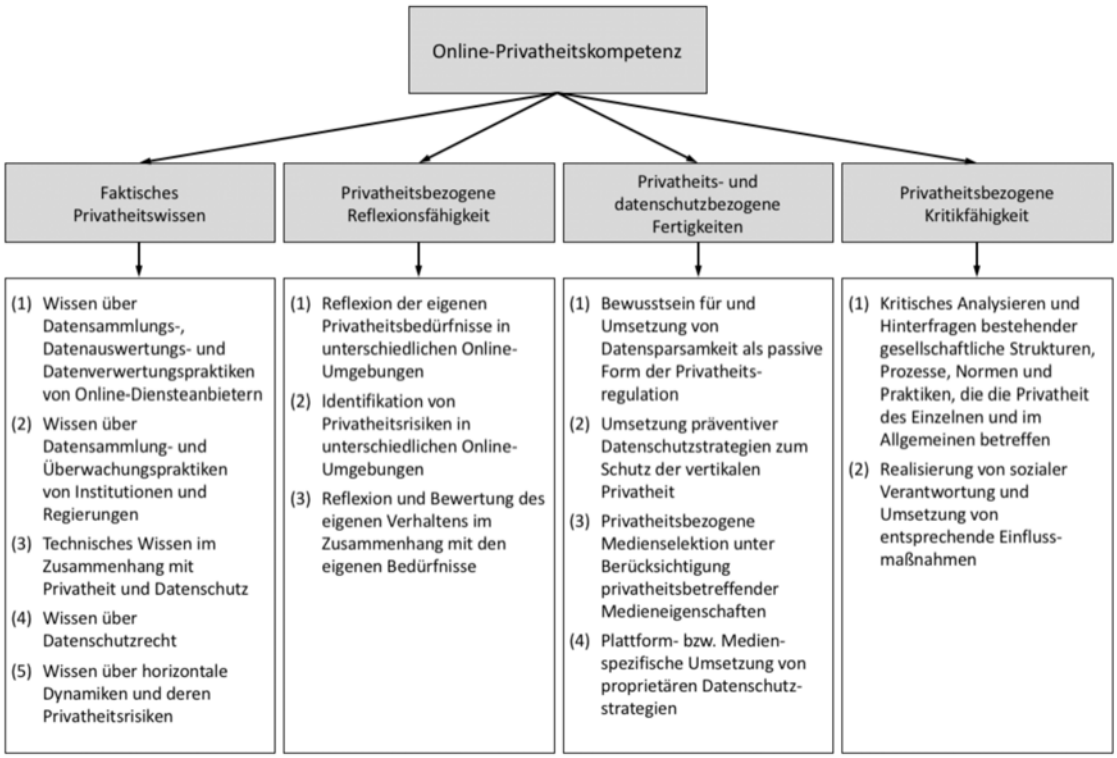


Abbildung 10: Vier Dimensionen der Online-Privatheitskompetenz [124, S. 11]

Wie Abb. 10 zeigt, wird die Online-Privatheitskompetenz in der Rekonzeptualisierung in vier Hauptdimensionen unterteilt. Das bisher untersuchte faktische Wissen (den Dimensionen von OPLIS entsprechend) wird um Reflexions- und Kritikfähigkeiten sowie spezifische Umsetzungsfertigkeiten ergänzt. Es wird argumentiert, dass erst ein solch umfassender, privatheitsbezogener Kompetenzbegriff, als angemessenere Voraussetzung für die Umsetzung des Ideals der informationellen Selbstbestimmung angesehen werden kann [124, S. 15].

Zwei Jahre später baut Philipp K. Masur auf seiner eigenen Arbeit auf und untersucht in *„How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information“* (2020) wie Online-Privatsphäre-Kompetenz Selbstdatenschutz und Selbstbestimmung im Informationszeitalter unterstützen kann. Dazu werden zwei Modelle präsentiert: Das Erste separiert die individuelle von der kollektiven Privatsphäre. Das Zweite unterscheidet zwischen einer negativen und einer positiven Perspektive auf Privatsphäre

und Datenschutz. Philipp K. Masur beschreibt, dass die Online-Privatsphäre-Kompetenz eine wichtige Rolle bei der Bewältigung der sozialen, wirtschaftlichen und institutionellen Dynamik spielt, aus der die aktuellen Bedrohungen der Privatsphäre des Einzelnen entstehen [123, S. 258-265].

Durch OPLIS und die Arbeiten von Philipp K. Masur wird deutlich, dass der Übergang von Datenschutz zu Selbstdatenschutz mit der Entwicklung einer Privatheits- und Privatsphärekompetenz einher gehen muss. Es zeigt sich, dass diese erst durch die eigene Reflexion entstehen kann: Neben dem Wissen über Datenschutz-Praktiken, -Rechte und -Risiken, ist das Entwickeln eines Bewusstseins durch kritisches Hinterfragen notwendig, um Selbstdatenschutz zu verstehen und effektiv anwenden zu können (siehe „Selbstdatenschutz“ in Abschnitt 2.3).

3.3.3 Herausforderungen beim Selbstdatenschutz

Von Alpers et al. wird in *„Herausforderungen bei der Entwicklung von Anwendungen zum Selbstdatenschutz“* (2017) die Frage der Bewertung von Urheberrecht und Wettbewerbsrecht im Spannungsverhältnis zum Selbstdatenschutz untersucht. Dieses Spannungsverhältnis entsteht beim Eingriff von technischen Lösungen (zur Unterstützung des Privatsphärenschutzes) in die Integrität urheberrechtlich geschützter Computerprogramme oder Geschäftsmodelle. Es wird vermutet, dass dieses Spannungsverhältnis existiert, solange Paradigmen wie PbD nicht von sämtlichen Anwendungen und Systemen berücksichtigt werden und dadurch der Einsatz von Anwendungen zum Selbstdatenschutz überflüssig wird [5, S. 1061-1071].

Die Herausforderung bei der Integration von Technologien zur Verbesserung der Privatsphäre in die Infrastruktur des Internets, werden in der Arbeit *„Integrating Privacy-Enhancing Technologies into the Internet Infrastructure“* (2017) von Harborth et al. vorgestellt. Das Ziel ist die Etablierung von *Privacy Enhancing Technologies* (PET) im Massenmarkt der Verbraucher. Es werden drei verschiedene Bereiche von PETs genannt: Schutz durch Anonymisierung auf Ebene von 1. ISPs, 2. Netzwerken und 3. dem 5G-Mobilfunknetz. Neben Vorschlägen zur Verbesserung von Benutzbarkeit und Leistung werden auch Geschäftsmodelle genannt, die bei der Integration der Technologien wichtig sind. Es wird davon ausgegangen, dass Entwicklungen in allen drei Tätigkeitsfeldern (Benutzbarkeit, Leistung und Geschäftsmodelle) erforderlich sind, um PETs in den Massenmarkt der Verbraucher zu bringen [82, S. 1-7].

Weitere Schwierigkeiten, bei der Einbettung von Privatsphäre in der Software-Entwicklung, werden von Senarath und Arachchilage in *„Why developers cannot embed privacy into software systems?: An empirical investigation“* (2018) untersucht. In einer Studie mit 36 Software-Entwicklern wurden die Probleme identifiziert, mit denen Software-Entwickler konfrontiert sind, wenn sie Datenschutz in Software-Anwendungen einbetten müssen. Die Ergebnisse zeigten, dass Entwickler praktische Probleme damit haben, Datenschutzanforderungen mit Entwicklungsmethoden in Beziehung zu setzen. Es fehlt ihnen an Wissen über formal etablierte Datenschutzkonzepte aus der Forschung wie z.B. PbD. Das Resul-

tat sind Softwareanwendungen bei denen Privatsphäre nur eingeschränkt oder gar nicht implementiert ist, weshalb eine entsprechende Ausbildung über Datenschutzpraktiken für Entwickler vorgeschlagen wird [154, S. 1-5].

Es werden Herausforderungen und Schwierigkeiten deutlich, die bei der Entwicklung und Anwendung von Selbstdatenschutz entstehen können. Diese liegen nicht nur in den offensichtlichen Bereichen wie der Implementierung von PETs oder deren Integration in die Infrastruktur des Internets, sondern können sich auch hinter Fragen nach Urheberrecht und Lauterkeit verbergen. Das Konzept von PbD zieht sich wie ein roter Faden als Lösungsvorschlag durch die betrachteten Arbeiten (siehe „Privatheit als Standard und Voreinstellung“ in Abschnitt 2.4.4).

3.3.4 Datenschutz auf dem Prüfstand

Um der Frage nachzugehen, warum die Privatsphäre von Nutzern oft vernachlässigt wird, untersuchen Coopamootoo et al. in *„Why Privacy Is All But Forgotten: An Empirical Study of Privacy & Sharing Attitude“* (2017) ob es Unterschiede zwischen der Einstellung von Nutzern zur Privatsphäre und zum Teilen von Inhalten gibt. In einer empirischen Studie zeigte sich, dass die Einstellung zur Privatsphäre bei einer Reihe von Verhaltensregeln, wie z.B. Ausdruck von Emotionen oder Beziehungen zu anderen, sich signifikant von der Einstellung zum Teilen von Inhalten unterscheidet. Die Ergebnisse deuten darauf hin, dass die Einstellung zum Datenschutz von defensiver Motivation und die Einstellung zum Datenaustausch von begehrender Motivation bestimmt sein kann [31, S. 97-114].

Rudolph et al. hingegen versuchen in *„Why Users Ignore Privacy Policies – A Survey and Intention Model for Explaining User Privacy Behavior“* (2018) herauszufinden, weshalb Nutzer Datenschutzrichtlinien oft ignorieren. Auf Basis einer Umfrage mit fast 1.400 Teilnehmern, wurde ein Intentionsmodell entwickelt (vgl. Abb. 11), um zu erklären, warum Nutzer die Schnittstellen zum Schutz der Privatsphäre nicht nutzen – obwohl sie dies im Allgemeinen gerne tun würden [144, S. 587]. Die Befragung ergab, dass nur 50% der Teilnehmer Datenschutzhinweise bei Online-Diensten beachten, obwohl 90% daran interessiert sind. Zusätzlich empfanden 70% der Befragten diese als zu lang und zu zeitaufwändig und 41% beschrieben sie als zu kompliziert [144, S. 590-591].

Um herauszufinden, wo die Barrieren liegen, die Nutzer daran hindern Maßnahmen in Bezug auf die Privatsphäre zu ergreifen, wurde ein Intentionsmodell entwickelt. Wie in Abb. 11 zu sehen ist, kombiniert das Modell Aspekte wie Bedürfnisse des Nutzers nach Privatsphäre, seine Motivation und Absichten, sowie zuvor genannte Barrieren. Diese existieren, falls die Möglichkeiten (Ressourcen) eines Nutzers geringer sind als die Anforderungen an die Datenschutz-Schnittstelle. Die resultierende Intention zur Verwendung von Privatsphäre-Schnittstellen, ergibt sich aus der intrinsischen Motivation des Nutzers die existierenden Barrieren zu überwinden. Es wird geschlussfolgert, dass Datenschutz-Schnittstellen nur dann genutzt werden, wenn diese Motivation alle vorherrschenden Barrieren überwiegen kann [144, S. 596-597].

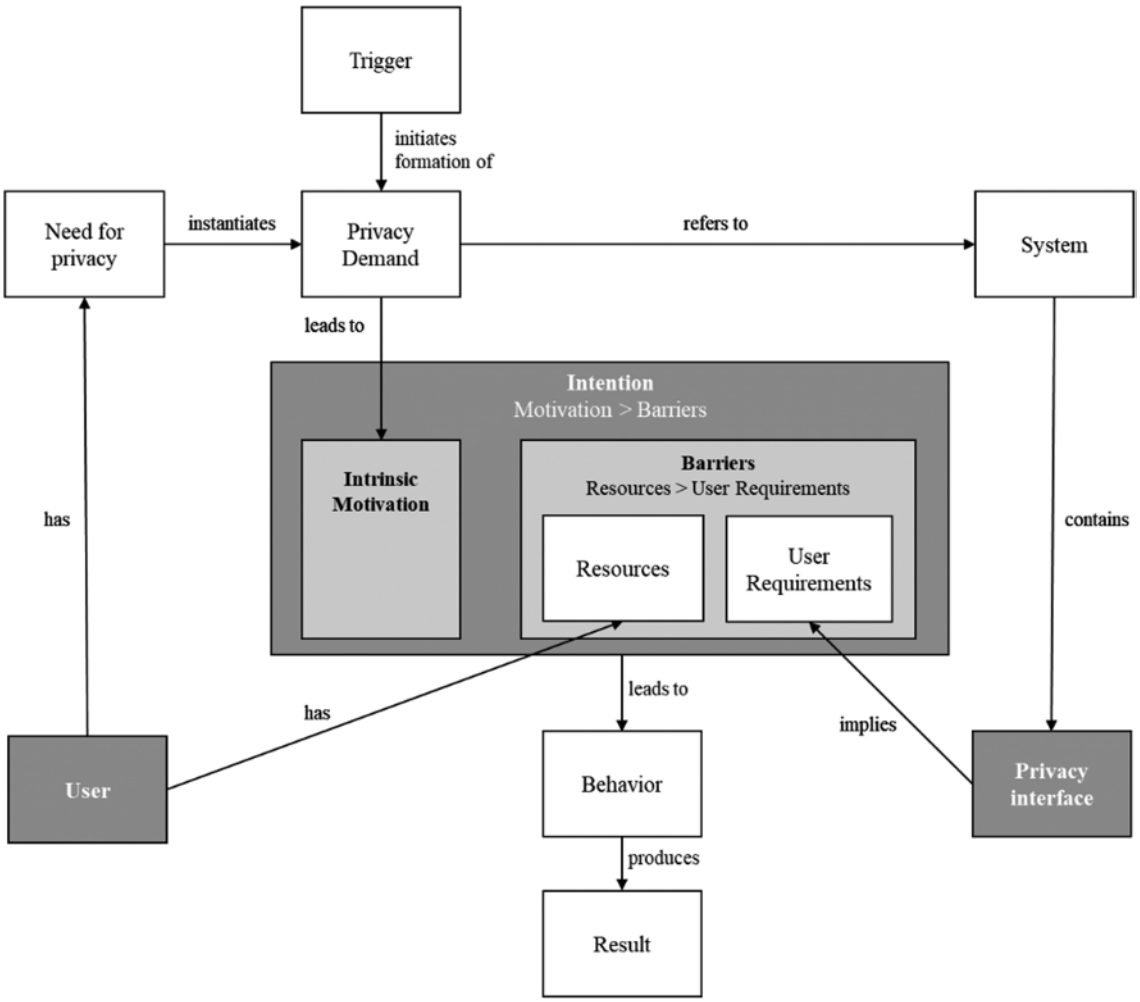


Abbildung 11: Intentionsmodell zur Anwendung von Privatsphäre-Schnittstellen [144, S. 592]

In einer anderen (verdeckten) Feldstudie untersuchten Herrmann und Lindemann in *„Obtaining personal data and asking for erasure: Do app vendors and website owners honour your privacy rights?“* (2016), ob die Rechte auf Zugang und Löschung von Daten in der Praxis ausgeübt werden können. Dazu wurde das Verhalten der Anbieter von 150 in Deutschland beliebten Smartphone-Apps und 120 Webseiten untersucht. Die Lösch-Aufforderungen wurden in 52–57% der Fälle erfüllt und weniger als die Hälfte der Anfragen zur Daten-Bereitstellung wurden zufriedenstellend beantwortet. Etwa 20% der Website-Betreiber hätten persönliche Daten auch an Betrüger weitergegeben [85, S. 1-11].

In der Arbeit *„PrivacyScore: Improving Privacy and Security via Crowd-Sourced Benchmarks of Websites“* (2017) stellen Maass et al. ein Portal zum Scannen von Webseiten vor, mit dem Sicherheits- und Datenschutzfunktionen überprüft und verglichen werden können. Ziel des Projekts ist es, durch die Transparenz, die sich aus den veröffentlichten Bewertungen ergibt, einen Anreiz für Eigentümer zu schaffen, ihre Webseiten zu verbessern. Viele Webseiten bieten heutzutage nur unzureichende Sicherheit und Privatsphäre, da Sicherheitsmaßnahmen ständig an neue Bedrohungen angepasst und Privatsphäre-Schutz bei Gestaltung und Betrieb berücksichtigt werden müssen. Vielen Betreibern fehlt ein Anreiz die dadurch entstehenden Mehrkosten zu tragen. Manchmal stehen Datenschutzmaßnahmen sogar im Widerspruch zu ihrem Geschäftsmodell [119, S. 1-13].

Es lässt sich zusammenfassen, dass die Umsetzung von anwendbarem Datenschutz und Selbstdatenschutz an vielen Stellen noch nicht richtig funktioniert. In vielen Fällen werden der Schutz von Privatsphäre vernachlässigt und Datenschutzrichtlinien ignoriert. Dies kann zum Teil mithilfe des Privacy-Paradox erklärt werden (siehe „Das Privacy-Paradox“ in Abschnitt 2.2.3), jedoch ergeben sich auch viele Hindernisse durch den Mangel einfacher und verständlicher Datenschutz-Optionen, bzw. sinnvoll gewählter Voreinstellungen zugunsten der Nutzer (siehe „Privatheit als Standard und Voreinstellung“ in Abschnitt 2.4.4). Die Anwendung von Datenschutzrechten (wie z.B. das Recht auf Zugang und Löschung von Daten) funktioniert bislang nur teilweise und die Notwendigkeit von Webseiten-Analysetools wie PrivacyScore macht deutlich, dass viele Dienste und Webseiten nur unzureichende Funktionen für Sicherheit und Privatheit implementieren.

3.4 Usability und Usable Privacy

Nachdem bereits Arbeiten aus den Bereichen Tracking, IoT und Datenschutz vorgestellt wurden, wird im Folgenden auf einige Betrachtungen zum Thema Usability eingegangen. Dies ist notwendig, um die Analyse themenverwandter Arbeiten abzuschließen und einen Überblick von bereits durchgeführten Usability-Untersuchungen zu Security- und Privacy-Tools zu bekommen.

3.4.1 Benutzbarkeit von Security- und Privacy-Tools

Von Whitten and Tygar wurde 1999 die Usability des damals aktuellen Email-Verschlüsselungsprogramms *PGP 5.0* untersucht. In dem zugehörigen Paper *„Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0“*, welches in einschlägigen Kreisen große Popularität erlangte, wurde evaluiert, ob Kryptographie-Neulinge mit PGP 5.0 eine effektive Sicherheit bei der Email-Verschlüsselung erreichen können. Die Analyse ergab eine Reihe von Designfehlern im UI, die zu Sicherheitsmängeln beitragen können. Der Nutzertest zeigte, dass die Mehrheit von Testteilnehmern nicht in der Lage war eine Nachricht mit PGP 5.0 zu signieren und zu verschlüsseln. Als Lösungsansatz für zukünftige UIs von Sicherheitssoftware wurde vorgeschlagen, dem Nutzer so schnell wie möglich ein minimales, aber präzises Modell der Sicherheitskonzepte zu vermitteln [174, S. 679 u. 700].

Einige Jahre später (2006) untersuchen Sheng et al. in ihrem Paper *„Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software“* die neuere Version des bereits untersuchten Email-Verschlüsselungsprogramms: *PGP 9*. Obwohl wichtige Fortschritte bei der automatischen Verschlüsselung von E-Mails gemacht wurden, blieb das Problem des Schlüsselzertifizierungsprozesses bei PGP 9 bestehen. Ebenso fehlten weiterhin Hinweise oder Rückmeldungen für den Anwender. Es wurden konkrete Verbesserungsvorschläge für die gefundenen Usability-Probleme aufgelistet, wie z.B. eine deutlich erkennbare Schlüsselverwaltung und bessere Feedback-Mechanismen [156, S. 1 u. 4].

Da zehn Jahre später (2016) der Nachfolger von PGP (*PGP Desktop*) nicht mehr weiter entwickelt wurde[44], untersuchten Ruoti et al. in *„Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client“* den modernen, web-basierten PGP-

44 Die PGP Corporation wurde 2010 von Symantec übernommen und 2019 von Broadcom Inc. gekauft

Client *Mailvelope*[45] (siehe *Secure Messaging Scorecard* bei „Chats, Emails und Telefonie verschlüsseln“ in Abschnitt 4.2.2). Die Ergebnisse zeigten, dass mehr als anderthalb Jahrzehnte nach der ursprünglichen Studie *„Why Johnny Can't Encrypt“* moderne PGP-Tools für die Masse immer noch unbrauchbar sind [145, S. 1].

Im Bereich Privacy-Tools wurde von Cranor et al. im Jahr 2006 in *„User interfaces for privacy agents“* die Benutzbarkeit des P3P-Benutzeragenten *Privacy Bird* untersucht. Das Ziel war die Herausforderungen bei der Entwicklung von Benutzeroberflächen für P3P-Benutzeragenten zu verstehen und Empfehlungen für Designer von Datenschutz-Tools zu entwickeln. Die Auswertung der Nutzerstudie mit zwölf Teilnehmern zeigte, dass Nutzer kurze Zusammenfassungen von Datenschutzinformationen schätzen, solange sie kritische Informationen nicht verbergen. Da ein Großteil der Nutzer nicht mit der von Datenschutzexperten verwendeten Terminologie vertraut sind, wurde die Verwendung von aussagekräftigen Ausdrücken als wichtig bewertet. Zusätzlich wurden die Zusammenfassung von Datenschutz-Informationen und eine Reduktion deren Granularität als Empfehlung für zukünftige Datenschutz-Werkzeuge identifiziert. Dies soll Nutzern dabei helfen die übermittelten Informationen besser zu verstehen und es ihnen ermöglichen, Konfigurationsentscheidungen leichter zu treffen [35, S. 135 u. 172-173].

Leon et al. untersuchten 2012 in der Arbeit *„Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising“* die Leistung populärer Werbeblocker auf einer großen Anzahl von Nachrichten-Webseiten. Darüber hinaus wurden die Vorteile von Werbeblockern für die Privatsphäre von Nutzern untersucht sowie die Mechanismen, welche von Websites eingesetzt werden, um ihnen entgegenzuwirken [111, S. 589]. Bei den evaluierten Tools, darunter auch *AdBlock Plus* und *Ghostery*[46], wurden schwerwiegende Usability-Mängel festgestellt. Es zeigt, dass der Status quo von 2012 nicht ausreichte, um Nutzer in die Lage zu versetzen, ihre Privatsphäre ausreichend zu schützen. Neben dem Mangel an Benutzerfreundlichkeit von ABT und TPT fehlte es Nutzern auch an ausreichenden Kenntnissen über Tracking-Technologien, um die vorhandenen Datenschutzinstrumente effektiv einsetzen zu können [111, S. 598].

Eine der jüngsten Untersuchungen zur Usability von Privacy-Tools wurde von Hubert et al. mit der Arbeit *„Usability von Browsererweiterungen zum Schutz vor Tracking“* (2020) durchgeführt. Mithilfe von Nutzertests wurde die Gebrauchstauglichkeit der vier bekannten Browser Add-ons AdBlock Plus, *uBlock Origin*, Ghostery und *Privacy Badger*[47] überprüft. Die Ergebnisse zeigten, dass Browsererweiterungen zum Schutz vor Tracking auch heutzutage noch eine Vielzahl an Usability-Mängeln aufweisen. Die Bewertung der Usability war sehr durchwachsen und bewegte sich eher in einem niedrigen bis mittleren Bereich. Gerade mal ein Werkzeug konnte mit einer Erfolgsrate von ca. 90% ein gutes Ergebniss erzielen. Als Kernprobleme, welche sich weitestgehend mit den Erkenntnissen von Leon et al. (2012) decken, wurden insbesondere mangelnde Verständlichkeit sowie fehlende Führung und Unterstützung von Nutzern identifiziert [91, S. 95-97 u. 104].

45 Mailvelope (mailvelope.com)
46 Adblock Plus (adblockplus.org), Ghostery (ghostery.com)
47 uBlock Origin (github.com/gorhill/uBlock), Privacy Badger (privacybadger.org)

Die vorgestellten Arbeiten und deren zeitlicher Verlauf machen deutlich, dass die zugrunde liegenden Konzepte von unbedarften Anwendern nicht verstanden und von Software-Herstellern nicht klar kommuniziert werden. Es sind integrierte Tutorials mit Schritt-für-Schritt-Anleitungen und zugängliche Beschreibungen der zugrunde liegenden Technologien notwendig. Zusätzlich werden aussagekräftige Feedback-Mechanismen und eine angemessene Reduktion auf die wesentlichen Inhalte benötigt (wie von Ruoti et al. [145, S. 4] und Cranor et al. [35, S. 172] vorgeschlagen). Nur dann sind Nutzer in der Lage, Sicherheits-Maßnahmen wie Email-Verschlüsselung zu ergreifen, oder ihre Privatsphäre mit TPT zu schützen, um Selbstdatenschutz effektiv anwenden zu können (siehe „Chats, Emails und Telefonie verschlüsseln“ und „Verwenden von Blocker-Software“ in Abschnitt 4.2.2).

3.4.2 Mentale Modelle von Nutzern

Da die Kunst der intuitiven Benutzbarkeit darin liegt „das mentale Modell der Benutzer zu verstehen und eine Informationsarchitektur und ein Interaktionsdesign zu entwickeln, die möglichst gut auf das mentale Modell abgestimmt sind“ [129, S. 112], wird im Folgenden auf Arbeiten über mentale Modelle von Nutzern zu Sicherheit und Privatheit eingegangen.

Raja et al. untersuchten 2009 in *„Revealing Hidden Context: Improving Mental Models of Personal Firewall Users“* die mentalen Modelle von Nutzern der Windows Vista Firewall (WVF). Es wurden Änderungen an den mentalen Modellen und dem Verständnis der Firewall-Einstellungen untersucht, nachdem Nutzer mit der WVF und einem modifizierten Prototyp gearbeitet hatten. Der Prototyp wurde so konzipiert, dass er die Entwicklung eines kontextuell vollständigeren mentalen Modells unterstützt, indem Informationen zum Netzwerkstandort und zur Verbindung mit einbezogen wurden [141, S. 1].

Der Prototyp half den Teilnehmern, ein korrektes und kontextbezogenes mentales Modell der Firewall zu entwickeln. Er verbesserte das Verständnis über die Auswirkungen der Firewall-Konfiguration deutlich. Nach der Verwendung des kontextuell erweiterten Prototyps gab es bei keinem der Nutzer gefährliche Missverständnisse über den Sicherheitszustand mehr. Obwohl das Ausblenden von Systemfunktionen und Anwendungsdetails die Usability von UIs verbessern kann, muss im Falle von Sicherheitssoftware die Komplexität gegen die Sicherheit abgewogen werden [141, S. 11].

Einige Jahre später wurde von Kang et al. untersucht, wie sich das Wissen von Nutzern über das Internet auf ihre Entscheidungen in Bezug auf Privatsphäre und Sicherheit auswirkt. In *„‘My Data Just Goes Everywhere:’ User Mental Models of the Internet and Implications for Privacy and Security“* (2015) wurden die mentalen Modelle von Nutzern mit Informatik- oder ähnlich technischem Hintergund im Vergleich zu Nutzern ohne einen derartigen Hintergund untersucht. Das Ergebnis zeigte starke Gegensätze beim Vergleich der mentalen Modellen von Nutzern beider Gruppen [101, S. 39].

Die Mehrheit von Nutzern ohne technischen Hintergrund verfügte über einfache, dienstleistungsorientierte mentale Modelle, während Nutzer mit Informatikausbildung über ein artikuliertes, vielschichtiges Modell des Internets, sowie beteiligte Komponenten und Organisationen verfügten. Sie drückten zusätzlich ein höheres Bewusstsein dafür aus, wer Zugang

zu ihren persönlichen Daten und Kommunikationen haben könnte. Trotz dieser Unterschiede konnte keine direkte Beziehung zwischen dem technischen Hintergrund der Nutzer und den ergriffenen Maßnahmen zum Privatsphäre-Schutz oder für Online-Sicherheit erkannt werden [101, S. 49].

Ein Jahr später wurde von Schaub et al. in *„Watching Them Watching Me: Browser Extensions Impact on User Privacy Awareness and Concern“* (2016) die Auswirkungen von Browser-Erweiterungen auf das Bewusstsein und die Besorgnis über Datenschutz von Nutzern untersucht. In einer Studie mit 24 Teilnehmern wurden die mentalen Modelle von Nutzern vor und nach der Verwendung von drei bekannten TPTs Ghostery, DoNotTrackMe (heute *BLUR*) und *Disconnect*[48] beaobachtet. Nach der Verwendung aller drei Erweiterungen ließ sich zwar bei allen Nutzern eine gesteigerte Sensibilisierung zum Thema Datenschutz nachweisen, jedoch war eine bleibende Verwirrung über viele Aspekte der Datenverfolgung zu beobachten. Bei der Untersuchung wurden zusätzlich Usability-Probleme festgestellt, welche die Wirksamkeit der Erweiterungen behindern [149, S. 1 u. 9-10].

Die aktuelle Untesuchung *„A Usability Evaluation of Privacy Add-ons for Web Browsers“* (2019) von Corner et al. liefert weitere Einblicke in das Bewusstsein von Nutzern über den Online-Datenschutz und ihre Einstellung zu Datenschutz-Add-ons. Bei der Usability-Evaluierung von drei populären Browser-Erweiterungen *DuckDuckGo Privacy Essentials*[49], Ghostery und Privacy Badger ging es neben der Benutzbarkeit insbesondere darum Vertrauen, Besorgnis und Kontrolle von Nutzern zu genannten Add-ons zu untersuchen. Die Auswertung von 30 Teilnehmern zeigte, dass die Menge an Informationen über gefundene Tracker das Vertrauen der Nutzer in das Add-on beeinflusst. Neben einer immer verfügbaren Hilfe-Funktion wurden Schritt-für-Schritt-Anleitungen, eine Suchfunktion für Fragen sowie die Integration eines Glossars mit Begriffen zum Online-Datenschutz als Optimierungen genannt. Zusätzlich wünschten sich Nutzer zur Reduzierung ihrer Besorgnis mehr Information über gefundene Tracker wie z.B. deren Zweck und Herkunft [32, S. 442 u. 457].

Es kann geschlussfolgert werden, dass sowohl Hintergrund als auch Erfahrung von Nutzern über den Umfang ihrer mentalen Modelle entscheiden. Im Bezug auf Sicherheit und Datenschutz ist dies ein entscheidender Faktor, der für das Bewusstsein von Nutzern über Gefahren und Risiken im Umgang mit ihren PD eine große Rolle spielt. Selbst Nutzer mit ausgeprägten mentalen Modellen zeigen allerdings ein Verhalten, das sich mit dem Privacy-Paradox beschreiben lässt (siehe „Das Privacy-Paradox“ in Abschnitt 2.2.3).

Zusätzlich wurde deutlich, dass im Bereich von Sicherheitssoftware die Reduktion von Anwendungsdetails zugunsten der Usability zu gefährlichen Missverständnissen führen kann. Da weniger ausgeprägte mentale Modelle die Ursache für dieses Problem sind, müssen gerade im Bereich von Sicherheit und Privatheit die Punkte Komplexität und Usability mit großer Sorgfalt gegeneinander abgewogen werden. Auch aktuelle Datenschutz-Erweiterungen sorgen durch mangelhafte Kommunikation und fehlende Funktionen noch für eine lückenhafte Entwicklung von mentalen Modellen über Tracking und Datenschutz.

48 BLUR (dnt.abine.com), Disconnect (disconnect.me)
49 DuckDuckGo Privacy Essentials (duckduckgo.com/app)

3.4.3 Usability-Evaluation und Methodik

Als Grundlage für Arbeiten aus dem Themenbereich Usability-Evaluation und Methodik kann das vierte Kapitel aus dem Buch *„Security and Usability: Designing Secure Systems that People Can Use“* (2005) von Cranor und Garfinkel genannt werden. Es geht darin um die Integration von Usability-Design und -Evaluation in den Software- und Hardware-Lebenszyklus von Datenschutz- und Sicherheitslösungen.

Eingangs wird darauf hingewiesen, dass Sicherheit und Privatheit bei der MSI selten die Hauptziele von Nutzern sind. Usability-Probleme bei Sicherheits- und Datenschutzanwendungen verursachen allerdings deutlich schlimmere Auswirkungen für Nutzer als bei Systemen anderer Art. Zusätzlich wird betont, dass die Nutzergruppe „Endwanwender“ praktisch aus jeder Bevölkerungsschicht stammen kann und die Funktionalität eines Systems den Fähigkeiten jeder einzelnen Person und ihrer individuellen Rolle gerecht werden muss. Anschließend werden Konzeption, Umsetzung und abschließende Evaluation als relevante Anwendungsbereiche bei der Entwicklung von Software und Hardware aufgezählt. Für jeden Bereich werden konkrete Methoden vorgestellt und Vorteile genannt, die eine Anwendung im jeweiligen Entwicklungsabschnitt mit sich bringt [34, S. 401-406].

Die Arbeit *„Auswahl einer geeigneten Methode zur Usability Evaluation“* (2008) von Philipp Jordan beschäftigt sich konkret mit der Fragestellung, wie eine passende Methode zur Usability Evaluation gefunden werden kann. Eine initiale Unterteilung in empirische und analytische Kategorien wird anhand der fünf Methoden *Benutzertests*, *Fragebögen*, *GOMS*, *Heuristische Evaluation* und *Cognitive Walkthrough* noch weiter spezifiziert. Anschließend werden konkrete Beispiele für jede Kategorie vorgestellt, bevor eine Bewertung hinsichtlich ihrer praktischen und wissenschaftlichen Relevanz vorgenommen wird. Anhand dieser Bewertung können die Methoden miteinander verglichen und eine geeignete Methode für den benötigten Anwendungsfall ausgesucht werden [100].

Um Einblicke in das vielschichtige Thema der Benutzbarkeit von Sicherheits- und Datenschutzwerkzeugen aus der Sicht von Nutzern zu bekommen, wurden in der Arbeit *„Usability Characteristics of Security and Privacy Tools: The User's Perspective“* (2018) von Topa und Karyda Merkmale der Gebrauchstauglichkeit von Sicherheits- und Datenschutzinstrumenten analysiert. Dabei war vor allem die Rolle von Usability-Merkmalen und die Identifikation kritischer Fragen zu Transparenz, Kontrolle, Zugänglichkeit und Konsistenz von PD relevant. Bei Interviews mit 150 Teilnehmern stellte sich heraus, dass neben Problemen mit dem Verständnis technischer Begriffe, die Nutzer-Präferenzen bei bestimmten Usability-Merkmalen unterschiedlich ausfallen: Obwohl eine zentrale Sammlung und Darstellung von Sicherheitseinstellungen und Statusindikatoren allgemein präferiert wird, sind die Vorlieben bei Darstellung von Hilfe-Optionen und Prozess-Automatisierung unterschiedlich. Die gewünschte Ausprägung von Darstellung und Kontrolle variiert hierbei von „einfach“ bis „detailliert“ [168, S. 231 u. 242-243].

Da sich die meisten Beiträge aus dem Bereich IT-Sicherheit und Datenschutz höchstens mit Evaluationen zur Usability, jedoch nicht mit UX befassen, wird von Weinhardt und Pierre in ihrer Arbeit *„Lessons learned – Conducting a User Experience evaluation of a Trust*

Policy Authoring Tool“ (2019) eine Evaluation der Benutzererfahrung mit einem Autorenwerkzeug für Vertrauensrichtlinien durchgeführt. Für die Durchführung einer UX-Studie in einem Labor wird ein hoch funktionaler Prototypen oder ein fast fertiges System empfohlen. Um valide Ergebnisse darüber zu erhalten, welche Grundbedürfnisse des Menschen sich wie befriedigen lassen, wird die Anwendung der Evaluationsmethode in Kombination mit Leitfaden-Interviews empfohlen. Das Erlebnis der Nutzererfahrung kann z.B. mithilfe des *User Needs Questionaire* (UNeeQ)[50] bewertet werden [172].

Zusammenfassend kann der Usability-Evaluation und Methodik von Sicherheits- und Datenschutzanwendungen eine hohe Wichtigkeit zugesprochen werden, da eine Nichtbeachtung große Risiken und Gefahren für die Nutzer darstellen kann. Des Weiteren lässt sich die Relevanz von Usability für die Zielgruppe der „Endanwender“ festhalten, deren Präferenzen in Bezug auf wichtige Merkmale mit wenigen Abweichungen eindeutig sind. Für die Evaluations-Methodik von Usability und UX gibt es bereits ausreichend vergleichende Literatur, um aus geeigneten Methoden auswählen zu können.

Nach der Vorstellung von Related Work kann abschließend folgendes Zwischenfazit gezogen werden: Mithilfe themenverwandter Arbeiten lässt sich die Annahme untermauern, dass allgegenwärtiges Tracking und Profiling Gefahren für Nutzer birgt. Die Nachbildung entsprechender Maßnahmen mithilfe von Algorithmen und Datensätzen bestätigt diese Annahme. Sie wird belegt durch Studien die das mangelnde Bewusstsein von Nutzern über entsprechende Praktiken nachweisen. Bereits existierende Privatshphäre-Risiken werden durch den vermehrten Einsatz von IoT- und „Smart Home“-Geräten noch verstärkt, da Industrie-Standards für PbD im Bereich vernetzter Hardware bislang fehlen.

Die Existenz guter Konzepte für Datenschutz und dessen Anwendung kann ebenfalls belegt werden, jedoch wird deutlich, dass diese ohne rechtliche Verpflichtung wirkungslos bleiben. Selbst mit entsprechender Gesetzes-Grundlage, bleiben Probleme bei der Implementierung und Anwendung von Datenschutz-Werkzeugen bestehen. Dies ist nicht zuletzt einer oftmals schlechten Usability von Sicherheits- und Datenschutz-Werkzeugen geschuldet, die auch heutzutage noch erhebliche Mängel aufweisen. Zusätzlich sorgen schwache mentale Modelle von Nutzern, deren Etablierung von Entwicklern, Designern und Herstellern nicht ausreichend bedacht wird, für Gefahren und Risiken im Umgang mit PD.

Die Arbeiten zu Tracking, Profiling und Blocking-Erweiterungen können in Abschnitt 4.2 bei der Erstellung des Maßnahmen-Katalogs zum Selbstdatenschutz aufgegriffen werden. Untersuchungen mit Schwerpunkt IoT- und Smart Home sind bei der Überprüfung des Funktionsumfangs von Privacy-Boxen in Abschnitt 5.1 relevant. Für die Definition der Zielgruppe in Abschnitt 5.2 können die Arbeiten über mentale Modelle hilfreich sein. Die Entwicklung der Methodik für die Untersuchung der Benutzbarkeit von Privacy-Boxen in Abschnitt 5.4 kann sich später an Arbeiten über Usability-Evaluation bedienen. Neu erarbeitet werden müssen alle Bereiche zu Privacy-Boxen, da es noch keine themenverwandten Arbeiten zu geben scheint. Dazu gehört neben der Marktübersicht und der repräsentativen Vorauswahl auch die Methodik zur Untersuchung der Usability von Privacy-Boxen.

50 UNeeQ (hci.iao.fraunhofer.de/content/dam/hci/de/documents/UXellence_UserNeedsQuestionnaire.pdf)

4 Selbstdatenschutz mit Privacy-Boxen

Nachdem in den vorherigen Kapiteln die Grundlagen und der aktuelle Forschungsstand betrachtet wurden, folgt zunächst eine Zusammenfassung der Problematik. Durch Aufzeigen möglicher Lösungsdomänen wird der Einsatzbereich konkretisiert, indem Nutzer mithilfe von Privacy-Boxen Selbstdatenschutz umsetzen können. Darauf folgt die Formulierung von Forschungsfragen, bevor im Detail auf Privacy-Boxen eingegangen wird. Nach einer Einführung zu Privacy-Boxen, folgt eine Auflistung konkreter Maßnahmen zum Selbstdatenschutz. Der daraus entstehende Werkzeug-Katalog bildet die Grundlage um den Anwendungsbereich von Selbstdatenschutz mit Privacy-Boxen definieren zu können. Nach einer Markt-Analyse, wird eine repräsentative Auswahl an Geräten ausgesucht, welche für die anstehende Untersuchung bestellt werden kann.

4.1 Problemstellung und Forschungsfragen

Das allgegenwärtige Tracking und Profiling in allen Bereichen des privaten Lebens ermöglicht Datensammlern Eingriffe in die Privatsphäre von Nutzern, wodurch Gefahren wie *Manipulation*, *Diskriminierung* und *Identitätsdiebstahl* entstehen. Aus den oft kontextlosen Nutzerdaten werden verzerrte digitale Abbilder erstellt, die zu Reputationsschäden führen können (siehe „Probleme, Risiken und Gefahren“ in Abschnitt 2.2.3).

Viele Nutzer haben zwar das Bedürfnis nach Schutz vor diesen Eingriffen, jedoch spiegelt sich dieses Verlangen nicht in ihren Handlungen wider (siehe „Das Privacy-Paradox“ in Abschnitt 2.2.3). Dieses Phänomen kann in mangelhaften mentalen Modellen von Nutzern über den Wert ihrer Daten, eingesetzte Tracking-Methoden und mögliche Schutzmaßnahmen seinen Ursprung haben (siehe „Mentale Modelle von Nutzern“ in Abschnitt 3.4.2).

Als zusätzliches Problem zeichnet sich ein Defizit an geeigneten Schutzmaßnahmen für die immer stärkere Etablierung von IoT-Geräten in „Smart Home“-Umgebungen ab (siehe „Sicherheit und Datenschutz bei Smart Homes“ in Abschnitt 3.2.2).

4.1.1 Lösungsdomäne

Als Optionen zur Lösung dieser Problematik wurden in den vorherigen Kapiteln rechtliche, organisatorische und technische Maßnahmen vorgestellt.

Rechtliche Maßnahmen funktionieren jedoch nur mit einer entsprechenden Verpflichtung, wie am Scheitern des P3P-Projekts und den Auswirkungen von DSGVO und ePVO gezeigt werden konnte (siehe „Konzepte für den Datenschutz“ in Abschnitt 3.3.1 und „Aktuelle Gesetzeslage“ in Abschnitt 2.3.1).

Organisatorische Maßnahmen wie Privacy by Design und Privacy by Default müssen von Herstellern, Designern und Entwicklern bereits zu einem frühen Zeitpunkt des Entwicklungsprozesses gewissenhaft umgesetzt werden, damit sie Nutzern einen Vorteil bieten (siehe „Privatheit als Standard und Voreinstellung“ in Abschnitt 2.4.4).

Bei technischen Maßnahmen kann zwischen vier Anwendungsdomänen mit unterschiedlichen Einflussbereichen unterschieden werden:

- Betriebssystem: Windows, macOS, Linux, iOS, Android
- Programm: Desktop-Anwendung, Smartphone-App, Browser-Plugin
- Netzwerk: Firewall, Gateway, Switch
- Uplink: Router, Modem

Die Betriebssystem-Domäne liegt in der Verantwortung der jeweiligen Hersteller. Das betrifft z.B. Unternehmen wie Microsoft, Apple, Google und die *Linux Foundation*[51]. Sie bestimmen, welche technischen Maßnahmen zum Schutz der Privatshphäre für Nutzer in Betriebssysteme implementiert werden. Lediglich bei Linux haben Nutzer, durch den „Open Source"-Code, erweiterte Möglichkeiten der Mitgestaltung.

Die Programm-Domäne hingegen liegt in der Verantwortung der Nutzer. Diese können hier selbst entscheiden, mit welchen Diensten, Apps oder Erweiterungen sie ihre Geräte vor Eingriffen in die Privatsphäre schützen wollen.

Die Netzwerk-Domäne befindet sich ebenfalls in der Hand der Nutzer, da diese im Wirkungsbereich der eigenen Wohnung entscheiden können, ob eine Firewall oder Netzwerk-Komponenten mit ähnlichen Schutzfunktionen eingesetzt werden.

Die Uplink-Domäne (Internet-Anschluss) ist die letzte Instanz auf der Nutzerseite, bei der noch ein selbstständiger Schutz möglich ist. Hier liegt die Entscheidung wieder bei den Herstellern, ob entsprechende Schutz-Maßnahmen in Router und Modems implementiert werden. Nutzer können lediglich durch die Modifikation von Firmware Schutz-Funktionen in geringem Umfang hinzufügen.

Es wird deutlich, dass Nutzern in vielen Bereichen lediglich die bereitgestellten Privacy-Einstellungen des jeweiligen Systems zur Verfügung stehen. Maßnahmen zum eigenständigen Schutz beschränken sich auf die Anwendungs-Domänen *Programm* und *Netzwerk*. Auf Programm-Ebene ist ein Schutz nur mit fragmentierten Lösungen für Einzelgeräte möglich. So gibt es entsprechende Software für PCs oder Apps für Tablets, Smart-Phones und Smart-TVs (siehe „Operative Maßnahmen" in Abschnitt 4.2.2), allerdings ist der Schutz von Wearables und IoT-Geräten bislang schwierig (siehe „Datenschutz im Internet of Things" in Abschnitt 3.2.1). Im Gegensatz dazu bietet die Netzwerk-Domäne die Möglichkeit, eine einheitliche Lösung für alle verbundenen Geräte zu erreichen. Dies wird durch eine Filterung des gesamten Netzwerk-Verkehrs erreicht, entweder mit Firewalls, die vor allem für den Einsatz im professionellen Bereich vorgesehen sind und dementsprechend Know-how erfordern, oder mit Privacy-Boxen, die für den Endverbraucher konzipiert sind.

Somit stellen Privacy-Boxen die vielversprechendste Lösung dar, die Nutzern zum Schutz ihrer Privatsphäre aktuell zur Verfügung steht. Sie versprechen Nutzern ohne viel technisches Know-how alle privaten Geräte vor den eingangs genannten Gefahren zu schützen [173]. In dieser Behauptung liegt die ursprüngliche Motivation für diese Arbeit begründet. Die Untersuchung der Benutzbarkeit von Privacy-Boxen hat zum Ziel, die Validität dieser Aussage zu überprüfen. Aus diesem Grund folgt zunächst die Definition der Forschungsfragen, bevor Privacy-Boxen intensiver betrachtet werden.

51 The Linux Foundation (linuxfoundation.org)

4.1.2 Forschungsfragen

Um der anstehenden Untersuchung von Privacy-Boxen eine möglichst konkrete Richtung zu geben, ist eine präzise Definition des Untersuchungsziels notwendig. Aus diesem Grund wird aus den Erkenntnissen der bisherigen Grundlagen und des aktuellen Forschungsstands zuerst eine generelle Forschungsfrage formuliert, die anschließend noch konkretisiert wird. Diese dient im weiteren Verlauf der Arbeit als Richtlinie für das angestrebte Vorgehen:

(F) *Wie ist die Usability von Privacy-Boxen zu bewerten, wenn Nutzer sich vor ungewollter Verwendung ihrer Daten sowie Eingriffen in die Privatsphäre schützen möchten?*

Die Forschungsfrage zielt darauf ab herauszufinden, ob eine gute Usability bei der Verwendung von Privacy-Boxen dem Nutzer bei der Umsetzung von Selbstdatenschutz hilft. Da diese Forschungsfrage noch zu generisch ist, wird sie im Folgenden durch zwei konkretere Forschungsfragen weiter spezifiziert:

(F1) *Ist es Nutzern möglich, Privacy-Boxen zum Schutz ihrer Daten und Privatsphäre korrekt anzuschließen und einzurichten?*

(F2) *Werden Nutzer bei typischen Anwendungsszenarien zum Selbstdatenschutz durch das User-Interface von Privacy-Boxen entsprechend unterstützt?*

Die genannten Forschungsfragen zielen hauptsächlich auf die Untersuchung der Usability von Privacy-Boxen bei deren Einrichtung (F1) und Verwendung (F2) ab. Bevor die Forschungsfragen jedoch beantwortet werden können, müssen zunächst die wichtigsten Grundlagen zu Privacy-Boxen erarbeitet werden.

4.1.3 Privacy durch Hardware

Für die zentrale Anwendung von Selbstdatenschutz gibt es mit sogenannten *Privacy-Boxen* fertige Hardware-Lösungen für Nutzer auf dem Markt. Technisch versierte Nutzer sind mit „Open Source“-DIY-Projekten auch in der Lage sich Privacy-Boxen selbst zu bauen. Es handelt sich dabei um elektronische Geräte, die in ein bestehendes Netzwerk integriert oder mit denen neue Netzwerke aufgebaut werden können. Der Begriff „Privacy-Box“ wird von *Comidio*, dem Hersteller der *TrutzBox*[52], wie folgt definiert:

> „Eine Privacy-Box ist ein elektronisches Gerät in Form einer Hardware-Software-Kombination, welches maximale Privatheit bei der Nutzung des Internets bietet.“ [148, S. 100]

Eine Privacy-Box fasst verschiedene Funktionen für eine verbesserte Sicherheit und Privatheit von Nutzern in einem Hardware-Produkt zusammen. Diese Schutzfunktionen sind in der Regel auch einzeln in Form von Software erhältlich. Je nach Gerät ist die Abdeckung der implementierten Schutzfunktionen jedoch unterschiedlich. Manche Geräte enthalten nur einen einzigen Schutzmechanismus, wohingegen andere Geräte eine Vielzahl von Funktionen bieten. Da diese sowohl die Bereiche Sicherheit als auch Privatheit betreffen können, werden die Geräte auch als *Security & Privacy-Box* bezeichnet.

52 Comidio GmbH (trutzbox.de/ueber-uns), TrutzBox (trutzbox.de)

Privacy-Boxen können je nach Modell und Funktionsweise unterschiedlich eingesetzt werden: Einige Boxen werden mit Kabel zwischen Router und Endgerät angeschlossen und können so den Verkehr zwischen beiden Geräten überwachen und bei Bedarf filtern. Andere Boxen werden einfach mit Kabel an ein bestehendes Netzwerk angeschlossen – dann ist jedoch eine zusätzliche Konfiguration auf Endgerät oder Router notwendig, um den Verkehr über die Privacy-Box umzuleiten. Eine dritte Möglichkeit besteht darin, das bestehende WLAN-Netz eines Routers zu ersetzen. Dafür wird die Privacy-Box an den Router angeschlossen und erzeugt ein eigenes WLAN-Netzwerk. Alle Endgeräte müssen anschließend das WLAN der Privacy-Box verwenden, um von ihren Schutzfunktionen zu profitieren.

Das Ziel einer Privacy-Box ist die Sicherheit und Privatheit des Nutzers bei möglichst vielen Tätigkeiten im Internet zu ermöglichen und zu schützen. Um überprüfen zu können, ob eine Privacy-Box diese Anforderung erfüllt, muss jedoch zuerst ein Katalog mit Maßnahmen erstellt werden, der Selbstdatenschutz bei Aktivitäten im Internet beschreibt. Anschließend kann bewertet werden, welche Selbstdatenschutz-Maßnahmen sich mithilfe einer Privacy-Box realisieren lassen. Aus diesem Grund erfolgt zunächst die Vorstellung konkreter Maßnahmen, mit denen Selbstdatenschutz umgesetzt werden kann.

4.2 Werkzeuge zum Selbstdatenschutz

Die folgende Übersicht an Werkzeugen zum Selbstdatenschutz fasst wichtige Maßnahmen zusammen, mit denen Nutzer ihre Privatsphäre bei Aktivitäten im Internet schützen können. Die Sammlung basiert unter anderem auf den zehn Schritten aus „Digitale Selbstverteidigung für Eilige“ von *selbstdatenschutz.info* und den 50 Schritten aus dem Kapitel „Fünf Verteidigungsstufen“ von Steffan Heuer. Es werden relevante Maßnahmen vorgestellt und anhand der Kategorien der *Sieben V der digitalen Selbstverteidigung* zusammengefasst und sortiert [121], [87, S. 228-229]:

I) Präventive Maßnahmen

a) Vorbereiten: Bewusstsein schaffen

1) Bewusstsein für den Wert von PD
2) Kenntnis über die Verwendung von Daten
3) Erkennen von Schwachstellen und Gefahren

b) Vorbeugen: Einsatz proaktiver Maßnahmen

4) Erstellen und Verwenden sicherer Passwörter
5) Datenschutzkritische Dienste vermeiden
6) Selbstreflexion vor dem Teilen von Inhalten

II) Operative Maßnahmen

c) Verweigern: Tracking erschweren

7) Verwenden von Blocker-Software
8) Device-Fingerprinting verhindern
9) Löschen von Sessions und Cookies

d) Verschleiern: Datenspuren verwischen
   10) Einsatz von Pseudonymen im Web
   11) Sichere DNS und VPN-Dienste nutzen
   12) Nutzung verschiedener Browser

e) Verschlüsseln: Private Informationen schützen
   13) Transport-Verschlüsselung verwenden
   14) Chats, Emails und Telefonie verschlüsseln
   15) Verschlüsseln von Daten und Datenträgern

III) Reaktive und Notfall-Maßnahmen

f) Verbannen: Einsatz reaktiver Maßnahmen
   16) Umstieg auf datenschutzfreundliche Dienste
   17) Social-Media säubern und digitaler Selbstmord
   18) Technologien vermeiden und abschalten

g) Vermindern: Schaden begrenzen
   19) Das Recht auf Vergessenwerden nutzen
   20) Reputationsmanagement anwenden

Mithilfe dieser Übersicht von Selbstdatenschutz-Werkzeugen werden in den nächsten Abschnitten die Maßnahmen anhand konkreter Beispiele vorgestellt. Der daraus entstehende Werkzeug-Katalog bildet die Grundlage, auf der anschließend entschieden werden kann, welche Maßnahmen mithilfe von Privacy-Boxen realisierbar sind und welche nicht.

4.2.1 Präventive Maßnahmen

Zu den präventiven Maßnahmen gehören *Vorbereiten* und *Vorbeugen*. Es geht darum, zuerst ein Bewusstsein für das Thema Datenschutz zu entwickeln. Mithilfe des Werts von Nutzerdaten können die damit verbundenen Schwachstellen und Gefahren erkannt werden, um daraufhin proaktive Maßnahmen für deren Schutz zu ergreifen.

Bewusstsein für den Wert von PD (Werkzeug 1)
Um ein Bewusstsein für den Wert von Personenbezogene Daten (PD) zu entwickeln, kann neben Studien und Insider-Informationen (siehe „Der Wert des Nutzers“ in Abschnitt 2.2.3), der „Data Calculator“ der Webseite *datum.org*[53] verwendet werden. Wie in Abb. 12 zu sehen ist, lässt sich der individuelle Wert von Daten eines Nutzers anhand einer Vielzahl von Parametern[54] bestimmen. Es gehören die Angabe von genutzten digitalen Diensten, das Teilen von Daten mit Orts- und Gesundheitsbezug, sowie der Grad der Anonymisierung zu den berücksichtigten Parametern. Durch Auswahl aller Dienste können hier je nach Anonymisierung-Grad Werte zwischen 680 und 2.000 US-Dollar für die Daten eines Nutzers erreicht werden.

53 Data Calculator (calc.datum.org)
54 Die Berechnung basiert auf ARPUs der gewählten Dienste oder branchenbasierten Näherungen [71]

Abbildung 12: Der *Data Calculator* bei maximaler Datenpreisgabe

Dieses Werkzeug kann nur bedingt von einer Privacy-Box realisiert werden. Bei der Einrichtung des Geräts wäre es zwar denkbar dem Nutzer Hinweise zur Sensibilisierung für den Wert von PD anzuzeigen, jedoch fehlt im alltäglichen Gebrauch ein Informations-Kanal. Auch für andere Nutzer des geschützten Netzwerks müsste auf ein zusätzliches Display z.B. mittels App o.Ä. zurückgegriffen werden.

Kenntnis über die Verwendung von Daten (Werkzeug 2)
Um herauszufinden, welche persönlichen Nutzerdaten erhoben und gespeichert werden, kann z.B. mithilfe des „Präferenzmanagements“ der Webseite *YourOnlineChoices.eu*[55] ermittelt werden, welche Anbieter mit Website-Betreibern zusammenarbeiten, um Nutzungsdaten zum Zwecke nutzungsbasierter Online Werbung (OBA) zu erheben [52]. Eine andere Option sind Datenschutz-Richtlinien[56] großer Unternehmen wie Google und Facebook, in denen aufgezeigt wird, welche Daten erfasst werden und zu welchen Zweck. Als dritte Möglichkeit bietet die Kategorie „Datenspuren und Datenschmutz“ der Webseite *selbstdatenschutz.info*[57] eine gute Übersicht darüber, welche Daten im alltäglichen Leben erfasst und gespeichert werden.

Auch dieses Werkzeug ist vor allem informationeller Natur und unterliegt damit ähnlichen Schwierigkeiten wie Werkzeug 1. Wenn eine Privacy-Box jedoch über einen zusätzlichen Feedback-Kanal verfügt, könnte dem Nutzer immer, wenn PD abgefragt oder verwendet werden, ein Hinweis angezeigt werden. Dies würde mit der Zeit für eine Sensibilisierung über die Verwendung von Nutzerdaten sorgen.

Erkennen von Schwachstellen und Gefahren (Werkzeug 3)
Beim Erkennen möglicher Schwachstellen und Gefahren kann zwischen persönlichen Risiken und denen von Systemen, Produkten oder Anwendungen unterschieden werden. Ersteres betrifft die persönliche Wahrnehmung von Sicherheit und Privatheit, sowie den Umgang

55 Präferenzmanagement (youronlinechoices.com/de/praferenzmanagement)
56 Google-Datentransparenz (safety.google/privacy), Facebook-Datenrichtlinie (facebook.com/policy)
57 Datenspuren und Datenschmutz (selbstdatenschutz.info/datenspuren)

mit den eigenen Daten; zweiteres den Umgang mit persönlichen Daten von Dritten. In beiden Fällen muss sich der Nutzer informieren: Zum einen darüber, in welchen Bereichen des Lebens Gefahren durch Datenpreisgabe entstehen können (z.B. durch Phishing, Malware oder Kostenfallen) und zum anderen über mögliche Schwachstellen in Systemen, Produkten oder Anwendungen (z.B. durch Hacks oder Datendiebstähle).

Das BSI stellt hierfür die Seite *BSI für Bürger*[58] bereit, auf der sowohl für private Themen rund um IT-Sicherheit sensibilisiert, als auch über öffentliche Sicherheitshinweise informiert wird. Eine andere Möglichkeit bietet die Webseite *HaveIbeenPwned.com*[59], welche neben Informationen über aktuelle Daten-Leaks auch eine Überprüfung anbietet, ob Email-Adressen davon betroffen sind. So lässt sich z.B. die Gefahr der Kompromittierung (unberechtigtes Eindringen Dritter) eines Nutzer-Kontos herausfinden, falls die Email-Adresse in einem der gestohlenen Datensätze auftaucht.

Wie auch die beiden Werkzeuge zuvor, basiert dieses Werkzeug auf der Aneignung von Wissen und Erfahrung durch den Konsum von Information. Auch hier ist eine Privacy-Box auf einen zusätzlichen Feedback-Kanal angewiesen, der z.B. mit aktuellen Nachrichten zu Daten- und Sicherheitspannen, oder über aktuelle Gefahren vor Phishing-Angriffen und Malware den Nutzer sensibilisiert.

Erstellen und Verwenden sicherer Passwörter (Werkzeug 4)
Zum Vorbeugen von Schwachstellen und Gefahren gehört das Ergreifen entsprechender proaktiver Maßnahmen, allem voran die Nutzung von sicheren Passwörtern und deren regelmäßige Änderung. Zum einen geht es darum, keine einfachen Passwörter wie „123456“ oder „qwert“[60] zu verwenden, zum anderen darum, das gleiche Passwort nicht bei mehreren Diensten zu nutzen. Simple, mehrfach genutzte Passwörter lassen sich leicht erraten, was zu einer Kompromittierung von mehreren Diensten gleichzeitig führen kann.

Aus diesem Grund gibt es Vorgaben für das Erstellen sicherer Passwörter, wie z.B. Mindestlänge und Verwendung aller verfügbaren Zeichen, die vom BSI herausgegeben werden. Da sich Passwörter, welche diese Kriterien erfüllen, nicht mehr gut merken lassen, werden Hilfsstrategien benötigt. Dies kann z.B. ein Merksatz sein, der Hinweise auf die verwendeten Zeichen gibt, oder die Nutzung eines Passwort-Managers[61]. Dieser speichert alle Passwörter sicher ab, wodurch man sich nur noch ein einziges (sicheres) Master-Passwort merken muss, um den Zugriff auf die gespeicherten Passwörter freizuschalten.

Eine Privacy-Box kann durchaus einen Dienst als lokaler Passwort-Manager bereitstellen. Anstatt sensible Passwörter Drittanbietern anzuvertrauen, können diese auch sicher auf der Privacy-Box im Heimnetz des Nutzers verwaltet und gespeichert werden. Damit dies für den Nutzer jedoch zufriedenstellend funktioniert müssen (wie schon bei den Werkzeugen zuvor) zusätzliche Services bereitgestellt werden: Dazu gehört neben Browser-Erweiterungen und Apps für Computer und Smartphones auch die Möglichkeit, sicher von überall aus der Welt auf die Privacy-Box zugreifen zu können.

58 BSI für Bürger – Ins Internet mit Sicherheit (bsi-fuer-buerger.de/BSIFB/DE/Home)
59 Have I been pwned? (haveibeenpwned.com)
60 Passwörter wie ‘123456’ und ‘qwert’ zählen immer noch zu den häufigsten Kombinationen [22]
61 Bekannte Passwort-Manager sind z.B. 1Password (1password.com) oder LastPass (lastpass.com)

Datenschutzkritische Dienste vermeiden (Werkzeug 5)
Eine weitere proaktive Maßnahme ist die Vermeidung von Diensten mit kritischen Datenschutzpraktiken wie Google, Facebook und Co. Dies hilft bereits im Vorfeld dabei, weniger persönliche Daten preiszugeben. Um die Datenschutz-Richtlinien eines Dienstes kritisch zu beleuchten, kann mit einem Blick auf den Firmensitz begonnen werden. Dienste, welche in einem Land beheimatet sind, das Mitglied der „Five Eyes“[62] ist, oder wo ein „Schlüssel-Offenlegungs-Gesetz“[63] existiert, können die Geheimhaltung von Daten schon per Gesetz nicht gewährleisten. Welche Mitgliedsstaaten ein Abkommen über Datenaustausch oder Gesetze über die Ausgabe von Sicherheits-Schlüsseln haben, kann auf der Webseite *privacytools.io*[64] unter dem Punkt „Providers“ nachgeschlagen werden.

Digitale Sprachassistenten wie *Google Assistant*, *Siri* oder *Alexa*[65], die sich mit Befehlen wie „OK Google“, „Hey Siri“ oder „Alexa“ aktivieren lassen, müssen, um auf diese Sprachbefehle reagieren zu können, dauerhaft mit aktiviertem Mikrofon zuhören. Durch unzureichende Aufklärung von Seiten der Hersteller wissen Kunden nicht genau, was mit diesen Sprachaufnahmen geschieht. Datenpannen der letzten Jahre belegen, dass Aufnahmen nicht nur nach einem Sprachbefehl versendet werden [92]. Auch wenn Amazon, Google und Apple diese Daten seit einem Jahr nicht mehr von Menschen auswerten lassen, ist es empfehlenswert, die Dienste zu meiden, oder die Nutzung auf proaktive Aktivierung umzustellen (z.B. per Tastendruck) [93].

Bei der Vermeidung von datenschutzkritischen Diensten kann eine Privacy-Box nur bedingt helfen. Zum einen ist wieder eine Sensibilisierung über Datenschutzpraktiken von genutzten Diensten denkbar, jedoch taucht auch hier das Problem des Feedback-Kanals wieder auf. Zum anderen können ungewollte Anfragen von IoT- und „Smart Home“-Geräten zwar blockiert werden, jedoch lässt sich für die Privacy-Box nur schwer feststellen, welche Anfragen während der Nutzung und welche vielleicht im Standby abgeschickt werden. Eine visuell aufbereitete Übersicht vergangener Anfragen wäre denkbar, die vom Nutzer anschließend interpretiert werden kann.

Selbstreflexion vor dem Teilen von Inhalten (Werkzeug 6)
Die letzte proaktive Maßnahme ist die persönliche Reflexion vor dem Teilen von Inhalten auf Sozialen Netzwerken, Blogs oder Webseiten. Der Tipp von Steffan Heuer: „Erst denken, dann posten. Erst denken, dann hosten.“ trifft diese Maßnahme im Kern [87, S. 19]. Gewisse Dinge sollten privat bleiben, daher muss abgewogen werden, ob z.B. Dokumente wie Bank- und Kreditkarten oder Personalausweis im Internet landen sollen. Ebenfalls ist es ratsam, mit privaten Informationen über Geburtstage, Urlaubspläne und Adressen von Wohnort, Bildungseinrichtungen und Arbeitgebern sparsam umzugehen. Auch Kommentare zum Umgang mit Alkohol und Drogen, über politische und religiöse Ausrichtung oder riskante Hobbys sollten besser Privatsache bleiben [87, S. 233-234]. Die Seite *ThinkBeforeSocial*[66] kann als Hilfe bei solchen Entscheidungen herangezogen werden.

62 Abkommen zwischen UK, USA, Australien, Canada und Neuseeland (UKUSA) zum Datenaustausch
63 Das „Schlüssel-Offenlegungs-Gesetz“ (engl. Key Disclosure Law) verlangt von Nutzern Sicherheitsschlüssel an Strafverfolgungsbehörden zu übergeben, zur Durchführung von strafrechtlichen Ermittlungen
64 PrivacyTools – Providers (privacytools.io/providers)
65 Google Assistant (assistant.google.com), Siri (apple.com/siri), Amazon Alexa (alexa.amazon.de)
66 Think Before Social (ais.co.th/thinkbeforesocial/en)

Bei der persönlichen Reflexion vor der Veröffentlichung privater Inhalte hat eine Privacy-Box nur wenig Mitspracherecht. Sie könnte zwar feststellen, wenn Inhalte von Nutzern auf sozialen Medien geteilt werden, jedoch müsste sie diese zunächst verstehen und dann hinsichtlich ihrer Relevanz auf mögliche Gefahren bewerten.

4.2.2 Operative Maßnahmen

Der Einsatz von operativen (aktiven) Maßnahmen beginnt damit, Trackern und Datensammlern die Arbeit durch Datenverweigerung zu erschweren. Durch das Verwischen digitaler Datenspuren kann dieser Prozess zusätzlich noch gesteigert werden. Das höchste Maß kann durch den Einsatz von Verschlüsselungs-Maßnahmen erreicht werden, was die Sammlung und Auswertung von Daten unverhältnismäßig erschwert.

Verwenden von Blocker-Software (Werkzeug 7)
Blocker-Werkzeuge können in drei Bereiche unterteilt werden: Werbung, Skripte und Tracking. Die Anwendungen sind hauptsächlich als Browser-Erweiterungen verfügbar, meist für *Chrome* und Firefox, oft für *Opera* und manchmal für Safari und *Edge*[67]. Es gibt mittlerweile auch Varianten, die als mobile Apps für Smartphones zur Verfügung stehen.

Ad Blocking Tools (ABT) sind Anwendungen zum Blockieren von Werbung, welche auf Basis von Filter-Listen entscheiden, welche Werbung angezeigt und welche blockiert wird. Die wohl bekanntesten Beispiele für derartige Anwendungen sind Adblock Plus und uBlock Origin für Blocker bzw. *EasyList* und *EasyPrivacy*[68] für Filter-Listen. Neben den Standard-Filter-Listen gibt es auch Listen mit unterschiedlichem Fokus: für mehr Privacy, gegen das Speichern von Cookies oder das Anzeigen von Social Media Widgets. Hierbei gibt es nicht nur „Black-“ sondern auch „White-Listen“, anhand derer sogenannte *Acceptable Ads*[68], also unschädliche, „qualitativ hochwertige“ Werbung, weiterhin dargestellt werden kann.

Skript-Blocker hingegen deaktivieren ausführbaren Code (meistens JavaScript), der beim Aufruf einer Webseite geladen wird. Je nach Anwendung und Einstellung wird somit entweder die Ausführung aller Skripte verhindert, oder mithilfe von Filter-Listen und Nutzer-Einstellungen individuell entschieden. Eine gewisse Granularität ist hierbei oft notwendig, da viele Seiten ohne die Ausführung von Skripten nicht mehr richtig funktionieren. Es besteht daher die Aufgabe zwischen Skripten zu unterschieden, die für die Webseite notwendig sind, oder für Tracking genutzt werden. Bekannte Beispiele solcher Anwendungen sind *NoScript*, *ScriptSafe* und *uMatrix*[69].

Das Verhindern von Tracking ist mithilfe von *Tracking Prevention Tools* (TPT) möglich, die Techniken von Ad- und Skript-Blockern kombinieren und erweitern. Sie prüfen beim Laden einer Webseite auf „Drittanbieter“-Domains die Bilder, Skripte und Werbung einbetten. Zusätzlich wird die Webseite auf Tracking-Techniken, wie eindeutig identifizierende Cookies und „Supercookies“, Tracking-Pixel und Browser-Fingerprinting analysiert und diese blockiert. Einige bekannte Beispiele sind Disconnect, Ghostery und Privacy Badger.

67 Google Chrome (google.com/chrome), Opera (opera.com), Microsoft Edge (microsoft.com/edge)
68 EasyList, EasyPrivacy (easylist.to), Acceptable Ads (acceptableads.com)
69 NoScript (noscript.net), ScriptSafe (andryou.com/scriptsafe), uMatrix (github.com/gorhill/uMatrix)

Der Privacy Badger geht sogar noch einen Schritt weiter und „lernt“ schädliche Tracker während der Nutzung zu blockieren. Sobald ein Tracker erkannt und von mehr als drei unterschiedlichen Seiten aufgerufen wurde, wird dieser blockiert[70]. Mithilfe der Webseite *PanoptiClick* von der Electronic Frontier Foundation (EFF) oder dem Anonymitätstest von *JonDonym*[71] lässt sich z.B. testen, ob der genutzte Browser und die installierten Erweiterungen den Nutzer vor Tracking schützen.

Der Einsatz von Blocker-Software mithilfe einer Privacy-Box ist sehr gut möglich und stellt in der Regel eine Kern-Funktionalität dar. In welchem Ausmaß diese jedoch implementiert ist, hängt vom jeweiligen Modell und Hersteller ab.

Device-Fingerprinting verhindern (Werkzeug 8)
Ein weiterer Punkt beim Verweigern von Daten betrifft das Zurücksetzen bzw. Abschalten von Werbe-IDs auf dem Smartphone und das Deaktivieren des eindeutigen Fingerabdrucks von Browsern. Die sogenannte Werbe-ID unter Android bzw. Ad-ID unter iOS lässt sich in den Einstellungen des jeweiligen Betriebssystems zurücksetzen. Zusätzlich gibt es die Möglichkeit, durch das Deaktivieren von personalisierter Werbung (Android) oder das Beschränken des Ad-Trackings (iOS) die Zuweisung einer eindeutigen Werbe-ID auch in Zukunft zu verhindern.

Der eindeutige Fingerabdruck eines Browsers kann mithilfe von Webseiten wie *AmIUnique* oder *UniqueMachine*[72] berechnet und angezeigt werden. Um sich vor Browser-Fingerprinting zu schützen, können mithilfe von Plugins wie *Random User-Agent*[73] die HTTP-Header-Attribute modifiziert oder mithilfe eines Skript-Blockers die JavaScript-Attribute verweigert werden. Es gibt zusätzlich noch eine Reihe von Plugins um Fingerprinting durch *Canvas*, *AudioContext*, *Fonts* oder *WebGL*[74] zu verhindern. Alternativ ist die Nutzung von Privacy-Browsern möglich (Werkzeug 12), die bereits mit Anti-Fingerprinting-Methoden ausgestattet sind [19].

Auch das Erkennen und Verhindern von Fingerprinting lässt sich mit einer Privacy-Box gut realisieren. Durch die geschickte Manipulation von Header-Attributen bei Anfragen der jeweiligen Netzwerkgeräte, können Tracker beim Versuch des Fingerprintings durcheinander gebracht werden.

Löschen von Sessions und Cookies (Werkzeug 9)
Der letzte Schritt beim Erschweren von Tracking ist das Löschen von Cookies und Browser-Sessions. Seit Einführung der DSGVO müssen alle Webseiten eine Zustimmung für die Platzierung von Cookies einholen. Dies geschieht in der Regel mithilfe von Cookie-Bannern oder Consent-Managern. Es ist ratsam, immer nur die notwendigen Cookies zu akzeptieren, auch wenn diese Option oft versteckt oder nicht als Standard vorausgewählt ist. Darüber hinaus sollten Cookies regelmäßig gelöscht werden. Dies geschieht zwar unter Umständen auf Kos-

70 Diese Funktion ist seit dem 07.10.2020 als Standard deaktiviert, da sie Nutzer identifizierbar macht [7]
71 Panopticlick 3.0 (panopticlick.eff.org), JonDonym Anonymitätstest (ip-check.info)
72 Am I Unique (amiunique.org/fp), Unique Machine (uniquemachine.org)
73 Random User-Agent (github.com/tarampampam/random-user-agent)
74 Canvas Fingerprint Defender, Font Fingerprint Defender, AudioContext Fingerprint Defender, WebGL Fingerprint Defender – MyBrowserAddon: Privacy & Security (mybrowseraddon.com/#products)

ten von Komfort, da gespeicherte Logins verloren gehen, aber es erschwert das Tracking mithilfe der UIDs, welche in Third-Party-Cookies gespeichert werden. Viele Browser ermöglichen mittlerweile das automatische Löschen von Cookies, Session und Surf-Historie beim Beenden des Programms.

Privacy-Boxen können zwar bereits gesetzte Cookies in Browsern nicht löschen, jedoch können sie verhindern, dass neue Cookies von Trackern gespeichert werden. Aus diesem Grund ist die Realisierung von Werkzeug 9 mit Privacy-Boxen nur teilweise möglich.

Einsatz von Pseudonymen im Web (Werkzeug 10)
Zu der zusätzlichen Verschleierung von Datenspuren gehört die Verwendung von Pseudonymen im Internet. Unabhängig von Plattform oder Dienst, sollte beim Anlegen eines neuen Profils anstelle des Klarnamens ein fiktiver Name gewählt werden (sofern dies möglich ist). Dabei ist es ratsam gewöhnliche, „langweilige“ Namen zu verwenden – Namen von prominenten Personen oder Figuren können u.U. ungewollte Aufmerksamkeit auf sich ziehen. Bei der Verwendung von mehreren Pseudonymen ist es empfehlenswert, die Zuordnung der entsprechenden Accounts irgendwo abzuspeichern.

Hierfür können z.B. auch Dienste wie Passwort-Manager genutzt werden (Werkzeug 4), um den Überblick nicht zu verlieren [87, S. 234-235]. Für das Registrieren unter Pseudonym gibt es Dienste, die bei der Erstellung fiktiver Email-Adressen oder Telefonnummern helfen. Beispiele dafür sind BLUR und *MySudo*[75], wobei Erstes eine Web-Lösung ist und Zweites als App für Smartphones zur Verfügung steht.

Bei der Verwendung von Pseudonymen im Web sind Privacy-Boxen wenig hilfreich. Auch hier sind höchstens Sensibilisierungsmaßnahmen mit zusätzlichem Feedback-Kanal denkbar oder die Mitbenutzung eines lokalen Passwort-Managers auf der Privacy-Box.

Sichere DNS und VPN-Dienste nutzen (Werkzeug 11)
Beim Surfen im Web wird für jeden Aufruf einer Webseite mithilfe von DNS-Resolvern aus der aufgerufenen URL die zugehörige IP-Adresse des Servers gebildet, um die Verbindung aufbauen zu können. Bei diesem Vorgang lassen sich ebenfalls Informationen über Nutzer sammeln (Logs), um darauf basierend Werbung zu schalten oder auf manipulierte Webseiten umzuleiten. Aus diesem Grund sollten sichere DNS-Anbieter verwendet werden, die verschlüsselte Verbindungen wie *DNS over HTTPS* (DoH) oder *DNS over TLS* (DoT) unterstützen. Beispiele sind *DNSforge* mit Server-Standort in Deutschland oder *1.1.1.1*[76] mit Server-Standort in den USA.

Durch die zusätzliche Verwendung eines VPNs ist es möglich, den Internet-Anschluss (IP-Adresse und Standort) eines Nutzers zu verschleiern. Der VPN-Server fungiert dann als öffentliche Instanz beim Aufruf einer Webseite, stellt IP-Adresse und Standort zur Verfügung und leitet alle Daten an den Nutzer über eine sichere und private Verbindung weiter. Der Einsatz von VPNs ist sowohl bei öffentlichen WLAN-Netzen (Hotels oder öffentliche Gebäude) zum Schutz vor Angriffen sinnvoll als auch zur Anonymisierung im Internet.

75 MySudo (mysudo.com)
76 DNSforge (dnsforge.de), 1.1.1.1 (1.1.1.1)

Es gibt viele VPN-Anbieter, jedoch sollte auf eine strikte „Keine-Logs-Richtlinie“ geachtet werden wie z.B. bei *NordVPN*, *ExpressVPN* und *CyberGhost*[77]. Eine Alternative dazu stellt der Dienst *JonDonym*[78] dar, der mithilfe eines Proxy-Clients den Datenverkehr durch eine Mixkaskade von Servern verschleiert, ähnlich dem Prinzip, das bei TOR[81] Anwendung findet. Zusätzlich wird mit *JonDoFox*[78] noch ein dazu kompatibler Browser für sicheres und anonymes Surfen bereitgestellt.

Die Bereitstellung von VPN- und DNS-Diensten ist mit einer Privacy-Box durchaus möglich und eine häufige Kern-Funktion vieler angebotener Geräte. Die VPN-Funktionen benötigen dabei zusätzliche Dienste, die einen Server-Endpunkt bereitstellen, oder den weltweiten Zugriff auf das Heimnetz ermöglichen.

Nutzung verschiedener Browser (Werkzeug 12)
Eine weitere Verschleierungsmaßnahme lässt sich durch die Nutzung verschiedener Browser realisieren. Hierdurch wird vor allem das bei Werkzeug 8 beschriebene „Tracking durch Browser-Fingerprinting“ durcheinander gebracht. Wenn bestimmte Webseiten kontinuierlich von demselben Browser aus aufgerufen werden, ordnen Tracker den unterschiedlichen Browsern individuelle Profile und damit Identitäten zu. Es stehen dafür die bereits genannten Browser Chrome, Firefox, Opera, Safari oder Edge zur Verfügung, von denen Firefox die besten Datenschutz-Optionen bietet [126].

Es gibt allerdings noch eine Reihe von Alternativ-Browsern, die speziell mit Fokus auf Sicherheit und Privatsphäre entwickelt werden. Populäre Beispiele sind *Brave*, *Waterfox* und *Iridium*[79]. Es handelt sich dabei um Browser auf Chromium- (Brave und Iridium) bzw. Firefox-Basis (Waterfox), die bereits standardmäßig Maßnahmen gegen Werbung und Tracker beinhalten. Der Vorteil dieser Browser besteht darin, dass alle Plugins und Erweiterungen, die für Chrome und Firefox existieren, mit ihnen kompatibel sind.

Weitere Browser-Alternativen wie z.B. *Epic Privacy Browser*, *ungoogled-chromium* oder *Pale Moon*[80] bieten zwar ähnliche Funktionen, sind aber teilweise veraltet, nicht Open Source oder stehen im Zusammenhang mit Sicherheitslücken oder Daten-Leaks. Auch der bekannte *TOR Browser* (bzw. *Onion Browser* für iOS)[81] steht unter dem Verdacht der Kompromittierung und der Kooperation mit der US-Regierung. Jedoch bietet er als Firefox-Variante mit integriertem Multi-Hop-VPN dennoch gute Optionen gegen Überwachung oder Tracking und hilft bei der Anonymisierung [126].

Bei der Verwendung von verschiedenen Browsern bzw. Privacy-Browsern kann eine Privacy-Box nicht viel helfen. Jedoch kann sie als eine Art Meta-Instanz dieses Werkzeugs gesehen werden, da sie die Privatheit jedes genutzten Browsers verbessert. Außerdem kann sie mit Änderungen der User-Agent-Attribute in Anfrage-Headern die Nutzung unterschiedlicher Browser simulieren.

77 NordVPN (nordvpn.com), ExpressVPN (expressvpn.com), CyberGhost (cyberghostvpn.com)
78 JonDonym (anonym-surfen.de), JonDoFox (anonym-surfen.de/jondofox)
79 Brave Browser (brave.com), Waterfox Browser (waterfox.net), Iridium Browser (iridiumbrowser.de)
80 Epic Privacy Browser (epicbrowser.com), ungoogled-chromium (github.com/Eloston/ungoogled-chromium), Pale Moon Browser (palemoon.org)
81 TOR Browser (torproject.org), Onion Browser (onionbrowser.com)

Transport-Verschlüsselung verwenden (Werkzeug 13)
Bei Verwendung und Einhaltung der Transportverschlüsselung geht es nicht um die Verschlüsselung der Information selbst, sondern um die Verschlüsselung des Transport-Protokolls. Beim Browsen im Internet betrifft es das Protokoll HTTP, beim Versenden von Emails POP3, IMAP und SMTP und beim Datentransfer FTP. Es gibt für jedes dieser Protokolle eine Variante, die Verschlüsselungs-Methoden nutzt. Dies wird durch ein zusätzliches „S“ in der Bezeichnung erkennbar, das für *Secure* steht. Diese Maßnahme sorgt dafür, dass Informationen während des Transports nicht mitgelesen werden können.

Beim Surfen im Internet sollte darauf geachtet werden, dass der Browser ein Schloss neben der URL anzeigt, ein Hinweis dafür dass die Verbindung mit der sicheren Protokoll-Variante HTTPS hergestellt wurde. Das Browser-Plugin *HTTPS Everywhere*[82] von der EFF kann dieses Verhalten z.B. erzwingen (wenn möglich). Beim Einrichten von Email-Clients wie *Apple Mail*, *Outlook*, oder *Thunderbird*[83] ist es empfehlenswert, die sicheren Protokoll-Varianten bei der Konfiguration eines Email-Anbieters zu verwenden. Dies lässt sich mithilfe der richtigen Ports sicherstellen: Port 995 gilt für POP3S, Port 993 für IMAPS und die Ports 465/587 gelten für SMTPS. Bei der Einrichtung eines FTP-Clients sollte entweder FTPS (nutzt SSL/TLS) oder SFTP (basiert auf SSH) als Protokoll verwendet werden.

Die Nutzung von Transport-Verschlüsselung kann mit einer Privacy-Box teilweise forciert und verbessert werden. Sie ist z.B. in der Lage unsichere Anfragen auf eine sichere Verbindung umzuleiten (HTTPS-Upgrade) oder Anfragen an unsichere Adressen zu unterbinden.

Chats, Emails und Telefonie verschlüsseln (Werkzeug 14)
Wenn der sichere Transport gewährleistet ist, folgt als nächster Schritt die Verschlüsselung des Inhalts. Dies stellt sicher, dass Inhalte nur vom Empfänger und nicht von Dritten gelesen werden können. Wenn jeweils nur die Kommunikationspartner am Ende der Verbindung die Information entschlüsseln können, wird von Ende-zu-Ende-Verschlüsselung gesprochen.

Bei der Verschlüsselung des Inhalts geht es konkret um den Schutz von Kommunikation, die zwischen zwei oder mehr Teilnehmern via Chat, Email oder Telefonie stattfindet. Bei der Vielzahl an verfügbaren Messaging-, Email- und Telefon-Diensten bietet die *Secure Messaging Scorecard* der EFF[84] eine gute Übersicht (vgl. Abb. 13). Diese wird zwar seit 2019 nicht mehr gepflegt, weshalb der Stand veraltet ist, jedoch reicht es für einen Eindruck über die Vielzahl an Diensten und deren (eventuell veraltete) Sicherheits-Standards aus.

Abb. 13 zeigt nur einen (modifizierten) Auszug der Secure Messaging Scorecard. Der Vergleich erfolgt anhand der Erfüllung folgender Kriterien: Transport-Verschlüsselung, Ende-zu-Ende-Verschlüsselung, Verifikation der Kontakt-Identität, Vorwärtsgerichtete Geheimhaltung (PFS), Open Source Code, Dokumentation der Sicherheitsmechanismen und kürzlich erfolgte Code-Prüfung. Die Dienste, welche miteinander verglichen werden, sind: *Facebook Messenger*, *iMessage*, *Jitsi*, Mailvelope, *GPGTools*, *Signal*, *Skype* und WhatsApp[85].

82 HTTPS Everywhere (eff.org/https-everywhere)
83 Apple Mail (support.apple.com/mail), Outlook (outlook.live.com), Thunderbird (thunderbird.net)
84 Secure Messaging Scorecard (eff.org/pages/secure-messaging-scorecard)
85 Facebook Messenger (messenger.com), iMessage (support.apple.com/explore/messages), Jitsi (jitsi.org), GPGTools (gpgtools.org), Signal (signal.org), Skype (skype.com)

Abbildung 13: Auszug der *Secure Messaging Scorecard* der EFF (modifiziert nach [53])

Davon sind Facebook Messenger, iMessage, Signal und WhatsApp Dienste für Kurznachrichten, Mailvelope und GPGTools werden für Email-Verschlüsselung genutzt und Jitsi sowie Skype sind Systeme für Video-Konferenzen. Die getroffene Auswahl soll lediglich einen Überblick über populäre Dienste und deren Sicherheits-Implementierung geben (Stand 2019). Anhand von Abb. 13 wird deutlich, dass die Nutzung von Facebook Messenger und Skype hinsichtlich der untersuchten Aspekte, eher vermieden werden sollte, wohingegen die Nutzung von Diensten wie Jitsi und Signal empfehlenswert ist.

Für die Verschlüsselung von Chats und Telefonaten kann z.B. der Dienst *Signal* genutzt werden, der Apps für alle gängigen Betriebssysteme anbietet. Sichere Video-Konferenzen lassen sich mithilfe des Dienstes *Jitsi* realisieren, der mit „Meet“ sowohl eine Server-Komponente als auch Apps für Smartphones bereitstellt. Email-Verschlüsselung lässt sich entweder mit S/MIME[86] und gängigen Email-Clients wie Apple Mail, Outlook oder Thunderbird realisieren oder mittels PGP[87]; dann werden jedoch die Erweiterungen GPG-Tools für Apple Mail, *Gpg4win* für Outlook oder *Enigmail* für Thunderbird[88] benötigt. Für die Nutzung von PGP auf Smartphones werden zusätzlich spezielle Apps notwendig.

Verschlüsseln von Daten und Datenträgern (Werkzeug 15)

Der letzte Schritt unter den operativen Maßnahmen ist das Verschlüsseln von Daten bzw. Datenträgern. Diese Schutzmaßnahme stellt sicher, dass Informationen an jedem Speicherort (unabhängig ob online oder offline) vor unbefugtem Zugriff durch Dritte geschützt sind. Wird ein gesamter Datenträger, z.B. ein USB-Stick oder eine Festplatte, verschlüsselt, so gilt dieser Schutz für alle darauf gespeicherten Daten. Es kann hierbei zwischen software-

86 S/MIME setzt ein gültiges X.509-Zertifikat für Email-Verschlüsselung voraus
87 PGP erfordert gültige Public-Key Schlüsselpaare zur Email-Verschlüsselung
88 Gpg4win (gpg4win.org), Enigmail (addons.thunderbird.net/de/thunderbird/addon/enigmail)

und hardwareseitiger Verschlüsselung unterschieden werden. Für Hardware-Verschlüsselung werden spezielle Geräte benötigt, welche die Technologie zum Verschlüsseln in der Hardware fest verbaut haben. Die Firma *Kingston* stellt z.B. SSDs und USB-Sticks mit Hardware-Verschlüsselung[89] her. Die Firma *iStorage* geht sogar noch einen Schritt weiter und bietet Festplatten und USB-Sticks an, die neben Hardware-Verschlüsselung noch mit einer zusätzlichen „On-board PIN"-Authentifizierung[90] gesichert werden können.

Die Software-Verschlüsselung hingegen ist mit jedem beliebigen Datenträger realisierbar. Das Programm *VeraCrypt*[91], eine Weiterentwicklung der bekannten Software *TrueCrypt*[91], kann hierfür z.B. verwendet werden. Falls jedoch nur einzelne Dateien verschlüsselt werden müssen, so kann dafür die Anwendung *Encrypto*[91] von *MacPaw* verwendet werden. Die Hersteller dieser Beispiele stellen Anwendungen sowohl für Windows als auch macOS und teilweise sogar für Linux bereit.

Die Verschlüsselung von Dokumenten und Datenträgern wird von Privacy-Boxen bisher nicht unterstützt. Hierfür werden entweder spezielle Programme auf dem jeweiligen Endgerät oder direkt in der Hardware verbaute Mechanismen verwendet. Es wäre jedoch denkbar, sowohl Datenträger über einen USB-Anschluss, als auch Netzwerkspeicher von einer Privacy-Box verschlüsseln zu lassen.

4.2.3 Reaktive und Notfall-Maßnahmen

Bei den reaktiven bzw. nachbereitenden Maßnahmen geht es in erster Linie um das Verbannen von digitalen Diensten und Technologien. Dies dient sowohl dem passiven Schutz durch Datensparsamkeit, als auch dem Wohlbefinden für Körper und Geist durch das Schaffen digitaler Freiräume. Die Notfall-Maßnahmen dienen der Schadensbegrenzung, im Fall eines bereits eingetretenen Schadens durch Reputationsverlust oder Identitätsdiebstahl.

Umstieg auf datenschutzfreundliche Dienste (Werkzeug 16)
Für den Fall dass Werkzeug 5 keine Anwendung findet, da bereits datenschutzkritische Dienste genutzt werden, hilft nur der konsequente Umstieg auf datenschutzfreundliche Alternativen. Die Werkzeuge 11 und 12 beschreiben mit „No-Log-VPNs" und „Privacy-Browsern" bereits zwei mögliche Umsetzungen dieser Maßnahme. Ein weiterer wichtiger Schritt betrifft den Wechsel von Suchmaschinen wie Google und *Bing*[92] zu Alternativen wie *Qwant*, *Startpage*, *DuckDuckGo* oder *Swisscows*[92].

Qwant wird in Frankreich betrieben und verspricht mit den Prinzipien „Privatsphäre und Neutralität" die Freiheit der Nutzer und den Schutz des digitalen Ökosystems zu wahren. Startpage, mit Firmensitz in den Niederlanden, nutzt Ergebnisse von Google, die Suche berücksichtigt die Anonymität und den Schutz der Privatsphäre allerdings mithilfe spezieller Verschleierungsmechanismen. DuckDuckGo kommt aus den USA und wirbt damit, den Nutzer weder mit Werbeanzeigen zu verfolgen noch persönliche Daten zu speichern, zu

89 Kingston IronKey (kingston.com/de/usb-flash-drives/ironkey-s1000-encrypted-usb-flash-drive)
90 iStorage diskashur (istorage-uk.com/de/product-category/encrypted-hdds-ssds)
91 VeraCrypt (veracrypt.fr), TrueCrypt (truecrypt.sourceforge.net), Encrypto (macpaw.com/encrypto)
92 Bing (bing.com), Qwant SAS (qwant.com), Startpage B.V. (startpage.com), Duck Duck Go Inc. (duckduckgo.com), Swisscows AG (swisscows.com)

sammeln oder zu teilen. Swisscows hingegen, mit Sitz in der Schweiz, präsentiert sich als unabhängige, innovative Suchmaschine mit Respekt vor Anonymität und Privatsphäre.

Bei „Social Media“-Plattformen gibt es neben Facebook, Twitter und Instagram mittlerweile einige dezentral organisierte Plattformen wie *Mastodon*, *diaspora** oder *friendica*[93], die mit Fokus auf Privatheit und Daten-Freiheit entwickelt werden. Die Plattformen sind Open Source und ermöglichen, dank dezentraler Struktur, auch den Betrieb eines eigenen Servers, sodass alle Daten tatsächlich in eigener Hand bleiben können. Einige Dienste ermöglichen sogar die Anbindung von anderen Plattformen, sodass bereits existierende News-Feeds eingebunden werden können.

Die Auflistung dieser Beispiele kann mit Alternativen von Diensten für Kalender und Kontakte (*EteSync*), Karten (*HERE WeGo*), Videos (*PeerTube*), Speicher (*Nextcloud*) und Emails (*ProtonMail*)[94] beliebig fortgeführt werden. Die Webseiten *privacytools.io* und *restoreprivacy.com*[95] bieten eine gute Übersicht solcher „Privacy Tools“ an. Die Auswahl reicht von Anbietern für Email, Hosting, VPN oder DNS über Suchmaschinen, Video-Plattformen, Browser und Browser-Plugins, bis hin zu Produktivitäts-Software und Betriebssystemen für Computer, Smartphones und Router.

Beim Umstieg auf datenschutzfreundliche Alternativ-Dienste können Privacy-Boxen einen wichtigen Teil beitragen. Viele der genannten Alternativen lassen sich auch auf Geräten wie einer Privacy-Box installieren und betreiben. Dies hängt wiederum stark von der Unterstützung des jeweiligen Geräts und des Herstellers ab. Mit zusätzlichem Feedback-Kanal sind auch gezielte Empfehlungen für den Umstieg denkbar. Daher kann dieses Werkzeug zumindest teilweise mit Privacy-Boxen umgesetzt werden.

Social-Media säubern und digitaler Selbstmord (Werkzeug 17)
Ein gewisses Risiko für Nutzer kann von sozialen Netzwerken ausgehen, da sich über die Jahre der Nutzung sowohl die persönlichen Einstellungen zu Datenschutz als auch die der Plattform ändern können. Aus diesem Grund sollten Accounts regelmäßig gepflegt und die Datenschutzeinstellungen überprüft werden. Sowohl Google als auch Facebook bieten dafür *Privatsphärechecks*[96] an, mithilfe derer die Privatsphäre-Einstellungen von Accounts geprüft und optimiert werden können. Diese Checks sind notwendig, da die stetig wachsende Anzahl von Einstellungen kaum noch von Nutzern überblickt werden kann.

Neben der Prüfung von Datenschutzeinstellungen lohnt es sich zusätzlich, alle Social Media Accounts regelmäßig aufzuräumen: dazu zählt die Einschränkung des Sichtbarkeits-Radius von Inhalten und das Löschen alter Beiträge wie Profilbilder, Posts und geteilte Medien. Persönliche Angaben sollten unter Berücksichtigung von Werkzeug 6 regelmäßig überprüft und gelöscht werden. Es gibt Dienste, mit denen Social Media Accounts nach Beiträgen zu bestimmten Themen durchsucht werden können. Mit *Scrubber* oder *Social Sweepster*[97]

93 Mastodon (joinmastodon.org), diaspora* (diasporafoundation.org), friendica (friendi.ca)
94 EteSync (etesync.com), HERE WeGo (wego.here.com), PeerTube (joinpeertube.org), Nextcloud (nextcloud.com), ProtonMail (protonmail.com)
95 Privacy and Security Tools (restoreprivacy.com/privacy-tools)
96 Google Privatsphärecheck (myaccount.google.com/intro/privacycheckup), Facebook Privatsphäre-Check (facebook.com/about/basics/manage-your-privacy)
97 Scrubber (scrubber.social), Social Sweepster (socialsweepster.com)

lassen sich so Beiträge z.B. über Alkohol und Drogen, Schimpfwörter oder Religion und Politik gezielt löschen.

Ein etwas konsequenterer Schritt ist das Löschen aller Beiträge von einer Plattform. Um dies bei Twitter oder Facebook zu erreichen, ohne jedoch Kontakte oder Freunde zu verlieren, können Anwendungen wie *TwitWipe* oder *Social Book Post Manager*[98] verwendet werden. Diese Maßnahme setzt die digitale Identität gewissermaßen zurück. Einträge in Suchmaschinen oder auf anderen Seiten bleiben jedoch weiter bestehen. Die einzige Steigerung ist nur noch mit dem „Digitalen Selbstmord“ möglich, also das vollständige Löschen des Accounts.

Beim Säubern und Aufräumen von Social-Media Accounts sind Privacy-Boxen nicht sehr hilfreich. Das Bereitstellen entsprechender Anleitungen könnten Privacy-Boxen mithilfe eines geeigneten Feedback-Kanals realisieren. Ebenso sind regelmäßige Erinnerung denkbar, z.B. wenn große Plattform-Betreiber Änderungen an ihren Datenschutz-Einstellungen vorgenommen haben.

Technologien vermeiden und abschalten (Werkzeug 18)
Beim Bezahlen mit EC- oder Kreditkarte, *Paypal* oder *Flattr*[99] können die hinterlegten Zahlungsinformationen dem Besitzer eindeutig zugewiesen werden. Dadurch entsteht eine nachvollziehbare Einkaufs-Historie, die sein Einkaufsverhalten widerspiegelt. Das gleiche gilt für Kunden- oder Rabatt-Karten wie *Deutschlandcard* oder *Payback*[100]. Auf ihnen wird zur Berechnung der Rabatte und Angebote der gesamte Einkauf vermerkt [120]. Aus diesen Gründen sollte auf beides verzichtet werden.

Für Offline-Einkäufe empfiehlt es sich daher entweder in Bar, mit anonymen Prepaid-Kreditkarten wie *paysafecard* oder verschlüsselt mit *Apple Pay*[101] zu bezahlen. Anonyme Online-Bezahlung wird, aufgrund des illegalen Angebots im Darknet, immer schwieriger. Einkäufe im Internet können ebenfalls mit anonymen Kreditkarten (bis 100 Euro Limit), oder Krypto-Währungen wie *Bitcoin* oder *Ethereum*[102] getätigt werden. Eine anonyme Bezahlung mit Paypal ist z.B. auch durch das Zusammenspiel verschiedener Anonymisierungs-Maßnahmen möglich [72].

Durch die Nutzung bestimmter Hardware, wie z.B. Webcams, Mikrofone und Smart Speaker, können ebenfalls Risiken für die Privatsphäre entstehen. Webcams und Mikrofone sollten nach Möglichkeit ausgesteckt oder abgeklebt werden, wenn sie nicht in Gebrauch sind. Zwar gibt es meist Indikatoren, die anzeigen wenn ein Gerät aktiv ist, leider fehlt oft eine hardwareseitige Verbindung, wodurch diese unbemerkt umgangen werden können [20]. Smart Speaker wie *Amazon Echo*, *Google Home* oder *HomePod*[103] sollten daher abgeschaltet, nur manuell aktiviert und in ein „unkritisches“ Zimmer (z.B. Wohnzimmer, Küche oder Flur) verbannt werden. Eine datenschutzfreundliche Alternative für einen digitalen

98 TwitWipe (twitwipe.com), Social Book Post Manager (social.techjunkie.com/delete-all-facebook-posts)
99 Paypal (paypal.com), Flattr (flattr.com)
100 Deutschlandcard (deutschlandcard.de), Payback (payback.de)
101 paysafecard (paysafecard.com), Apple Pay (apple.com/apple-pay)
102 Bitcoin (bitcoin.de), Ethereum (ethereum.org)
103 Amazon Echo (amazon.de/echo), Google Home (google.de/home), HomePod (apple.com/homepod)

Sprachassistenten gab es mit *snips*[104], der als DIY-Projekt startete, jedoch Ende 2019 von der Firma *Sonos*[104] gekauft wurde.

Die Nützlichkeit von Privacy-Boxen für dieses Werkzeug entspricht in etwa dem von Werkzeug 5: Eine Sensibilisierung über zusätzliche Informations-Kanäle ist denkbar, ebenso das vollständige oder teilweise Blockieren von IoT- und „Smart Home"-Geräten.

Das Recht auf Vergessenwerden nutzen (Werkzeug 19)
Sind sensible Daten erst einmal im Internet, ist es nicht so einfach, diese wieder zu entfernen. Allerdings gibt es mittlerweile rechtliche Grundlagen, die zum Erreichen dieses Ziels genutzt werden können.

Das „Recht auf Vergessenwerden" erhielt durch das Google-Urteil des Europäischen Gerichtshofs im Jahr 2014 große mediale Aufmerksamkeit. Seitdem haben Privatpersonen das Recht, von Suchmaschinenbetriebern die Löschung bestimmter Einträge zu verlangen. Seit dem Inkrafttreten der DSGVO hat das „Recht auf Vergessenwerden" in Artikel 17 mit dem *Recht auf Löschung* eine gesetzliche Manifestierung: „Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen (...)" [39].

Google bietet Nutzern mit dem „Ersuchen um Entfernung von Inhalten gemäß europäischem Datenschutzrecht" seitdem die Möglichkeit, URLs zum Zweck des Datenschutzes aus der Google-Suche zu entfernen. Es wurden mittlerweile fast eine Million Anträge auf Entfernung gestellt, von denen etwas weniger als 50% bewilligt wurden [75]. Um Inhalte von Webseiten und anderen Plattformen löschen zu lassen, ist es allerdings meist notwendig, den Anbieter oder Betreiber zu kontaktieren und mit der Löschung zu beauftragen.

Eine Privacy-Box könnte bei diesem Werkzeug lediglich mit der Bereitstellung von Informationen behilflich sein, indem z.B. „Best Practices" und Adressen für die Anwendung des Rechts auf Vergessenwerden über einen entsprechenden Weg bereitgestellt werden.

Reputationsmanagement anwenden (Werkzeug 20)
Für den Fall, dass sich Informationen mithilfe von Werkzeug 19 nicht entfernen lassen, hilft nur noch richtig angewendetes Reputationsmanagement, um die Informationen wieder „verschwinden" zu lassen. Dazu muss jedoch der Bekanntheitsgrad der Betroffenen berücksichtigt werden. Nach Mathias Klang, Spezialist für Datenschutz und Rechtsinformatik der Universität Göteborg, ist die Schadensbegrenzung umso einfacher, je höher ihr Bekanntheitsgrad ist: negative Informationen können ignoriert oder sogar zum Vorteil genutzt werden [87, S. 89].

Bei weniger bekannten Personen ist die Aufgabe schwieriger zu bewältigen: negative Informationen müssen aufwändig mit einer Vielzahl von positiven überschwemmt werden. Diese Informationen müssen zusätzlich SEO-optimiert sein, sodass die schlechten Ergebnisse bei der Suche auf die zweite oder dritte Seite verdrängt werden. Da die meisten Menschen nicht

104 snips (snips.ai), Sonos (sonos.com)

mehr als die ersten zehn Suchergebnisse berücksichtigen, ist dies eine effektive (wenn auch nur temporäre) Methode [87, S. 92]. Wie bereits in Abschnitt 2.2.3 (Probleme, Risiken und Gefahren) unter dem Punkt „Reputationsverlust“ beschrieben, gibt es Dienstleister, die sich speziell auf das Gebiet Reputationsmanagement spezialisiert haben und dabei helfen können, einen geschädigten Ruf wiederherzustellen.

Wie schon bei Werkzeug 19 beschränkt sich die Nützlichkeit einer Privacy-Box bei diesem Werkzeug auf die Bereitstellung von Informationen und Kontakten, mithilfe derer ein Nutzer beim Reputationsmanagement Hilfe bekommt.

Nachdem konkrete Werkzeuge zum Selbstdatenschutz aus allen Kategorien der *Sieben V der digitalen Selbstverteidigung* vorgestellt und hinsichtlich ihrer Umsetzbarkeit in Privacy-Boxen bewertet wurden, folgt anschließend eine Tabelle, in welcher die Ergebnisse nochmal übersichtlich zusammengefasst werden:

		Umsetzbarkeit des Werkzeugs mit Privacy-Boxen	ja	teils	nein
Präventiv	Vorbereiten	W1: Bewusstsein für den Wert von PD		✓	
		W2: Kenntnis über die Verwendung von Daten		✓	
		W3: Erkennen von Schwachstellen und Gefahren		✓	
	Vorbeugen	W4: Erstellen und Verwenden sicherer Passwörter	✓		
		W5: Datenschutzkritische Dienste vermeiden			✓
		W6: Selbstreflexion vor dem Teilen von Inhalten			✓
Operativ	Verweigern	W7: Verwenden von Blocker-Software	✓		
		W8: Device-Fingerprinting verhindern	✓		
		W9: Löschen von Sessions und Cookies		✓	
	Verschlei.	W10: Einsatz von Pseudonymen im Web			✓
		W11: Sichere DNS und VPN-Dienste nutzen	✓		
		W12: Nutzung verschiedener Browser		✓	
	Verschlüss.	W13: Transport-Verschlüsselung verwenden	✓		
		W14: Chats, Emails und Telefonie verschlüsseln	✓		
		W15: Verschlüsseln von Daten und Datenträgern			✓
Reaktiv	Verbannen	W16: Umstieg auf datenschutzfreundliche Dienste		✓	
		W17: Social-Media säubern und digitaler Selbstmord			✓
		W18: Technologien vermeiden und abschalten			✓
	Vermin.	W19: Das Recht auf Vergessenwerden nutzen			✓
		W20: Reputationsmanagement anwenden			✓

Tabelle 2: Realisierbarkeit von Selbstdatenschutz-Werkzeugen mit Privacy-Boxen

Die Maßnahmen werden in Tabelle 2 mit „ja“, „nein“ und „teils“ bewertet, wobei letzteres bedeutet, dass eine Realisierung mit Privacy-Boxen nur teilweise oder mit zusätzlichen Komponenten möglich ist.

Wie in Tabelle 2 sichtbar wird, können die Werkzeuge 4, 7, 8, 11, 13 und 14 mit Privacy-Boxen realisiert werden. Die Werkzeuge 1–3, 9, 12 und 16 sind nur teilweise oder mithilfe von zusätzlichen Komponenten umsetzbar. Die Werkzeuge 5, 6, 10, 15 und 17–20 lassen sich jedoch nicht mithilfe einer Privacy-Box verwirklichen. Im weiteren Verlauf der Arbeit wird der Fokus auf die von Privacy-Boxen realisierbaren Maßnahmen gelegt. Nach einer Marktübersicht folgt eine Vor-Auswahl von Privacy-Boxen, welche anschließend auf die Implementierung der realisierbaren Werkzeuge untersucht wird.

4.3 Marktanalyse und Geräteübersicht

Für einen aktuellen Überblick und die Einordnung von „Privacy-Boxen“ im Bereich von Privacy- und Security-Hardware, folgt eine Marktübersicht. Generell kann Privacy-Hardware in Produkte für professionelle Nutzung (engl. „Business“) und Produkte für Endverbraucher (engl. „Consumer“) eingeteilt werden. Die Produkte aus dem Consumer-Segment lassen sich noch in Einsatzbereich und Zielgruppe unterteilen: Es gibt kabelgebunde Lösungen für den stationären Einsatz (Kontext „Zuhause“) und portable Lösungen für den mobilen Einsatz (Kontext „Unterwegs“). Bei der Zielgruppe kann zusätzlich zwischen Nutzern mit und ohne technischem Know-how unterschieden werden. Nutzer mit technischer Expertise haben zusätzlich die Möglichkeit, sich Produkte aus „Open Source“- und DIY-Projekten selbst zusammen zu bauen. Aufgrund des thematischen Fokus auf die Gruppe der Privat-Nutzer sind die Produkte aus dem Business-Segment weniger relevant und werden nur zur Vollständigkeit erwähnt.

4.3.1 Kommerzielle Produkte

Aus dem Bereich der kommerziellen Produkte werden zu Beginn drei Geräte des Business-Sektors vorgestellt. Anschließend verlagert sich der Fokus auf den Consumer-Bereich, bei dem es auch ein paar Produkte in einer Business-Variante oder auf Anfrage für Unternehmen zu kaufen gibt.

Business-Produkte
Für die Vollständigkeit der Übersicht und zur Abgrenzung von Consumer-Produkten werden einige Produkte aus dem Business-Bereich vorgestellt. Die Geräte, welche für den professionellen Einsatz konzipiert sind, haben einen deutlichen Fokus auf Sicherheit. Nur sehr wenige Geräte bieten auch Schutzfunktionen für die Privatheit an, welche sich in den meisten Fällen auf die Funktionen VPN und Inhaltsfilterung beschränken:

- **Zyxel USG FLEX 100**: Die *USG FLEX 100* Firewall von *Zyxel*[105] zeichnet sich durch einen „Multilayer-Schutz“ aus, der neben Mechanismen wie *Stateful Packet Inspection* (SPI), *Intrusion Prevention System* (IPS) und Viren-Erkennung auch Funktionen für Inhaltsfilterung, Email-Schutz (Anti-Spam) und VPN beinhaltet [160].

105 Zyxel USG FLEX 100 (zyxel.com/de/de/products_services/USG-FLEX-Firewall-USG-FLEX-100)

- **Cisco Meraki MX64W**: Das *Meraki MX64W* von *Cisco*[106] wird als „All in one Wireless, Security, and SD-WAN“ beworben. Es bietet neben den Funktionen einer normalen Firewall zusätzlich die Filterung von Inhalten, Viren und Phishing an, weshalb sie auch als *Next Generation Firewall* (NGFW) bezeichnet wird [160].

- **SonicWall NGFW TZ**: Die *TZ-Serie* der NGFWs von *SonicWall*[107] bietet neben normalen Firewall-Schutzfunktionen mit einer neuartigen Real-Time Deep Memory Inspection und feingranularen Inhaltsfiltern noch weitere Möglichkeiten. So können z.B. anstatt ganzer Webseiten nur unerwünschte Inhalte wie Java, ActiveX und Cookies blockiert werden [158, S. 1-2].

Die vorgestellten Geräte sind grundsätzlich Netzwerk-Firewalls aus dem Profi-Segment mit erweiterter Funktionalität. Deshalb werden sie von den Herstellern auch als NGFW beworben. „Richtige“ Privacy-Boxen gibt es für den Business-Bereich nur in Form von Produkt-Varianten aus dem Consumer-Sektor.

Consumer-Produkte (Stationär)

Im Bereich der stationären Consumer-Hardware gibt es bereits einige Produkte auf dem Markt, die im Folgenden vorgestellt werden. Bei den vorgestellten Geräten verschiebt sich der Schwerpunkt zwischen Sicherheit und Privatheit abhängig vom jeweiligen Hersteller:

- **Bitdefender BOX 2**: Die *Bitdefender BOX* ist ein Gerät des rumänischen Cybersecurity-Unternehmens *Bitdefender*[108] und verspricht neben einer verbesserten Sicherheit aller Heimnetz-Geräte Verbesserungen für Datenschutz und Privatshpäre der Nutzer. Es werden neben dem Schutz vor Malware, Phishing und Betrug mehr Sicherheit für sensible Daten und beim Surfen im Internet geboten. Für einen besseren Schutz der Privatsphäre werden Inhaltsfilterung, VPN, Kindersicherung und Abwehr von Netzwerkangriffen genannt. Zusätzlich wird mit einer zentralen App eine intuitive und benutzerfreundliche Steuerung versprochen. Die Bitdefender BOX kann als eigener Router eingerichtet oder in ein bestehendes Netzwerk integriert werden. Sie kostet 100 Euro und funktioniert nur in Kombination mit dem Jahres-Abonnement einer passenden Bitdefender Sicherheits-Software (zusätzlich 100 Euro pro Jahr) [15].

- **F-Secure SENSE**: Der *F-Secure SENSE* ist ein Sicherheitsrouter der finnischen Cybersecurity-Firma *F-Secure*[109]. Er ist dafür konzipiert, die Internetaktivitäten aller vernetzten Geräte im Privat-Haushalt vor Cyberangriffen zu schützen. Dazu werden schädliche Webseiten und andere Bedrohungen blockiert. Zum Schutz der Privatsphäre stehen neben Tracking-Abwehr ein Passwort-Manager und VPN zur Verfügung. Für die Netzwerkverwaltung und Einrichtung gibt es eine mobile App, welche sowohl bei Installation und Überwachung helfen, als auch laufend über den Sicherheitsstatus aller Netzwerk-Geräte informieren kann. Der F-Secure SENSE kostet 100 Euro und funktioniert ebenfalls in Kombination mit dem Abonnement einer entsprechenden Sicherheits-Suite (zusätzlich 80 Euro pro Jahr) [64].

106 Cisco Meraki MX64W (meraki.cisco.com/product/security-sd-wan/small-branch/mx64w)
107 SonicWall NGFW TZ-Serie (sonicwall.com/de-de/products/firewalls/entry-level)
108 Bitdefender BOX (bitdefender.de/box), Bitdefender GmbH (bitdefender.de)
109 F-Secure SENSE (f-secure.com/de/home/products/sense), F-Secure GmbH (f-secure.com/de)

- **TrutzBox Home**: Die *TrutzBox* des deutschen Unternehmens *Comidio* ist ein Gerät mit Fokus auf Datenschutz und Privatsphäre, was schon im Produkt-Slogan „back to privacy“ deutlich wird. Die Schutzfunktionen sind in fünf Bereiche unterteilt [30]:

  1. *TrutzBrowse* bietet „spurenarmes und anonymes Surfen im Internet“ durch Verschleierung von Fingerabdruck und Anonymisierung.
  2. *TrutzMeeting & TrutzChat* ermöglichen „sichere Webmeetings und Chats“ durch abhörsichere Chat- und Konferenz-Dienste.
  3. *TrutzMail* erlaubt den „Versand sicherer Emails“ durch eine automatische Verschlüsselung.
  4. *TrutzContent* bietet „maximalen Schutz für Kinder und Familie“ durch die Filterung von unerwünschten Webseiten und Inhalten.
  5. *TrutzBase* schützt vor „Viren und Hackerangriffen“ mit Anti-Virus- und Firewall-Funktionalität.

  Die TrutzBox kann über ein Dashboard verwaltet werden und der Quellcode ist öffentlich verfügbar. Das Home-Paket der TrutzBox kostet zwischen 270 und 320 Euro[110] und funktioniert ebenfalls nur in Kombination mit einem Abonnement für die benötigten Service-Dienste (zusätzlich 60 Euro pro Jahr) [30].

- **Winston Privacy Filter**: Der *Winston Privacy Filter* der amerikanischen Firma *Winston Privacy*[111] ist ebenfalls ein Gerät mit Fokus auf Internet-Privatsphäre. Er bietet neben dem Schutz durch Blockieren von Werbung und Malware auch einen intelligenten Schutz vor Tracking durch Cookies und Fingerprinting-Methoden. Zusätzlich wird mithilfe von verschlüsselten DNS-Anfragen und einem Peer-to-Peer Privacy-Mesh die Spionage von Standort- und ISP-Tracking erschwert. Die Geräte-Konfiguration, sowie Aktivitäts-Monitoring und detaillierte Berichte können mit einem übersichtlichen Dashboard dargestellt werden. Der Winston Privacy Filter wird über ein Kabel an den Router angeschlossen und kostet 150 US Dollar. Er funktioniert nur zusammen mit einem jährlichen Abonnement für die Nutzung der Cloud-Services (zusätzlich 120 US Dollar pro Jahr) [175].

- **RATtrap**: Die *RATtrap* des amerikanischen Startups *IoT Defense*[112] ist ein Gerät, das dem Nutzer mehr Sicherheit und Privatheit bieten soll. Die RATtrap kann kein eigenes Netzwerk aufbauen, sondern nur in eine bestehende Kabelverbindung z.B. zwischen Modem und Router eingefügt werden. Sie verspricht den Schutz aller mit dem Netzwerk verbundenen Geräte vor Malware, Phishing, Identitätsdiebstahl und Datenschutzverletzungen. Der Privatsphäre-Schutz für Nutzer wird durch Inhaltsfilterung, zusätzliches Ad-Blocking und Echtzeit-Aktualisierungen für neue Bedrohungen realisiert. Mithilfe einer mobilen App können sowohl Statistiken visualisiert als auch Echtzeit-Benachrichtigungen empfangen werden. Die RATtrap kostet 90 US Dollar und benötigt ein aktives Abonnement für die Nutzung der Web-Services (zusätzlich 110 US Dollar pro Jahr) [37].

110 Preise ohne bzw. mit WLAN-Modul, das Business-Paket mit mehr Speicher kostet ca. 1.000 Euro
111 Winston Privacy Filter, Winston Privacy LLC (winstonprivacy.com)
112 RATtrap (myrattrap.com), IoTDefense Inc. (iotdef.com)

Neben den vorgestellten Geräten gibt es noch ein paar weitere Produkte, die allerdings schon ihr End of Life (EoL) erreicht haben, also nicht mehr weiter entwickelt oder vertrieben werden. Dazu zählen die *Cujo Smart Firewall*[113] und der *Norton Core*[114] aus den USA sowie die *Enigmabox*[115] aus der Schweiz.

Consumer-Produkte (Portabel)
Im Vergleich zu stationärer Hardware gibt es kaum tragbare Geräte, die zum Schutz von Sicherheit und Privatheit für Nutzer beitragen können. Es werden zwei Beispiele vorgestellt, die zurzeit am Markt erhältlich sind:

- **Keezel 2.0**: *Keezel* ist eine portable Cyber-Security Firewall von einer gleichnamigen niederländischen Firma[116]. Das Gerät soll Nutzer unterwegs vor Phishing, Malware, Schnüfflern und Hackern schützen. Dieser Schutz wird mithilfe von VPN-Verschlüsselung, Phishing-Filtern und Ad-Blockern realisiert. Der integrierte Akku hält laut Hersteller-Angaben bis zu 20 Stunden. Die Standard-Anwendung von Keezel ist die Verbindung zu einem öffentlichen WLAN, z.B. in Hotels, Flughäfen und Cafés. Keezel lässt sich jedoch auch per Kabel oder über Zellular-Netz betreiben, indem ein LAN-Adapter bzw. 3G/4G-Adapter am bereitgestellten USB-Port angeschlossen wird. Mit einem zusätzlichen Keezel kann ein direkter VPN-Tunnel zwischen zwei Geräten hergestellt werden. Keezel kostet einmalig 200 Euro und lässt sich mit einem kostenlosen Plan nutzen. Für höhere Geschwindigkeiten, mehr VPN-Server und häufigere Updates der Phishing-Filter gibt es einen Premium-Plan (zusätzlich 60 Euro pro Jahr) [103].

- **InvizBox Go**: Die *InvizBox* der gleichnamigen Firma aus Irland gibt es in zwei Varianten: für den stationären Einsatz als *InvizBox 2* und als portable Variante in Form der *InvizBox Go*[117]. Die InvizBox Go schützt Nutzer unterwegs durch die Verschlüsselung des gesamten Datenverkehrs durch eine VPN-Verbindung. Zusätzlich ist ein Ad-Blocker zum Schutz vor Werbung und betrügerischen Webseiten integriert, der regelmäßig aktualisiert wird. Dieser portable VPN-Router funktioniert nur über WLAN-Netzwerke und verspricht Sicherheit mit einer No-Log-Richtlinie für VPN-Verbindungen und Vertrauen durch „Open Source“-Code. Er lässt sich außerdem mit einer InvizBox 2 im Heimnetzwerk koppeln und ermöglicht so einen direkten und sicheren Zugriff auch von unterwegs. Die InvizBox kostet 100 US Dollar und benötigt ein aktives Service-Abonnement für den Zugriff auf die VPN-Server (zusätzlich 80 US Dollar pro Jahr) [95].

Auch in dieser Kategorie gibt es neben den vorgestellten Produkten noch ein weiteres Gerät, dass bereits EoL erreicht hat. *Dojo* vom israelischen Startup *Dojo-Labs*[118] wurde 2017 vom Cybersecurity-Unternehmen *Bullguard*[119] übernommen, verschwand aber 2018

113 Cujo Smart Firewall, EoL: Januar 2019 (getcujo.com/smart-firewall-cujo – Snapshot vom 12.12.2018)
114 Norton Core, EoL: Februar 2019 (us.norton.com/core)
115 Enigmabox, EoL: April 2019 (enigmabox.net – Snapshot vom 03.04.2019)
116 Keezel (eu.keezel.co)
117 InvizBox 2, InvizBox Go, InvizBox Ltd. (invizbox.com)
118 Dojo, EoL: August 2018 (dojo.bullguard.com/dojo-by-bullguard – Snapshot vom 27.08.2018)
119 BullGuard Deutschland GmbH (bullguard.com/de)

wieder vom Markt. Es passt auch nur eingeschränkt in die Kategorie portabler Produkte, da sich der Bewegungs-Radius auf das Haus des Nutzers beschränkt. Das Gerät kann dort zwar beliebig platziert werden, muss jedoch zum Laden auf eine Basis-Station gestellt werden, die wiederum mit Kabel zwischen Modem und Router angeschlossen wird.

4.3.2 Kickstarter Produkte

Die Größe der Unternehmen von bereits vorgestellten Produkten variiert zwischen Start-Ups und Groß-Konzernen. Einige der Firmen haben bereits eine Finanzierung über *Kickstarter* abgeschlossen oder zumindest versucht: Die Finanzierung von RATtrap[120] über Crowdfunding schlug fehl, wohingegen InvizBox[121] und Winston[122] erfolgreiche Kampagnen auf Kickstarter nachweisen können. Es folgen ein paar weitere Kickstarter-Projekte, deren Erfolg oder Bekanntheit etwas geringer ausgefallen sind:

- **anonabox Pro**: Die *anonabox* war eines der ersten Kickstarter-Projekte[123], welches Nutzern anonymen Internet-Zugang mithilfe einer Hardware-Box versprach. Nach dem äußerst erfolgreichen Start einer Kickstarter-Kampagne im Jahr 2014 wurde das Projekt nach wenigen Tagen vom Plattformbetreiber aufgrund von Regelverletzungen gestoppt [159]. Im Jahr 2015 wurde ein zweiter, erfolgreicher Versuch über die Plattform *Indiegogo*[123] gestartet. Die anonabox wird mit Kabel an den Router angeschlossen und leitet den gesamten Netzwerkverkehr über das TOR-Netzwerk oder einen VPN-Server um. Die Pro-Version der anonabox bietet neben verbesserter Leistung zusätzlich einen Webserver, Filesharing und WLAN als Funktionen an. Es gibt verschiedene Ausführungen der anonabox vom gleichnamigen US-Amerikanischen Hersteller, die Nutzer einmalig zwischen 80 und 120 US Dollar kosten [115].

- **Relaxbox/Tarnomat**: Die *Relaxbox* wurde 2015 erfolgreich auf Kickstarter[124] finanziert und war eine Lösung für Nutzer, um sicher und sorgenfrei im Internet zu surfen. Die Box schützt vor Viren und Trojanern durch Einbruchs-Erkennung, Antivirensoftware und Inhaltsfilter. Die Privatsphäre der Nutzer wird mit Antifingerprinting-Techniken und VPN-Verschlüsselung geschützt. Zusätzlich wird ein Schutz vor Cyberkriminalität und Abmahnungen durch die Störerhaftung von den deutschen Herstellern versprochen [104]. Ende 2016 erreichte das Projekt EoL, jedoch besteht für Relaxbox-Kunden mittlerweile die Möglichkeit, bereits gekaufte Geräte weiter zu verwenden: Der deutsche Hersteller des *Tarnomat*[124], einer Privacy-Box mit ähnlicher Funktionalität, bietet ein Wechselangebot an, da die Hardware der Geräte miteinander kompatibel ist. Ein Tarnomat kostet 80 Euro und benötigt einen aktiven Tarif für den Zugang zur Infrastruktur (zusätzlich 90 Euro pro Jahr) [164].

- **eBlocker 2**: Das *eBlocker*-Projekt startete Anfang 2016 auf Kickstarter[125] und wurde erfolgreich finanziert. Das daraus hervorgehende deutsche Unternehmen *eBlocker*

120 RATtrap – Kickstarter 2016 (kickstarter.com/profile/iotdef/created)
121 Team InvizBox – Kickstarter 2015 & 2017 (kickstarter.com/profile/683682172/created)
122 Winston Privacy – Kickstarter 2019 (kickstarter.com/projects/winstonprivacy/created)
123 anonabox (anonabox.com) – Indiegogo 2015 (indiegogo.com/individuals/8936930/campaigns)
124 Relaxbox – Kickstarter 2015 (kickstarter.com/profile/470304262/created), Tarnomat (tarnomat.com)
125 eBlocker (eblocker.org) – Kickstarter 2016 (kickstarter.com/profile/eblocker/created)

GmbH entwickelte mit dem eBlocker ein Gerät, das Online-Tracking und Werbung verhindert, vor Malware und Internet-Gefahren schützt, schädliche und jugendgefährdenden Inhalte blockiert und für Anonymität beim Surfen sorgt. Dieser Schutz betrifft alle mit dem Netzwerk verbundenen Geräte und soll auch unterwegs möglich sein. Ebenso ist ein DNS-Schutz und die Nutzung des TOR-Netzwerks möglich. Der eBlocker lässt sich über ein Dashboard oder mit einer iOS-App konfigurieren. Nach einer erfolglosen Finanzierungsrunde musste das Unternehmen 2019 die Insolvenz anmelden und stellte den Geschäftsbetrieb ein. Seitdem wird das Projekt durch Spenden finanziert und als „Open Source"-Projekt fortgeführt. Mit entsprechend technischem Know-how kann die bereitgestellte Software auf einem *Raspberry Pi* oder *Banana Pi*[126] installiert und ein eBlocker selbst gebaut werden. Die Kosten für die dafür notwendige Hardware belaufen sich auf rund 60 Euro [50].

- **AKITA**: Das Produkt *Akita* ist ein Netzwerk-Scanner für den Einsatz mit IoT- bzw. „Smart Home"-Geräten und wurde 2017/18 bei einer Kampagne auf Kickstarter[127] mit dem Slogan „Instant Privacy for Smart Homes" beworben. Akita schützt die Sicherheit und Privatshpäre von Nutzern, indem es das Heim-Netzwerk auf ungewöhnliche Aktivitäten überwacht und diese sofort blockiert. Hierbei wird ein *Intrusion Prevention System* (IPS) anstelle von *Deep Package Inspection* (DPI) genutzt, um die Privatheit der Daten zu respektieren. Über eine mobile App wird der Nutzer zusätzlich benachrichtigt und kann entsprechende Maßnahmen ergreifen. Die Funktionsweise von AKITA gleicht einem „digitalen Wachhund" (woher auch der Produkt-Name stammt) dessen Netzwerk-Schutz Nutzer einmalig 130 US Dollar kostet [4].

Die vorgestellten Crowdfunding-Kampagnen sind überwiegend erfolgreiche Beispiele aus einer Auswahl von Projekten, die zum Teil weniger Relevanz für diese Arbeit haben (z.B. *Fingbox*[128]), deren EoL bereits erreicht ist (z.B. *AdTrap*[129] und *ArmorVPN*[130]) oder die weniger erfolgreich waren (z.B. *Bettiex*[131]).

4.3.3 Open Source und DIY Produkte

Neben den genannten Crowdfunding-Kampagnen gibt es noch eine Reihe von „Open Source"-Projekten, die DIY-Lösungen für Bastler und Technik-Enthusiasten ermöglichen. Es wird eine Auswahl an bekannten und vielversprechenden Projekten vorgestellt:

- **Pi-hole 5**: Das *Pi-hole*-Projekt[132] ist eine *Raspberry Pi*-basierte Lösung zur netzwerkweiten Filterung von Werbung. Das Projekt startete 2015 und hat sich seitdem zu einer großen Plattform mit automatischer Installation auf unterschiedlichen Betriebssystemen weiter entwickelt. Der Pi-hole kann im Netzwerk als DNS-Server konfiguriert und mit einem VPN-Dienst kombiniert werden, sodass sich auch mobile Geräte

126 Raspberry Pi (raspberrypi.org), Banana Pi (banana-pi.org)
127 AKITA (akita.cloud) – Kickstarter 2017/18 (kickstarter.com/profile/akita/created)
128 Fingbox (fing.com/fingbox) – Indigogo 2017 (indiegogo.com/individuals/15294910/campaigns)
129 AdTrap – Kickstarter 2018 (kickstarter.com/profile/600284081/created)
130 ArmorVPN – Kickstarter 2018 (kickstarter.com/profile/armorvpn/created)
131 Bettiex – Kickstarter 2020 (kickstarter.com/profile/denisk/created)
132 Pi-hole (pi-hole.net) – Quellcode (github.com/pi-hole/pi-hole)

unterwegs schützen lassen. Durch die Einrichtung als DHCP-Server kann sogar das gesamte Netzwerk mit dem Pi-hole verwaltet werden. Über ein Web-Interface können Nutzer Statistiken zu Netzwerk-Nutzung und -Filterung einsehen, Filter-Listen verwalten und Einstellungen vornehmen. Seit Version fünf wird sogar eine Client-spezifische Filterung unterstützt. Das Projekt wird durch Spenden finanziert und der Source-Code steht frei zur Verfügung. Einzig für die nötige Hardware müssen Nutzer etwa 60 Euro bezahlen [116].

- **Syncloud**: Die *Syncloud*[133] ist ein persönlicher Server zum Betreiben eigener Webservices von Zuhause aus. Zu den angebotenen Diensten, die auf der Syncloud genutzt werden können, gehört u.A. das Blockieren von Werbung mit der Pi-hole Software. Des Weiteren werden ein eigener VPN-Server, File-Sharing sowie private Chats, Telefonie und Web-Meetings angeboten. Es kann sogar ein eigener Mailserver und ein eigenes soziales Netzwerk betrieben werden. Zusätzlich stehen neben dem Hosting für Webseiten und Blogs noch ein eigener Git-Server und die Synchronisation von privaten Notizen zur Verfügung. Da der Quellcode frei verfügbar ist, kann die Syncloud auf einer Vielzahl Linux-basierter Hardware, wie *Raspberry Pi* oder *Banana Pi* betrieben werden. Es gibt allerdings auch fertig vorkonfigurierte Geräte in verschieden Leistungsstufen, zwischen 120 und 320 britischen Pfund, zu kaufen [118].

- **upribox 3**: Die *upribox*, oder auch *Usable Privacy Box*[134], startete 2014 als studentisches Projekt der *FH St. Pölten* in Österreich. Es wurde von der Initiative *netidee* gefördert und gewann 2015 den *IPA netidee Sonderpreis* im Bereich Privacy. Als Hardware-Plattform kommt erneut ein *Raspberry Pi* zum Einsatz. Die upribox stellt eine Möglichkeit für mehr Privatsphäre im Internet dar. Die Inbetriebnahme soll schnell und unkompliziert sein, das Gerät wird einfach an den heimischen Internet-Router angeschlossen. Anschließend hat der Nutzer die Wahl zwischen „Silent“- und „Ninja“-Modus, der entweder Werbung und Tracking verhindert oder den Internetverkehr durch das TOR-Netzwerk anonymisiert. Eine fertige Box kostet 125 Euro, da diese aber nicht mehr verkauft wird, müssen Nutzer die Software auf einem Raspberry Pi selbst installieren (etwa 60 Euro einmalige Hardware-Kosten) [38].

- **FreedomBox**: Das Projekt *FreedomBox*[135] wurde 2010 von Eben Moglen, Professor für Recht an der *Columbia Law School* in New York und Gründer des *Software Freedom Law Center* (SFLC), ins Leben gerufen. Sein Ziel ist es, Nutzer in die Lage zu versetzen, die Kontrolle über die Infrastruktur des Internets zurück zu erlangen und Data-Mining, Überwachung und Zensur zu vermeiden. Die FreedomBox ist eine Art privater Server auf preiswerter Hardware, der mit „Open Source“-Software läuft. Als Funktionen stehen VPN-Server, Ad-Blocker, Hosts für Email, Videokonferenzen, Chats, Webseiten, Wikis oder Blogs, Kalender- und Kontakt-Synchronisation sowie Cloud- und Netzwerkspeicher zur Verfügung. Die Software lässt sich auf *Raspberry Pi*, *Orange Pi*, *BeagleBone Black*[136] und vielen weiteren Linux-basierten Boards in-

133 Syncloud Ltd. (syncloud.org) – Quellcode (github.com/syncloud/platform)
134 upribox (upribox.org) – Quellcode (github.com/usableprivacy/upribox), netidee (netidee.at)
135 FreedomBox (freedombox.org) – Quellcode (salsa.debian.org/freedombox-team/freedombox)
136 Orange Pi (orangepi.org), BeagleBone Black (beagleboard.org/black)

stallieren. Alternativ kann eine vorkonfigurierte Box des Herstellers *Olimex*[137] für 70 Euro erworben werden [127].

- **Anonymebox 3 Plus**: Die *Anonymebox*[138] ist ein Projekt des Raspberry Pi & Maker Shops *pi3g*, das einen anonymen Zugang zum Internet über TOR herstellt. Nutzer haben die Möglichkeit, ihre Internet-Kommunikation zu verschlüsseln und die eigene IP-Adresse jederzeit zu ändern. Die Installation und Nutzung soll einfach sein, sodass keine Computer- oder IT-Kenntnisse erforderlich sind. Die Anonymebox besteht aus einem *Raspberry Pi* mit einem zusätzlichen LAN-Adapter. Nach dem Anschluss der Anonymebox an den Router soll anonymes Surfen bereits möglich sein. Die Anonymebox 3 Plus kostet Nutzer einmalig 190 Euro, es ist allerdings auch möglich, die frei verfügbare Software eigenständig auf bereits vorhandener Hardware zu installieren. Es gibt einen Turbo-Modus, mit dem eine erhöhte Verbindungs-Geschwindigkeit über zwei VPN-Server möglich ist, der jedoch zusätzliche Kosten verursacht (zusätzlich 120 Euro pro Jahr) [9].

Nachdem Hardware-Lösungen für Privacy-Boxen aus unterschiedlichen Bereichen vorgestellt wurden, erfolgt im Anschluss ein Vergleich, um aus der Vielzahl an Produkten eine repräsentative Vorauswahl zu bestellen.

4.4 Repräsentative Vorauswahl

Wie anhand der vorgestellten Geräte deutlich wird, ist der Funktionsumfang von Privacy-Boxen sehr unterschiedlich. Für eine bessere Übersicht werden daher ähnliche Funktionen der Geräte gruppiert und anschließend in Tabelle 3 übersichtlich zusammengefasst.

4.4.1 Funktionen zum Selbstdatenschutz

Die ermittelten Selbstdatenschutz-Funktionen werden in sechs unterschiedliche Bereiche gruppiert: Die erste Gruppe betrifft den Bereich der Sicherheit, weshalb Funktionen wie *Anti-Virus*, *Firewall*, *IoT-Monitor* und *Passwort-Manager* dazu gehören (vgl. Tabelle 3).

Die zweite Gruppe betrifft den Schutz vor Tracking und ungewollten Inhalten sowie Methoden zur Anonymisierung. Aus diesem Grund werden die Funktionen *Inhaltsfilterung*, *Ad-Blocking* und *Anti-Tracking* einsortiert. Die Funktionen *DNS-Schutz*, *VPN-Tunnel* sowie *Privacy-Mesh* bzw. *TOR-Netzwerk* gehören ebenfalls dazu (vgl. Tabelle 3).

Die dritte Gruppe wiederum sammelt Funktionen, die Vertraulichkeit bieten, wie abhörsichere *Telefonie*, geschützte *Web-Meetings* sowie verschlüsselte *Chats* und *Emails*. Auch das Betreiben eines privaten *sozialen Netzwerks* wird zu dieser Gruppe gezählt (vgl. Tabelle 3).

In die vierte Gruppe werden Funktionen eingeordnet, die Alternativ-Dienste zu Anbietern mit kritischen Datenschutzpraktiken darstellen. Dazu gehören die Synchronisation von *Notizen*, Terminen (*Kalender*), Kontakten (*Adressbuch*) oder auch von Dateien (*Cloudspeicher*). Der Betrieb eigener Server für *Web-Hosting*, *Email*-Versand und Code-Verwaltung (*Git*) wird auch dazu gezählt (vgl. Tabelle 3).

137 Pioneer-FreedomBox (olimex.com/Products/OLinuXino/Home-Server/Pioneer-FreedomBox-HSK)
138 Anonymebox (anonymebox.com) – Quellcode (download.pi3g.com)

Bereich	Consumer-Produkte							Kickstarter/DIY-Produkte							
Kategorie	**Stationär**					**Portabel**		**Kickstarter**				**Open Source**			
Privacy-Box	Bitdefender BOX 2	F-Secure SENSE	TrutzBox Home	Winston Privacy Filter	RATtrap	Keezel 2.0	InvizBox Go	anonabox Pro	Relaxbox/Tarnomat	eBlocker 2	AKITA	Syncloud R	upribox 3	FreedomBox	Anonymebox 3 Plus
Anti-Virus	✓	✓	✓						(✓)						
Firewall	✓	✓	✓		✓	✓					(✓)				
IoT-Monitor	✓	✓									✓		✓		
Passwort-Man.		✓													
Inhaltsfilter	✓	✓	✓		✓					✓					
Ad-Blocker			(✓)	✓	✓	✓	✓		✓	✓		✓	✓	✓	
Anti-Tracking		✓	✓	✓	(✓)					✓		(✓)	✓		
DNS-Schutz			✓	✓	✓			✓	(✓)	✓		✓		✓	✓
VPN-Tunnel	✓	✓	✓			✓	✓	✓	✓	✓		✓	✓	✓	(✓)
Mesh/TOR				✓				✓		✓			✓	✓	✓
Sichere Email			✓												
Sichere Chats			✓									✓		✓	
Web-Meetings			✓									✓		✓	
Priv. Telefonie			✓									✓		✓	
Soz. Netzwerk												✓			
Notizen												✓			
Kalender														✓	
Adressbuch														✓	
Cloudspeicher								✓				✓		✓	
Web-Hosting								✓				✓		✓	
Email-Server			✓									✓		✓	
Git-Server												✓			
Open Source			✓				✓			✓		✓	✓	✓	✓
Dashboard			✓	✓			✓	✓	✓	✓		✓	✓	✓	✓
Mobile App	✓	✓			✓	✓	✓			(✓)	✓	(✓)			
Mobiler Schutz			(✓)			✓	✓			(✓)		(✓)	(✓)		
Router	✓	✓	✓							✓		✓	✓		
WLAN	✓	✓	(✓)			✓	✓	✓	✓		✓		✓	✓	✓
Kaufpreis in €	100	100	320	~130	~75	200	~85	~100	80	(60)	~110	~110	(60)	70	190
Abo-Preis in €	100	80	60	~100	~95	(60)	~70		90						(120)

Tabelle 3: Funktionen, Eigenschaften und Preise von Privacy-Boxen im Vergleich[139]

139 Die Ergebnisse beruhen ausschließlich auf Angaben von Herstellern oder Projekt-Dokumentationen, Einträge in Klammern treffen nur bedingt zu (unter Einschränkungen, Mehraufwand oder Mehrkosten), Preise mit ~ sind umgerechnet und gerundet von US Dollar (Kurs: 1,18) oder Pfund (Kurs: 1,10) zu Euro.

In der fünften Gruppe werden Eigenschaften aufgelistet, die Vertrauen und Transparenz, Art der Bedienung sowie Einsatzmöglichkeiten von Privacy-Boxen beschreiben. Für das Vertrauen wird die Eigenschaft des *„Open Source"-Code* verwendet. Die Bedienung der Geräte ist mithilfe von *Web-Dashboards* oder mobilen *Smartphone-Apps* möglich. Zuletzt bieten einige Geräte die Möglichkeit an, als eigenständiger *Router*, mit eigenem *WLAN*-Netzwerk oder sogar unterwegs (*Mobiler Schutz*) verwendet zu werden (vgl. Tabelle 3).

Die sechste und letzte Gruppe betrifft Kosten, die für Anschaffung und Betrieb der genannten Privacy-Boxen anfallen. Dies sind ausschlaggebende Kriterien für die Massentauglichkeit eines Produkts am Markt. Die einmaligen Anschaffungskosten (*Kaufpreis* für fertige Produkte) liegen, zwischen Extrema von 70 Euro (FreedomBox) und 320 Euro (TrutzBox), bei einem Durschnittspreis von etwa 130 Euro. Die laufenden Abonnement-Kosten (*Abo-Preis*) für die Anbindung an entsprechende Services der Hersteller belaufen sich auf durchschnittlich 90 Euro pro Jahr (vgl. Tabelle 3).

4.4.2 Auswahl von Geräten zur Bestellung

Um mithilfe dieser Übersicht eine repräsentative Vorauswahl aus den vorgestellten Produkten bestimmen zu können, werden einige Kriterien beachtet: Zum einen wird aus jeder der vorgestellten Produkt-Kategorien ein Gerät ausgewählt. Zum anderen muss eine gewisse Funktionalität gewährleistet sein, damit ein Vergleich vielfältige Ergebnisse liefern kann. Zuletzt muss das Gerät bestellbar sein und in Deutschland funktionieren, um im Rahmen einer Untersuchung eingesetzt werden zu können.

Da der *Winston Privacy Filter* nicht nach Deutschland geliefert wird und aufgrund fehlender Abdeckung der Mesh-Funktionalität dort auch nicht funktioniert, fällt er aus der ersten Produkt-Kategorie „Consumer (Stationär)" heraus. Aus der zweiten Kategorie „Consumer (Portabel)" wird aufgrund des geringeren Umfangs an Datenschutz-Funktionen das Produkt *InvizBox Go* ausgeschlossen. In der dritten Kategorie „Kickstarter" werden die Geräte *anonabox Pro*, *Relaxbox/Tarnomat* und *AKITA* aufgrund der geringen Anzahl an Funktionen nicht berücksichtigt. In der letzten Kategorie „Open Source" sind *upribox 3* und *Anomymebox 3 Plus* die am wenigsten interessanten Produkte für einen Vergleich, ebenfalls aufgrund der geringeren Funktionalität (vgl. Tabelle 3).

Somit bleiben acht Geräte als repräsentative Vorauswahl für die vorgestellten Privacy-Boxen übrig. Diese bilden die Grundlage in den folgenden Kapiteln und werden für diesen Zweck bestellt, bzw. die entsprechenden Komponenten für den Zusammenbau organisiert. Das bedeutet jedoch nicht, dass alle acht Geräte im Rahmen der Usability-Evaluierung untersucht werden. Abhängig von tatsächlicher Lieferbarkeit und -dauer können sich noch weitere Einschränkungen ergeben. Der begrenzte Zeitrahmen dieser Arbeit schränkt die Vorauswahl zusätzlich ein; es können nur ein, maximal zwei Paare vergleichbarer Geräte für die Untersuchung ausgewählt werden.

Im Anschluss folgt eine Darstellung der repräsentativen Vorauswahl von Privacy-Boxen. Diese wird in zwei Untergruppen aufgeteilt: Die erste Gruppe betrifft „Consumer-Produkte" (stationäre und *portable*). Die zweite Gruppe wird aus einer Vereinigung von *Kick-*

starter- und „Open Source“-Produkten gebildet. Zu den „Consumer-Produkten“ gehören: Bitdefender BOX 2, F-Secure SENSE, TrutzBox Home, RATtrap und *Keezel 2.0* (vgl. Abb. 14a–14e). Zu den *Kickstarter*- und „Open Source“-Produkten werden *eBlocker 2*, Syncloud R und FreedomBox gezählt (vgl. Abb. 14f–14h).

Consumer-Produkte (stationär und *portabel*)

(a) Bitdefender BOX 2 [15]

(b) F-Secure SENSE [64]

(c) TrutzBox Home [30]

(d) RATtrap [37]

(e) *Keezel 2.0* [103]

Kickstarter- und „Open Source“-Produkte

(f) *eBlocker 2* [50]

(g) Syncloud R [118]

(h) FreedomBox [127]

Abbildung 14: Repräsentative Vorauswahl von Privacy-Boxen

Nachdem mit diesen acht Geräten (vgl. Abb. 14) eine repräsentative Vorauswahl an Privacy-Boxen für die Bestellung definiert wurde, ist im folgenden Kapitel die Evaluations-Methodik der thematische Schwerpunkt. Mithilfe der Methodik kann im weiteren Verlauf die Usability einiger Privacy-Boxen aus dieser Vorauswahl untersucht und die Ergebnisse miteinander verglichen werden.

5 Evaluationsmethodik für Privacy-Boxen

Nach den Grundlagen zu Privacy-Boxen, einem Funktions-Katalog für Selbstdatenschutz und der repräsentativen Vorauswahl von Geräten, ist es Ziel dieses Kapitels die Methodik zu entwickeln, anhand derer die Privacy-Boxen untersucht und die Forschungsfragen beantwortet werden können. Zu Beginn werden die bisherigen Erkenntnisse zum Selbstdatenschutz mit Privacy-Boxen in ein Modell überführt, welches als Grundlage zur Entwicklung der Methodik verwendet wird. Nach einer Analyse der Zielgruppe folgt die Definition von Anwendungsszenarien, bevor die Evaluations-Methodik beschrieben wird.

5.1 Untersuchungsgegenstand

Zu Beginn der Erarbeitung einer Methodik für die Usability-Evaluation von Privacy-Boxen wird der Untersuchungsgegenstand noch weiter konkretisiert. Bezug nehmend auf die Definition aus Abschnitt 4.1.3 (Privacy durch Hardware), ist eine Privacy-Box ein elektronisches Gerät, welches maximale Privatheit bei der Nutzung des Internets bietet. Es geht im Folgenden darum, die Begriffe „maximale Privatheit“ und „Nutzung des Internets“ noch weiter zu präzisieren. Zuerst wird aus den bereits vorgestellten Funktionsbereichen von Privacy-Boxen ein Feature-Modell erstellt, mit dessen Hilfe eine Zuordnung von Selbstdatenschutz-Funktionen und -Werkzeugen möglich wird. *Feature* bedeutet so viel wie „Merkmal“[140], also beschreibt ein Feature-Modell alle wichtigen Merkmale eines bestimmten Gegenstands.

5.1.1 Feature-Modell von Privacy-Boxen

In Abschnitt 4.4.1 (Funktionen zum Selbstdatenschutz) wurden die ermittelten Funktionen von Privacy-Boxen zum Selbstdatenschutz bereits in unterschiedliche, zusammenhängende Gruppen sortiert. Diese Gruppen stellen unterschiedliche Bereiche dar, in denen Privacy-Boxen Nutzern einen Schutz bieten können und dienen als Grundlage für die Erstellung des Feature-Modells. Das Ziel des Modells ist es, aus den verschiedenen Bereichen und Funktionen des Selbstdatenschutzes mit Privacy-Boxen eine strukturierte Grundlage für die Entwicklung der Methodik zu schaffen.

Abb. 15 zeigt das Feature-Modell von Privacy-Boxen. Die fünf Bereiche werden dabei anhand der äußeren Beschriftungen den drei Grundpfeilern von Privacy-Boxen zugeordnet: 1. *Sicherheit* (dunkelrot), 2. *Privatheit* (rot und hellrot) und 3. *Benutzbarkeit* (schwarz). Dabei ist die farbliche Einteilung so gewählt, dass der zu untersuchende Bereich in schwarz und alle Bereiche mit Funktionen oder Eigenschaften von Privacy-Boxen in rot dargestellt werden.

Neben den fünf Bereichen besteht das Modell zusätzlich aus drei Ringen. Der innerste Ring definiert dabei das Selbstdatenschutz-Ziel des jeweiligen Bereichs (*Was* soll erreicht werden?). Der mittlere Ring beschreibt Auswirkungen für Situationen in denen Nutzer das Ziel erreichen wollen (*Wann* oder *warum* soll das Ziel erreicht werden?). Der äußere Ring hingegen enthält konkrete Funktionen oder Eigenschaften, mit deren Umsetzung das Ziel des Bereichs erreicht werden kann (*Wie* soll das Ziel erreicht werden?).

140 Feature, Übersetzung Englisch-Deutsch (de.langenscheidt.com/englisch-deutsch/feature)

Die *Sicherheit* ist ein wichtiger Grundpfeiler von Privacy-Boxen und bestimmt den ersten Bereich des Modells (vgl. Abb. 15 dunkel-roter Abschnitt). Obwohl sie nicht das primäre Ziel einer Privacy-Box darstellt, gilt Sicherheit doch als wichtige, *präventive* Maßnahme zum Selbstdatenschutz. Sie schützt z.B. vor Missbrauch oder Diebstahl von PD durch Dritte. Das Ziel des Bereichs „Sicherheit“ ist der Aufbau eines privaten IT-Sicherheitsmanagements. Dieser *IT-Schutz* dient dem Erkennen von Schwachstellen und dem Verhindern von Gefahren durch Schutz-Funktionen wie *Anti-Virus*, *Firewall* und *IoT-Monitor*. Zusätzlich stärkt die Verwendung eines *Passwort-Managers* die Sicherheit des Nutzers und *Open Source* Code schafft Transparenz und Vertrauen in das Gerät bzw. den Hersteller.

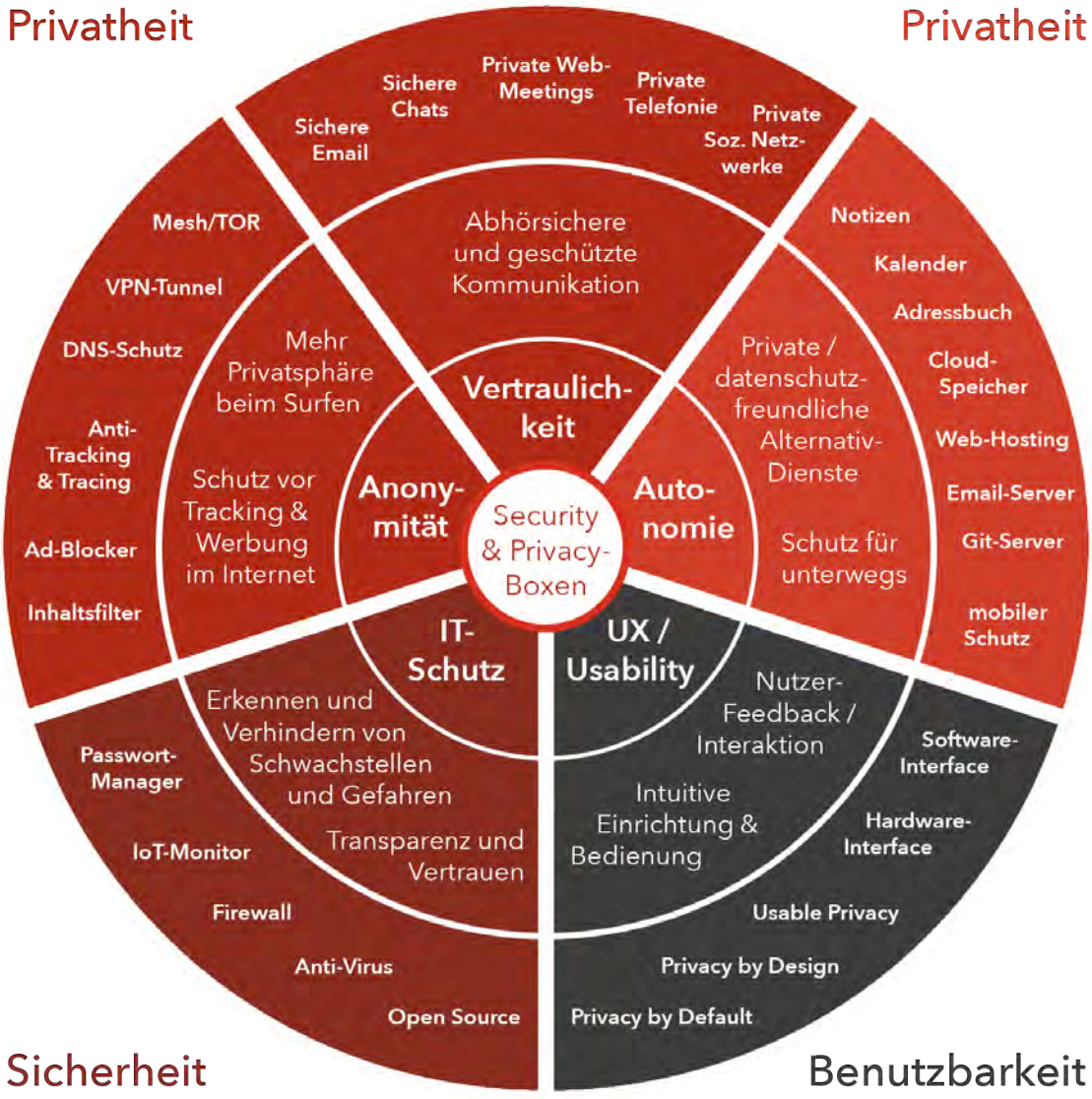


Abbildung 15: Feature-Modell von Privacy-Boxen[141]

Die *Privatheit* ist der zweite und wichtigste Grundpfeiler von Privacy-Boxen und bestimmt den zweiten, dritten und vierten Bereich des Modells (vgl. Abb. 15 rote und hell-rote Abschnitte). Die Privatheit ist das Hauptziel einer Privacy-Box und lässt sich zusätzlich in *operative* (rote) und *reaktive* (hell-rote) Anwendungsbereiche unterteilen.

141 Das Modell ist inspiriert von den *TrutzFunktionen* der *Trutzbox* (trutzbox.de/trutzfunktionen)

Die *operativen* Bereiche (vgl. Abb. 15 rote Abschnitte) werden von aktiven Selbstdatenschutz-Maßnahmen bestimmt, die während der Nutzung des Internets angewendet werden. Anonymität als „Dimensionen der Privatheit“ (siehe „Dimensionen der Privatheit“ in Abschnitt 2.1.1) und Vertraulichkeit stellen die Ziele der beiden operativen Bereiche dar.

Anonymität bietet Nutzern mehr Privatsphäre beim Surfen sowie Schutz vor OBA und ungewolltem Tracking und Tracing im Internet. Dieser Schutz kann mithilfe von *Inhaltsfiltern*, *Ad-Blockern* und Methoden für *Anti-Tracking & Tracing* realisiert werden, bzw. lässt sich durch den Einsatz von *DNS-Schutz*, *VPN-Tunneln* oder *Mesh/TOR*-Netzwerken noch steigern.

Vertraulichkeit hingegen bietet abhörsichere und *geschützte Kommunikation*, zwischen mehreren Teilnehmern, was einer „Funktion der Privatheit“ (siehe „Funktionen der Privatheit“ in Abschnitt 2.1.1) entspricht. Vertraulichkeit wird durch verschlüsselte *Chats* und *Emails*, private *Web-Meetings* und *Telefonie* sowie den Austausch von Nachrichten und Inhalten in selbst betriebenen, *privaten Sozialen Netzwerken* ermöglicht.

Der *reaktive* Bereich der Privatheit (vgl. Abb. 15 hell-roter Abschnitt) betrifft Selbstdatenschutz-Maßnahmen, die häufig erst eingesetzt werden, nachdem bereits eine Nutzung erfolgt ist (z.B. durch den Wechsel von Google-Mail zu einem selbst betriebenen Mail-Dienst). *Autonomie* stellt als weitere „Funktion der Privatheit“ (siehe „Funktionen der Privatheit“ in Abschnitt 2.1.1) das Ziel dieses Bereichs dar. Autonomie ermöglicht Nutzern die Unabhängigkeit von den Diensten großer Unternehmen die u.U. kritische Datenschutzpraktiken verfolgen. Die Nutzung privater Alternativ-Dienste für die Synchronisation von *Notizen*, *Kalendern* und *Adressbüchern* trägt zur Autonomie bei. Auch das private Betreiben von *Cloudspeichern*, *Web-Hostings* und Servern für *Email* und Code-Verwaltung (*Git*) gehören dazu. Zusätzlich bietet ein *mobiler Schutz* für Unterwegs dem Nutzer zusätzliche Autonomie bei der Anwendung von Selbstdatenschutz.

Die *Benutzbarkeit* macht den letzten Grundpfeiler von Privacy-Boxen aus (vgl. Abb. 15 schwarzer Abschnitt). Eine gute *UX/Usability* gilt als Ziel dieses Bereichs, denn eine intuitive Einrichtung und einfache Bedienbarkeit sind der Schlüssel zum erfolgreichen Selbstdatenschutz. *Usable Privacy*, *Privacy by Design* und *Privacy by Default* sind Gestaltungsansätze, die zu einer guten Usability beitragen können (siehe „Privatheit als Standard und Voreinstellung“ in Abschnitt 2.4.4). Die genannten Faktoren betreffen die Gestaltung der von Privacy-Boxen bereitgestellten Kanäle für Nutzer-Interaktion und -Feedback. Diese können sowohl in Form von *Software-* als auch *Hardware-Interfaces* realisiert sein.

Die Zuordnung von Eigenschaften und Funktionen zu den fünf Bereichen des Feature-Modells ist jedoch nicht exklusiv, d.h. Funktionen können sowohl in anderen als auch mehreren Bereichen des Modells Anwendung finden.

Anhand des Feature-Modells lässt sich Selbstdatenschutz mit Privacy-Boxen durch die zugehörigen Eigenschaften und Funktionen sehr anschaulich beschreiben. Damit ist der Untersuchungsgegenstand ausreichend definiert, sodass im nächsten Schritt die Begriffe von „maximaler Privatheit“ bzw. „maximalem Schutz“ noch weiter spezifiziert werden können.

5.1.2 Maximaler Schutz mit Privacy-Boxen

Der „maximale Schutz“, welcher für Nutzer mithilfe von Privacy-Boxen möglich ist, kann als die höchste Übereinstimmung mit den durch Privacy-Boxen realisierbaren Privacy-Werkzeugen beschrieben werden (vgl. Tabelle 2 „Realisierbarkeit von Selbstdatenschutz-Werkzeugen mit Privacy-Boxen“). Um diese Übereinstimmung zu ermitteln, folgt eine Zuordnung von Werkzeugen und Funktionen zum Selbstdatenschutz. Der Vergleich von möglichen Werkzeugen (siehe „Werkzeuge zum Selbstdatenschutz“ in Abschnitt 4.2) mit in Privacy-Boxen verfügbaren Funktionen (siehe „Funktionen zum Selbstdatenschutz“ in Abschnitt 4.4.1) erfolgt anhand des Feature-Modells (vgl. Abb. 15). Zusätzlich wird der erstellte Werkzeug-Katalog dabei validiert bzw. auf Vollständigkeit überprüft.

Im ersten Bereich (vgl. „IT-Schutz“ in Abb. 15) wird deutlich, dass die Funktionen *Anti-Virus*, *Firewall* und *IoT-Monitor* noch nicht vom Werkzeug-Katalog abgedeckt werden. Da Schwachstellen in der Sicherheit automatisch zur Folge haben, dass auch die Privatheit gefährdet ist, müssen diese Punkte berücksichtigt werden. Die drei genannten Funktionen passen am besten zu Werkzeug 3 (Erkennen von Schwachstellen und Gefahren). Durch eine Umformulierung zu „Erkennen von Schwachstellen und Verhindern von Gefahren“ lässt sich das Werkzeug entsprechend anpassen. Die Funktion des *Passwort-Managers* passt eindeutig zu Werkzeug 4 (Erstellen und Verwenden sicherer Passwörter). Die Eigenschaft des *Open Source Code* wird häufig verwendet, um beim Nutzer durch Transparenz Vertrauen in das Produkt zu schaffen, und lässt sich am ehesten als Parallele zu Werkzeug 3 (Erkennen von Schwachstellen und Gefahren) sehen. Die Einführung von *„Vertrauen in Produkt und Anbieter“* als wichtige Eigenschaft (E1) von Privacy-Boxen erscheint jedoch passender.

Der zweite Bereich (vgl. „Anomymität“ in Abb. 15) zeigt mit der Funktion *Inhaltsfilter*, einen weiteren Punkt auf, der im Werkzeug-Katalog noch nicht berücksichtigt wird. Die Parallelen zu Werkzeug 5 (Datenschutzkritische Dienste vermeiden) lassen sich durch eine Umformulierung zu „(Datenschutz-) Kritische Dienste und Inhalte vermeiden“ allerdings zunutze machen. Die Funktionen *Ad-Blocker* und *Anti-Tracking* werden eindeutig von Werkzeug 7 (Verwenden von Blocker-Software) beschrieben. Werkzeug 8 (Device-Fingerprinting verhindern) und Werkzeug 9 (Löschen von Sessions und Cookies) passen ebenfalls dazu. Die Formulierung von Werkzeug 9 muss für die Einordnung jedoch zu „Löschen von Sessions und Blockieren von Cookies“ angepasst werden. Die Funktionen *DNS-Schutz*, *VPN-Tunnel* und *Mesh/TOR* passen gut zu Werkzeug 11 (Sichere DNS und VPN-Dienste nutzen).

Im dritten Bereich (vgl. „Vertraulichkeit“ in Abb. 15) betreffen die Funktionen *Sichere Email*, *Sichere Chats*, *Private Web-Meetings* und *Private Telefonie* den Einsatz geschützter und vertraulicher Kommunikation. Sie lassen sich daher in Werkzeug 14 (Chats, Emails und Telefonie verschlüsseln) wiederfinden. Die Funktion *Privates Soziales Netzwerk* passt ebenfalls dazu, kann allerdings auch zu Werkzeug 16 (Umstieg auf datenschutzfreundliche Dienste) eingeordnet werden.

Der vierte Bereich (vgl. „Autonomie“ in Abb. 15) beinhaltet Funktionen die zur Synchronisation von privaten und persönlichen Daten (PD) wie *Notizen*, *Kalender* und *Adressbuch* genutzt werden können. Das Betreiben privater Instanzen von Diensten wie *Cloudspeicher*,

Web-Hosting, *Email-Server* und *Git-Server* sorgt ebenfalls für Schutz und Privatheit von Nutzerdaten. Die genannten Werkzeuge dieses Bereichs lassen sich somit alle Werkzeug 16 (Umstieg auf datenschutzfreundliche Dienste) zuordnen. Der Punkt *Mobiler Schutz* betrifft jedoch eine weitere, noch nicht berücksichtigte Eigenschaft: Es beschreibt die Möglichkeit für Nutzer, sich auch unterwegs vor ungewollten Eingriffen in die Privatsphäre zu schützen. Als *„Mobiler Schutz für unterwegs“* lässt sich dieser Punkt in eine wichtige Eigenschaft (E2) von Privacy-Boxen überführen.

Der letzte Bereich (vgl. „UX/Usability“ in Abb. 15) beinhaltet Eigenschaften von Privacy-Boxen und Design-Prinzipien mit denen eine gute Benutzbarkeit erreicht werden kann. Die Kanäle für Interaktion und Feedback zwischen Nutzer und Privacy-Box, die für Einrichtung, Konfiguration und Überwachung des Geräts zur Verfügung stehen, können mittels Software- und Hardware-Interfaces realisiert sein. Daraus ergibt sich mit *„Interfaces für Interaktion und -Feedback“* eine neue wichtige Eigenschaft (E3) für Privacy-Boxen. Die Gestaltung der Hardware entscheidet zuletzt in welchen Betriebs-Modi eine Privacy-Box eingesetzt werden kann: Neben dem Einsatz als vollwertiger Router, bieten manche Geräte nur die Integration in ein bestehendes Netzwerk, wohingegen andere Geräte ein eigenes, geschütztes Netzwerk aufbauen können. Aus diesem Grund lässt sich mit *„Schnittstellen und Konnektivität“* eine weitere wichtige Eigenschaft (E4) von Privacy-Boxen definieren.

Die Zuordnung von Selbstdatenschutz-Werkzeugen und -Funktionen von Privacy-Boxen wird im Folgenden nochmal übersichtlich zusammengefasst. Alle Werkzeuge, die im Rahmen der Zuordnung einer Anpassung bedurften, sind im Folgenden mit einem Stern (*) gekennzeichnet. Alle sechs der mit Privacy-Hardware vollständig realisierbaren Selbstdatenschutz-Werkzeuge (vgl. Tabelle 2 – Spalte „ja“) lassen sich auch in Form von Funktionen bei Privacy-Boxen wieder finden:

- Werkzeug 4 – Erstellen und Verwenden sicherer Passwörter
- Werkzeug 7 – Verwenden von Blocker-Software
- Werkzeug 8 – Device-Fingerprinting verhindern
- Werkzeug 11 – Sichere DNS und VPN-Dienste nutzen
- Werkzeug 13 – Transport-Verschlüsselung verwenden
- Werkzeug 14 – Chats, Emails und Telefonie verschlüsseln

Von den mit Privacy-Hardware nur eingeschränkt anwendbaren Selbstdatenschutz-Werkzeugen (vgl. Tabelle 2 – Spalte „teils“) wird mit drei von sechs Werkzeugen die Hälfte durch Funktionen bei Privacy-Boxen abgedeckt (zwei Werkzeuge jedoch nur durch Anpassung):

- Werkzeug 3* – Erkennen von Schwachstellen und Verhindern von Gefahren
- Werkzeug 9* – Löschen von Sessions und Blockieren von Cookies
- Werkzeug 16 – Umstieg auf datenschutzfreundliche Dienste

Sogar von den acht mit Privacy-Hardware nicht umsetzbaren Selbstdatenschutz-Werkzeugen (vgl. Tabelle 2 – Spalte „nein“) kann durch Anpassung ein Werkzeug von Privacy-Boxen (zumindest teilweise) realisiert werden:

- Werkzeug 5* – (Datenschutz-) Kritische Dienste und Inhalte vermeiden

Des Weiteren wird deutlich, dass es neben den Werkzeugen vier wichtige Eigenschaften von Privacy-Boxen gibt, die zur Qualität und Umsetzbarkeit des Selbstdatenschutzes beitragen:

1. Vertrauen in Produkt und Anbieter
2. Mobiler Schutz für unterwegs
3. Interfaces für Interaktion und -Feedback
4. Schnittstellen und Konnektivität

Mit dieser Übersicht an Werkzeugen und Eigenschaften von Privacy-Boxen zum Selbstdatenschutz ist die Definition von „maximalem Schutz“ ausreichend spezifiziert. Er vereint sowohl die „maximale Privatheit“ als auch die „maximale Sicherheit“ miteinander, die durch den Einsatz von Privacy-Boxen möglich ist. Im folgenden Abschnitt wird die Zielgruppe von Privacy-Boxen analysiert, um typische Anwendungsszenarien bestimmen zu können, anhand derer sich geeignete Geräte für die Untersuchung auswählen lassen.

5.2 Zielgruppendefinition

Um die Zielgruppe von Privacy-Boxen bestimmen zu können, ist es notwendig die Unterschiede an Wissen, Erfahrung und Motivation von Nutzern im Bezug auf Sicherheit und Privatheit zu kennen und zu verstehen. Hierfür wird auf die Methode *Personas* zurückgegriffen: „Personas sind fiktive, aber auf empirischen Informationen beruhende, Nutzerbeschreibungen. Die Beschreibungen repräsentieren reale Verhaltensweisen, Aufgaben und Ziele der Nutzergruppen.“ [108, S. 18]. Nach einer Vorstellung verschiedener Nutzertypen wird anschließend ermittelt, welche Geräte aus der Vorauswahl für sie geeignet sind.

5.2.1 Datenschutz-Nutzertypen (Personas)

Die Arbeiten zu wissenschaftlichen Personas im Bereich der Privatheit reichen zurück bis in die späten 70er Jahre. Der Politologe Alan F. Westin, Autor der *„Vier Formen des Privaten“* (siehe „Dimensionen der Privatheit“ in Abschnitt 2.1.1), führte zwischen den Jahren 1978 und 2004 über 30 Umfragen zum Thema Privatheit durch [109, S. 3]. Im Report der *„Harris-Equifax Consumer Privacy Survey“* von 1991 wurde von Westin eine Einteilung in drei unterschiedliche Nutzer-Kategorien ermittelt [109, S. 5]:

1. Die Datenschutz-Fundamentalisten
2. Die Pragmatiker
3. Die Unbekümmerten

Dabei machen die *Pragmatiker* mit durchschnittlichen Bedenken den Großteil der Befragten aus (57%), gefolgt von den *Datenschutz-Fundamentalisten* mit hohen Bedenken (25%) und den *Unbekümmerten* mit geringen Bedenken zum Datenschutz (18%). Die Bewertung erfolgte anhand von vier Fragen zum Datenschutz-Bewusstsein [109, S. 5].

In der Arbeit *„Privacy Personas: Clustering Users via Attitudes and Behaviors toward Security Practices“* (2016) von Dupree et al. wird diese Einteilung nochmals verfeinert. Die Kategorie der „Pragmatiker“ wird in die Rollen der *Faulen Experten*, der *Selbstausgebildeten Techniker* und der *Amateure* unterteilt. Die „Datenschutz-Fundamentalisten“ finden

sich als *Fundamentalisten* wieder und die „Unbekümmerten“ werden als *Geringfügig Besorgte* bezeichnet [43, S. 5233]. Die Ergebnisse der Befragung von über 200 Teilnehmern spiegeln deutlich Westin's Ergebnisse wider (bewertet nach den ursprünglichen Fragen und Kategorien): 58% wurden als „Pragmatiker“, 26% als „Fundamentalisten“, und 16% als „Geringfügig Besorgte“ eingestuft [43, S. 5234].

Der ursprüngliche Fragen-Katalog von Westin wurde für die Bewertung der Nutzertypen von Dupree et al. jedoch stark erweitert: Die Teilnehmer mussten aus insgesamt 16 Themenbereichen Fragen zu aktuellen Sicherheits- und Datenschutz-Aspekten beantworten. Wie in Abb. 16 zu sehen ist, machen die „Fundamentalisten“ mit nur 3% einen verschwindend geringen Anteil aus, wohingegen die „Amateure“ mit 34% den größten Anteil ausmachen. Danach folgen mit vergleichbar großen Anteilen die „Geringfügig Besorgten“ mit 23%, die „Faulen Experten“ mit 22% und die „Techniker“ mit 18% (vgl. Abb. 16).

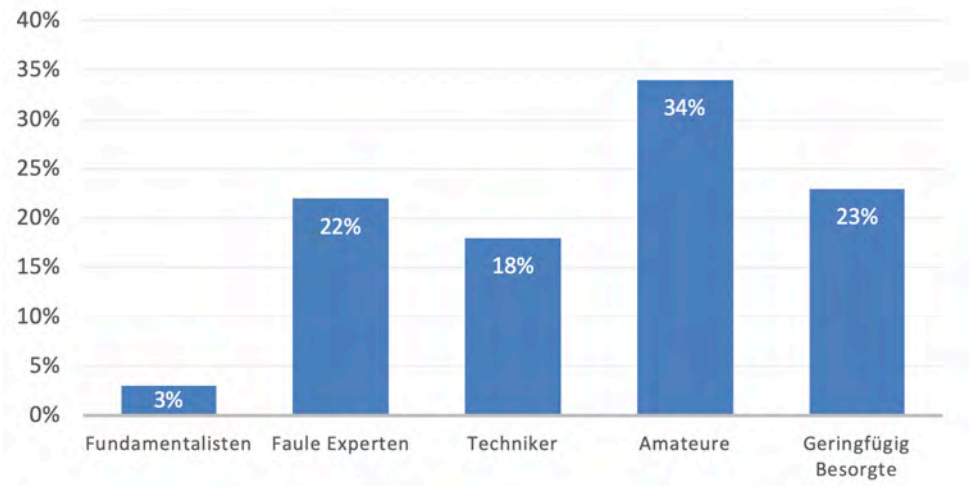


Abbildung 16: Verteilung verschiedener Nutzertypen (übersetzt nach [43, S. 5235])

Die fünf unterschiedlichen Nutzertypen werden dabei von Dupree et al. wie folgt definiert:

1. **Fundamentalisten** *(viel Wissen, hohe Motivation)*: Sie haben wenig oder kein Vertrauen in Sicherheitstechnologien und achten sorgfältig auf Sicherheitsindikatoren von Webseiten, die sie besuchen. Ihre Passwortschemata sind mehrschichtig und wichtige Passwörter einzigartig. Der angewendete Schutz geht über den Computer hinaus, zum Beispiel durch Verschlüsselung externer Speichergeräte. Sie sind sehr besorgt um ihre Privatsphäre, verweigern u.U. die Anmeldung bei datenschutzkritischen Diensten und verabscheuen die Überwachung durch Tracking. Mit der fortgeschrittenen Kenntnis über Sicherheits-Themen und entsprechende Software-Tools benötigen sie fein-granulare Einstellungs-Möglichkeiten. Sie helfen anderen nur widerwillig und betrachten diese als ungebildet und unsicher [43, S. 5233].

2. **Faule Experten** *(viel Wissen, geringe Motivation)*: Sie sind sachkundig und wählen Bequemlichkeit vor Sicherheit sowie Geselligkeit vor Privatsphäre. Sie rechtfertigen ihre Untätigkeit mit dem Glauben, dass sie kein Angriffsziel darstellen. Sie ergreifen allerdings bestimmte Maßnahmen, um sich selbst zu schützen: Ihre Passwortschemata sind vielschichtig, sie schreiben Passwörter gar nicht oder nur sicher auf und teilen diese

lediglich mit vertrauenswürdigen Personen. Alle Informationen, die sie online stellen, bewerten sie als für die Öffentlichkeit geeignet. Sie verfügen zwar über fortgeschrittene Fähigkeiten beim Einsatz von Schutz-Software, nutzen diese Fähigkeit jedoch, um den Interaktionsbedarf mit Sicherheits-Themen zu minimieren. Sie sind hilfsbereiter als Fundamentalisten, da sie die Bemühungen anderer positiv beurteilen [43, S. 5234].

3. **Techniker** *(mittleres Wissen, hohe Motivation)*: Techniker sind zwar hoch motiviert, haben aber weniger Wissen als die „faulen Experten“ und „Fundamentalisten“. Sie lesen Online-Nachrichten und Blogs, um sich über Sicherheits-Themen zu informieren und versuchen, Informationen zu verstehen, bevor sie nach ihnen handeln. Sie haben ein begrenztes Vertrauen in die Privatsphäre-Einstellungen von sozialen Netzwerken (wie z.B. Facebook). Sie sind daher passive Nutzer und ziehen die Privatsphäre der sozialen Online-Präsenz vor. Ihre Passwörter sind schwächer als die der „faulen Experten“ oder „Fundamentalisten“ und basieren, obwohl sie einzigartig und persönlich sind, zumeist auf einer einheitlichen Grundlage. Techniker haben zwar Bedenken hinsichtlich ihrer Sicherheit (z.B. Angriffe oder Viren), diese können aber auch aufgeschoben oder vergessen werden. Techniker sind zwar bereit, ihr Verhalten zu ändern, wenn ihnen genügend Information zur Verfügung gestellt wird, aber sie neigen dazu, lieber ihrer Intuition zu vertrauen [43, S. 5234].

4. **Amateure** *(mittleres Wissen, mittlere Motivation)*: Sie beginnen damit, sich über Sicherheitskonzepte zu informieren, aber die Herausforderung besteht darin, dass sie nicht ausreichend motiviert und/oder sachkundig genug sind, um gute von schlechten Ratschlägen zu unterscheiden. Daher nehmen sie u.U. Änderungen an ihren Praktiken vor, die auf schwachen oder ungenauen Ratschlägen beruhen. Obwohl sie nur begrenzt motiviert sind, benutzen sie einige Software-Tools zum Schutz ihrer Sicherheit, wie z.B. Virenschutz, Firewall oder Werbeblocker. Sie vertrauen den drahtlosen Netzwerken die sie benutzen, auch wenn sie diese nicht selbst verwalten. Informationen, die sie online preisgeben, unterliegen gewissen Beschränkungen und ihre verwendeten Passwörter sind in der Regel mehrschichtig bei mittlerer bis starker Sicherheit. Trotz geringer Motivation sind sie, wie die Techniker auch, bereit sich selbst zu schützen, wenn Ihnen ausreichend Information zur Verfügung gestellt wird. Sie betrachten andere, im Vergleich zu sich selbst, als etwas weniger sicher und gebildet [43, S. 5234].

5. **Geringfügig Besorgte** *(wenig Wissen, geringe Motivation)*: Sie verfügen nur über begrenzte Kenntnisse von Sicherheitskonzepten und ihr Wissen entspringt Mundpropaganda oder anderen informellen Quellen. Sie vertrauen drahtlosen Netzwerken und Webseiten, die vorgeben, sicher zu sein. Sie mögen Fallback-Authentifizierung (z.B. Passwort-Wiederherstellung per Email) und Anti-Virus-Lösungen sind der einzige bekannte Software-Schutz. Sie haben nur einen kleinen Satz an Passwörtern, von denen eines stark favorisiert wird. Änderungen werden nur aufgrund von externen Auslösern vorgenommen z.B. durch strengere Passwortrichtlinien. Sie wissen, dass es Bedrohungen gibt, machen sich aber keine Sorgen darüber. Sie halten es für unwahrscheinlich, dass ihnen etwas passiert und sind daher nicht motiviert, mehr für die Sicherheit zu tun oder darüber zu lernen [43, S. 5234].

Nach der Vorstellung verschiedener Nutzertypen mit unterschiedlichem Datenschutz- und Sicherheits-Bewusstsein, werden anschließend die Nutzertypen ermittelt, welche bei der Verwendung von Privacy-Boxen besonders auf eine gute Usability angewiesen sind.

5.2.2 Zielgruppe für Privacy-Boxen

Um die Relevanz von Usability bei Privacy-Boxen für die vorgestellten Nutzertypen zu bewerten, wird zusätzlich die Arbeit von Rudolph et al. *„Usable Specification of Security and Privacy Demands: Matching User Types to Specification Paradigms“* (2019) zu Hilfe genommen. In der Arbeit geht es um die Zuordnung verschiedener Spezifikationsparadigmen für Datenschutzeinstellungen von Privacy Dashboards zu den bereits vorgestellten Nutzertypen. Hierfür werden die fünf Nutzertypen von Dupree et al. in einer Übersicht den Eigenschaften „Wissen“ und „Motivation“ entsprechend eingeordnet. Die Benennung der Nutzertypen wird bis auf die Rolle des „Amateurs“ beibehalten, welcher als *Bemühter Amateur* bezeichnet wird (vgl. Abb. 17).

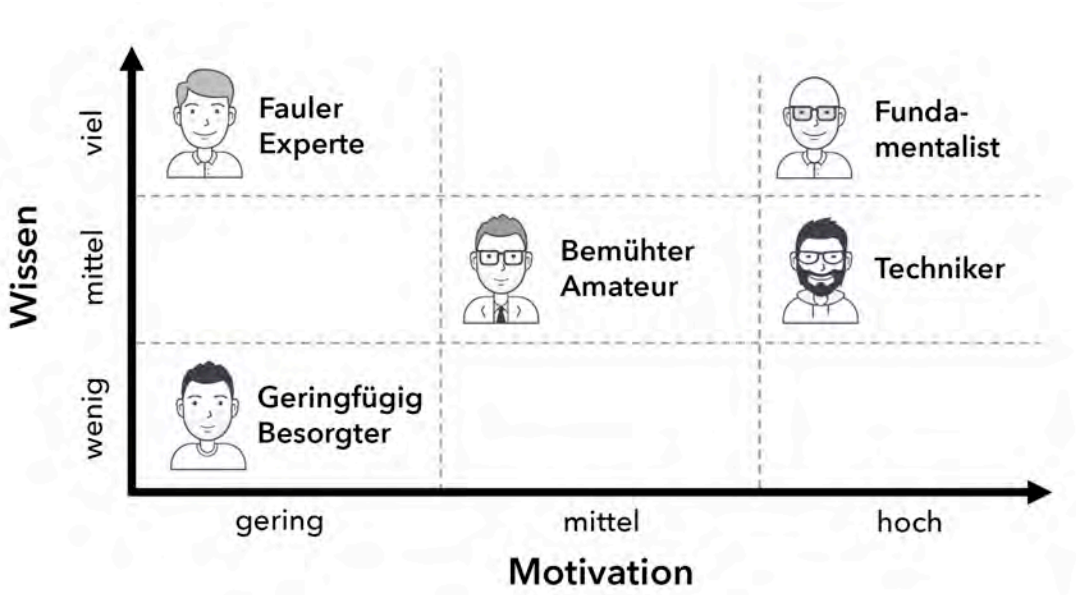


Abbildung 17: Wissen und Motivation der fünf Nutzertypen (übersetzt nach [143, S. 251])

Unter Berücksichtigung der Typenbeschreibung von Dupree et al. mangelt es sowohl den *Geringfügig Besorgten* als auch den *Faulen Experten* an Motivation, um sich mit Sicherheits- und Datenschutz-Themen auseinanderzusetzen. Selbstdatenschutz ist für sie von geringem Interesse, da ihnen entweder das Bewusstsein über die Risiken fehlt oder diese aus Bequemlichkeit in Kauf genommen werden. Somit lässt sich schlussfolgern, dass ihnen die Bereitschaft fehlen wird, Geld für den Erwerb einer Privacy-Box auszugeben sowie den Aufwand für deren Anschluss und Einrichtung zu investieren. Für Nutzer beider Gruppen sind Privacy-Boxen daher von geringem Interesse, ebenso deren Usability-Eigenschaften.

Die *Fundamentalisten* im Gegensatz dazu, sind aufgrund ihrer intrinsischen Motivation und dem daraus resultierenden Know-How ohnehin Experten auf den Gebieten Sicherheit und Datenschutz. Da ihnen das Vertrauen in Sicherheitstechnologien schwer fällt, ist anzunehmen, dass auch die Anschaffung einer Privacy-Box einer gewissen Skepsis unterliegt. Durch

den Wunsch nach fein-granularen Einstellungs-Möglichkeiten, spielt eine gute Usability bei Privacy-Boxen für sie keine große Rolle. Aufgrund ihrer Erfahrung beherrschen sie sowohl die Einrichtung von komplexen Systemen, als auch den individuellen Schutz verschiedener Endgeräte. Privacy-Boxen können für *Fundamentalisten* zwar von Interesse sein, jedoch spielt die Usability für sie keine entscheidende Rolle.

Es bleiben daher noch die *Bemühten Amateure* und die *Techniker* übrig, welche beide über ein mittleres Verständnis von Sicherheits- und Datenschutz-Themen verfügen. Sie haben das notwendige Bewusstsein über Risiken und Gefahren und möchten den Schutz ihrer Sicherheit und Privatheit verbessern. Aufgrund ihres begrenzten Wissens sind Privacy-Boxen ein geeignetes Mittel, um dieses Ziel zu erreichen. Eine gute Usability bei der Einrichtung und Verwendung ist allerdings von großer Wichtigkeit: Abhängig von der jeweiligen Motivation des Nutzers kann die Usability von Privacy-Boxen über den Erfolg bei der Anwendung von Selbstdatenschutz entscheiden (vgl. Abb. 11 „Intentionsmodell“ in Abschnitt 3.3.4)

Die *Bemühten Amateure* sind, aufgrund ihrer mittleren Motivation, auf fertige Produkte von Herstellern am Markt angewiesen. Eine Privacy-Box muss für sie demnach „Plug-and-Play“-Eigenschaften besitzen, sich also ohne große technische Hürden anschließen und einrichten lassen. Die *Techniker* wiederum haben durch ihre erhöhte Motivation den Vorteil, sich ein gewisses technisches Know-how anzueignen. Damit steht ihnen die Möglichkeit offen, sich mithilfe von Anleitungen und „Open Source“-Projekten auch Privacy-Boxen selbst zu bauen und diese zu betreiben. Zusätzlich können sie sich so den Wunsch nach Erweiterbarkeit oder Anpassbarkeit ihrer Privacy-Boxen erfüllen – entweder durch Eigeninitiative oder mithilfe einer aktiven DIY-Community.

Es lässt sich also zeigen, dass die beiden Nutzertypen „Bemühte Amateure“ und „Techniker“ den größten Mehrwert von Privacy-Boxen haben: Sie können dem Wunsch nach Selbstdatenschutz, trotz ihres mittleren Wissens-Niveaus über Sicherheit und Privatheit, nachkommen. Aus diesem Grund werden die Nutzer beider Gruppen als Zielgruppe für Privacy-Boxen definiert. Unter Berücksichtigung der Verteilung von Nutzertypen (vgl. Abb. 17) zeigt sich, dass *Bemühte Amateure* mit 34% den größten Anteil an Nutzern ausmachen, wohingegen *Techniker* mit 18% einen deutlich kleineren Teil darstellen. Nimmt man die Anzahl beider Nutzergruppen jedoch zusammen, so ergibt sich mit 52% eine Zielgruppe für Privacy-Boxen, die mehr als die Hälfte aller Nutzer ausmacht. Das Ergebnis der Nutzerzugehörigkeit von Dupree et al. wurde auch von Rudolph et al. nochmals bestätigt: Die Aufteilung der Nutzertypen bei 61 Befragten zeigte sich fast identisch [143, S. 253].

Mithilfe der Zielgruppe lässt sich die Relevanz der Usability von Privacy-Boxen als entscheidender Faktor darstellen: Damit Nutzer der Zielgruppe Selbstdatenschutz mit Privacy-Boxen effektiv, effizient und zufriedenstellend umsetzen können, muss ihre Motivation mögliche Hindernisse bei Einrichtung und Nutzung überwiegen können. Dafür ist eine gute Benutzbarkeit der Geräte notwendig, was bei Privacy-Boxen die Kanäle der Interaktion und des Feedbacks zwischen Nutzer und Gerät betrifft. Die *Bemühten Amateure* sind dabei auf Produkte aus dem Consumer-Bereich angewiesen, wohingegen *Techniker* zusätzlich Produkte aus dem Kickstarter- und DIY-Bereich nutzen können.

Da keine Methodik zur Bewertung und zum Vergleich der Usability von Privacy-Boxen gefunden werden konnte, können die Geräte der repräsentierten Vorauswahl nicht anhand eines vorgegebenen Bewertungsschemas klassifiziert werden. Daher wird im Rahmen dieser Arbeit zunächst ein vereinfachter Ansatz gewählt, indem ähnliche Privacy-Boxen miteinander verglichen werden. Das Ziel ist es, diesen Ansatz mithilfe von häufigen Nutzerszenarien so zu erweitern, dass eine Gewichtung von Funktionen möglich wird, die für den Selbstdatenschutz besonders relevant sind. So lässt sich ein erster Maßstab entwickeln, mithilfe dessen die Benutzbarkeit von Privacy-Boxen untereinander verglichen werden kann.

Da sich die Anforderungen der zwei identifizierten Nutzertypen an die Privacy-Boxen jedoch unterscheiden können, wird im nächsten Schritt überprüft, ob die bisherige Zuordnung nach Produkt-Kategorien der bestellten Privacy-Boxen (siehe „Auswahl von Geräten zur Bestellung“ in Abschnitt 4.4.2) noch valide ist.

5.2.3 Überprüfung der Geräte-Vorauswahl

Die bisherige Einschätzung zu den Einsatzbereichen der Privacy-Boxen aus der repräsentativen Vorauswahl basiert lediglich auf der Einteilung in verschiedene Produkt-Kategorien (vgl. Tabelle 3 „Funktionen, Eigenschaften und Preise von Privacy-Boxen im Vergleich“). Um diese Einschätzung mit den Anforderungen der Zielgruppe abzugleichen, wird bei allen Geräten eine Einschätzung des initialen Einrichtungs-Aufwands vorgenommen. Zu diesem Zweck werden die bestellten Privacy-Boxen einmal ausgepackt, um einen Eindruck über die „Plug-and-Play“-Fähigkeit jedes einzelnen Geräts zu erhalten. Diese wird als Entscheidungskriterium genutzt, um zu bewerten, ob die Consumer-Produkte für die *Bemühten Amateure* und die „Open Source“/DIY-Produkte für die *Techniker* geeignet sind.

Der erste Eindruck beim Öffnen der Verpackung und Sichtung der gelieferten Komponenten zeigt, dass diese Zuordnung bei fast allen Geräten valide ist. Die *TrutzBox*, welche in der Variante *„TrutzBox-Home mit WLAN-Modul zum Selbsteinbau“* bestellt wurde, bildet dabei jedoch eine Ausnahme. Die Überprüfung zeigt, dass Nutzer zur Inbetriebnahme einen erhöhten Bedarf an technischem Wissen und Motivation benötigen. Da diese Eigenschaften bei der Nutzergruppe der *Bemühten Amateure* geringer ausgeprägt sind, wird die *TrutzBox* in die Gruppe der für *Techniker* relevanten Geräte eingeordnet.

In Tabelle 4 werden die Privacy-Boxen der repräsentativen Vorauswahl den ermittelten Nutzertypen zugeordnet. Zusätzlich wird die Tabelle dazu verwendet, den Funktionen der Privacy-Boxen die zugehörigen Privacy-Ziele (siehe „Feature-Modell von Privacy-Boxen“ in Abschnitt 5.1.1) sowie Privacy-Werkzeuge und Geräte-Eigenschaften (siehe „Maximaler Schutz mit Privacy-Boxen“ in Abschnitt 5.1.2) zuzuordnen.

Mithilfe dieser Übersicht lässt sich bereits eine Tendenz erkennen, wie die Relevanz unterschiedlicher Privacy-Bereiche bei Privacy-Boxen einzuschätzen ist: Die Funktionen zum privaten *IT-Schutz* zeigen vor allem bei Privacy-Boxen für *Bemühte Amateure* eine verstärkte Ausprägung, wobei zwei Privacy-Werkzeuge (W3*, W4) und eine Eigenschaft (E1) zugeordnet werden können. Im Bereich der Funktionen für mehr *Anonymität* im Internet ist bei Privacy-Boxen beider Nutzertypen eine hohe bis sehr hohe Ausprägung festzustellen. Diese

spiegelt sich auch in der Zuordnung von insgesamt sechs passenden Privacy-Werkzeugen (W5*, W7, W8, W9*, W11 und W13) wider (vgl. Tabelle 4).

Nutzertyp	**Bem. Amateur**				**Techniker**				Selbstdatenschutz-Werkzeuge und Eigenschaften	Selbstdatenschutz-Ziele (Modell)
Privacy-Box	Bitdef. BOX 2	F-Sec. SENSE	RATTrap	Keezel 2.0	TrutzBox Home	eBlocker 2	Syncloud R	FreedomBox		
Anti-Virus	✓	✓			✓				W3*	IT-Schutz
Firewall	✓	✓	✓	✓	✓				W3*	
IoT-Monitor	✓	✓							W3*	
Passwort-Manager		✓							W4	
Open Source Code					✓	✓	✓	✓	E1	
Inhaltsfilter	✓	✓	✓		✓	✓			W5*	Anonymität
Ad-Blocker			✓	✓	(✓)	✓	✓	✓	W7, W9*	
Anti-Tracking		✓	(✓)		✓	✓	(✓)		W7, W8, W9*	
DNS-Schutz			✓		✓	✓	✓	✓	W11	
VPN-Tunnel	✓	✓		✓	✓	✓	✓	✓	W11, W13	
Mesh/TOR						✓		✓	W11	
Sichere Email					✓				W14	Vertraulichkeit
Sichere Chats					✓		✓	✓	W14	
Web-Meetings					✓		✓	✓	W14	
Private Telefonie					✓		✓	✓	W14	
Soziales Netzwerk							✓		W14, W16	
Notizen							✓		W16	Autonomie
Kalender								✓	W16	
Adressbuch								✓	W16	
Cloudspeicher							✓	✓	W16	
Web-Hosting							✓	✓	W16	
Email-Server					✓		✓	✓	W16	
Git-Server							✓		W16	
Mobiler Schutz				✓	(✓)	(✓)	(✓)		E2	
Web Dashboard					✓	✓	✓	✓	E3	Usability/UX
Smartphone App	✓	✓	✓	✓		(✓)	(✓)		E3	
Router-Funktion	✓	✓			✓	✓	✓		E4	
WLAN-Netzwerk	✓	✓		✓	(✓)			✓	E4	

Tabelle 4: Vergleich von Produkt-Kategorie und Zielgruppe der repräsentativen Vorauswahl – Zuordnung von Werkzeugen, Eigenschaften und Zielen des Selbstdatenschutzes

Funktionen, die auf *Vertraulichkeit* bei der Kommunikation abzielen, sind jedoch nur bei Privacy-Boxen für *Techniker* zu finden, wobei sich zwei Privacy-Werkzeuge (W14, W16) zuordnen lassen. Auch Funktionen die zu mehr *Autonomie* beitragen, werden fast ausschließ-

lich von Geräten für *Techniker* unterstützt – ihnen kann ein Privacy-Werkzeug (W16) und eine Eigenschaft (E2) zugeordnet werden. Im Bereich der *Usability/UX* ist die Verteilung von Eigenschaften (E3, E4) bei beiden Nutzertypen relativ ausgeglichen. Allerdings wird den *Bemühten Amateuren* das UI nur in Form von *Smartphone Apps* angeboten, wohingegen *Techniker* neben *Web Dashboards* teilweise auch Apps nutzen können (vgl. Tabelle 4).

Anhand der hohen Anzahl unterschiedlicher Privacy-Werkzeuge und der hohen Ausprägung von Privacy-Funktionen, scheint sich der Bereich mit Ziel der *Anonymität* als ein wichtiger Bereich von Privacy-Boxen abzuzeichnen. Dies lässt vermuten, dass Privacy-Boxen mit einer hohen Übereinstimmung an Funktionen in diesem Bereich (F-Secure SENSE/RATtrap und TrutzBox Home/eBlocker 2) besonders interessant für die Untersuchung sein werden. Mit der Identifikation zweier Nutzertypen als relevante Zielgruppe für Privacy-Boxen und der Zuordnung von bestellten Geräten der repräsentativen Vorauswahl, sind zwei wichtige Schritte zur Beantwortung der Forschungsfragen erfolgt. Für die Beantwortung der zweiten Forschungsfrage (F2) ist zusätzlich die Identifikation typischer Anwendungsszenarien erforderlich, welche daher im nächsten Abschnitt untersucht werden.

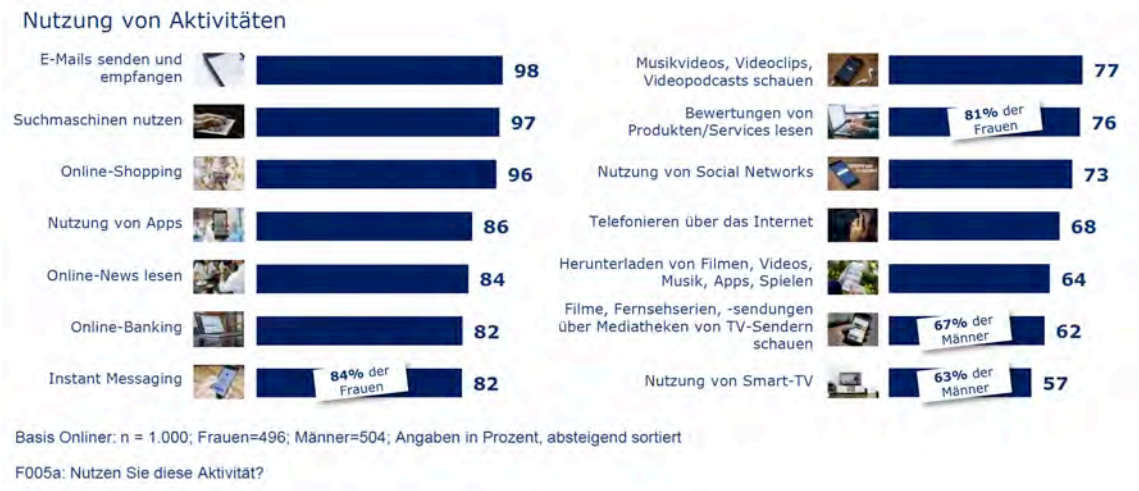
5.3 Anwendungsszenarien

Für die Bestimmung von Anwendungsszenarien, bei denen Privacy-Boxen für mehr Sicherheit und Privatheit eingesetzt werden, folgt zunächst die Untersuchung häufig genutzter Internetaktivitäten und Maßnahmen zum Schutz vor Datenmissbrauch. Mit ihnen lassen sich Aufgaben bestimmen, die bei der Nutzung von Privacy-Boxen eine zentrale Rolle spielen und zur Identifikation wichtiger Anwendungsbereiche genutzt werden können. Im Rahmen der Usability-Evaluation können die Aufgaben dann zur Beantwortung der zweiten Forschungsfrage (F2) untersucht werden.

5.3.1 Anwendungsbereiche von Privacy-Boxen

Um Anwendungsbereiche von Privacy-Boxen zu identifizieren, folgt zunächst eine Vorstellung von Aktivitäten der Internetnutzung anhand der Studie *„Digitale Nutzung in Deutschland 2018“* vom Bundesverband Digitale Wirtschaft (BVDW) [26, S. 21-22]. Bei der Umfrage mit 1.000 Teilnehmern wurden 504 Männer und 496 Frauen zur Nutzung von Internetaktivitäten befragt. Die folgenden Ergebnisse werden nach absteigender Häufigkeit (in Prozent der Nutzung) vorgestellt. Dabei zeichnen sich das „Senden und Empfangen von Emails“ (98%), die „Nutzung von Suchmaschinen“ (97%) und das „Online-Shopping“ (96%) als die drei häufigst genutzten Aktivitäten aus (vgl. Abb. 18a).

Im oberen Bereich der häufigsten Internet-Aktivitäten schließen sich die „Nutzung von Apps“ (86%), das „Lesen von Online-News“ (84%), Geldgeschäfte durch „Online-Banking“ (82%) und „Instant Messaging“ über Kurznachrichten-Dienste (82%) an. In der zweiten Hälfte der Liste finden sich das „Anschauen von Videos“ (77%), das „Lesen von Produkt-Bewertungen“ (76%) und die „Nutzung von Sozialen Netzwerken“ (73%). Das Ende der häufigeren Aktivitäten machen „Telefonate über das Internet“ (68%), „Downloads von Videos, Musik und Spielen“ (64%) sowie das „Anschauen von Filmen und Serien über Online-Mediatheken“ (62%) bzw. die „Nutzung von Smart-TVs“ (57%) aus (vgl. Abb. 18a).



(a) Nutzung von Aktivitäten im Internet Teil 1 (modifiziert nach [26, S. 20])

(b) Nutzung von Aktivitäten im Internet Teil 2 (modifiziert nach [26, S. 21])

Abbildung 18: Nutzung von Aktivitäten im Internet nach Häufigkeit

Bei den durchschnittlich genutzten Aktivitäten führen das „Lesen von News auf öffentlichen Screens“ (55%) sowie das „Schauen von Filmen und Serien über Streaming-Dienste“ (54%) die Liste an, gefolgt von der „Nutzung von Cloud-Diensten“, dem „Hören von Musik über Webradios“ und dem „Anschauen von Live-Streams“ (alle drei 48%). Bei den weniger genutzten Internet-Aktivitäten folgen das „Hören von Musik über Streaming-Portale“ (42%) sowie das „Lesen von E-Books auf E-Readern“ (35%). Die am wenigsten genutzten Aktivitäten sind das „Bezahlen mit App oder Handy“ (25%), „Online-Dating“ (22%) und die „Nutzung von Smartwatches oder Fitness-Trackern“ (21%), wobei diese von einem deutlich höheren Anteil jüngerer Nutzer durchgeführt werden (vgl. Abb. 18b).

Um aus den Aktivitäten der Internetnutzung typische Szenarien für Privacy-Boxen abzuleiten, werden alle Aktivitäten (vgl. Abb. 18) zunächst in gemeinsamen Anwendungsbereichen des Feature-Modells gruppiert (siehe Anhang A.1). Für die Ermittlung der Relevanz eines Bereichs, werden die Aktivitäten ihrer Anwendungshäufigkeit entsprechend berücksichtigt. Somit lässt sich für jeden Anwendungsbereich eine Gewichtung bestimmen, welche auf der Häufigkeit zugehöriger Internetaktivitäten beruht (die zugrunde liegende Berechnung kann in Anhang A.1 nachvollzogen werden).

Viele der Aktivitäten werden mittels Browser oder App ausgeführt und können als „Surfen im Internet“ bezeichnet werden. Ein geringerer Anteil an Aktivitäten betrifft den Austausch von persönlichen Informationen und wird daher unter „Web-Kommunikation“ zusammengefasst. Neben Aktivitäten ohne Relevanz für Privacy-Boxen (News auf öffentlichen Screens lesen), betrifft die „Nutzung von Cloud-Diensten“ den kleinsten Anteil an Aktivitäten.

Den Anwendungsbereichen können nun passende Privacy-Ziele des Feature-Modells zugeordnet werden: Beim „Surfen im Internet“ wollen Nutzer ihre *Anonymität* durch den Schutz vor Werbung und Tracking bewahren. Während des Austauschs von Informationen ist Nutzern die *Vertraulichkeit* von Daten durch eine geschützte „Web-Kommunikation“ wichtig. Zuletzt können Nutzer *Autonomie* erlangen, wenn sie Alternativ-Dienste einsetzen und diese als „Cloud-Dienste nutzen“.

Auch wenn fast alle Studienteilnehmer Internetaktivitäten ausführen, die sich beim *Surfen im Internet* abspielen (97% der Befragten nutzen Suchmaschinen) und *Web-Kommunikation* zum Inhalt haben (98% der Befragten senden und empfangen Emails), so zeigt die Einordnung von Häufigkeiten der Internetaktivitäten in *Anwendungsbereiche von Privacy-Boxen* deutliche Tendenzen:

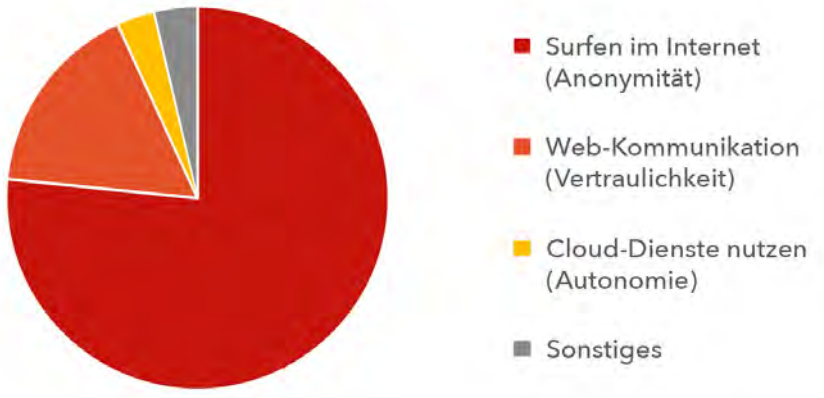


Abbildung 19: Einordnung von Internetaktivitäten in Anwendungsbereiche von Privacy-Boxen

Etwa drei Viertel der typischen Nutzerszenarien spielen sich beim „Surfen im Internet“ (rot) ab, sodass Privacy-Maßnahmen mit Ziel der *Anonymität* besonders häufig erforderlich werden. Knapp ein Viertel der Nutzerszenarien hat „Web-Kommunikation“ (orange) zum Inhalt, wodurch das Ziel der *Vertraulichkeit* insgesamt weniger relevant erscheint. Die Nutzung von „Cloud Diensten“ (gelb) hingegen, zeigt mit einem sehr geringen Anteil an Nutzerszenarien, dass Privacy-Maßnahmen mit Ziel der *Autonomie* bei Privacy-Boxen kaum eine Relevanz haben, ähnlich wenig wie „Sonstige“ (grau) Aktivitäten (vgl. Abb. 19).

Des Weiteren fällt auf, dass bei häufig genutzten Internetaktivitäten der Bereich „Sicherheit“ nicht explizit auftaucht. Dies lässt sich zum einen durch den passiven Charakter von Sicherheitsmaßnahmen erklären. Zum anderen bestätigt es die Einordnung von *Sicherheit* in den präventiven Bereich des Feature-Modells und macht nochmal deutlich, dass Internetaktivitäten nur die *operativen* (rot und orange) und *reaktiven* Bereiche (gelb) des Selbstdatenschutzes betreffen. Die Analyse von Internetaktivitäten bestätigt zudem die erwartete Relevanz des Privacy-Ziels *Anonymität* (rot) für Privacy-Boxen (vgl. Abb. 19).

5.3.2 Schutzpotenzial von Privacy-Boxen

Nachdem bereits Anwendungsbereiche von Privacy-Boxen für die Privacy-Ziele *Anonymität*, *Vertraulichkeit* und *Autonomie* des Feature-Modells identifiziert werden konnten, fehlt noch eine Aussage über das Privacy-Ziel im Bereich „Sicherheit“. Dazu wird im folgenden Schritt überprüft, welche Maßnahmen Nutzer bereits zum Schutz vor Datenmissbrauch einsetzen. Dies geschieht anhand der Umfrage *„Einsatz von Maßnahmen zum Schutz vor Datenmissbrauch im Internet 2017“* von Statista [161]. Die Ergebnisse der Umfrage mit 1.037 Teilnehmern werden nach absteigender Häufigkeit (in Prozent der Nutzung) gezeigt:

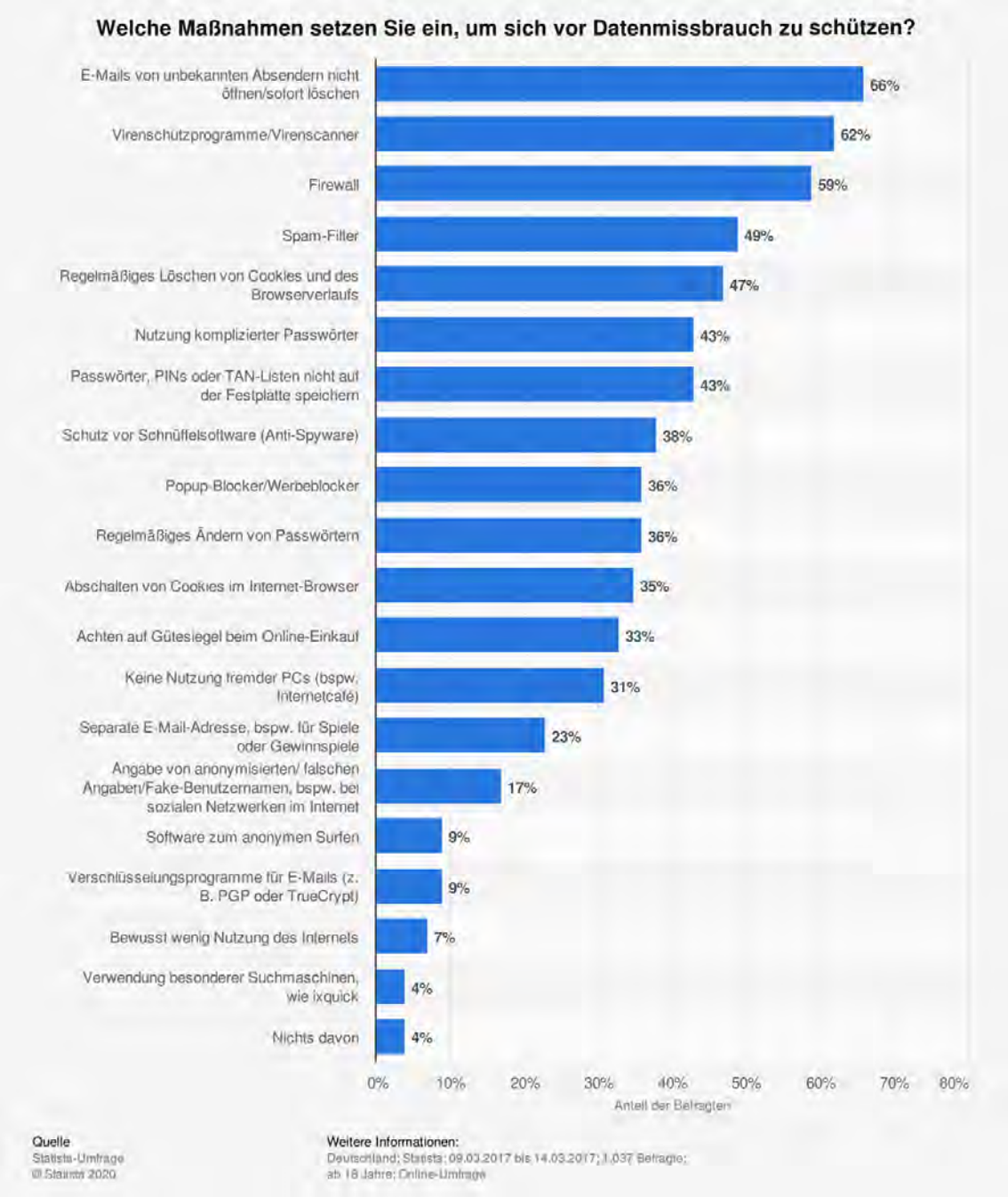


Abbildung 20: Einsatz von Maßnahmen zum Schutz vor Datenmissbrauch (mod. nach [161])

Wie in Abb. 20 zu sehen ist, sind die häufigsten Maßnahmen von Nutzern zum Schutz vor Datenmissbrauch die Vorsicht bei „E-Mails von unbekannten Absendern“ (66%), die Ver-

wendung von „Virenschutzprogrammen oder Virenscannern“ (62%) und der Einsatz von „Firewalls“ (59%). Im mittleren Bereich der häufigen Maßnahmen folgen die Verwendung von „Spam-Filtern“ (49%), das regelmäßige „Löschen von Cookies und Browserverlauf“ (47%), die „Nutzung komplizierter Passwörter“ (43%) und das Vermeiden, „Passwörter, PINs oder TAN-Listen auf der Festplatte zu speichern“ (43%). Das Ende der häufigen Maßnahmen machen der „Schutz vor Schnüffelsoftware (Anti-Spyware)“ (38%), die Verwendung von „Popup-Blockern oder Werbeblockern“ (36%) sowie das regelmäßige „Ändern von Passwörtern“ (36%) aus.

Die weniger häufigen Maßnahmen zum Schutz vor Datenmissbrauch beginnen mit dem „Abschalten von Cookies im Internet-Browser“ (35%), dem Achten auf „Gütesiegel beim Online-Einkauf“ (33%) und dem Vermeiden der „Nutzung fremder PCs (z.B. in Internetcafés)“ (31%). Die Verwendung von „separaten E-Mail-Adressen für Gewinnspiele“ (23%), „Pseudonymen in sozialen Netzwerken“ (17%) sowie „Software zum anonymen Surfen“ (9%) folgen im unteren Bereich. Die am wenigsten genutzten Maßnahmen sind der Einsatz von „E-Mail Verschlüsselung“ (9%), „reduzierte Internet-Nutzung“ (7%) und die Verwendung von „Datenschutz-Suchmaschinen“ (4%) (vgl. Abb. 20).

Bei der Betrachtung von Maßnahmen, die Nutzer zum Schutz vor Datenmissbrauch einsetzen, wird deutlich, dass Tätigkeiten aus dem Bereich „Sicherheit“ auftauchen. Um jedoch die Relevanz der vorgestellten Maßnahmen beurteilen zu können, erfolgt erneut eine Gruppierung in gemeinsame Anwendungsbereiche des Feature-Modells. Dabei wird die Häufigkeit der Verwendung von Maßnahmen mit berücksichtigt (siehe Anhang A.2). So kann für jeden Bereich von Privacy-Boxen erneut eine Gewichtung ermittelt werden, welche auf der Häufigkeit der zugehörigen Schutzmaßnahmen beruht (die zugrunde liegende Berechnung kann in Anhang A.2 nachvollzogen werden).

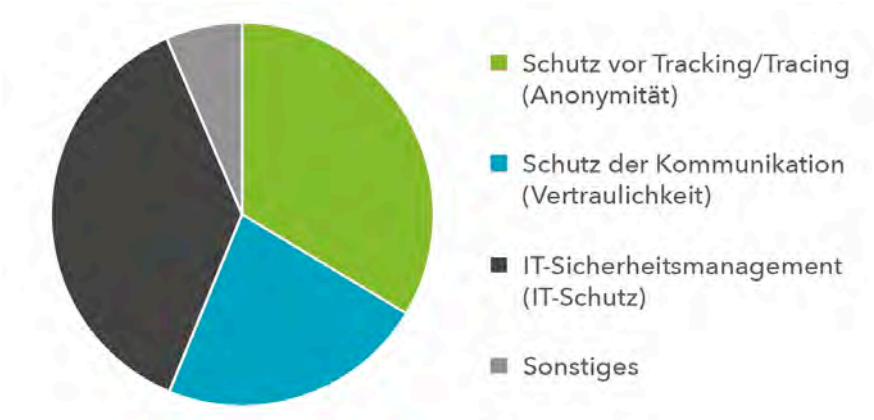


Abbildung 21: Einordnung von Schutzmaßnahmen in Anwendungsbereiche von Privacy-Boxen

In Abb. 21 wird die Zuordnung von Maßnahmen zum Schutz vor Datenmissbrauch zu den *Schutzbereichen von Privacy-Boxen* gezeigt. Es wird deutlich, dass Maßnahmen zum „Schutz vor Tracking/Tracing“ (grün) das Ziel der *Anonymität* verfolgen. Beim „Schutz der Kommunikation“ (blau) betreffen die ergriffenen Maßnahmen die *Vertraulichkeit*. Die gesuchten Maßnahmen aus dem Bereich „Sicherheit“ haben mit dem Aufbau eines privaten „IT-Sicherheitsmanagements“ (schwarz) den privaten *IT-Schutz* zum Ziel. Unter „Sonsti-

ges“ (grau) werden Maßnahmen gesammelt, die für Privacy-Boxen keine Relevanz haben (z.B. Vermeidung fremder PC’s in Internetcafés).

Häufige Maßnahmen der Studienteilnehmer betreffen den „Schutz der Kommunikation“ (66% der Befragten löschen Emails von unbekannten Absendern) und das private „IT-Sicherheitsmanagement“ (62% der Befragten nutzen Virenschutzprogramme und 59% eine Firewall). Maßnahmen zum „Schutz vor Tracking/Tracing“ werden hingegen weniger bis selten genutzt (47% der Befragten löschen und 35% deaktivieren Cookies im Browser, 9% der Befragten nutzen Software zum anonymen Surfen und 4% Datenschutz-Suchmaschinen).

Die Einordnung von Schutzmaßnahmen in Anwendungsbereiche von Privacy-Boxen (vgl. Abb. 21) zeigt, dass das „IT-Sicherheitsmanagement“ (schwarz) mit Ziel des privaten *IT-Schutzes* den größten Teil der verwendeten Schutzmaßnahmen (über ein Drittel) einnimmt. Eine ähnliche Relevanz für Nutzer stellt der Schutz der *Anonymität* mit Maßnahmen zum „Schutz vor Tracking/Tracing“ (grün) dar (ein weiteres Drittel). Die *Vertraulichkeit* mit Maßnahmen zum „Schutz der Kommunikation“ (blau) scheint Nutzern weniger wichtig zu sein (knapp ein Viertel). „Sonstige“ Maßnahmen machen einen geringen Anteil aus.

Schließlich lässt sich festhalten, dass keine der genannten Maßnahmen den Umstieg auf alternative Cloud-Dienste adressiert, wodurch das Ziel von „*Autonomie* durch Alternativ-Dienste“ weg fällt. Für die Gegenüberstellung von Aktivitäten und Schutzmaßnahmen fehlen somit in den Bereichen „Cloud-Dienste“ und „IT-Sicherheit“ Daten für einen Vergleich. Daher werden in Abb. 22 lediglich Aktivitäten und Schutzmaßnahmen in den Bereichen „Surfen“ und „Kommunikation“ in Relation gebracht (die zugrunde liegende Berechnung kann in Anhang A.3 nachvollzogen werden):

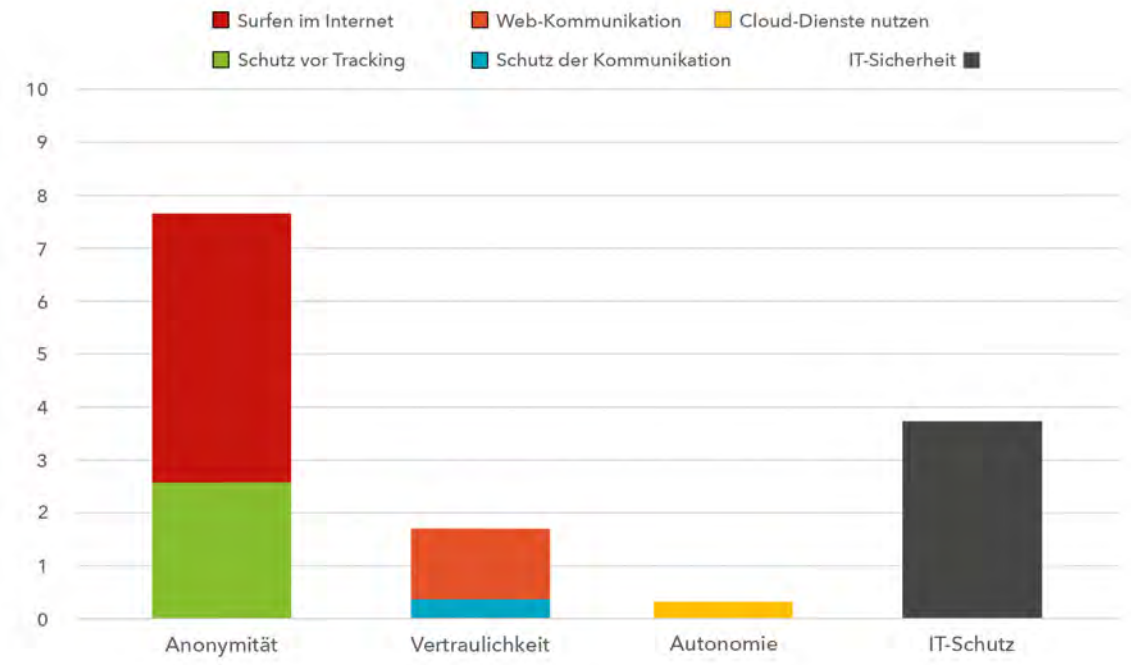


Abbildung 22: Verhältnis von Internetaktivitäten zu Schutzmaßnahmen als Gewichtung

In Abb. 22 wird das Verhältnis von Aktivitäten und Schutzmaßnahmen in den Bereichen „Surfen“ (rot/grün) und „Kommunikation“ (orange/blau) dargestellt. Es lässt sich zeigen,

dass etwa nur ein Drittel der Aktivitäten beim *Surfen im Internet* mit einem *Schutz vor Tracking* (grün) stattfinden. Zwei Drittel der Aktivitäten beim *Surfen im Internet* (rot) sind ungeschützt und stellen ein Verbesserungspotenzial für Privacy-Boxen im Bereich „Surfen“ dar. Bei den Aktivitäten der *Web-Kommunikation* lässt sich zeigen, dass etwa nur ein Viertel der Aktivitäten mit einem *Schutz der Kommunikation* (blau) durchgeführt wird. Drei Viertel der *Web-Kommunikation* (orange) findet ohne Schutz statt und bedeutet ebenfalls ein Verbesserungspotenzial für Privacy-Boxen im Bereich „Kommunikation“.

Durch den Vergleich der Bereiche „Surfen“ und „Kommunikation“ wird deutlich, dass das Verbesserungspotenzial von Privacy-Boxen bei der *Web-Kommunikation* mit drei Viertel zwar relativ hoch ist, allerdings im Vergleich zum Verbesserungspotenzial beim *Surfen im Internet* nur einen geringeren Anteil ausmacht (absolut). Da die Anzahl häufiger Aktivitäten beim *Surfen im Internet* insgesamt deutlich höher liegt, macht das Verbesserungspotenzial von zwei Drittel somit den größten Anteil aus (absolut). Damit lässt sich der Anwendungsbereich „Schutz vor Tracking/Tracing“ tatsächlich als wichtigster Bereich von Privacy-Boxen bestätigen, da er das größte Verbesserungspotenzial bietet, das von Privacy-Boxen noch ausgeschöpft werden kann.

Das Verbesserungspotenzial in den Bereichen „Cloud-Dienste“ und „IT-Sicherheit“ lässt sich aufgrund fehlender Daten nicht ermitteln. Damit ist es nicht als Kriterium für die Gewichtung aller Anwendungsbereiche von Privacy-Boxen geeignet. In den Bereichen „Surfen“ und „Kommunikation“ kann es allerdings als Indiz für deren Relevanz gewertet werden. Das Ziel bei der Auswahl von Geräten und Szenarien für die Usability-Untersuchung ist es jedoch, die Relevanz aller Anwendungsbereiche von Privacy-Boxen entsprechend zu berücksichtigen. Aus diesem Grund wird auf die Gesamt-Häufigkeiten von Aktivitäten und Schutzmaßnahmen zurückgegriffen, um daraus eine Gewichtung abzuleiten.

Die Skala aus Abb. 22 wird für diesen Zweck verwendet und jedem Bereich das entsprechende Maximum für die Gewichtung zugeteilt (gerundet). Dabei steht der Wert 0 für keine und der Wert 10 für eine sehr hohe Häufigkeit an Aktivitäten oder Schutzmaßnahmen in dem jeweiligen Bereich. Daraus ergeben sich folgende Gewichte für die identifizierten Anwendungsbereiche:

- Surfen im Internet: Wert 8 (hohe Anzahl häufiger Aktivitäten)
- Web-Kommunikation: Wert 2 (geringe Anzahl häufiger Aktivitäten)
- Cloud-Dienste nutzen: Wert 0 (zu geringe Anzahl häufiger Aktivitäten)
- IT-Sicherheitsmanagement: Wert 4 (mittlere Anzahl häufiger Maßnahmen)

Auf Grundlage dieser Gewichtung werden im nächsten Abschnitt Geräte aus der repräsentativen Vorauswahl und damit schließlich typische Anwendungsszenarien für die Usability-Evaluation ausgewählt.

5.3.3 Geräteauswahl und Nutzerszenarien

Mithilfe einer Priorisierung der Anwendungsbereiche von Privacy-Boxen ist es nun möglich, relevante Geräte und Nutzerszenarien für die Usability-Evaluation zu bestimmen. Zunächst

wird in der repräsentativen Vorauswahl von Privacy-Boxen nach Geräten gesucht, die bei einem Vergleich der Usability-Ergebnisse die größtmögliche Aussagekraft zur Beantwortung der Forschungsfragen generieren. Dabei werden beide Nutzertypen der Zielgruppe berücksichtigt, weshalb insgesamt vier Geräte – jeweils zwei pro Nutzertyp – für die Untersuchung ausgewählt werden.

Um aus der Vorauswahl von Privacy-Boxen die „interessantesten“ Geräte für eine Usability-Evaluation zu ermitteln, werden jeweils zwei Geräte innerhalb der Gruppe eines Nutzertyps gesucht, welche die größte Schnittmenge an vergleichbaren Funktionen mit einer hohen Relevanz für Selbstdatenschutz bieten. Durch dieses Auswahlkriterium wird zum einen sichergestellt, dass die ausgewählten Geräte genug vergleichbare Funktionen bieten, damit sich eine Usabilility-Untersuchung durchführen lässt. Zum anderen werden Privacy-Funktionen untersucht, die Nutzer tatsächlich im Alltag benötigen. Die Relevanz der einzelnen Funktionen ergibt sich dabei durch die Gewichtung des zugehörigen Anwendungsbereichs.

Für vier Bereiche der Feature-Modells von Privacy-Boxen konnte eine Gewichtung der entsprechenden Anwendungsbereiche ermittelt werden. Der fünfte Bereich des Feature-Modells betrifft die *Usability*, welche im Rahmen der anstehenden Untersuchung ermittelt wird. In dem Bereich sind auch die Software- und Hardware-Interfaces eingeordnet, welche bei der Evaluation untersucht werden. Diese bestimmen nicht nur darüber, wie das Gerät bedient wird, sondern auch in welchen Betriebs-Modi eine Privacy-Box verwendet werden kann (z.B. Aufbau eines eigenen Netzwerks oder Integration in ein bestehendes Netzwerk). Aus diesem Grund wird dem Bereich als Kategorie *Interfaces* bei der Gewichtung mit dem Wert 6 noch zusätzlich eine mittel-hohe Relevanz zugewiesen.

Im Folgenden wird die Berechnung von Vergleichswerten für die Auswahl von Privacy-Boxen aus der repräsentativen Vorauswahl erläutert: Zu Beginn wird für jede Funktion aus Tabelle 4 bei zwei zu vergleichenden Privacy-Boxen die Unterstützung überprüft. Bieten beide Geräte die Funktion an (auch unter Bedingungen) so wird ihr zum Zeichen der Vergleichbarkeit der Wert 1 zugeteilt, ansonsten nicht. Anschließend wird jeder Eintrag der einen Wert enthält mit dem zugehörigen Gewichtungsfaktor des Anwendungsbereichs multipliziert. Danach wird für jeden Anwendungsbereich die Summe aller beinhalteten Werte gebildet. Durch Addition aller Bereichs-Summen lässt sich bereits der Gesamt-Wert für den Vergleich zweier Geräte bestimmen. Als Ergebnis wird der Gesamt-Wert anschließend mit einem Faktor auf ein Maximum von 10 skaliert und entsprechend auf- oder abgerundet (die zugrunde liegende Berechnung kann in Anhang A.4 nachvollzogen werden).

Mithilfe dieser Gewichtung, lässt sich die vorherige Vermutung über die Aussagekraft beim Vergleich von Privacy-Boxen, die am Ende von Abschnitt 5.2.3 (Überprüfung der Geräte-Vorauswahl) angestellt wurde, anhand eines berechneten Werts überprüfen. Dieser Wert repräsentiert die potenzielle Aussagekraft des Vergleichs zweier Privacy-Boxen hinsichtlich ihrer Usability unter Berücksichtigung von häufigen Nutzungsaktivitäten. Er kann als Entscheidungshilfe bei der Wahl von Privacy-Boxen für eine Usability-Evaluation gesehen werden, mit dem Ziel, dabei relevante Anwendungszenarien für Nutzer zu berücksichtigen. In Tabelle 5 werden die Ergebnisse der Berechnung (siehe Anhang A.4) für die Vergleich-

barkeit von Privacy-Boxen aus der repräsentativen Vorauswahl dargestellt. Die Skala geht dabei vom Wert 0 (keine vergleichbaren Funktionen mit hoher Relevanz) bis zum Wert 10 (totale Übereinstimmung vergleichbarer Funktionen mit hoher Relevanz).

–	Bitdef. BOX	**F-Sec. SENSE**	RATtrap	Keezel 2.0	*Bem. Amateur*
TrutzBox	–	**5**	2	2	**Bitdef. BOX**
eBlocker 2	**6**	–	3	2	F-Sec. SENSE
Syncloud R	5	5	–	2	RATtrap
FreedomBox	5	4	4	–	Keezel 2.0
Techniker	**TrutzBox**	eBlocker 2	Syncloud R	FreedomBox	–

Tabelle 5: Berechnung der Vergleichbarkeit von Privacy-Boxen

In Tabelle 5 werden sowohl die Ergebnisse von Geräte-Vergleichen der *Bemühten Amateure* (rechts/oben), als auch der *Techniker* (links/unten) dargestellt. Ein höherer Wert spricht hierbei für eine größere Aussagekraft beim Vergleich von Usability-Ergebnissen. Bei den geeigneten Privacy-Boxen für *Techniker* erscheint demnach ein Vergleich der Geräte „eBlocker 2“ und „TrutzBox Home“ mit einem Ergebnis von 6 Punkten besonders erfolgsversprechend. Bei den Geräten für *Bemühten Amateure* zeichnet sich bei dem Vergleich zwischen „F-Secure SENSE“ und „Bitdefender BOX 2“ mit dem Ergebnis von 5 Punkten das aussichtsreichste Ergebnis ab.

Somit kann ein Teil der Vermutung aus Abschnitt 5.2.3 (Überprüfung der Geräte-Vorauswahl) bestätigt und ein anderer Teil widerlegt werden: Bei den *Technikern* entspricht die berechnete Empfehlung der vermuteten Geräte-Auswahl. Bei den *Bemühten Amateuren* jedoch zeigt sich, dass anstelle von „RATtrap“ das Gerät „Bitdefender Box 2“ interessanter für einen Vergleich mit „F-Secure SENSE“ zu sein scheint. Ausschlaggebend hierfür ist anscheinend die höhere Anzahl an vergleichbaren Funktionen im Bereich der „IT-Sicherheit“.

Auf Grundlage der Bewertung von Tabelle 5 können für die anstehende Usability-Untersuchung und den anschließenden Vergleich die Geräte „eBlocker 2“ und „TrutzBox Home“ als Privacy-Boxen für den Nutzertyp *Techniker* festgelegt werden.

Mit der Schnittmenge an gemeinsamen Funktionen beider Geräte lassen sich schließlich die zu untersuchenden Anwendungsszenarien für *Techniker* definieren. Diese werden alle aus dem Bereich „Surfen im Internet“ (hohe Anzahl häufiger Aktivitäten) ausgewählt, um viele relevante Nutzeraktivitäten abzudecken (siehe Anhang A.4 Spalte „Trutz/eBlock“). Somit werden folgende fünf typische Anwendungsszenarien für *Techniker* definiert:

1. Einrichtung von *Anti-Tracking* zur Vermeidung von Tracking und Tracing
2. Einstellen des *DNS-Schutzes* zur Abwehr von Spionage durch den ISP
3. Verwendung eines *VPN-Tunnels* für mehr Anonymität und Sicherheit
4. Konfiguration von *Ad-Blockern* zum Verhindern von OBA
5. Aktivieren von *Inhaltsfiltern* zum Schutz vor kritischen Inhalten

Für den Nutzertyp *Bemühter Amateur* ergeben sich anhand der Bewertung von Tabelle 5 die Geräte „F-Secure SENSE“ und „Bitdefender BOX 2“ für die Usability-Evaluation und den Vergleich. Da die Schnittmenge der Funktionen aus dem Bereich „Surfen im Internet“ nicht ausreicht, werden zusätzlich noch vergleichbare Funktionen aus dem nächst relevanten Bereich „IT-Sicherheit“ (mittlere Anzahl häufiger Maßnahmen) hinzugenommen (siehe Anhang A.4 Spalte „BOX/SENSE“). Somit lassen sich folgende Anwendungsszenarien für *Bemühte Amateure* definieren:

1. Verwendung eines *VPN-Tunnels* für mehr Anonymität und Sicherheit
2. Aktivieren von *Inhaltsfiltern* zum Schutz vor kritischen Inhalten
3. Konfiguration der Netzwerk-*Firewall* zum Schutz vor Cyber-Angriffen
4. Einrichtung von *Anti-Virus* zum Schutz vor Viren und Malware
5. Einstellen des *IoT-Monitors* zum Erkennen und Vermeiden von Gefahren

Nachdem Geräte für die Untersuchung festgelegt und typische Anwendungsszenarien für Privacy-Boxen definiert wurden, sind alle Grundlagen vorhanden, die zur Beantwortung der Forschungsfragen notwendig sind. Im nächsten Abschnitt erfolgt daher der letzte notwendige Schritt: die Festlegung der Evaluations-Methode um die Usability der ausgewählten Privacy-Boxen zu bewerten.

5.4 Evaluationsmethode

Zur Bestimmung einer geeigneten Evaluationsmethode für die Usability von Privacy-Boxen kann auf Abschnitt 2.4.3 (Usability Engineering und -Evaluation) aus dem Grundlagenteil und Abschnitt 3.3.1 (Konzepte für den Datenschutz) aus Related Work zurückgegriffen werden. Zu Beginn lässt sich festhalten, dass die anstehende Evaluation sowohl *summativer*, als auch *komperativer* Natur ist. Zum einen findet die Bewertung am Ende des Entwicklunsgprozesses statt – die Privacy-Boxen sind bereits entwickelt und auf dem Markt – zum anderen wird die Usability unterschiedlicher Privacy-Boxen miteinander verglichen. Im nächsten Schritt geht es darum, die Kriterien für die anstehende Untersuchung festzulegen.

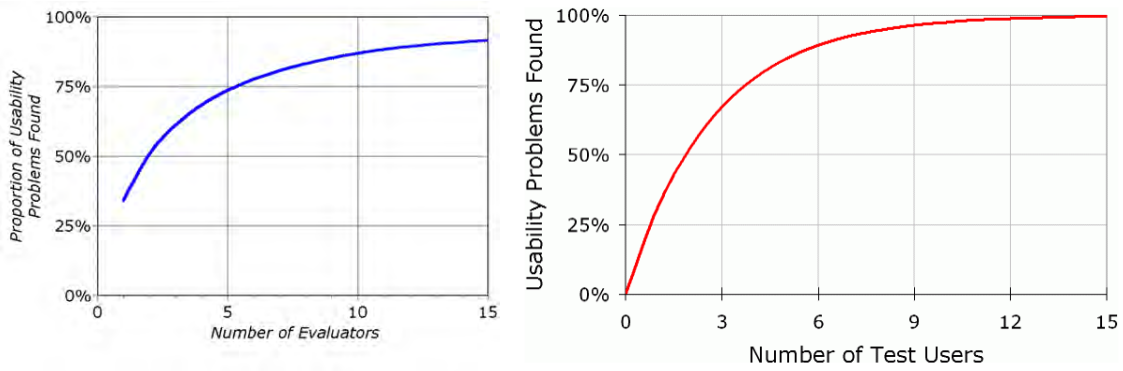
5.4.1 Art und Weise der Evaluation

Die grundlegende Entscheidung bei der Wahl einer geeigneten Evaluationsmethode betrifft die Frage, ob die Usability von Privacy-Boxen mithilfe einer analytischen oder empirischen Methode untersucht werden soll (siehe „Usability Evaluation“ in Abschnitt 2.4.3). Zur Beantwortung dieser Fragestellung werden Stärken und Schwächen von expertenorientierter (analytischer) und anwenderorientierter (empirischer) Evaluation einander gegenüberstellt.

Eine analytische Evaluation ist gut dafür geeignet, um einen Überblick über ein bestimmtes Anwendungsfeld zu bekommen, da sie die Betrachtung eines breiten Bereichs von Usability-Aspekten ermöglicht. Sie wird häufig als ein erster Schritt eingesetzt, um in neuen Forschungs-Bereichen das notwendige Grundlagen-Wissen zu erarbeiten, auf dem später z.B. eine empirische Evaluation aufbauen kann. Für eine analytische Evaluation wird einerseits zwar ein hohes Expertenwissen benötigt, andererseits ist die Untersuchung weniger

zeit- und kostenaufwendig, als eine empirische Evaluation (vgl. „Aufwand vs. Validität von Usability-Evaluationsmethoden“ in Abb. 7). In der Regel lassen sich bereits mit fünf Usability-Experten 75% aller Usability-Probleme in einer analytischen Evaluation aufdecken (vgl. Abb. 23a) [135].

Eine empirische Evaluation dagegen eignet sich besonders gut für Untersuchungen aus Forschungs-Bereichen, in denen bereits erste Ergebnisse vorliegen. Das Ziel der Untersuchung muss bereits sehr konkret sein, da ein hoher Aufwand für die Betrachtung eines sehr kleinen Bereichs erbracht werden muss. Die Formulierung von Forschungsfragen ist daher deutlich eingeschränkter, da diese schon sehr genau auf einen bestimmten Bereich abzielen müssen. Eine empirische Evaluation folgt auf analytische Untersuchungen oft als ein zweiter Schritt, um bereits identifizierte Probleme im Detail zu überprüfen oder in speziellen Teil-Bereichen weitere Probleme aufzudecken. Bei einem Usability-Test lassen sich bereits mit vier Probanden bis zu 75% aller Usability-Probleme finden (vgl. Abb. 23b) [136].



(a) Experten zu Usability-Problemen [135] (b) Probanden zu Usability-Problemen [136]

Abbildung 23: Anzahl Experten/Probanden zu gefundenen Usability-Problemen

Da zum Thema Privacy-Boxen keine vergleichbaren Arbeiten im Bereich der Forschung gefunden werden konnten (siehe „Aktueller Forschungsstand / Related Work“ in Kapitel 3), beschränkt sich das Zurückgreifen auf bestehende Arbeiten auf Einzel- und Teil-Lösungen wie z.B. die Bewertung der Usability von Browser-Erweiterungen in der Arbeit *„Usability von Browsererweiterungen zum Schutz vor Tracking“* von Hubert et al. [91]. Da es bei der Usability-Evaluation von Privacy-Boxen jedoch um die Untersuchung von Gesamtlösungen zum Selbstdatenschutz in Form von Hardware geht, schlägt diese Arbeit einen neuen, bisher unbeschrittenen Pfad ein.

Aufgrund des Mangels an „echtem“ Related Work zum Thema Privacy-Boxen, dem bereits vorhandenen Expertenwissen und dem Wunsch nach Reduzierung des Aufwands bei der Validierung der sehr aufwändig erarbeiteten Methodik, wird für die Untersuchung der Usability von Privacy-Boxen in dieser Arbeit eine analytische Evaluation ausgewählt. Diese Entscheidung wird zusätzlich durch den begrenzten Zeitrahmen dieser Arbeit und besondere organisatorische Hürden, die bei einer empirischen Evaluation in der Corona-Zeit auftreten, beeinflusst. Das Risiko bei dieser Entscheidung, nicht alle Usability-Probleme im Rahmen der Untersuchung aufzudecken wird an dieser Stelle eingegangen. Es wird mehr Wert darauf gelegt, die Wirkungsweise der Methodik zu demonstrieren, als eine Vollstän-

digkeit bei der Usability-Evaluation hinsichtlich gefundener Probleme oder untersuchter Geräte zu erreichen.

Im nächsten Schritt geht es darum, Evaluationsmethoden für die Bestimmung der Usability von Privacy-Boxen festzulegen, die zur Beantwortung beider Forschungsfragen geeignet sind. Während die erste Forschungsfrage (F1) auf die Einrichtung und Inbetriebnahme von Privacy-Boxen abzielt, beschäftigt sich die zweite Forschungsfrage (F2) mit typischen Anwendungsszenarien zum Selbstdatenschutz. Aus diesem Grund müssen für die Beantwortung beider Forschungsfragen zwei etwas unterschiedliche Methoden entwickelt werden.

5.4.2 Die Out-of-Box Experience

Um die Nutzererfahrung bei Einrichtung und Inbetriebnahme von Privacy-Boxen für die erste Forschungsfrage (F1) bewerten zu können, müssen die unterschiedlichen Schritte der Nutzer, vom Auspacken und Anschließen der Privacy-Boxen, über die Konfiguration bis hin zur erstmaligen Benutzung untersucht werden. Da diese Nutzerinteraktionen sowohl die Hardware- als auch Software-Interfaces der Geräte betreffen, ist es notwendig, an dieser Stelle den Methoden-Bereich der Usability auf die UX zu erweitern (siehe „User Experience (UX)“ in Abschnitt 2.4.2).

Moya und Burgess, Mitarbeiterinnen bei Microsoft in den Bereichen *Customer Experience Program* und *Hardware User Assistance*, zeigen in *„Out of Box and First Time User Experiences“* (2011) die Bedeutung der Out-of-Box Experience (OOBE) in Zusammenhang mit dem gesamten Lebenszyklus eines Produktes:

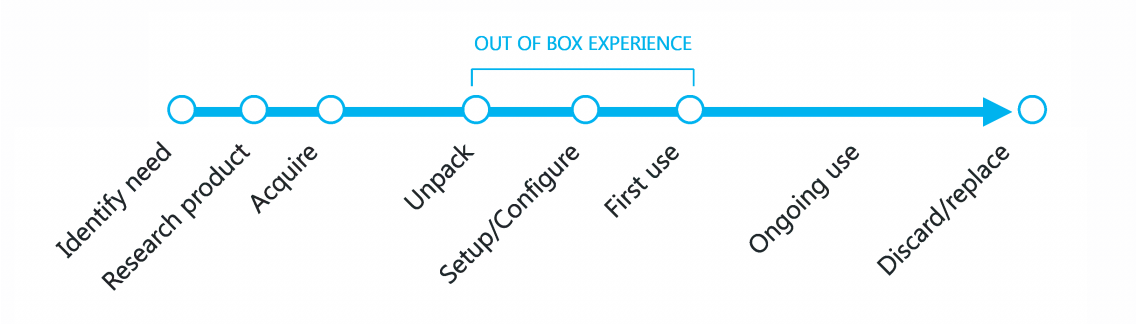


Abbildung 24: Out-of-Box Experience im Produkt-Lebenszyklus (mod. nach [131, S. 5])

Wie in Abb. 24 zu sehen ist, besteht der Produkt-Lebenzsyklus aus mehreren Phasen: In der ersten Phase geht es um die Identifikation der Notwendigkeit, die Recherche und den Kauf eines neuen Produkts. Die zweite Phase betrifft das Auspacken, die Konfiguration und die Erstbenutzung des neuen Produkts: die OOBE. Anschließend folgt mit der fortlaufenden Benutzung des Produkts die dritte Phase, welche den Primärzweck der Produktanschaffung ausmacht. In der vierten und letzten Phase endet durch Entsorgung oder Austausch der Lebenszyklus des Produkts.

Die OOBE (Phase 2 des Produkt-Lebenzsyklus) kann zur Beantwortung der ersten Forschungsfrage (F1) untersucht werden. Die „fortlaufende Benutzung“ wiederum (Phase 3 des Produkt-Lebenzsyklus) lässt sich zur Beantwortung der zweiten Forschungsfrage (F2)

untersuchen. In den Phasen 1 und 4 des Produkt-Lebenzsyklus lassen sich zwar ebenfalls relevante Punkte identifizieren, da sie jedoch wenig zur Beantwortung der Forschungsfragen beitragen können, werden sie von der Untersuchung ausgeschlossen (es könnten z.B. Sicherheits- und Datenschutz-Bedenken bei Nutzern vor dem Kauf und der Umgang mit PD bei Entsorgung oder Stilllegung des Produkts untersucht werden).

Moya und Burgess definieren UX-Ziele, mit deren Berücksichtigung ein Nutzer durch den Prozess von Auspacken, Einrichten und erstmaligem Gebrauch des Produkts geführt werden kann [131, S. 43]:

- Intuitives Öffnen der Verpackung
- Logisches Offenbaren von Informationen und Komponenten
- Einfache Entscheidungen durch sinnvolle Standardeinstellungen
- Verständliche Kombinationen aus Text und Bildern
- Sicherheitsvorkehrungen für häufige Fehler
- Deutliches Feedback nach erfolgreichem Abschluss
- Unterstützung beim Übergang von Installation zu Nutzung
- Vermeidung von Störquellen bei der Einrichtung
- Zeitliche Limitierung für die Einrichtungsdauer

Die vorgestellten UX-Ziele können als Orientierung bei einer Ermittlung der OOBE von Privacy-Boxen verwendet und in ausführlicherer Form in Anhang B.1 gefunden werden. Sie dienen als Leitlinie bei der Evaluation der OOBE in der anstehenden Untersuchung.

Als weitere Grundlage, die sich konkret mit diesem Thema befasst, wird die Arbeit *„HMD vs. PDA: A Comparative Study of the User Out-of-Box Experience“* (2009) von Serif und Ghinea verwendet. In einer *komperativen* Studie wird die OOBE eines *Head-Mounted Displays* (HMD) und eines *Personal Digital Assistant* (PDA) untersucht und verglichen. Es werden vier häufige Fehlerquellen genannt, welche die OOBE negativ beeinflussen können [155, S. 5]:

1. Initiale Einrichtungszeit
2. Zu viele Kabel, Stecker und Adapter
3. Eine überwältigende Menge an Dokumentation
4. Verwirrender Inhalt von Benutzerhandbüchern

Zusätzlich sind in der Arbeit Fragenbögen für acht unterschiedliche Kategorien der OOBE enthalten, welche zwar für eine Nutzer-Studie konzipiert wurden, jedoch für die Untersuchung in dieser Arbeit als Grundlage verwendet werden können. Die acht Kategorien in denen die UX untersucht wird, werden im Folgenden vorgestellt [155, S. 8-9]:

1. **Verpackung:** Diese Kategorie misst die ersten Eindrücke bezüglich der Geräte-Verpackung. Idealerweise sollte ein Produkt so verpackt sein, dass es leicht und sicher an einen Zielort transportiert und der Inhalt jedes Kartons eindeutig identifiziert werden kann.

2. **Auspacken:** In dieser Kategorie geht es darum, die Leichtigkeit und Effizienz beim Auspacken des Produkts festzustellen. Das Ziel ist es, dass die Vorbereitung des Geräts für den Aufbau schnell und einfach erfolgt.

3. **Aufbau:** Beim Aufbau wird untersucht, ob die physische Anordnung und der Zusammenbau von Komponenten mit Leichtigkeit erfolgt und ob die zugehörigen Anleitungen intuitiv gestaltet sind. Das Ziel ist es, alle Komponenten so schnell wie möglich für den Gebrauch vorzubereiten und dabei keine Gelegenheit für Fehler zu lassen.

4. **Einschalten:** Hierbei geht es um die Gestaltung der Einschalterfahrung: Dazu gehören Punkte wie Rückmeldungen, ob der Aufbau erfolgreich war und visuelle Belohnungen wie z.B. Dankes- und Willkommens-Meldungen. Das Ziel ist es, sofort zu überprüfen, ob die Einrichtung oder der Zusammenbau ordnungsgemäß durchgeführt wurde und alles korrekt funktioniert.

5. **Konfiguration:** Dieser Bereich misst die Konfigurationserfahrung nach der erfolgreichen Installation. Das Ziel der Konfiguration ist es, unter minimaler Benutzerinteraktion möglichst automatisiert und transparent zu sein.

6. **Erstbenutzung:** Diese Kategorie misst die leichte Zugänglichkeit von Funktionen und Möglichkeiten des Produkts. Das Hauptziel besteht darin, dem Nutzer zu bestätigen, dass die Entscheidung für das Produkt sinnvoll war, und ihm das Vertrauen zu geben, dass Produkt in vollem Umfang nutzen zu können.

7. **Arbeiten:** In diesem Bereich wird untersucht, wie einfach es ist, sinnvolle Aktivitäten mit dem Produkt durchzuführen. Das Hauptziel besteht darin, das Gerät produktiv einzusetzen.

8. **Hilfe:** Hier wird typischerweise die Verfügbarkeit von Hilfsquellen bei jedem Schritt der ersten Erfahrung untersucht, wie z.B. schriftliche Anweisungen, Fehlerbehebungen, Online-Support und Hilfegruppen. Ziel ist es, bei der Lösung von Problemen zu helfen, und so schnell wie möglich Support zu erhalten.

Die Schritte 1-6 lassen sich zur Untersuchung der OOBE von Privacy-Boxen verwenden. Allerdings muss der Schritt 3 für den Nutzertyp „Techniker“ noch erweitert werden. Für ihn ist neben dem Zusammenbau der Hardware noch die Installation der „Open Source“-Software notwendig. Dazu gehört der Download einer aktuellen Firmware und das Installieren auf den Datenspeicher des jeweiligen Geräts. Daher wird ein für *Techniker* notwendiger Unterpunkt hinzugefügt:

3.1 **Installation:** Diese Kategorie untersucht, ob der Download und die Installation von aktueller Firmware gut dokumentiert und einfach durchzuführen ist. Das Ziel ist es, die benötigte Firmware so schnell und einfach wie möglich auf dem Gerät zu installieren.

Der 7. Schritt betrifft die Erledigung von typischen Anwendungsszenarien, deren Untersuchung zur Beantwortung der zweiten Forschungsfrage (F2) im nächsten Abschnitt erarbeitet wird. Der 8. Schritt wiederum betrifft die Verfügbarkeit und Bereitstellung von

Support- und Hilfe-Themen. Da er sowohl für die OOBE als auch für die Ausführung typischer Anwendungsszenarien relevant ist, wird er zur Ergänzung beider Forschungsfragen mit betrachtet. Die vollständige Liste mit Fragen zur Evaluation und Bewertung der OOBE wurde übersetzt und für eine Verwendung mit Privacy-Boxen angepasst. Alle Fragen wurden in positiver Form formuliert und können in Anhang B.2 nachgeschlagen werden.

5.4.3 Vergleich von Evaluationsmethoden

Da die Fragen aus Schritt 7 der OOBE-Evaluation allerdings nicht zur Beantwortung der zweiten Forschungsfrage (F2) ausreichen, steht im nächsten Schritt die Wahl einer passenden Methode aus dem Katalog der analytischen Verfahren an, um die typischen Anwendungsszenarien zu untersuchen.

Zu diesem Zweck werden die vier im Grundlagenteil bereits vorgestellten analytischen Methoden *Heuristische Evaluation* (HE), *Cognitive Walkthrough* (CW), *GOMS* und *Guideline-Review* (GR) (siehe „Analytische Evaluation (expertenorientiert)“ in Abschnitt 2.4.3) hinsichtlich verschiedener Gütekriterien untersucht und bewertet. Dabei werden Bewertungen der genannten Methoden aus verschiedenen Arbeiten miteinander verglichen. Dieses Vorgehen hilft dabei, die Bewertungen der einzelnen Autoren zu validieren und möglichst viele Gütekriterien bei der Wahl einer passenden Methodik mit einzubeziehen.

Zu Beginn des Vergleichs wird auf die bereits im Grundlagenteil verwendete Vorstellung von Evaluationsmethoden zurückgegriffen: Im zehnten Kapitel „Usability-Testing“ des Buches *User Experience Design* vergleicht Christian Moser sowohl analytische als auch empirische Evaluationsmethoden hinsichtlich verschiedener Gütekriterien: Es werden „Fachwissen“, „Aufwand“ und „Effektivität“ nach praktischer Relevanz sowie „Validität“, „Reliabilität“ und „Objektivität“ nach wissenschaftlicher Relevanz gruppiert. Dabei werden die Methoden mithilfe eines Drei-Sterne-Systems bewertet, wobei ein Stern eine „geringe“ und drei Sterne eine „hohe“ Ausprägung bedeuten [130, S. 225].

Eine weitere Bewertung von Evaluationsmethoden findet sich im „Methodenhandbuch zur nutzerzentrierten Entwicklung“ des *Kompetenzzentrums Usability für den Mittelstand* (KUM). Hier werden verschiedene Methoden hinsichtlich Kriterien zum *Aufwand-Nutzen-Verhältnis* wie „Relevanz“, „Aufwand zur Durchführung“, „Anpassbarkeit des Aufwands“ und einer „Anwendungsempfehlung“ sowie *Expertisenfaktoren* wie „notwendige Expertise“, „Aufwand zum Expertisenaufbau“, „Anpassbarkeit notwendiger Expertise“ und einer „Handlungsempfehlung“ verglichen. Die Bewertung erfolgt mithilfe eines Ampel-Systems, wobei die Zuordnung der Ampel-Farben unterschiedlich ist (grün kann je nach Kontext „gering“ oder „hoch“ bedeuten) [108, S. 5-6].

Die dritte Bewertung bedient sich des Vergleichs aus dem vierten Kapitel „Methoden der Usability-Evaluation“ des gleichnamigen Buches von Sarodnick und Brau. Es wird ebenfalls zwischen Kriterien mit Praxisrelevanz und wissenschaftlicher Relevanz unterschieden. Die bereits genannten Kriterien mit Praxisrelevanz werden um den „Detaillierungsgrad“ der Methode sowie eine Unterscheidung zwischen „materiellem-“ und „zeitlichem Aufwand“ erweitert. Im Bereich der wissenschaftlichen Relevanz kommt als „Evaluator-Effekt“ noch

ein Experten-bezogenes Kriterium dazu. Die Bewertung findet mithilfe eines Drei-Punkte-Systems statt, wobei ein Punkt einem „geringen“ und drei Punkte einem „hohen“ Ausmaß entsprechen [147, S. 201-202].

Der letzte Vergleich von Usability-Methoden stammt aus der bereits im „Related Work“-Teil erwähnten Arbeit *„Auswahl einer geeigneten Methode zur Usability Evaluation“* von Philipp Jordan (siehe „Usability-Evaluation und Methodik“ in Abschnitt 3.4.3). Die Vorgehensweise ist der von Sarodnick und Brau ähnlich – es wird ebenfalls ein Drei-Punkte-System zur Bewertung verwendet. Jordan übernimmt zudem die Güte-Kriterien von Sarodnick und Brau und erweitert diese um Kriterien wie „Identifikation individueller Nutzungsprobleme“, „Anwendbarkeit im Entwicklungsprozess“, „Standardisierungsgrad“ und „Bandbreite der erhobenen Daten“ [100, S. 76-77].

Um die vier vorgestellten Arbeiten miteinander vergleichen zu können, werden zunächst die unterschiedlichen Bewertungen normalisiert. Die Bewertungen von Ampel-, Sterne- und Punkte-System werden dabei wie folgt in Zahlenwerte umgerechnet:

1.0 für Bewertungen mit • / ∗ / • (entspricht einer schlechten/geringen Ausprägung)

2.0 für Bewertungen mit • / ∗ ∗ / • • (entspricht einer mittleren Ausprägung)

3.0 für Bewertungen mit • / ∗ ∗ ∗ / • • • (entspricht einer guten/hohen Ausprägung)

Dabei muss, vor allem bei den unterschiedlichen Bewertungen des Ampel-Systems, auf den jeweiligen Kontext geachtet werden, sodass die neue Bewertung Sinn ergibt.

Anschließend werden die teilweise voneinander abweichenden Bezeichnungen von Kategorien vereinheitlicht und zusammengeführt. Bei den Bezeichnungen der Kategorien mit praktischer Relevanz werden *zeitlicher* und *materieller* „Aufwand“ zusammengefasst, „Qualifikation“ mit „Fachwissen“ gleichgesetzt und „Effizienz“ mit „Produktivität“ in Relation gebracht. Bei den Kategorien mit wissenschaftlicher Relevanz werden die Begriffe „Validität“ und „Vorhersagekraft“, „Objektivität“ und „Unbeeinflussbarkeit“ sowie „Reliabilität“ und „Zuverlässigkeit“ als gleichwertig betrachtet.

Für die Berechnung wird jeder Methode in jeder Kategorie die normalisierte Bewertung des entsprechenden Autors eingetragen (falls vorhanden). Bei zusammengefassten Kategorien (z.B. fasst Aufwand „zeitliche“ und „materielle“ Ausprägungen zusammen) wird bereits gemittelt. Anschließend werden für jede Kategorie Mittelwerte aus den Bewertungen der Autoren gebildet. Von diesen Kategorie-Werten werden anschließend erneut Mittelwerte für die Bereiche „Praktische Relevanz“ und „Wissenschaftliche Relevanz“ bestimmt. Zuletzt wird von den Werten aller Kategorien ein Mittelwert berechnet und das Ergebnis für die jeweilige Methode auf- oder abgerundet (die zugrunde liegende Berechnung kann in Anhang A.5 nachvollzogen werden).

Da ein hoher Aufwand bei der Evaluation im Rahmen dieser Arbeit als Nachteil zu sehen ist, wird die Kategorie „Aufwand“ negativ bewertet[142]. Wie in Abb. 25 zu sehen ist, sind HE und GOMS im geringen (-1,5) bis mittleren Bereich (-1,8) deutlich weniger aufwändig in der Durchführung als CW oder GR im mittleren (-2,0) bis hohen Bereich (-2,3). Die Kategorie „Expertenwissen“ hingegen wird positiv bewertet, da der Expertiseaufbau im

Rahmen dieser Arbeit als positiver Einfluss für die Untersuchung gesehen wird. GR und HE benötigen im hohen Bereich (2,5) ein deutlich größeres Expertenwissen als CW oder GOMS im mittleren Bereich (2,0).

Neben „Aufwand“ und „Expertenwissen“ werden noch „Effizienz“, „Detailgrad“, „Flexibilität“ und „Individualität“ zu den Kriterien mit praktischer Relevanz gezählt. Die durchschnittliche praktische Relevanz der Methoden GR und GOMS liegt mit 1,7 bzw. 1,8 fast im mittleren Bereich. Der CW schneidet mit 2,2 schon überdurchschnittlich ab, wobei die praktischer Relevanz der HE mit 2,7 fast im guten Bereich liegt (vgl. Abb. 25).

Die wissenschaftliche Relevanz wird aus den Kategorien „Validität“, „Objektivität“ und „Reliabilität“ gebildet. Hier liegen die Methoden GR und GOMS mit Durchschnitts-Werten von 2,3 bzw. 2,4 fast im guten Bereich. Sie schneiden deutlich besser als CW und HE ab, die es mit Werten von 1,8 bzw. 1,9 fast in den mittleren Bereich schaffen:

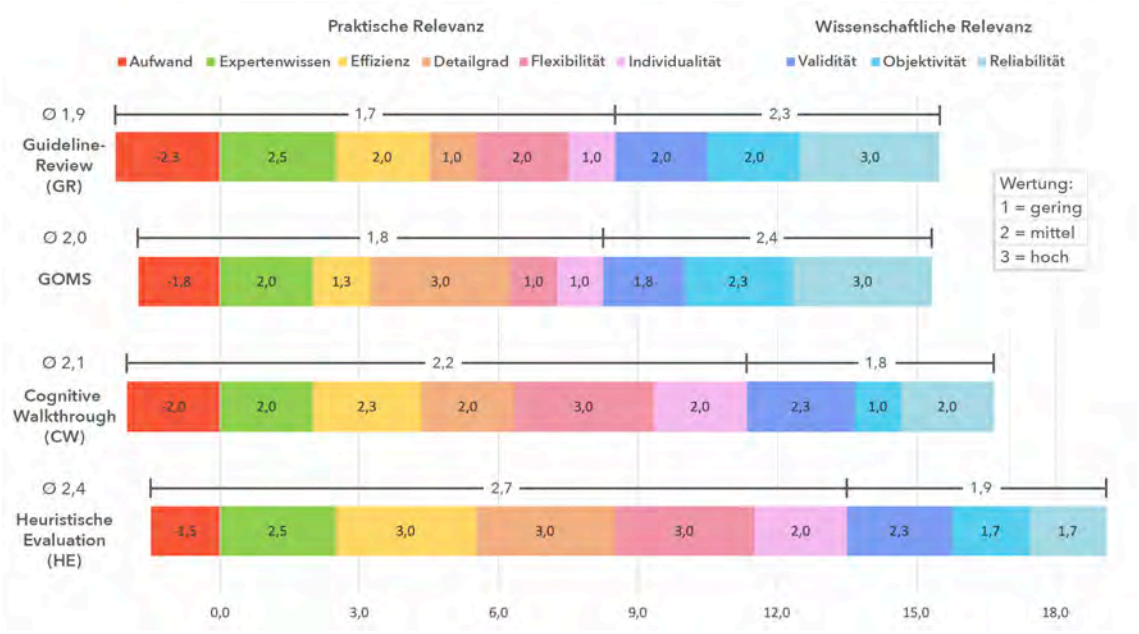


Abbildung 25: Vergleich von analytischen Evaluationsmethoden[142]

Wie in Abb. 25 zu sehen ist, liegt die Methode HE, unter Berücksichtigung aller Güte-Kriterien, mit einer Gesamt-Relevanz von 2,4 im fast hohen Bereich und tritt damit als die vielversprechendste Methode aus diesem Vergleich analytischer Evaluations-Methoden hervor. Es folgen mit etwas Abstand die Methoden CW, GOMS, und GR dicht hintereinander im mittleren Relevanz-Bereich mit Werten von 2,1, 2,0 und 1,9 (siehe auch Anhang A.5).

5.4.4 Methode des Heuristic Walkthrough

Die HE ist eine sehr populäre Methode für analytische Usability-Untersuchungen, da sie einfach zu verstehen ist und sich leicht anwenden lässt. Jedoch ist die Methode wenig strukturiert, da dem Evaluator die Liste mit Heuristiken als einzige Orientierungshilfe zur Verfügung steht. Es fehlt der Fokus auf konkrete Benutzeraufgaben, was zu vereinfachten Bewertungen und Falsch-Identifikation von Usability-Problemen führen kann. Dies

142 Die negative Bewertung des „Aufwands“ dient nur dem besseren Verständnis, da ein hoher Aufwand sonst einem kleinen Wert entspräche. In der Berechnung wurden positive Werte verwendet (Anhang A.5).

geschieht, wenn ein Verstoß gegen Heuristiken außerhalb des Nutzungskontextes betrachtet und somit als Fehler bewertet wird [153, S. 219].

Der CW ist ebenfalls eine etablierte analytische Methode für Usability-Evaluationen, die einen sehr strukturierten Prozess bietet. Die Durchführung geschieht mit einer Liste von Benutzeraufgaben, die jeweils anhand von vier Fragen bewertet werden müssen. Während es der HE an Struktur fehlt, kann der CW zu viele Vorgaben liefern, was Evaluatoren bei der Exploration eines Systems entmutigen kann. Dies schränkt ihre Fähigkeit ein, Probleme zu finden, die nicht direkt mit der ausgeführten Aufgabe zusammenhängen. Die sehr detaillierte Beschreibung von Nutzeraufgaben kostet zusätzlich Zeit beim Erstellen und Ausführen der Untersuchung mittels CW [153, S. 219].

Um die genannten Nachteile zu vermeiden und die Stärken beider Methoden zu vereinen, entwickelte Andrew Sears 1997 den *Heuristic Walkthrough* (HW): Er kombiniert die Freiform-Evaluation und Usability-Heuristiken aus der HE mit Benutzeraufgaben und Fragen zu wichtigen Teilen des Interaktionsprozesses aus dem CW. Der HW umfasst daher sowohl eine freiform- als auch eine aufgabenbasierte Evaluation, wobei der Evaluator von einer priorisierten Liste von Nutzeraufgaben, einer Liste von Usability-Heuristiken und einer Liste von „Gedanken-fokussierenden“ Fragen geleitet wird [153, S. 219]. Der HW besteht aus zwei Durchläufen:

Der erste Durchlauf zählt als *aufgabenorientierte Evaluation*. Sie wird von Nutzeraufgaben angeleitet und von „Gedanken-fokussierenden“ Fragen unterstützt. Die Nutzeraufgaben bestehen aus wichtigen und häufig genutzten Tätigkeiten, können aber auch zusätzliche Aktivitäten mit geringer Relevanz beinhalten. Die Aufgaben sind der Nutzungshäufigkeit entsprechend mit einer Priorisierung versehen. Der Evaluator untersucht die Nutzeraufgaben in beliebiger Reihenfolge und verbringt dabei so viel Zeit, wie er für nötig erachtet. Die Priorität leitet ihn jedoch bei der Auswahl von zu untersuchenden Aufgaben an. Der erste Durchlauf stellt sicher, dass die Erfahrung des Evaluators mit dem System aufgabenorientiert abläuft, ebenso wie bei Nutzern, die lernen das System zu benutzen [153, S. 220].

Bei der Untersuchung von Nutzeraufgaben kann sich der Evaluator an vier Fragen orientieren, die zum Nachdenken anregen und aus dem CW abgeleitet sind (eine ausführlichere Liste der Fragen kann in Anhang B.3 gefunden werden) [153, S. 220-221]:

1. Werden die Nutzer wissen, was sie als nächstes tun müssen?
2. Werden die Nutzer bemerken, dass es ein Steuerelement (z.B. Schaltfläche, Menü) gibt, mit dem sie den nächsten Teil ihrer Aufgabe erledigen können?
3. Wenn die Nutzer das Steuerelement gefunden haben, werden sie dann wissen, wie es zu benutzen ist (z.B. Anklicken, Doppelklick, Pulldown-Menü)?
4. Wenn die Nutzer die richtige Aktion ausführen, werden sie dann sehen, dass Fortschritte bei der Erledigung der Aufgabe gemacht werden?

Der zweite Durchlauf stellt eine *Freiformauswertung* dar und ermöglicht es dem Evaluator, jeden Aspekt des Systems zu untersuchen. Dabei lässt er sich von den im ersten Durchlauf gewonnen Erkenntnissen, der Liste an Nutzeraufgaben, den gedankenfokussierenden Fra-

gen und den Usability-Heuristiken leiten [153, S. 221]. Jede etablierte Liste von Usability-Heuristiken kann verwendet werden, wobei häufig die *„10 Usability Heuristics for User Interface Design“* von Jakob Nielsen aus dem Jahr 1994 zum Einsatz kommen [134].

Auch wenn Nielsen's Heuristiken sich über die Jahre hinweg bewährt haben, sind sie zu unspezifisch, um bei einer Evaluation konkret angewendet werden zu können. Die *„First Principles of Interaction Design“* von Bruce Tognazzini, welche 2014 in einer überarbeiteten und erweiterten Fassung erschienen sind, bieten an dieser Stelle einen deutlich höheren Detailgrad, der für den Evaluator von Vorteil ist [167].

Um aus den beiden bewährten Heuristiken von Nielsen und Tognazzini einen Katalog mit konkreten Fragen für die Durchführung einer HE zu erstellen, kombinierte Toni Granollers 2018 beide Heuristiken miteinander. In der Arbeit *„Usability Evaluation with Heuristics, Beyond Nielsen's List“* entwickelt Granollers eine neue Liste mit Usability-Heuristiken, die aus dem Vergleich und der Integration von Eigenschaften beider Heuristiken hervorgeht:

Nielsen		Tognazzini			Resulting Principles
Visibility of system status	⇔	Visible Navigation	+	Discoverability	**1.- Visibility and system state**
Match between system and the real world	⇔	Human Interface Objects	+	Metaphors, Use of	**2.- Connection between the system and the real world, metaphor usage and human objects**
User control and freedom	⇔	Explorable Interfaces			**3.- User control and freedom**
Consistency and standards	⇔	Consistency			**4.- Consistency and standards**
Recognition rather than recall	⇔	Anticipation	+	Learnability	**5.- Recognition rather than memory, learning and anticipation**
Flexibility and efficiency of use	⇔	Efficiency of the User	+	Efficiency of the User	**6.- Flexibility and efficiency of use**
Help users recognize, diagnose, and recover from errors					**7.- Help users recognize, diagnose and recover from errors**
Error prevention					**8.- Preventing errors**
Aesthetic and minimalist design	⇔	Aesthetics	=	Simplicity	**9.- Aesthetic and minimalist design**
Help and documentation					**10.- Help and documentation**
		Protect Users' Work	+	State	**11.- Save the state and protect the work**
		Colour	+	Readability	**12.- Colour and readability**
		Autonomy			**13.- Autonomy**
		Defaults			**14.- Defaults**
		Latency Reduction			**15.- Latency reduction**

Abbildung 26: Kombination der Heuristiken von Nielsen und Tognazzini (mod. n. [76, S. 61])

Wie in Abb. 26 zu sehen ist, definiert Granollers folgende 15 Prinzipien, indem er die Usability-Heuristiken von Nielsen mit denen von Tognazzini kombiniert und ergänzt (eine ausführlichere Liste der Heuristiken kann in Anhang B.4 gefunden werden, übersetzt nach [76, S. 62]):

1. Sichtbarkeit und Systemstatus
2. Verbindung zwischen System und realer Welt, Metaphorik und menschliche Objekte
3. Kontrolle und Freiheit des Nutzers
4. Konsistenz und Standards
5. Erkennen statt Erinnern, Lernen und Vorhersehen
6. Flexibilität und Effizienz der Nutzung
7. Nutzern helfen, Fehler zu erkennen, zu diagnostizieren und zu beheben
8. Fehler vermeiden
9. Ästhetische und minimalistische Gestaltung
10. Hilfe und Dokumentation
11. Speichern des Zustands und Sichern der Arbeit
12. Farbe und Lesbarkeit
13. Autonomie
14. Standardeinstellungen
15. Reduzieren der Wartezeit

Jede der 15 Heuristiken stellt zusätzlich eine Reihe konkreter Fragen bereit, die in einer für die Usability günstigen Weise formuliert sind. In der Literatur werden Gestaltungsprinzipien in verschiedenen Ausführungen vorgestellt. Die Formulierungen in unterschiedlicher Form (z.B. positiv und negativ oder eine Mischung aus beidem) sowie Varianten mit und ohne Frageform können den Evaluator bei der Arbeit verwirren. Da Fragesätze intuitiver, direkter und einfacher für die Evaluationsaufgabe zu verstehen sind, werden alle Beschreibungen der Usability-Prinzipien in Frageform formuliert [76, S. 63].

Darüber hinaus werden alle Fragen so formuliert, dass eine Beantwortung mit „Ja“ eine gute Benutzbarkeit des Merkmals darstellt – folglich bedeutet „Nein“ das Gegenteil. Falls die Beantwortung nicht eindeutig ist, kann mit „Weder noch“ ein Mittelwert definiert werden. Ist eine Frage für das Merkmal irrelevant, so dient die Antwort „Nicht anwendbar“ dazu, sie als unbedeutend zu markieren. Diese 4-Optionen-Bewertungsskala bestehend aus „Ja“, „Weder noch“, „Nein“ und „Nicht anwendbar“ (vgl. Tabelle 6), hilft dem Evaluator dabei, sich während der Untersuchung nicht mit der Bewertung des Schweregrads von Problemen auf einer Skala beschäftigen zu müssen [76, S. 63].

Somit lassen sich unzuverlässige Antworten gegen Ende der Evaluation vermeiden. Häufig lässt mit fortschreitender Zeit die Präzision des Evaluators, bei der Bewertung von Problemen, nach. Dabei ist es wichtiger alle Usability-Probleme zu finden, als direkt eine Bewertung des Schweregrads vorzunehmen. Dieser lässt sich auch später noch mithilfe der priorisierten Aufgabenreihenfolge bestimmen. Zusätzlich steht es jedem Evaluator frei, für jedes Problem so viele qualitative Kommentare zu verfassen wie nötig (z.B. für andere Evaluatoren oder verantwortliche Programmierer) [76, S. 63].

Zuletzt ermöglicht die Methode eine Quantifizierung der Ergebnisse, wodurch die Benutzbarkeit des evaluierten Interfaces berechnet werden kann. Dieser endgültige als „Usability-Prozentsatz“ (UP) bezeichnete Wert ermöglicht es, sowohl unterschiedliche UIs als auch die Bewertungen verschiedener Evaluatoren miteinander zu vergleichen. Für die Berechnung des UPs werden daher alle Antworten mit folgender Bewertung gewichtet (vgl. Tabelle 6):

Antwort	Bewertung
Ja	1 Punkt
Weder noch	0,5 Punkte
Nein	0 Punkte
Nicht anwendbar	–

Tabelle 6: Skala zur Bewertung der Usability-Evaluation [76, S. 63]

Durch den Ausschluss von nicht zutreffenden Antworten, die Addition aller Werte und einer Division durch die Anzahl relevanter Antworten, wird ein Prozentsatz bestimmt, der die Usability des Interfaces in einer vergleichbaren Zahlenform darstellt [76, S. 63].

Da eine analytische Evaluation anhand von Usability-Heuristiken den Themenbereich von Privacy-Boxen nur einseitig betrachtet, wird im Folgenden darauf eingegangen, ob Privacy-Heuristiken für die Usability-Evaluation von Privacy-Boxen relevant sind und dabei berücksichtigt werden müssen.

5.4.5 Berücksichtigung von Privacy-Heuristiken

Zur Überprüfung der Relevanz von Privacy-Heuristiken für die Usability-Evaluation von Privacy-Boxen werden drei unterschiedliche Ansätze geprüft, welche jeweils die *DSGVO* (siehe „Aktuelle Gesetzeslage“ in Abschnitt 2.3.1) zur Grundlage haben: 1. *Usable Privacy Criteria*, 2. *Privacy Design Strategies* und 3. *Digital Privacy Nudges*.

Usable Privacy Criteria

Der erste Ansatz stellt ein neues Modell zur Bewertung des Datenschutzes in *„Making GDPR Usable: A Model to Support Usability Evaluations of Privacy“* (2020) vor. Johansen und Fischer-Hübner kombinieren dabei Datenschutz-Prinzipien mit Usability-Kriterien. Dazu werden aus der DSGVO brauchbare Kriterien für den Datenschutz auf Grundlage von Usability-Zielen extrahiert, sodass beim Erreichen des jeweiligen Datenschutz-Ziels der Grad der Benutzbarkeit gemessen werden kann [98, S. 1].

Das entworfene Modell wird in Form eines Würfels dargestellt, dessen drei Achsen von 1. *Datenschutz-Prinzipien*, 2. *Rechten der Betroffenen* und 3. *Usability-Kriterien zum Schutz der Privatsphäre* dargestellt werden. Anschließend werden „Usable Privacy“-Grundsätze anhand der Rechtsgrundlage von *DSGVO* unter Berücksichtigung des Nutzungskontexts nach *ISO/IEC 29100* (siehe „Datenschutzprinzipien“ in Abschnitt 2.3.2) und der Usability-Ziele aus *DIN EN ISO 9241-11* (siehe „Konzept der Gebrauchstauglichkeit“ in Abschnitt 2.4.2) hergeleitet [98, S. 9].

Zuerst definieren Johansen und Fischer-Hübner fünf „Usable Privacy“-Kriterien. Anschließend werden 30 Datenschutz-Ziele aus der DSGVO abgeleitet und unter Nennung der entsprechenden Gesetzesstellen den Kategorien zugeordnet. Zuletzt werden 24 „Usable Privacy“-Grundsätze daraus extrahiert (eine Übersetzung der Liste kann in Anhang B.5 gefunden werden) [98, S. 15-31]. Nach Übersetzung und Analyse dieser Privacy-Heuristiken wird deutlich, dass sie auf die Perspektive von Verantwortlichen und Betroffenen bei der Erhebung, Verarbeitung, Speicherung und Weitergabe von personenbezogenen Daten (PD) ausgelegt sind.

Für eine Usability-Untersuchung von Privacy-Boxen sind diese Privacy-Heuristiken relevant und hilfreich, wenn Anwendungsszenarien untersucht werden, bei denen PD erhoben, verarbeitet oder gespeichert werden. Dies ist bei Nutzerszenarien für „abhörsichere und geschützte Kommunikation“ (Privacy-Ziel: *Vertraulichkeit*) oder beim „Einsatz privater und datenschutzfreundlicher Alternativ-Dienste“ (Privacy-Ziel: *Autonomie*) der Fall.

Für die Usability-Untersuchung von Privacy-Boxen im Rahmen dieser Arbeit kann jedoch keine Mehrwert durch die Anwendung der Privacy-Heuristiken ermittelt werden. Bei den zu untersuchenden Anwendungsszenarien von Privacy-Boxen werden keine PD erhoben, verarbeitet oder gespeichert. Bei den definierten Nutzerszenarien (siehe „Geräteauswahl und Nutzerszenarien“ in Abschnitt 5.3.3) geht es um „Privatsphäre beim Surfen im Internet“ und „Schutz vor Tracking und Tracing“ (Privacy-Ziel: *Anonymität*) sowie das „Erkennen von Schwachstellen“ und „Verhindern von Gefahren“ (Privacy-Ziel: *IT-Schutz*).

Privacy Design Strategies

Der zweite Ansatz versucht die Lücke zwischen dem rechtlichen Rahmen der (damals noch vorgeschlagenen) DSGVO, verfügbaren Datenschutz-Designstrategien und technologischen Umsetzungsmaßnahmen (Stand 2015) zu schließen. Die Arbeit *„Privacy and Data Protection by Design – from policy to engineering“* wurde von der European Union Agency for Cybersecurity (ENISA) gefördert. Sie kombiniert Datenschutz mit Usable Privacy, indem auf den elf Datenschutzprinzipien aus *ISO/IEC 29100* (siehe „Datenschutzprinzipien“ in Abschnitt 2.3.2) und den sieben *Grundprinzipien des PbD* (siehe „Privatheit als Standard und Voreinstellung“ in Abschnitt 2.4.4) aufgebaut wird [57, S. 5-6].

Die Arbeitsgruppe leitet ebenfalls Prinzipien der Privatsphäre und des Datenschutzes aus dem Rechtsrahmen von *EU Richlinie 95/46/EG* und dem *Vorschlag zur DSGVO* (siehe „Entwicklung der Datenschutzgesetze“ in Abschnitt 2.3.1) ab und ordnen sie den entsprechenden Gesetzesstellen zu. Auf dieser Grundlage werden acht *Privacy-Design-Strategien* entwickelt, die auf der Arbeit von Hoepmann (siehe Tabelle 1 „Anwendbarkeit von Strategien zu Prinzipien beim Datenschutz“) aufbauen und die Arbeit von Gürses et al. (siehe „Konzepte für den Datenschutz“ in Abschnitt 3.3.1) berücksichtigen. Für einige der acht Strategien werden konkrete Entwurfsmuster genannt, mit deren Hilfe eine Umsetzung von *Privacy-Design-Strategien* möglich oder überprüfbar wird [57, S. 18-22]:

Prinzip	*Privacy-Design-Strategie*	*Entwurfsmuster zur Umsetzung*
Minimieren	Beschränkung der Menge an PD auf ein Minimum	− Selektion vor der Erhebung + Anonymisierung und Pseudonym
Verbergen	Verbergen der Beziehung von Daten untereinander und vor der Öffentlichkeit	+ Verschlüsseln von Daten + Heterogene Netzwerke − Entkoppeln von Ereignissen
Trennen	Getrennte Verarbeitung oder Speicherung von PD	–
Aggregieren	Verarbeitung von PD mit höchstem Verdichtungsgrad und geringstem Detailgrad	− Zeitlich getrennte Verdichtung + Dynamische Standortverteilung
Informieren	Angemessenes Informieren bei Verarbeitung von PD	− P3P-Datenschutzrichtlinien − Meldungen über Datenverletzungen
Kontrollieren	Vollmacht für Betroffene bei Verarbeitung von PD	− Identitätsmanagement + Ende-zu-Ende-Verschlüsselung
Durchsetzen	Durchsetzbarkeit von Datenschutzrichtlinien	− Zugriffskontrolle − Digitale Rechteverwaltung
Demonstrieren	Nachweis zur Einhaltung von Datenschutzrichtlinien	− Datenschutzmanagement-Systeme − Protokollierung und Prüfung

Legende: + = Mit Privacy-Box umsetzbar. − = Nicht mit Privacy-Box umsetzbar.

Tabelle 7: Privacy-Design-Strategien und Entwurfsmuster [57, S. 19-22]

Wie in Tabelle 7 zu sehen ist, lassen sich bei den Prinzipien „Minimieren“, „Verbergen“, „Aggregieren“ und „Kontrollieren“ Entwurfsmuster erkennen, die mithilfe von Privacy-Boxen umgesetzt werden können (mit + markiert). Mit einer *Anonymisierung* von Daten beim *Surfen im Internet* können Priacy-Boxen zum Prinzip „Minimieren“ beitragen.

Mit der Nutzung von *Mesh/TOR*-Netzwerken kann durch Privacy-Boxen eine heterogene und dynamische Datenverteilung erreicht werden, was zu den Prinzipien „Verbergen“ und „Aggregieren“ passt. Zusätzlich können Daten bei der *Kommunikation* Ende-zu-Ende-verschlüsselt oder mittels VPN-Tunnel auch während dem Transport geschützt werden, was zu den Prinzipien „Verbergen“ und „Kontrollieren“ beiträgt.

Abgesehen von der Möglichkeit den *Privacy-Design-Strategien* durch eine Zuordnung zu Datenschutz-Funktionen von Privacy-Boxen eine Relevanz zu geben, fehlt ihnen ein konkreter Maßstab, um im Rahmen einer Usability-Untersuchung eine Aussagekraft über die Wirkungsweise zu entfalten. Zusätzlich reduziert sich die Schnittmenge an untersuchbaren Strategien auf die Prinzipien „Minimieren“ und „Verbergen“, aufgrund der zuvor definierten Anwendungsszenarien. Aus diesen Gründen werden Entwurfsmuster zur Umsetzung der *Privacy-Design-Strategien* bei der Usability-Untersuchung nicht mit einbezogen.

Digital Privacy Nudges

Im dritten und letzten Ansatz geht es um die Verwendung von „Privacy Nudges“. Beim *Nudging*, was in etwa „leichtes Anstoßen“ oder „Stupsen“ bedeutet[143], geht es darum, das Verhalten eines Benutzers in eine bestimmte Richtung zu lenken, ohne dabei Optionen zu verbieten. Im Bezug auf Privacy sollen „Nudges“ den Nutzern dabei helfen, „bessere“ Datenschutzentscheidungen zu treffen.

Bereits im Jahr 2006 zeigten Cranor et al. mit der Untersuchung des P3P-Tools *Privacy Bird* die Bedeutung von Feedback zu datenschutzrelevanten Informationen. Der Aspekt wurde von Leon et. al 2012 aufgegriffen und einem Mangel an Kenntnissen der Nutzer über datenschutzkritische Themen zugeschrieben. 2020 konkretisiert Hubert et al. den Grund auf mangelnde Verständlichkeit sowie fehlende Führung und Unterstützung von Nutzern bei Datenschutzrelevanten Prozessen (siehe „Benutzbarkeit von Security- und Privacy-Tools“ in Abschnitt 3.4.1). Der zeitliche Verlauf der Arbeiten verdeutlicht die immer stärkere Konkretisierung dieser Vorgehensweise über die Jahre hinweg.

Eine wichtige Grundlage zum Thema „Nudging“ im Bezug auf Privacy- und Security-Themen wird in der Arbeit *„Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online“* (2017) von Acquisti et al. gelegt. Nach ausführlicher thematischer Herleitung und dem Aufzeigen von sowohl positiven als auch negativen Einflüssen, die Privacy-Nudging mit sich bringen kann, werden sechs relevante Dimensionen herausgearbeitet [2, S. 44:13]. Die Arbeit wird von Schomberg et al. aufgegriffen und mithilfe weiterer Literatur in *„Ansatz zur Umsetzung von Datenschutz nach der DSGVO im Arbeitsumfeld: Datenschutz durch Nudging“* (2019) um den Kontext digitaler Arbeitssysteme erweitert. Die daraus resultierenden sechs *Privacy-Nudge-Prinzipien* werden in Abb. 27 dargestellt und im Folgenden mit konkreten Beispielen eingeführt [152, S. 333-334]:

1. **Standards:** „Default Nudges“ stellen Standardeinstellungen für die Privatsphäre in Systemen dar, die von Individuen in digitalen Umgebungen zumeist nicht ihren Bedürfnissen angepasst werden. Somit bleiben die voreingestellten Optionen in den meisten Fällen, unverändert bestehen. Standards stellen zudem oft einen „Anker“ für Nutzer

143 Nudge, Übersetzung Englisch-Deutsch (de.langenscheidt.com/englisch-deutsch/nudge)

dar, gegen den weitere Enscheidungsoptionen unbewusst abgewogen werden. Standards gelten als sehr effektiv, da sie in digitalen Systemen das Maß der angestrebten Datensparsamkeit vorgeben.

2. **Farbelemente:** Sie eignen sich sehr gut als „Privacy Nudges“, denn durch farbliche Markierungen kann die Aufmerksamkeit schnell auf bestimmte Elemente gelenkt werden. Somit lassen sich bestimmte Entscheidungs-Optionen verstärkt hervorheben. Im angegebenen Beispiel wird z.B. der Button für die Einstellung „Privat“ in grüner Farbe hervorgehoben, um den Nutzer zu beeinflussen diese Option zu wählen (vgl. Abb. 27). Die Vorteile der Farbelemente zeigen sich vor allem in der einfachen Umsetzung von „Nudges“, die den Nutzer schnell und effektiv dazu bewegen, seine Entscheidungen bezüglich des Datenschutzes und der Privatsphäre zu überdenken.

3. **Information:** Die Wahrscheinlichkeit einer Privatsphäre-Verletzung ist für Nutzer häufig nicht nachvollziehbar und wird oft unterschätzt. Nutzer tendieren dazu, risikoreiche Entscheidungen in Bezug auf den Schutz der eigenen Privatsphäre zu treffen. Um diesem Problem entgegenzuwirken, wird der Nutzer über Risiken und Konsequenzen seines Handelns aufgeklärt. Ein Beispiel ist die Anzeige der Anzahl an Personen, welche die Nachrichten eines Nutzers sehen können (vgl. Abb. 27). Basierend auf diesen Informationen kann er eine fundierte Entscheidung in Bezug auf die eigene Privatsphäre treffen.

4. **Feedback:** Die Bereitstellung von Feedback, welches auf das bisherige Nutzungsverhalten hinweist, kann ebenfalls als „Privacy Nudge“ genannt werden. Es hilft dabei beim Nutzer ein Bewusstsein über seine bisherigen Entscheidungen und deren Konsequenzen aufzubauen. Als Beispiel können Fortschritts-Balken zur Visualisierung von Passwort-Komplexität oder preisgegebenen Profildaten genannt werden (vgl. Abb. 27). So werden Nutzer spielerisch dazu motiviert, ein komplexeres Passwort zu wählen, oder weniger Profildaten preiszugeben.

5. **Zeitverzögerung:** Bei digitalen Entscheidungen über die Privatsphäre werden oftmals risikoreiche und wenig durchdachte Entscheidungen getroffen, ohne mögliche Spätfolgen zu bedenken. Um dem entgegenzuwirken, kann eine zeitliche Verzögerung als „Privacy Nudge“ verwendet werden. Als Beispiel kann ein Countdown von fünf Sekunden verwendet werden, bevor eine Nachricht mit privaten Inhalten veröffentlicht wird (vgl. Abb. 27). In dieser Zeit besteht weiterhin die Möglichkeit, die Nachricht zurückzuziehen, zu bearbeiten oder die Wartezeit zu überspringen. So kann der Nutzer dazu bewegt werden, weniger impulsiv zu agieren und die Nachricht sowie mögliche negative Konsequenzen zu überdenken.

6. **Soziale Norm:** Die Wirkung dieser „Privacy Nudges“ basiert auf dem Prinzip von sozialen Normen: Der Nutzer leitet dabei aus dem Verhalten seiner Mitmenschen ab, inwiefern es angemessen ist, persönliche Informationen zu teilen. Ist für Nutzer z.B. erkenntlich, dass 75% Prozent der Kollegen ihre Telefonnummer nicht im Arbeitsprofil angegeben haben (vgl. Abb. 27), kann diese Information als Referenzpunkt für das eigene Verhalten herangezogen werden. Diese „Nudges“ können verwendet werden, um Nutzer zu besseren Entscheidungen in Bezug auf den Schutz ihrer Daten zu befähigen.

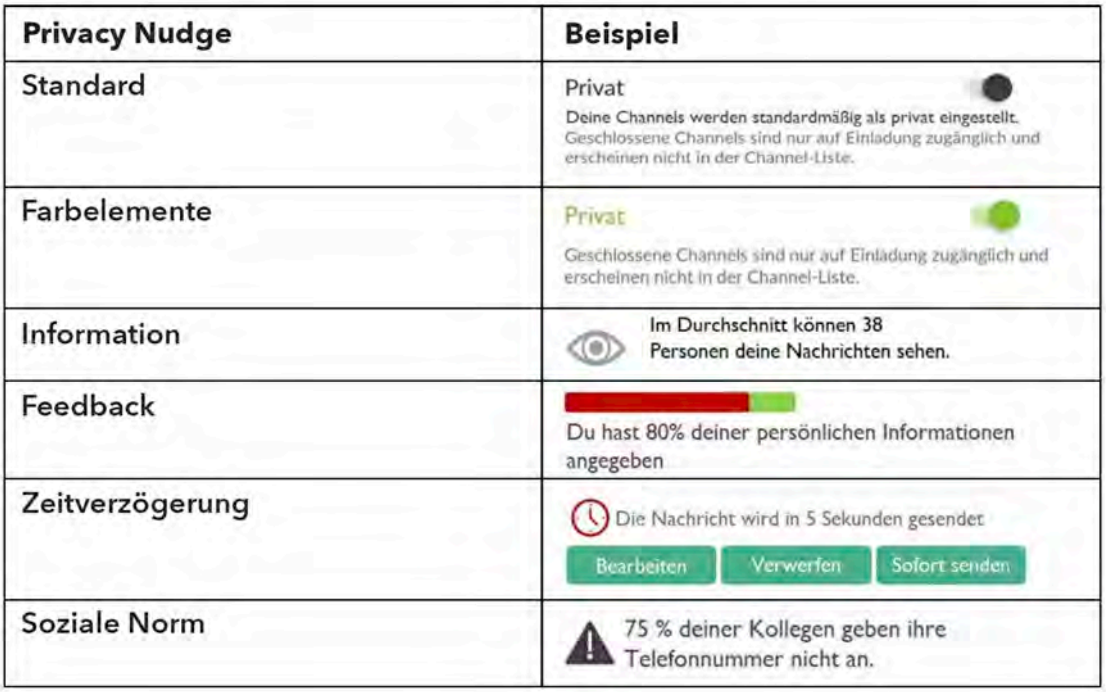


Abbildung 27: Sechs Prinzipien Digitaler Privacy Nudges (mod. nach [152, S. 332])

Um zu ermitteln, welche der vorgestellten „Privacy Nudges“ (vgl. Abb. 27) von Nutzern präferiert werden, untersuchen Schöbel et al.[144] in *„Understanding User Preferences of Digital Privacy Nudges – A Best-Worst Scaling Approach“* (2020) die Nutzerpräferenzen zur Einordnung in einer Skala von „best“ (beste) bis „worst“ (schlechteste) „Nudges“. Um ihre vorherige Arbeit zu validieren, wurde aus 22 vergleichbaren Arbeiten zum Thema „Privacy Nudging“ eine Schnittmenge von acht verschiedenen „Privacy Nudges“ gebildet.

Dabei bleiben die bisherigen Kategorien gleich, nur *Farbelemente* werden unterteilt in Ausprägungen mit „roter“ und „grüner“ Farbe und die „Fortschrittsanzeige“ aus *Feedback* erhält eine eigene Kategorie. Bei der Umfrage mit 177 Teilnehmern wurden an erster Stelle „Privacy Nudges“ in Form von *Standards* präferiert, gefolgt von *Farbelementen* in roter und grüner Ausprägung. *Feedback*, *Information* und *Soziale Norm* folgen im Anschluss und am wenigsten favorisiert werden *Zeitverzögerung* und *Fortschrittsanzeige* [151, S. 3920-3924]. Eine Abbildung der erweiterten Kategorien inklusive „Nutzer-Ranking“ kann in Anhang B.6 gefunden werden.

Da „Privacy Nudges“ sehr universell einsetzbar sind, auch außerhalb des Kontexts der Verarbeitung von PD, und als Heuristiken eine Schnittmenge der Bereiche Usability und Privacy darstellen, werden sie bei der Usability-Evaluation von Privacy-Boxen berücksichtigt. Durch die ermittelten Nutzerpräferenzen steht sogar eine Bewertungsskala zur Verfügung, sodass im Rahmen der Usability-Evaluation untersucht werden kann, inwiefern von Nutzern präferierte „Privacy Nudges“ in UIs von Privacy-Boxen implementiert sind.

Im nächsten Kapitel wird zunächst die Vorgehensweise der Usability-Untersuchung zusammengefasst, bevor diese anschließend dokumentiert und die Ergebnisse vorgestellt werden.

144 Der Hauptteil der Autoren entspricht dem Team der vorherigen Arbeit bis auf Sabrina Schomberg

6 Untersuchung von Privacy-Boxen und Ergebnisse

Nachdem die Methodik für die Usability-Evaluation und den anschließenden Vergleich von Privacy-Boxen erarbeitet wurde, folgt zunächst eine Zusammenfassung des Untersuchungs-Ablaufs. Anschließend wird die Durchführung der Untersuchung dokumentiert und es werden die Ergebnisse vorgestellt. Diese werden anschließend diskutiert, interpretiert und auf Gültigkeit überprüft, bevor die Forschungsfragen (F1) und (F2) beantwortet werden. Im letzten Kapitel folgen ein Fazit und der Ausblick für zukünftige Arbeiten.

6.1 Durchführung der Untersuchung

Nachdem der Untersuchungsgegenstand und die Zielgruppe mit zwei relevanten Nutzertypen in den Abschnitten 5.1 und 5.2 beschrieben wurden, konnten in Abschnitt 5.3 typische Anwendungsszenarien und relevante Geräte für die Evaluation ausgewählt werden. Nach der Entwicklung einer Evaluations-Methodik in Abschnitt 5.4, wird im Folgenden ein konkreter Fahrplan für die Usability-Untersuchung von Privacy-Boxen vorgestellt.

6.1.1 Beschreibung der Vorgehensweise

Bevor die Untersuchung durchgeführt wird, erfolgt die Beschreibung der Vorgehensweise. Die Untersuchung der Privacy-Boxen wird dabei in fünf Phasen unterteilt:

1. Ermittlung der Out-of-Box Experience (OOBE) anhand der Heuristiken von Moya und Burgess (Anhang B.1) und der Fragebögen von Serif und Ghinea (Anhang B.2)
2. Untersuchung der Usability mit typischen Anwendungsszenarien und Usability-Heuristiken mit Heuristic Walkthrough (HW) nach Granollers (Anhänge B.3 und B.4)
3. Überprüfung der Implementierung von Privacy-Heuristiken in Form von Privacy-Nudges nach Schomberg et. al und Bewertung nach dem User-Ranking von Schöbel et al. (Anhang B.6)
4. Auswertung der Ergebnisse und Berechnung von UX-, Usability- und Privacy-Scores
5. Vergleich von Ergebnissen mit einem Gerät aus der selben Nutzer-Gruppe

Bei der Untersuchung werden vier Privacy-Boxen aus der repräsentativen Vorauswahl untersucht (siehe „Geräteauswahl und Nutzerszenarien“ in Abschnitt 5.3.3), jeweils zwei Geräte für die Nutzertypen „Bemühte Amateure“ und „Techniker“:

Geräte für „Bemühte Amateure“

- Bitdefender BOX 2
- F-Secure SENSE

Geräte für „Techniker“

- TrutzBox Home
- eBlocker 2

Dabei werden aufgrund der unterschiedlichen Funktionsausprägung der Geräte für jeden Nutzertyp fünf unterschiedliche Anwendungsszenarien untersucht. Diese werden ihrer Wichtigkeit entsprechend, anhand der Relevanz von Anwendungsbereich und Funktion (siehe „Schutzpotenzial von Privacy-Boxen“ in Abschnitt 5.3.2), wie folgt priorisiert:

Szenarien für „Bemühte Amateure“

1. Verwendung eines *VPN-Tunnels*
2. Aktivieren von *Inhaltsfiltern*
3. Konfiguration der Netzwerk-*Firewall*
4. Einrichtung von *Anti-Virus*
5. Einstellen des *IoT-Monitors*

Szenarien für „Techniker“

1. Einrichtung von *Anti-Tracking*
2. Einstellen des *DNS-Schutzes*
3. Verwendung eines *VPN-Tunnels*
4. Konfiguration von *Ad-Blockern*
5. Aktivieren von *Inhaltsfiltern*

Bei den Szenarien für „Bemühte Amateure“ werden die Aufgaben zur Einrichtung von *VPN-Tunnel* und *Inhaltsfilter* höher priorisiert, da sie zum relevanten Anwendungsbereich „Surfen im Internet“ gehören. Aufgaben zur Konfiguration von *Firewall*, *Anti-Virus* und *IoT-Monitor* aus dem nächst relevanten Bereich des „IT-Schutzes“ folgen im Anschluss. Bei den „Technikern“ gehören alle Szenarien zum relevanten Anwendungsbereich „Surfen im Internet“. Daher werden Aufgaben wie *Anti-Tracking*, *DNS-Schutz* und *VPN-Tunnel*, mit einer hohen Auswirkung beim „Schutz vor Tracking/Tracing“, stärker priorisiert, als Aufgaben zur Einrichtung von *Ad-Blockern* und *Inhaltsfiltern* mit geringerer Auswirkung.

Alle Heuristiken, welche zur direkten Bewertung der Usability/UX verwendet werden, sind in positiver Frageform formuliert, sodass sie nach dem Bewertungsschema von Granollers ausgewertet werden können (siehe Tabelle 6). Einzig für die Untersuchung von Privacy-Nudges fehlt noch ein Bewertungsschema, welches im Rahmen der „Auswertung der Ergebnisse“ in Abschnitt 6.2.1 erarbeitet wird. Im folgenden Abschnitt wird die Vorgehensweise der Untersuchung anhand der soeben zusammengefassten Kriterien dokumentiert und beschrieben.

6.1.2 Vorbereitungen und Pilot-Evaluation

Bevor mit der Durchführung der Untersuchung begonnen wird, werden im Vorfeld Pilot-Durchläufe mit Privacy-Boxen unternommen, die nicht für die Untersuchung ausgewählt wurden. Dies hat den Vorteil, dass die Abläufe für den Evaluator bereits verinnerlicht werden können, ohne dass der Vergleich relevanter Geräte und damit das Ergebnis im Vorfeld beeinflusst wird. Zusätzlich ermöglicht es die Funktionsweise der OOBE-Untersuchung zu überprüfen, welche für Privacy-Boxen adaptiert wurde und die Anwendbarkeit und Korrektheit der deutschen Übersetzung von Usability-Heuristiken zu validieren.

Beim ersten Durchlauf wird die Untersuchung mit der Privacy-Box *RATtrap* pilotiert (Durchführung eines Testdurchlaufs). Dabei fällt bereits auf, dass einige Fragen zur Verpackung weniger relevant sind (z.B. „Transportfähigkeit“), jedoch eine Beurteilung des Verpackungs-Designs fehlt. Des Weiteren fehlt eine Frage zur Vollständigkeit von Komponenten für die initiale Inbetriebnahme, im Fall von *RATtrap* ist ein zusätzlicher Adapter für das US-Netzteil notwendig. Zusätzlich wird deutlich, dass bei der Einrichtung einer Privacy-Box ein Benutzer-Account eingerichtet und das Gerät verknüpft bzw. eine Lizenz aktiviert werden muss. Da dieser Schritt bei vielen Privacy-Boxen notwendig ist (siehe Zeile „Abo-Preis in €“ in Tabelle 3), wird eine entsprechende Kategorie mit dem Punkt „Registrierung“ hinzugefügt.

Die Usability-Evaluation lässt sich mit dem Gerät *RATtrap* nicht pilotieren, da die automatische Konfiguration des Geräts mit den Cloud-Diensten fehlschlägt. Aus diesem Grund wird die bereits verbesserte OOBE mit der Privacy-Box *Keezel 2.0* erneut getestet. Die Einrichtung ist hier durch einen beigelegten Quickstart-Guide besonders übersichtlich gestaltet, was als zusätzliche Frage mit aufgenommen wird. Zudem wird deutlich, dass es keine „perfekte“ Abfolge der Fragen gibt, da die Reihenfolge der Einrichtung von Gerät zu Gerät variiert. Einige Fragen können bereits früher, manche erst später beantwortet werden. Auch bei diesem Durchlauf lässt sich die OOBE nicht erfolgreich abschließen, da das Gerät den Neustart nach Abschluss der Konfiguration verweigert.

Da in den ersten beiden Test-Durchläufe jeweils Produkte für den Nutzertyp „Bemühter Amateur“ berücksichtigt wurden, ist ein dritter Durchlauf notwendig, um auch noch die speziellen Fragen der OOBE für den Nutzertyp „Techniker“ zu testen. Hierfür wird die Privacy-Box *Syncloud R* auf einem *Raspberry Pi 3+*[145] eingerichtet. Bei den für „Techniker“ relevanten Fragen wird deutlich, dass nicht nur die Installation der Firmware, sondern auch der Zusammenbau der Privacy-Box an sich berücksichtigt werden muss. Beides geschieht vor dem Aufbau und Anschluss des Geräts. Die Identifikation der Syncloud im Heimnetz wird mithilfe einer mobilen App gelöst. Dabei wird deutlich, dass die zur Konfiguration benötigte App auf gängigen Plattformen verfügbar sein muss. In diesem Fall ist die App lediglich für Android verfügbar. Für die Untersuchung stehen daher sowohl ein *iPhone 6S*[146] mit iOS, als auch ein *Galaxy A6*[147] mit Android zur Verfügung.

Für den Test-Durchlauf der Usability-Evaluation wird die Installation und Konfiguration eines *Pi-hole* auf der Syncloud als typisches Anwendungsszenario durchgeführt. Dabei tauchen bei einigen der übersetzten Fragen Probleme mit der Formulierung auf und werden dementsprechend überarbeitet. Zudem wird bei der Einrichtung des Pi-hole als DNS-Server in der *FRITZ!Box*[148] des Heim-Netzwerks deutlich, dass eine Fehl-Konfiguration bei der Untersuchung den Ausfall des Internets zur Folge haben kann. Aus diesem Grund wird mithilfe einer weiteren FRITZ!Box ein unabhängiges Sub-Netz aufgebaut, mit dem die Untersuchung „gefahrlos“ durchgeführt werden kann.

Zuletzt fällt auf, dass Teile der Bewertung von „Hilfe und Support“ sich bei OOBE und HW doppeln, weshalb die Fragen so angepasst werden, dass sie sich klar voneinander unterscheiden. Zur Berücksichtigung der letzten Heuristik von Moya und Burgess (H8: „Die Einrichtung darf nicht zu lange dauern“, siehe Anhang B.1), wird zusätzlich die bei der OOBE benötigte Zeit gemessen. Diese Zeitmessung wird (aus Interesse) auch bei der Durchführung von Nutzeraufgaben im Rahmen der Usability-Evaluation durchgeführt.

Nach den Vorbereitungen und Pilot-Durchläufen für die Evaluation von OOBE, Usability und Usable-Privacy, wird im folgenden Abschnitt mit der Untersuchung der ausgewählten Privacy-Boxen begonnen. Dabei können für die OOBE maximal 37 bzw. 44 Punkte („Bemühte Amateure“/„Techniker“) und beim HW maximal 60 Punkte erreicht werden.

145 Raspberry Pi 3 Model B+ (raspberrypi.org/products/raspberry-pi-3-model-b-plus)
146 Apple iPhone 6S (support.apple.com/kb/sp726)
147 Samsung Galaxy A6 (samsung.com/de/support/model/SM-A600FZDNDBT)
148 AVM FRITZ!Box (avm.de/produkte/fritzbox)

6.1.3 Dokumentation der Untersuchung

Für die Usability-Untersuchung der Privacy-Boxen wird eine FRITZ!Box verwendet, welche den Zugang zum Internet, mehrere Netzwerk-Anschlüsse (LAN) und ein drahtloses Netzwerk (WLAN) bereitstellt. Als Einrichtungs-Geräte stehen ein iPhone 6S (iOS 14), ein Galaxy A6 (Android 10) sowie ein *ASUS Laptop*[149] (Windows 10, Ubuntu 18) und ein *Apple MacBook*[150] (macOS Catalina) zur Verfügung. Die Untersuchung der ausgewählten Privacy-Boxen beginnt mit den Geräten des Nutzertyps „Bemühter Amateur“ (siehe „Datenschutz-Nutzertypen (Personas)“ in Abschnitt 5.2.1).

Bitdefender BOX 2

Für die „Bemühten Amateure“ wird zuerst die *Bitdefender BOX 2* (BOX) untersucht (vgl. Abb. 28a). Die Untersuchung beginnt mit der OOBE, wobei direkt das ansprechende Verpackungs-Design auffällt. Der Karton lässt sich schwer öffnen, dafür sind alle Komponenten klar geordnet und es liegt direkt ein Quickstart-Guide bereit. Entgegen der ersten Vermutung befindet sich die Inventar-Liste jedoch nicht im Handbuch, sondern kann erst nach kurzer Suche auf der äußeren Verpackung entdeckt werden. Zusätzlich wird kein Hinweis auf die enthaltene „Bitdefender Total Security“ Software-Suite entdeckt.

Dem Verpackungs-Design folgend, ist auch die BOX selbst ansprechend gestaltet (vgl. Abb. 28a). Entgegen des schweren Gewichts der Verpackung ist die BOX allerdings sehr leicht und wirkt dadurch weniger hochwertig. Der Übergang von Handbuch zur App für die Einrichtung und Konfiguration der BOX ist mithilfe von QR-Codes sehr schnell und einfach möglich (mit iOS über die Kamera-App, bei Android ist zusätzlich eine QR-Code-App notwendig). Die *Bitdefender Central App*[151] lässt sich allerdings auch über die Suche im *App Store* oder *Play Store*[152] finden (vgl. Abb. 28b). Die Einrichtung wird anschließend mithilfe der App schrittweise erklärt und illustriert. Allerdings können Einzelschritte nicht widerrufen, sondern nur der gesamte Prozess abgebrochen werden.

Unter Anleitung ist der Aufbau der BOX einfach möglich, der Anschluss von Kabeln ist jedoch nicht farblich, sondern nur mit Symbolen gekennzeichnet. Durch den farbigen LED-Ring mit Animationen ist der Zustand der BOX immer gut zu erkennen. Die jeweilige Bedeutung kann dabei im Handbuch nachgeschlagen werden. Die verschiedenen Anschluss-Optionen werden nicht illustriert, die Central App zeigt lediglich eine Auswahl in Text-Form an. Auch im Handbuch gibt es dazu nur weitere QR-Code-Links zu *YouTube*-Videos[153].

Die Registrierung des im Rahmen der Einrichtung anzulegenden Nutzer-Accounts funktioniert schnell, die Eingabe einer Lizenz zur Aktivierung des Geräts ist nicht notwendig. Das Gerät wird nach der Verknüpfung mit dem Nutzer-Account automatisch aktiviert. Nach erfolgreicher Einrichtung ist die Konfiguration der BOX über die Central App möglich, allerdings werden weder ein Tutorial noch „Erste Schritte“ angezeigt, um das UI und die wichtigsten Funktionen kennenzulernen.

149 ASUS Zenbook UX32VD (asus.com/DE/supportonly/UX32VD/HelpDesk_Knowledge)
150 Apple MacBook Pro 13” 2017 (support.apple.com/kb/SP754)
151 Bitdefender Central App (apps.apple.com/de/app/bitdefender-central/id969933082)
152 App Store (apple.com/de/app-store), Play Store (play.google.com/store)
153 YouTube (youtube.com)

Die gesamte Einrichtung wurde mit der iOS-App auf einem iPhone 6S durchgeführt (vgl. Abb. 28b) und dauerte knapp eine halbe Stunde. Von 37 möglichen Punkten waren 36 Punkte bewertbar (vgl. Tabelle 6), von denen die BOX bei Evaluation der OOBE insgesamt 31 Punkte erreicht (siehe Anhang C.1). Anschließend wird mit der Evaluation der Usability anhand von typischen Anwendungsszenarien fortgefahren.

(a) Bitdefender BOX 2 (b) Bitdefender Central App

Abbildung 28: Bitdefender BOX 2 und Bitdefender Central App (iPhone 6S)

Die erste Nutzer-Aufgabe besteht in der Einrichtung eines *VPN-Tunnels*, um den privaten Datenverkehr zu schützen und persönliche Informationen wie IP-Adresse und Standort zu verschleiern. Der einzige Hinweis innerhalb der Central App ist die Möglichkeit, ein kostenpflichtiges Upgrade auf *Premium VPN*[154] vorzunehmen. Nach längerer Suche für eine entsprechende Funktion wird deutlich, dass VPN weder über die Central App noch die BOX genutzt werden kann.

Die VPN-Funktion ist zwar in der *Total Security*[155] Software-Suite enthalten, lässt sich aber auf dem verwendeten Testgerät (iPhone 6S) nur mithilfe einer weiteren App nutzen. Nach Download der entsprechenden *VPN App*[156] und Login mit dem zuvor erstellten Nutzer-Account ist die Einrichtung und Nutzung eines VPNs möglich, allerdings nur mit einem begrenzten Kontingent von 200 Megabyte (MB) pro Tag und nicht über die BOX.

Die zweite Aufgabe hat mit der Aktivierung von *Inhaltsfiltern* den Schutz vor kritischen Diensten und Inhalten zum Ziel. Auch für diese Funktion ist eine intensive Suche und Auseinandersetzung mit allen Bereichen der Central App notwendig. Die Lösung kann schließlich in der Nutzerverwaltung gefunden werden: Sie ermöglicht die Zuordnung von Geräten im geschützten BOX-Netzwerk zu einzelnen Personen oder dem gesamten Haushalt. Nach mehreren Versuchen lässt sich feststellen, dass die Verwaltung eines *Inhaltsfilters*

154 Bitdefender Premium VPN (bitdefender.de/solutions/vpn.html)
155 Bitdefender Total Security (bitdefender.de/solutions/total-security.html)
156 Bitdefender VPN App (apps.apple.com/de/app/bitdefender-vpn/id1499633482)

erst nach dem Anlegen eines Benutzers vom Typ „Kind“ möglich wird. Im Profil des Kindes sind entsprechende Kategorien von Web-Inhalten (Glücksspiel, Pornografie, Rauschmittel) bereits blockiert und können nach Bedarf angepasst werden. Der Test mithilfe eines zweiten Geräts (Galaxy A6) zeigt jedoch, dass der Inhaltsfilter des entsprechenden Nutzers nur nach Installation und Einrichtung der zusätzlichen *Parental Control App*[157] funktioniert.

Die Untersuchung kann anschließend nicht fortgeführt werden, da alle die BOX betreffenden Funktionen in der Central App nicht mehr dargestellt werden. Da das geschützte WLAN weiterhin zur Verfügung steht, ist zunächst nicht klar, wo das Problem liegt. Nachdem die BOX trotz diverser Neustarts signalisiert, dass etwas nicht stimmt (rot drehender LED-Ring), muss sie auf Werkseinstellungen zurückgesetzt und nochmals neu eingerichtet werden. Auch wenn dieser Prozess gut dokumentiert und einfach durchzuführen ist, so stellt er doch einen „Showstopper“[158] bei der Benutzung des Geräts dar.

Nach dieser Unterbrechung wird mit der dritten Aufgabe, der Konfiguration und Einrichtung der Netzwerk-*Firewall*, fortgefahren. Hierzu lässt sich keinerlei Information in der Central App finden, weder im Bereich zur Konfiguration der BOX, noch an anderen Stellen. Lediglich der Begrüßungs-Bildschirm gibt mit der Benachrichtigung „Ihr Zuhause ist sicher“ einen Hinweis darauf, dass der Netzwerk-Schutz, also vielleicht auch die Firewall, aktiv ist. Eine Übersicht oder Möglichkeit zur Konfiguration der Netzwerk-Firewall fehlt, es werden lediglich die MB an „geschütztem Datenverkehr“ angezeigt (vgl. Abb. 28b).

Bei der vierten Aufgabe ist die Einrichtung eines Schutzes durch *Anti-Virus*-Maßnahmen das Ziel. Wie schon bei der ersten Aufgabe, lässt sich innerhalb der Central App kein direkter Hinweis auf die Einrichtung eines Anti-Virus-Schutzes finden. Auf der Startseite gibt es im unteren Bereich mit „Erweitern Sie Ihre Sicherheitszone“ einen Hinweis, dass ein erweiterter Schutz für Computer und Smartphones existiert. Dem Download-Link folgend, ist auf Umwegen die Installation der *Mobile Security App*[159] möglich. Neben des VPN-Schutzes, der schon aus der VPN App bekannt ist, gibt es hier noch einen zusätzlichen „Internet-Schutz“. Die Aktivierung dieses zusätzlichen Filters schlägt unter iOS allerdings fehl, mit Android wiederum kann der Schutz genutzt werden.

Die fünfte und letzte Aufgabe betrifft die Aktivierung eines *IoT-Monitors* zur Überwachung auf ungewöhnliche Netzwerk-Aktivitäten. Hierzu findet sich sowohl auf der Startseite als auch im Menü unter „Mehr“ die Option eines Netzwerk-Scanners. Dieser ist allerdings nur manchmal, überwiegend nach Beitritt eines von der BOX nicht geschützten WLAN-Netzwerks, in der App verfügbar. Die zugrunde liegende Logik wird nicht kommuniziert und führt zu Verwirrung, da bereits gewohnte UI-Elemente manchmal verschwinden. Nach Durchführung des Scan-Vorgangs wird eine Netzwerk-Übersicht mit Informationen über ISP, Router und verbundene Geräte angezeigt. Ob dieser Netzwerk-Scan von der BOX auch eigenständig durchgeführt wird, bleibt unklar.

Die Usability-Evaluation der BOX wurde überwiegend mit der iOS-App auf dem iPhone 6S durchgeführt, es wurde zudem die Android-App auf dem Galaxy A6 berücksichtigt. Ins-

157 Bitdef. Parental Control App (apps.apple.com/de/app/bitdefender-parental-control/id1255210149)
158 Als „Showstopper“ wird ein gravierender Fehler bezeichnet, der den gesamten Folge-Prozess blockiert
159 Bitdef. Mobile Security App (apps.apple.com/de/app/bitdefender-mobile-security/id1255893012)

gesamt sind bei der Bewertung der Usability mit HW 60 Punkte möglich. Je nach Gerät und Funktionalität kann dieses Maximum jedoch auch geringer ausfallen. Bei der Untersuchung der BOX waren 56 Punkte bewertbar (vgl. Tabelle 6), von denen 37 Punkte bei der Evaluation erreicht wurden (siehe Anhang C.2). Bei der Untersuchung auf Privacy-Nudges konnten mit „Standard-Passwort für WLAN“, „Systemstatus in der App“, „Countdown bei Geräte-Neustart“ und „Passwort-Komplexität bei Registrierung“, vier Elemente aus unterschiedlichen Kategorien identifiziert werden (siehe Anhang C.4).

F-Secure SENSE

Als zweites Gerät für die „Bemühten Amateure“ wird der *F-Secure SENSE* (SENSE) untersucht (vgl. Abb. 29a). Auch die Evaluation des SENSE beginnt mit der OOBE beim Aufbau. Die Verpackung ist ansprechend und durchdacht gestaltet: Es beginnt bei der kleinen Stoff-Lasche, mit deren Hilfe sich der Inhalt einfach aus der äußeren Hülle ziehen lässt. In der Hand verbleibt anschließend eine Schnellstart-Karte aus hochwertigem Karton. Diese offenbart eine Inventar-Liste aller beinhalteten Komponenten, einen QR-Code zum Download der Konfigurations-App und Links für weitere Hilfe und Support. Jeder Zentimeter an Verpackungs-Platz ist sinnvoll genutzt und mit entsprechenden Symbolen gekennzeichnet, sodass alle Komponenten schnell gefunden werden können.

Beim Aufbau fällt neben dem Design auch das Gewicht des SENSE positiv auf, wodurch das Gerät hochwertig wirkt. Die Anschlüsse auf der Rückseite sind farblich markiert, was den richtigen Anschluss von Kabeln sehr einfach macht. Der Download der Einrichtungs-App ist im Gegensatz zur BOX über einen einheitlichen QR-Code gelöst. Dieser führt auf eine Webseite, von der sich die benötigte Variante der *F-Secure SENSE Router App*[160] vom jeweiligen App-Store herunterladen lässt (vgl. Abb. 29b).

Nach Installation der App auf dem iPhone 6S wird zuerst der SENSE über eine Bluetooth-Verbindung gekoppelt. Dies stellt sich im Anschluss als Vorteil heraus, da erst ganz am Ende der Einrichtung die App zum Beitritt des gesicherten WLANs verlassen werden muss. Hier wird das benötigte Passwort von der App bereits in die Zwischenablage kopiert und kann in den WLAN-Einstellungen einfach eingefügt werden.

Neben der sehr intuitiven und einfachen Einrichtung durch die Router-App steht zusätzlich ein Handbuch in acht verschiedenen Sprachen zur Verfügung. Auf der ersten Seite werden direkt alle Anschluss-Möglichkeiten des SENSE anschaulich illustriert. Zudem finden sich die Zustände des Segment-Displays ausführlich im Handbuch beschrieben. Dies hilft dabei, während der Einrichtung alle Schritte des Geräts nachvollziehen zu können. Zusätzlich gibt es für jeden Zustand des Geräts eine entsprechende Handlungsempfehlung.

Während der gesamten Einrichtung muss weder ein Nutzer-Account angelegt, noch eine Lizenz zur Aktivierung der Cloud-Dienste eingegeben werden. Es ist zudem einfach möglich, einen Schritt zurück zu gehen, ohne dass der Prozess abbricht. Am Ende der Einrichtung aktualisiert SENSE automatisch die Firmware und zeigt den erfolgreichen Abschluss der Konfiguration an. Anschließend fehlt eine Erklärung über die wichtigsten Funktionen des SENSE in Form von „ersten Schritten“ oder einem Tutorial.

160 F-Secure SENSE Router App (apps.apple.com/de/app/f-secure-sense-router/id1062846796)

Die Einrichtung wurde, wie schon bei der BOX, mithilfe der iOS-App und dem iPhone 6S durchgeführt (vgl. Abb. 29b) und dauerte ebenfalls etwa eine halbe Stunde. Von den 37 möglichen Punkten sind 34 Punkte bewertbar (vgl. Tabelle 6), von denen der SENSE 33 Punkte bei Ermittlung der OOBE erreicht (siehe Anhang C.1). Im Anschluss folgt die Ermittlung der Usability des SENSE anhand von typischen Anwendungsszenarien.

(a) F-Secure SENSE Router (b) F-Secure SENSE Router App

Abbildung 29: F-Secure SENSE Router und -App (iPhone 6S)

Die Einrichtung eines *VPN-Tunnels* ist erneut die erste Nutzer-Aufgabe. In den App-Funktionen und -Einstellungen kann allerdings nichts über VPN gefunden werden. Es wird nach einiger Suche deutlich, dass keine VPN-Funktion in der Router-App verfügbar ist. Des Weiteren stellt sich heraus, dass die beinhaltete Ein-Jahres-Lizenz eine Nutzung der Software-Suite *F-Secure TOTAL*[161] nicht einschließt. Erst nach der Registrierung mit einer Lizenz und dem Download der *Freedome VPN App*[162] ist die Einrichtung und Nutzung eines VPN-Tunnels möglich, jedoch ohne Verwendung des SENSE Routers.

Die entsprechende Stelle zur Erledigung der zweiten Aufgabe, die Aktivierung von *Inhaltsfiltern*, ist schnell zu finden: In den Einstellungen unter dem Menü-Punkt „More“ sind alle Schutz-Funktionen des Routers übersichtlich aufgelistet. Darunter sind auch Einstellungen für den Inhaltsfilter zu finden, diese beschränken sich allerdings auf das Hinzufügen von Webseiten, die von der Filterung ausgenommen werden sollen („Whitelist“). Es lässt sich nicht herausfinden, welche Seiten standardmäßig gefiltert werden („Blacklist“). Somit können auch keine neuen Seiten zur individuellen Filterung hinzugefügt werden.

Die dritte Aufgabe hat die Konfiguration der *Firewall* zum Ziel. Diese lässt sich ebenfalls in den Einstellungen der Router-App finden, allerdings sind die Möglichkeiten sehr eingeschränkt: Die einzige Option der Firewall-Konfiguration besteht im Anlegen von Port-Freigaben in Form von Weiterleitungen für Ports von bestimmten IP-Adressen.

161 F-Secure TOTAL (f-secure.com/de/home/products/total)
162 F-Secure Freedome VPN App apps.apple.com/de/app/f-secure-freedome-vpn/id771791010

Die Konfiguration eines Schutzes durch *Anti-Virus*-Maßnahmen ist Inhalt der vierten Aufgabe. Bei den bereits genannten Einstellungen der Schutz-Funktionen des Routers sind die Optionen „Geräte-Schutz“ und „Browser-Schutz“ schon per Voreinstellung aktiv. Die Recherche nach einem erweiterten Schutz führt lediglich zur Installation der *SAFE App*[163]. Dabei wird schnell deutlich, dass sich der Schutz nur auf Aktivitäten des in der App implementierten Browsers bezieht und nicht in Zusammenhang mit SENSE steht.

Für die letzte Aufgabe ist die Einrichtung eines IoT-Monitors notwendig. Die einzig verwandte Funktion kann in der Router-App im Bereich „Geräte“ gefunden werden. Es lassen sich dort alle Geräte anzeigen, die mit dem gesicherten Netzwerk verbundenen sind, auch getrennte Geräte werden dort aufgelistet. Diese Liste kann zwar aktualisiert, allerdings nicht als Scan- oder Monitor-Funktion bezeichnet werden.

Die Usability-Evaluation wurde mit der iOS-App auf dem iPhone 6S durchgeführt. Zum Vergleich wurde auch die Android-App auf dem Galaxy A6 untersucht. Optionen zur Verwaltung des SENSE waren keine zu finden[164]. Die Bewertung der Usability wurde ausschließlich für die Router-App und die beinhalteten Funktionen des SENSE durchgeführt. Insgesamt sind 56 der 60 möglichen Punkte bewertbar (vgl. Tabelle 6), von denen 43 Punkte bei der Untersuchung erreicht wurden (siehe Anhang C.2). Bei der Analyse von Privacy-Nudges wurden mit „Standard-Schutz von Geräten“ und „-Surfaktivität“, „Systemstatus in der App“ und „Einrichtungsfortschritt“ vier Elemente identifiziert (siehe Anhang C.4).

Nach der Analyse von Geräten für die „Bemühten Amateure“ werden im Anschluss die ausgewählten Privacy-Boxen für den Nutzertyp „Techniker“ untersucht (siehe „Datenschutz-Nutzertypen (Personas)“ in Abschnitt 5.2.1).

TrutzBox Home

Die *TrutzBox Home* wird als erstes Gerät für die „Techniker“ untersucht (vgl. Abb. 30). Die Ermittlung der OOBE beginnt erneut mit der Verpackung: Die TrutzBox ist in einem braunen Karton verpackt, der keine besondere Hilfe zum Öffnen anbietet. Die Vollständigkeit der Komponenten lässt sich mithilfe eines Lieferscheins und der „TrutzBox Setup-Anleitung“ überprüfen. Zusätzlich liegt eine „WLAN Einbau-Anleitung“ und eine „TrutzLegitimierung“ dabei. Die Dokumente sind auf verschiedenfarbige Papiere gedruckt, von denen sich die TrutzLegitimierung in rot als besonders wichtig vom Rest abhebt.

Die einzelnen Schritte für den Einbau der WLAN-Karte sind in der Einbau-Anleitung genau beschrieben und mithilfe von Bildern illustriert. Es wird sogar auf die „Erdung“ vor dem Öffnen der ESD-Hülle[165] zum Schutz der Komponenten vor elektrischer Entladung, hingewiesen. Der Einbau des WLAN-Moduls ist einfach, lediglich die Montage der Antennen gestaltet sich schwierig, da die Montage-Löcher eine spezielle Form aufweisen.

Die Installation von neuer Firmware auf der TrutzBox wurde vom Hersteller wegen einer längeren Lagerzeit zwischen Lieferung und Inbetriebnahme empfohlen. Der Prozess ist im

163 F-Secure SAFE App (apps.apple.com/de/app/f-secure-safe/id572847748)
164 Aufgrund der Bluetooth-Verbindung kann vermutlich nur ein Gerät den SENSE-Router verwalten.
165 ESD: Electrostatic Discharge/Elektrostatische Entladung (arbeitsschutz-express.de/de/lexikon/esd)

Normalfall allerdings nicht notwendig. Der Firmware-Download ist schwierig zu finden, erst nach genauer Untersuchung des Online-Wikis kann ein Link beim Punkt „Beschreiben der SSD“[166] gefunden werden. Ob es sich dabei um die aktuellste Version der Firmware handelt ist nicht überprüfbar. Der Quellcode ist zwar Open Source, aber das Repository[167] ist schwer zu finden und lässt keine offiziellen Releases zum Download erkennen.

Der Prozess für die Installation der Firmware wird im Online-Wiki gut erklärt und mithilfe der Software *Etcher*[168] und einem USB-Stick mit 32 GB Speicherplatz durchgeführt. Die TrutzBox kann anschließend über den USB-Anschluss mit neuer Firmware „betankt“ werden (Wortlaut des Herstellers). Der Kopiervorgang auf den internen Speicher funktioniert allerdings erst beim zweiten Versuch. Anschließend können die Einrichtungs-Schritte der Anleitung befolgt werden. Die Konfigurations-Bereitschaft der TrutzBox lässt sich, durch Mangel an Feedback, jedoch nicht eindeutig erkennen. Der Aufruf des UI über den Browser des MacBooks scheitert zunächst. Erst nach Austausch des beigelegten LAN-Kabels wird die TrutzBox als Netzwerkgerät erkannt.

Abbildung 30: TrutzBox Home mit eingebautem WLAN

Nach diesem „Showstopper“ verläuft die anschließende Einrichtung ohne weitere Probleme. Der Konfigurations-Assistent ermöglicht es, die Einrichtung auch ohne die beigelegte Anleitung erfolgreich abzuschließen. Dabei werden Accounts angelegt, die TrutzBox wird mit der Legitimierung beim Hersteller registriert und das WLAN-Netzwerk wird eingerichtet. Vor Abschluss der Einrichtung aktualisiert die TrutzBox automatisch die Software. Beim Login in das UI offenbart sich der zweite „Showstopper“: Das bei der Einrichtung vergebene Administrator-Passwort wird beim Login nicht akzeptiert.

Somit wird eine Wiederholung der gesamten Einrichtung notwendig. Aus Mangel eines Reset-Knopfes, zum Zurücksetzen auf Werkseinstellungen, wird eine erneute Installation der Firmware mithilfe eines schnelleren USB3-Sticks vorgenommen. Bei der zweiten Konfiguration wird bewusst auf die Verwendung spezieller Sonderzeichen im Administrator-Passwort verzichtet. Der Login nach Abschluss der zweiten Einrichtung funktioniert und

166 Wiki (wiki.trutzbox.de/view/TrutzBox_Handbuch#Anleitung_für_das_Beschreiben_der_SSD)
167 Quellen der Trutzbox-Software (update.comidio.com/repo/source)
168 balena Etcher (balena.io/etcher)

das Dashboard der TrutzBox wird angezeigt. Allerdings gibt es weder „Erste Schritte“ noch ein Tutorial, welche bei der Erstbenutzung durch das UI führen (vgl. Abb. 31).

Abbildung 31: Übersicht des TrutzBox-Dashboards nach Einrichtung und Nutzung

Die Einrichtung wurde auf dem MacBook im Safari-Browser durchgeführt und dauerte etwa zwei Stunden bei der ersten Einrichtung (inklusive Montage) und etwa eine halbe Stunde im zweiten Anlauf (exklusive Montage). Da bei der OOBE für „Techniker“ Zusammenbau und Installation berücksichtigt werden, liegt das erreichbare Maximum höher als bei den „Bemühten Amateuren“. Von 44 möglichen Punkten sind 42 Punkte bewertbar (vgl. Tabelle 6), von denen die TrutzBox 29,5 Punkte bei der OOBE erreicht (siehe Anhang C.1). Im Anschluss werden die Usability und das UI mithilfe typischer Nutzeraufgaben untersucht.

Zu Beginn werden die verschiedenen Betriebs-Modi der TrutzBox näher betrachtet. Die Variante, welche von der Anleitung bei der Einrichtung vorgegeben wird, ist der *Proxy-Modus*: Die TrutzBox agiert dabei als eine Art „Stellvertreter“ für den Router, indem der gesamte Datenverkehr über sie umgeleitet wird. Durch den Einbau des WLAN-Moduls ist der *Transparent-Modus* allerdings die bessere Wahl: Dabei wird jedes Gerät, welches sich mit dem WLAN der TrutzBox verbindet, automatisch und ohne Umleitung geschützt.

Damit der Schutz allerdings funktioniert, ist für jedes Gerät die Installation des TrutzBox *Root-Zertifikats* notwendig. Da die TrutzBox dieses Zertifikat selbst ausstellt, muss das Vertrauen ihr gegenüber auf jedem Endgerät manuell erteilt werden. Die Funktionsweise der TrutzBox entspricht damit einem vertrauenswürdigen „Man-in-the-Middle“. Nur so kann die Trutzbox auch verschlüsselte HTTPS-Verbindungen untersuchen. Das Root-Zertifikat kann über das Admin-Panel der TrutzBox auf jedem Gerät heruntergeladen werden.

Im Rahmen der Untersuchung wurde die Einrichtung mit allen verfügbaren Testgeräten durchgeführt: iPhone 6S (iOS), Samsung A6 (Android), MacBook (macOS) und Zenbook

(Windows und Linux). Der Installations-Prozess ist je nach Plattform und Browser unterschiedlich und ohne technisches Vorwissen nicht trivial durchzuführen. Mithilfe der vielfältigen Anleitungen im TrutzBox-Wiki ist diese Aufgabe jedoch zu schaffen, auch wenn die Anleitungen teilweise nicht ganz aktuell sind. Ein zusätzliches Gerät ist dabei hilfreich, da ansonsten zwischen Anleitung und Konfiguration gewechselt werden muss.

Die erfolgreiche Konfiguration wird anschließend durch das „TrutzBurg-Schild“ angezeigt. Dieses Overlay-Symbol zeigt sowohl die Anzahl impliziter Server-Aufrufe[169] (rechts) als auch die Anzahl geblockter Server-Aufrufe (links) an (vgl. Abb. 32). Die Aggressivität dieser Vorgehensweise lässt sich über einen „Security-Slider“ zwischen den Werten 1 (höchste Anonymität) und 10 (keine Anonymität) individuell einstellen. Die Konfiguration dieses *TrutzBrowse*-Mechanismus kann sowohl pro Seite, durch Auswahl des TrutzBurg-Schilds, als auch global in den Einstellungen definiert werden.

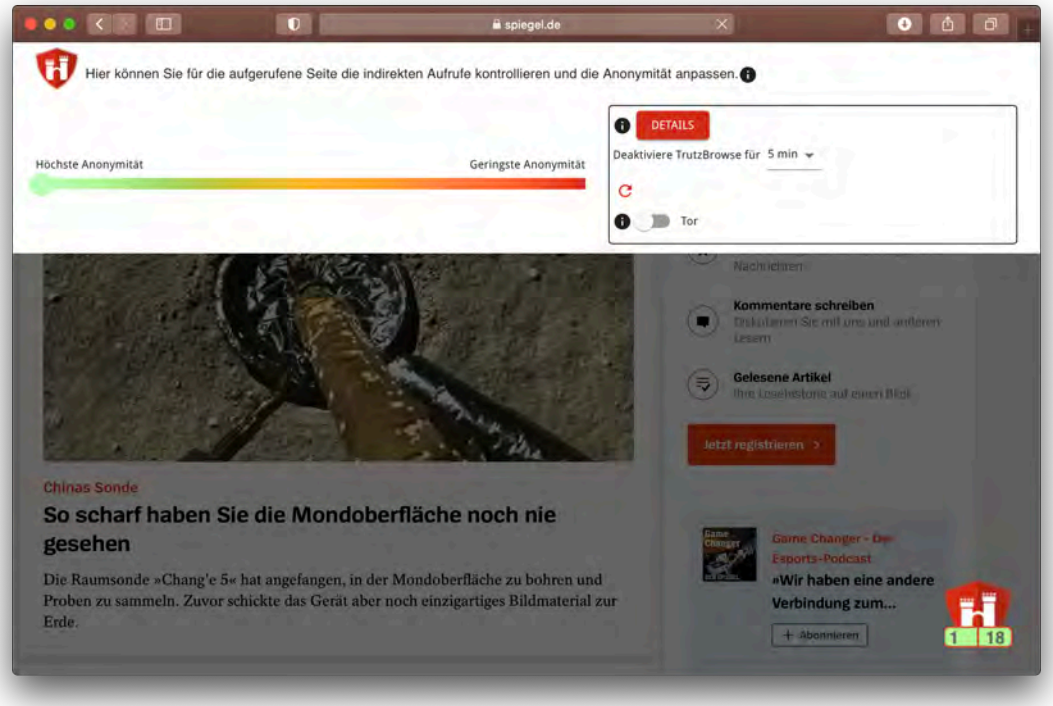


Abbildung 32: *TrutzBrowse* mit *Security-Slider* und *TrutzBurg-Schild* (spiegel.de)

Es gibt eine weitere Maßnahme, um den *Anti-Tracking*-Schutz für die erste Aufgabe zu konfigurieren. Zusätzlich zum Slider existiert eine globale „Blacklist“, mit der Inhalte zu speziellen Themengebieten gezielt blockiert werden können. Dabei ist der Schutz vor „Trackern“ und „Spyware“ bereits vorausgewählt, durch setzen des Filters für „Werbung“ lässt sich die vierte Aufgabe, das Aktivieren von *Ad-Blockern*, erledigen. Der Zusammenhang von „Blacklist“ und „Slider“ wird jedoch nicht direkt ersichtlich, zudem ist die Vielzahl an möglichen Optionen zunächst überwältigend.

Die zweite Aufgabe betrifft das Aktivieren eines *DNS-Schutzes*. Nach ausführlicher Suche in allen Funktions-Bereichen, lässt sich keine Funktion in Zusammenhang mit DNS finden. Lediglich im *Webmin-Bereich*, einer Verwaltungs-Oberfläche für die internen Trutzbox-

169 Implizite Server-Aufrufe erfolgen mit der ursprünglichen Anfrage, sind aber an andere Server gerichtet

Systeme, ist ein Eintrag über DNS vorhanden. Da allerdings davor gewarnt wird, dass Veränderungen in diesem Bereich die komplette Funktionalität der TrutzBox einschränken können, wird die Aufgabe an dieser Stelle abgebrochen.

Die Aktivierung eines VPN-Tunnels, zur Erledigung der dritten Aufgabe, ist über den Bereich „Netzwerk“ durch Einrichtung des *Fernzugriffs* möglich. Dazu muss im ersten Schritt *TrutzDynDns* aktiviert werden, damit die TrutzBox aus dem Internet erreicht werden kann. Anschließend ist die Generierung eines LetsEncrypt-Zertifikats[170] für die DynDNS-Adresse möglich, bevor der VPN-Server aktiviert werden kann. Dazu muss aber manuell sichergestellt werden, dass der VPN-Port (1194) im Router vorher freigegeben ist. Die Generierung der VPN-Zertifikate nimmt einige Zeit in Anspruch (es werden 30 Minuten angegeben).

Nach der erfolgreichen Aktivierung des VPN-Servers kann der Fernzugriff anschließend im Bereich der Benutzer-Verwaltung aktiviert werden. Beim Download der VPN-Konfiguration über das Dashboard, welche für die Verbindung eines Endgeräts benötigt wird, passiert jedoch nichts. Die Datei zur VPN-Konfiguration lässt sich allerdings auch über das interne Email-System der TrutzBox herunterladen (*TrutzMail*). Anschließend ist eine Übertragung auf das gewünschte Endgerät möglich (iPhone 6S), auf dem zunächst noch ein VPN-Client (*OpenVPN-App*[171]) installiert werden muss. Anschließend lässt sich die VPN-Konfiguration einrichten und eine VPN-Verbindung zur TrutzBox vom Smartphone aus herstellen.

Die fünfte und letzte Aufgabe betrifft die Konfiguration von *Inhaltsfiltern*. Dazu lassen sich im Verwaltungs-Bereich der TrutzBox sowohl Filtergruppen, als auch Filterlisten konfigurieren (*TrutzContent*). Bei den Filtergruppen handelt es sich um vorkonfigurierte „Blacklists“ für verschiedene Altersgruppen, die einzelnen Geräten zugeordnet werden können. Zusätzlich lassen sich die blockierten Themenbereiche bei Bedarf anpassen und es können eigene Filtergruppen erstellt werden. Die Filterlisten hingegen stellen eine Vielzahl an vordefinierten Listen dar, welche zu blockierende Domains/URLs beinhalten. Sie stellen die Grundlage für die Filterung nach Themenbereichen in den Filtergruppen dar.

Die Untersuchung der Usability wurde mit dem MacBook im Safari-Browser durchgeführt. Von den 60 möglichen Punkten sind bei der Usability-Evaluation 58 Punkte bewertbar (vgl. Tabelle 6), von denen 39 Punkte von der TrutzBox erreicht wurden (siehe Anhang C.2). Bei der Analyse von Privacy-Nudges ließen sich insgesamt 13 Elemente identifizieren: Standards bei *Security-Slider* und *Filterlisten*, Feedback durch das *TrutzBurg-Symbol* sowie *Systemstatus* und *Verbindungsprotokolle*, um einige Beispiele zu nennen (siehe Anhang C.4).

eBlocker 2

Als zweites Gerät für den Nutzertyp „Techniker“ wird der *eBlocker 2* untersucht. Für den Zusammenbau wird ein *Raspberry Pi 4*[172] inklusive Original-Netzteil, ein *Flirc Case*[173] mit passiven Kühleigenschaften und eine schnelle microSD-Karte mit 16 GB Speicherplatz verwendet (vgl. Abb. 33). Diese Konfiguration entspricht den Empfehlungen der „eBlocker: Do It Yourself – Selbstbau“-Anleitung [51].

170 Let’s Encrypt (letsencrypt.org)
171 OpenVPN Connect App (apps.apple.com/de/app/openvpn-connect/id590379981)
172 Raspberry Pi 4 Model B (raspberrypi.org/products/raspberry-pi-4-model-b)
173 Flirc Raspberry Pi 4 Case (flirc.tv/more/raspberry-pi-4-case)

Die Evaluation der OOBE beginnt mit einer Analyse der Verpackungen, welche allesamt die beinhalteten Komponenten erkennen lassen. Diese können einfach auspackt und in korrekter Art und Weise zusammen gebaut werden. Auch wenn dieser Prozess nicht in der Anleitung auf der eBlocker-Webseite erklärt wird, ist ein Zusammenbau der Komponenten intuitiv möglich. Anschließend muss die aktuelle Version der Firmware (*eBlockerOS*), heruntergeladen werden. Der entsprechende Download ist sowohl auf der Startseite, als auch in der Anleitung prominent platziert. Anhand der Release-Notes[174] lässt sich zudem feststellen, dass die Version nicht dem aktuellsten, sondern dem vorherigen Release entspricht.

Die Firmware kann mithilfe des Programms *Etcher* auf die microSD-Karte kopiert werden, der dafür notwendige Card-Reader wird in der Anleitung explizit erwähnt. Anschließend kann die Speicherkarte eingesteckt und der Raspberry Pi der Anleitung entsprechend angeschlossen werden. Auch auf das hierfür benötigte LAN-Kabel wird in der Anleitung hingewiesen. Nach dem Einschalten werden mindestens fünf Minuten Wartezeit empfohlen, bevor die Konfiguration des eBlockers beginnen kann. Diese lässt sich sowohl über eine iOS-App[175], als auch mithilfe des Browsers durchführen. Zur Vergleichbarkeit mit der TrutzBox wird die Einrichtung über das MacBook mit dem Safari-Browser durchgeführt.

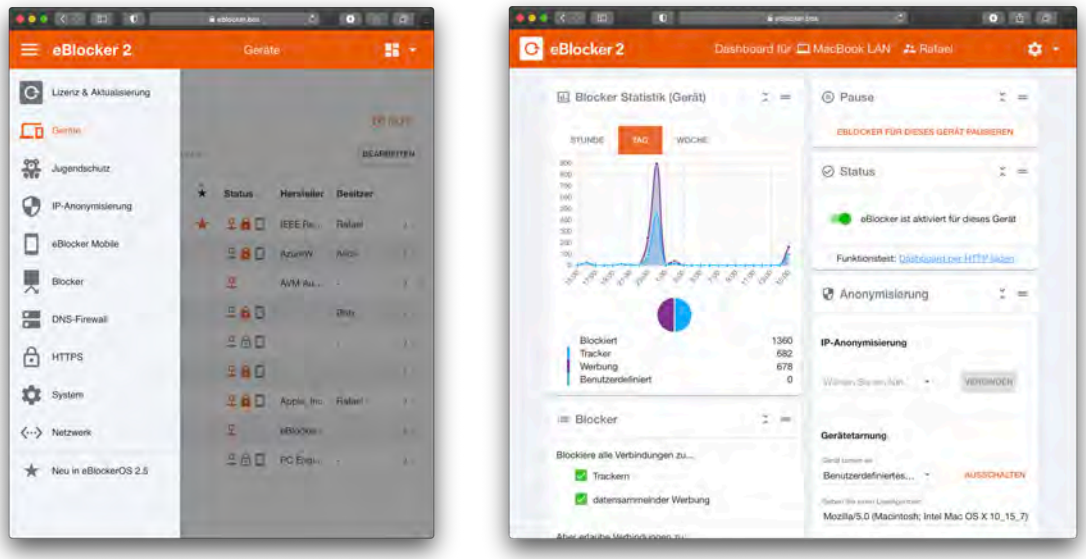
Abbildung 33: eBlocker 2 mit einem Raspberry Pi 4

Zu Beginn der Einrichtung, welche sich auf Englisch oder Deutsch durchführen lässt, wird der Systemstatus des eBlockers direkt angezeigt. Die Konfiguration beginnt mit der Aktivierung einer kostenlosen Lizenz und der Entscheidung, ob neue Netzwerk-Geräte automatisch vom eBlocker geschützt werden sollen. Anschließend führt der eBlocker ein Update auf die neuste Firmware durch, um nach erfolgreichem Abschluss die Konfigurations-Oberfläche anzuzeigen (vgl. Abb. 34a). Die gesamte Einrichtung, inklusive Zusammenbau und Installation, dauerte eine dreiviertel Stunde. Von 44 erreichbaren Punkten für die OOBE sind 40 Punkte bewertbar (vgl. Tabelle 6), von denen der eBlocker 32 Punkte erreicht (siehe Anhang C.1).

Auch wenn ein Tutorial nach Abschluss der Konfiguration fehlt, werden in der Anleitung „erste Schritte“ genannt, die nach Abschluss der Einrichtung empfohlen werden. Dazu zählt zunächst die Aktivierung des HTTPS-Schutzes beim eBlocker und die Installation des *eBlocker-Zertifikats* auf allen verbundenen Netzwerkgeräten. Die anschließende Empfehlung ist die Markierung von „vertrauenswürdigen Apps“ in den Einstellungen, um Probleme mit bereits genutzten Programmen, Diensten und Apps zu vermeiden [51].

174 Release Notes eBlockerOS 2.5 (eblocker.org/de/release-notes/2-5)
175 eBlocker App (apps.apple.com/de/app/eblocker/id1500942271)

Die Einstellung für HTTPS ist direkt im Menü zu finden. Vor der Aktivierung wird die Notwendigkeit des Vorgangs (um auch verschlüsselte Verbindungen untersuchen zu können) nochmal beschrieben. Für die Installation des eBlocker Root-Zertifikats gibt es einen Assistenten, welcher schrittweise und mit Bildern durch den Prozess leitet. Wie bei der TrutzBox auch, wird das Zertifikat auf allen Testgeräten installiert. Dabei passt der *HTTPS-Assistent* die Anleitung automatisch an das entsprechende Gerät bzw. Betriebssystem an. Somit ist die Einrichtung auch ohne Vorkenntnisse sehr einfach und schnell durchführbar.



(a) eBlocker 2 Konfiguration

(b) eBlocker 2 Dashboard

Abbildung 34: Konfiguration und Dashboard nach Einrichtung und Nutzung des eBlocker 2

Der Zugriff auf den Administrations-Bereich des eBlockers ist anfangs ohne Beschränkung möglich und muss durch die Einrichtung eines Administrator-Passworts manuell geschützt werden. Dies erleichtert zwar zunächst die Einrichtung des eBlockers auf allen Geräten, lässt aber die Möglichkeit offen, dass der Verwaltungs-Bereich für jeden Netzwerkteilnehmer zugänglich bleibt. Nach Abschluss der HTTPS-Einrichtung öffnet der eBlocker zum ersten Mal das Dashboard. Dabei handelt es sich um eine vom Nutzer konfigurierbare Übersichts-Seite, welche den Zustand der unterschiedlichen Funktionen des eBlockers und Statistiken über die vergangenen Netzwerk-Aktivitäten zeigt (vgl. Abb. 34b).

Die erfolgreiche Konfiguration von eBlocker und dem jeweiligen Endgerät wird durch ein kleines eBlocker-Symbol angezeigt. Es erscheint auf jedem Gerät bei dem der Schutz richtig konfiguriert ist als transparentes Overlay-Symbol. Anhand einer kleine Zahl wird die Summe von geblockten Werbe- und Tracking-Versuchen der aktuellen Webseite angezeigt. Durch die Auswahl des Symbols öffnet sich eine Statusbar, welche Details über geblockte Inhalte offenbart und Anpassungen am Schutzverhalten ermöglicht (vgl. Abb. 35).

Die Auswahl von „vertrauenswürdigen Apps“, findet sich ebenfalls in den Einstellungen des HTTPS-Schutzes. Hier lassen sich aus einer umfassenden Liste bereits genutzte Apps und Webseiten auswählen. Je nach Auswahl aktiviert der eBlocker entsprechende Regeln oder Ausnahmen, um die Funktionsweise des gewählten Dienstes zu gewährleisten. Neben

jedem Dienst steht eine Beschreibung, welche die Notwendigkeit der Ausnahme für den jeweiligen Service erklärt und die betroffenen Domains oder IP-Adressen auflistet.

Um mit der Einrichtung von *Anti-Tracking*-Maßnahmen, für die erste Aufgabe fortzufahren, wird im Anschluss der Menü-Punkt „Blocker“ betrachtet. Hier wird zwischen den Kategorien *Domain-* und *Pattern-Blocker* unterschieden. Die Optionen „Werbung“, „Tracking“ und „Malware & Phishing“ sind in beiden Kategorien bereits als Standard aktiv. Somit ist die vierte Aufgabe (Aktivierung von *Ad-Blockern*) bereits erledigt. Zusätzlich zu den bereits vorkonfigurierten Filterlisten des eBlockers lassen sich noch eigene Listen hinzufügen.

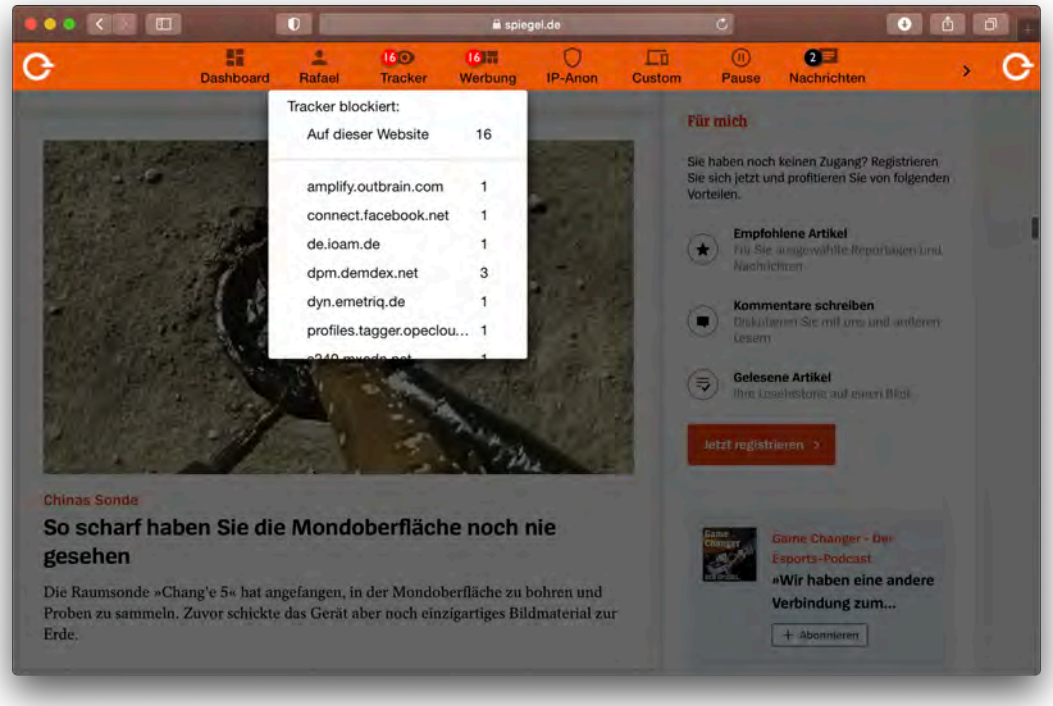


Abbildung 35: eBlocker 2 Browser-Overlay mit Statusbar (spiegel.de)

Es wird mit der zweiten Aufgabe fortgefahren: Zur Konfiguration des *DNS-Schutzes* werden die Einstellungen der DNS-Firewall des eBlockers untersucht. Die Firewall ist standardmäßig aktiv und erlaubt es Domain-Namen entweder über den ISP, das TOR-Netzwerk oder einen externen DNS-Server aufzulösen. Die bereits vorausgewählten externen DNS-Server (1.1.1.1 und 9.9.9.9) können gelöscht, bearbeitet oder erweitert werden. Kriterien wie Antwortzeit, Zuverlässigkeit und eine daraus ermittelte Bewertung ermöglichen eine schnelle Beurteilung über die Qualität der verwendeten DNS-Server.

Die dritte Aufgabe betrifft die Einrichtung eines privaten VPN-Tunnels. Da somit die Nutzung des eBlockers auch unterwegs möglich ist, wird die Funktion *eBlocker Mobile* genannt. Nach der Aktivierung führt ein Assistent durch die notwendigen Schritte. Es gibt die Möglichkeit ein DynDNS des eBlockers zu nutzen, die Funktion ist allerdings noch in der Erprobungsphase (beta). Anschließend werden die benötigten Ports im Router (mittels *UPnP*[176]) vom eBlocker selbst zugewiesen. Durch den speziellen Aufbau des Test-Netzwerks, muss dieser Schritt allerdings manuell vorgenommen werden. Zuletzt wird bei einem Verbindungstest geprüft, ob der eBlocker aus dem Internet erreicht werden kann.

176 Universal Plug & Play (UPnP) ermöglicht Software die automatische Freigabe von Ports im Router

Für die Vergleichbarkeit mit der TrutzBox, wird die Einrichtung des VPN auf einem mobilen Endgerät erneut mit dem iPhone 6S durchgeführt. Über das eBlocker-Dashboard kann im Bereich *eBlocker Mobile* ein Assistenten genutzt werden, der die gesamte Konfiguration anleitet. Dazu gehören Anweisungen zur Installation der OpenVPN-App, zum Download der VPN-Konfigurations-Datei und deren Einrichtung in der OpenVPN-App. Dieser Prozess läuft über die eBlocker-App für iOS reibungslos ab, wohingegen mit dem mobilen Safari-Browser ein paar zusätzliche Schritte notwendig sind.

Die letzte Aufgabe für den Abschluss der Untersuchung betrifft die Konfiguration von *Inhaltsfiltern*. Diese lassen sich im Bereich „Jugendschutz“ finden, wo neben der Einrichtung und Verwaltung von Nutzern sowohl „Blacklists“ als auch „Whitelists“ von Webseiten gepflegt werden können. Bei den verbotenen Webseiten sind bereits Kategorien wie „Glücksspiel“, „Pornographie“ und „Unangemessene Inhalte“ vordefiniert, es lassen sich aber auch eigene Kategorien anlegen. Nach Auswahl eines Nutzers lassen sich individuelle Beschränkungen für Webseiten-Zugriffe sowie Zeiten und Dauer der erlaubten Nutzung einrichten.

Die Zugriffsbeschränkungen werden dabei nach zwei konträren Grundsätzen eingerichtet: Entweder generelles Erlauben aller Webseiten und Blockieren einzelner Kategorien (*Blacklisting*), oder generelles Verbieten aller Webseiten und Erlauben von Ausnahmen (*Whitelisting*). Es ist allerdings auch eine Kombination möglich, bei der sowohl verbotene Kategorien aus „Blacklists“ als auch Ausnahmen aus „Whitelists“ berücksichtigt werden. Die Optionen werden dabei gut formuliert, sodass wenig Verwirrung bei der Einrichtung entstehen kann.

Die Evaluation der Usability wurde wieder mit dem MacBook im Safari-Browser durchgeführt. Von den 60 möglichen Punkten sind bei der Untersuchung 59 Punkte bewertbar (vgl. Tabelle 6), von denen der eBlocker 50,5 Punkte in der Evaluation erreicht (siehe Anhang C.2). Bei der Überprüfung auf Privacy-Nudges konnten 16 unterschiedliche Elemente identifiziert werden. Als Beispiele seien Standards bei *Inhaltsfiltern*, *DNS-Firewall* und *Blockern* sowie grüne Elemente für *HTTPS-* und *VPN-Modus* genannt (siehe Anhang C.4).

Damit ist die Durchführung der Untersuchung abgeschlossen und es kann im nächsten Abschnitt mit der Auswertung und Interpretation von Ergebnissen fortgefahren werden.

6.2 Evaluation der Ergebnisse

Um die Ergebnisse der Untersuchung interpretieren und vergleichen zu können, müssen die ermittelten Daten zunächst ausgewertet werten. Dazu werden für Bewertungen von OOBE, Benutzbarkeit und Privacy-Nudges entsprechende Scores für UX, Usability und Privacy berechnet sowie die gemessenen Zeiten aller Einzelaufgaben bestimmt. Nach der Festlegung einer Bewertung-Skala für jede ermittelte Metrik, können anschließend die berechneten Scores in aussagekräftige Bewertungen umgewandelt werden.

6.2.1 Auswertung der Ergebnisse

Sowohl bei Untersuchung der OOBE als auch bei Evaluation der Usability von Privacy-Boxen lässt sich auf Grundlage der verwendeten Methodik ein Usability-Score (UP) als

Ergebnis berechnen. Dieser Prozent-Wert ermöglicht zwar den Vergleich von Ergebnissen, um allerdings die Auswertung der jeweiligen Untersuchung zu verstehen, ist die Übersetzung in eine verständliche Bewertung notwendig.

Zu diesem Zweck werden die ermittelten Akzeptanz-Bereiche und Adjektiv-Bewertungen von Bangor et al. aus der Arbeit *„An Empirical Evaluation of the System Usability Scale“* (2008) verwendet [8, S. 592]. Dabei wurde mithilfe einer empirischen Untersuchung eine Bewertungs-Skala des *System Usability Scale* (SUS) entwickelt und gängige Bewertungen bestimmten Werten auf der Skala zugeordnet. Da die Ergebnisse des SUS häufig in Prozent berechnet werden und Granollers Bewertung einer vereinfachten Form des SUS entspricht, wird die folgende Skala als Richtlinie zur Bewertung verwendet:

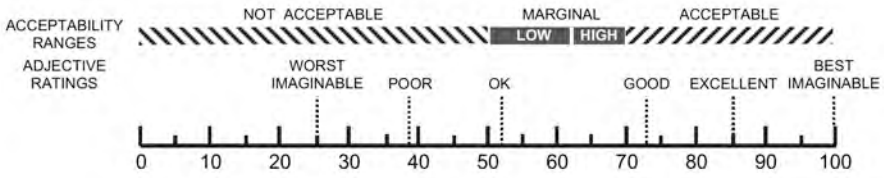


Abbildung 36: Bewertungs-Skala für OOBE und Usability [8, S. 592]

In Abb. 36 lassen sich sowohl die Akzeptanz-Bereiche als auch die Adjektiv-Bewertungen erkennen: Ergebnisse im Bereich von 0% bis 50% werden dabei als nicht akzeptabel eingestuft. Ergebnisse zwischen 50% und 70% liegen im Grenzbereich und Ergebnisse zwischen 70% und 100% im Akzeptanzbereich. Die Adjektiv-Bewertungen entsprechen dabei folgenden Ergebnis-Werten, denen noch entsprechende deutsche Begriffe zugeordnet werden:

Ergebnis	Bewertung	Original-Bewertung
100%	Perfekt	best imaginable
85%	Sehr Gut	excellent
73%	Gut	good
52%	Ausreichend	ok
39%	Mangelhaft	poor
25%	Ungenügend	worst imaginable

Tabelle 8: Skala zur Auswertung von OOBE und Usability

Nachdem eine Bewertungsskala für UX- und Usability-Scores festgelegt wurde (vgl. Tabelle 8), wird noch eine Skala zur Bewertung der Zeitmessung bei der OOBE benötigt. Daher wird folgende Bewertung definiert (für „Techniker“ gilt aufgrund der Berücksichtigung von *Zusammenbau und Installation* die doppelte Zeit der „Bemühten Amateure“):

Zeit (Amateur)	Zeit (Techniker)	Bewertung
10 Minuten	20 Minuten	Sehr Gut
20 Minuten	40 Minuten	Gut
30 Minuten	60 Minuten	Ausreichend
45 Minuten	90 Minuten	Mangelhaft
60+ Minuten	120+ Minuten	Ungenügend

Tabelle 9: Skala zur Zeit-Bewertung der OOBE

Nachdem für alle Metriken entsprechende Bewertungsskalen festgelegt wurden (vgl. Tabellen 8 und 9), können anschließend die Ergebnisse (Scores) der Untersuchungen für OOBE und Usability von Privacy-Boxen ausgewertet werden.

OOBE-Score

Für die Berechnung der OOBE-Scores werden für alle untersuchten Privacy-Boxen die Summen aller bei der Untersuchung erreichten Punkte durch die Anzahl an insgesamt bewertbaren Punkten geteilt. Dieser Wert ist bei jeder Privacy-Box unterschiedlich, abhängig vom entsprechenden Funktionsumfang. Durch die Bildung dieser individuellen Maxima wird jedoch sichergestellt, dass kein Gerät aufgrund fehlender Funktionalität oder Eigenschaften bei Bewertung der UX/Usability benachteiligt wird.

In Tabelle 10 werden bereits die zusammengefassten Summen der einzelnen Kategorien aufgeführt, die Einzelbewertungen können in Anhang C.1 nachgeschlagen werden. Aufgabe „O8 Arbeiten“ wurde bewusst ausgelassen, da die beim HW verwendeten Nutzeraufgaben zusammen mit den Usability-Scores im Anschluss ausgewertet werden. Die ersten beiden Spalten zeigen die acht Kategorien, welche in der OOBE untersucht wurden, mit den jeweils maximal erreichbaren Punkten: Das sind in Summe 37 Punkte für die „Bemühten Amateure“ und 44 Punkte für die „Techniker“, was jeweils einer *perfekten* OOBE von 100% entsprechen würde. In den restlichen acht Spalten finden sich die Bewertungen (Scores) und Zeiten (in Minuten) der einzelnen Privacy-Boxen, gruppiert nach zugehörigem Nutzertyp.

Bei den „Bemühten Amateuren“ beginnt die *Bitdefender BOX 2* (BOX), welche mit 31 von 36 bewertbaren Punkten 86% erreicht, was einer *sehr guten* OOBE entspricht. Es gab Abzüge für die schwer zu findende Inventarliste und wenig kontrastreiche Symbole beim Anschluss. Ein Abbruch der Einrichtung anstelle einer „Zurück“-Funktion sowie das Fehlen von Illustrationen der Anschluss-Optionen und eines Tutorials bei der Erstbenutzung wurden zusätzlich kritisiert. Die benötigte Zeit für den Aufbau liegt mit unter 30 Minuten noch im *ausreichenden* Bereich (vgl. Spalte „BOX“ in Tabelle 10).

Nutzertyp		Bemühter Amateur				Techniker			
Security & Privacy-Box		**BOX**		**SENSE**		**TrutzBox**		**eBlocker**	
Kategorie	Max.	Score	Zeit	Score	Zeit	Score	Zeit	Score	Zeit
O1 Verpackung	5	3,0	01:30	4,0	01:00	1,5	01:30	4,5	01:30
O2 Auspacken	5	4,5	04:30	5,0	03:00	4,5	03:30	2,0	03:00
O3 Aufbau	6	5,5	03:30	6,0	03:45	5,5	03:00	4,5	01:00
O3t Installation	(7)	–	–	–	–	5,5	40:30	5,0	16:00
O4 Einschalten	4	4,0	03:00	4,0	02:30	2,0	03:00	2,0	05:30
O5 Konfiguration	7	6,0	07:00	7,0	14:45	5,5	07:00	6,0	13:00
O6 Registrierung	2	2,0	06:00	–	–	2,0	03:00	1,0	–
O7 Erstbenutzung	4	3,0	02:00	3,0	01:15	2,5	01:30	3,5	02:00
O9 Hilfe	4	3,0	–	4,0	–	2,0	–	3,5	–
Summe/Maximum	(37|44)	31/36	–	33/34	–	29,5/42	–	32/40	–
OOBE-Score | Zeit		**86%**	**27:30**	**97%**	**26:15**	**70%**	**63:00**	**80%**	**42:00**

Legende: Die angegebenen Zeiten sind Werte in Minuten.

Tabelle 10: Auswertung der Out-of-Box Experience von Privacy-Boxen

Der *F-Secure SENSE* (SENSE) folgt im Anschluss an die BOX mit insgesamt 33 von 34 bewertbaren Punkten und erreicht damit 97%, was einer *fast perfekten* OOBE entspricht. Von Verpackung bis Einrichtung ist der SENSE ein sehr durchdachtes Produkt, den einzigen Abzug gab es aufgrund des fehlenden Tutorials bei der Erstbenutzung. Mit etwas mehr als 25 Minuten liegt die Einrichtungszeit des SENSE noch im *fast guten* Bereich (vgl. Spalte „SENSE“ in Tabelle 10).

Im Bereich der „Techniker“ erreicht die *TrutzBox Home* (TrutzBox) mit insgesamt 29,5 von 42 bewertbaren Punkten ein Ergebnis von 70%. Das entspricht einer *fast guten* OOBE, Abzüge gab es für die wenig ansprechende Verpackung und die etwas schwierige Montage der WLAN-Antenne. Des Weiteren fielen die schlechte Verlinkung und mangelnde Überprüfbarkeit der Firmware negativ auf. Die USB-Ports neben dem Strom-Anschluss sind zudem ungünstig positioniert, da es beim Entfernen eines USB-Sticks zum Wackelkontakt kommen kann. Neben fehlenden farblichen Anschluss-Markierungen ist zudem die Konfigurations-Bereitschaft der TrutzBox nicht zu erkennen (kein Feedback).

Das Auftreten von zwei „Showstoppern“, verletzt jedoch die siebte Heuristik von Moya und Burgess (H7: „Dem Nutzer darf bei der Einrichtung nichts in die Quere kommen“, siehe Anhang B.1). Durch ein defekt beigelegtes Kabel und Probleme mit dem Administrator-Passwort nach erfolgreicher Einrichtung, kann die OOBE der TrutzBox deshalb nur noch mit *ausreichend* bis *mangelhaft* bewertet werden. Bei der Verwendung eines USB2-Sticks ist die Einrichtungszeit mit 120 Minuten zusätzlich als *ungenügend* zu bewerten. Bei Verwendung eines schnellen USB3-Sticks kann die Einrichtungszeit mit 63 Minuten noch als *ausreichend* angesehen werden (vgl. Spalte „TrutzBox“ in Tabelle 10).

Zuletzt schließt der *eBlocker 2* (eBlocker) die Bewertung der OOBE mit 32 von 40 bewertbaren Punkten ab. Das entspricht einem Ergebnis von 80%, was eine *fast sehr gute* OOBE bedeutet. Abzüge gab es durch die fehlende Anleitung zum Zusammenbau der Komponenten, sowie dem Bereitstellen einer älteren Firmware. Zusätzlich fehlt Feedback über den Systemzustand und die Konfigurationsbereitschaft des eBlockers. Die Zeit für Zusammenbau, Installation und Einrichtung liegt mit 42 Minuten noch im *guten* Bereich (vgl. Spalte „eBlocker“ in Tabelle 10).

Anwendungsszenarien

Für die Usability-Bewertung mit Heuristic Walkthrough (HW) wurden die Privacy-Boxen im ersten Durchlauf (*aufgabenorientierte Evaluation*) nach der Einrichtung anhand typischer Anwendungsszenarien untersucht und kennengelernt. Deren Erfolg gibt Aufschluss über die Qualität der eingangs betriebenen Recherche über implementierte Funktionen der Privacy-Boxen bzw. über die Wahrheitsgetreue der Hersteller-Auskunft. Da sie zusätzlich zur Beantwortung der zweiten Forschungsfrage (F2) relevant sind, werden die in Abschnitt 6.1.3 (Dokumentation der Untersuchung) beschriebenen Nutzeraufgaben im Anschluss ebenfalls ausgewertet.

In Tabelle 11 werden auf der linken Seite die Anwendungsszenarien der *Bemühten Amateure* und auf der rechten Seite die der *Techniker* aufgelistet. Dabei wurde für jede Privacy-Box einmal die Lösbarkeit und die benötigte Zeit (in Stunden) der jeweiligen Aufgabe bewertet.

Bemühter Amateur					Techniker				
Gerät	**BOX**		**SENSE**		**TrutzBox**		**eBlocker**		Gerät
Aufgabe	Lösbar	Zeit	Lösbar	Zeit	Lösbar	Zeit	Lösbar	Zeit	**Aufgabe**
VPN	(×)	00:32	(×)	00:24	✓	01:50	✓	00:50	Tracking
Inhaltsf.	✓	00:20	(✓)	00:10	×	00:21	✓	00:39	DNS
Firewall	×	00:03	✓	00:02	✓	00:55	✓	00:44	VPN
Virus	(×)	00:05	×	00:04	✓	00:04	✓	00:07	Ad-Block
Monitor	(✓)	00:02	×	00:05	✓	00:05	✓	00:15	Inhaltsf.
Ergebnis	**30%**	**01:02**	**30%**	**00:45**	**80%**	**03:15**	**100%**	**02:35**	**Ergebnis**

Legende: Die angegebenen Zeiten sind Werte in Stunden.
✓= Die Aufgabe ist lösbar. (✓) = Die Aufgabe ist nur teilweise lösbar.
× = Die Aufgabe ist nicht lösbar. (×) = Die Aufgabe ist anders lösbar.

Tabelle 11: Auswertung der beim HW untersuchten Anwendungsszenarien

Lösbare Aufgaben für die jeweilige Privacy-Box sind mit einem Haken versehen: ✓. Aufgaben die sich nur teilweise mit der Privacy-Box lösen lassen, sind mit einem Haken in Klammern markiert: (✓). Dies betrifft z.B. den nur manuell ausführbaren IoT-Monitor der BOX oder den Inhaltsfilter des SENSE, der nur „Whitelisting“ ermöglicht. Nicht mit der Privacy-Box realisierbare Aufgaben, sind durch ein Kreuz gekennzeichnet: ×. Aufgaben, die zwar lösbar sind, aber nur außerhalb des Kontexts der Privacy-Box, sind mit einem Kreuz in Klammern versehen: (×). Dies betrifft vor allem die VPN-Aufgaben bei BOX und SENSE, die nur mit einer zusätzlichen App gelöst werden konnten (vgl. Tabelle 11).

Durch eine Bewertung von *lösbaren* Aufgaben mit einem Punkt, *teilweise lösbaren* Aufgaben mit 0,5 Punkten und *nicht* bzw. nur *anders lösbaren* Aufgaben mit 0 Punkten, lassen sich die Prozente der Aufgaben bestimmen, die mit jeder Privacy-Box gelöst werden konnten. So waren mit BOX und SENSE nur 30% der Nutzeraufgaben für *Bemühte Amateure* lösbar, bei einem Zeitaufwand von 62 bzw. 45 Minuten. Mit der TrutzBox konnten 80% der Nutzeraufgaben für *Techniker* in drei Stunden und 15 Minuten gelöst werden. Mit dem eBlocker ließen sich alle Aufgaben (100%) in zweieinhalb Stunden lösen (vgl. Tabelle 11).

Usability-Score

Nach Abschluss der Nutzeraufgaben wurde im zweiten Durchlauf des HW (*Freiformauswertung*) die Bewertung anhand der Heuristiken von Granollers durchgeführt. In Tabelle 12 sind bereits die Ergebnisse der einzelnen Kategorien zusammengefasst, die vollständige Bewertung der Einzelaufgaben kann in Anhang C.2 gefunden werden. Der Aufbau entspricht dabei der Tabelle für die OOBE-Auswertung (vgl. Tabelle 10): In den linken zwei Spalten befinden sich die untersuchten Usability-Kategorien mit den jeweils maximal erreichbaren Punkten. Das beste Gesamtergebnis entspricht 60 Punkten und damit einer perfekten Usability von 100%. Die vier restlichen Spalten enthalten die Bewertungen jeder untersuchten Privacy-Box in der entsprechenden Kategorie, gruppiert nach zugehörigem Nutzertyp.

Die BOX als erstes Gerät für „Bemühte Amateure“ erreicht bei der Untersuchung 37 von 56 bewertbaren Punkten. Das Ergebnis von 66% liegt noch im akzeptablen Grenzbereich

Nutzertyp		Bemühter Amateur		Techniker	
Security & Privacy-Box		**BOX**	**SENSE**	**TrutzBox**	**eBlocker**
Kategorie	Max.	Score	Score	Score	Score
U1 Systemstatus	5	3,0	4,0	4,5	5,0
U2 Metaphorik	4	4,0	4,0	4,0	4,0
U3 Kontrolle	3	1,0	1,0	2,0	2,0
U4 Konsistenz	6	5,5	5,0	5,0	6,0
U5 Erlernbarkeit	5	2,5	3,5	3,0	4,0
U6 Flexibilität	6	1,0	1,0	2,0	3,0
U7 Warnungen	4	3,0	3,0	1,0	3,5
U8 Toleranz	3	2,0	2,0	0,5	2,0
U9 Gestaltung	4	3,5	4,0	3,0	4,0
U10 Hilfe/Doku.	5	2,0	4,0	2,0	4,5
U11 Zustände	3	1,5	1,0	2,0	2,0
U12 Lesbarkeit	4	2,5	3,0	3,0	3,0
U13 Autonomie	3	2,0	2,5	2,5	3,0
U14 Standards	3	1,5	3,0	3,0	2,5
U15 Wartezeit	2	2,0	2,0	1,5	2,0
Summe/Maximum	60	37/56	43/56	39/58	50,5/59
Usability-Score		**66%**	**77%**	**67%**	**86%**

Tabelle 12: Auswertung der Usability-Evaluation von Privacy-Boxen mit HW

und lässt sich damit als *ausreichende* Usability mit der Tendenz zu *gut* bewerten (vgl. Spalte „BOX“ in Tabelle 12). Die „Unterbringung“ der BOX-Verwaltung in der Bitdefender Central App führt dazu, dass die Einstellungen schwer zu finden und Funktionen erst durch Ausprobieren ersichtlich werden (z.B. Inhaltsfilter). Zusätzlich fehlen eine Zustandsverwaltung sowie die Verwendung von Favoriten oder eine Auflistung häufig verwendeter Funktionen. Das Ignorieren von Tippfehlern in der Suche, Informationsredundanz sowie der Mangel einer Hilfe-Funktionen, führten zusätzlich zu Abzügen bei der Bewertung. Zuletzt wurden der Mangel an Personalisierbarkeit und fehlende Berücksichtigung von Nutzern mit Sehschwäche kritisiert. Unter Berücksichtigung des „Showstoppers“ im ersten Evaluations-Durchlauf, welcher einen Werksreset mit Neueinrichtung der BOX erforderlich machte, kann die Usability jedoch nur noch mit *mangelhaft* bewertet werden.

Der SENSE erreicht bei der Evaluation 43 von 56 bewertbaren Punkten und erreicht damit ein Ergebnis von 77% was einer *fast sehr guten* Usability entspricht (vgl. Spalte „SENSE“ in Tabelle 12). Abzüge in der Untersuchung gab es beim SENSE ebenfalls durch Fehlen von Zustandsmanagement, Favoriten und zuletzt genutzten Funktionen. Trotz des sehr strukturierten Aufbaus fehlten ein einheitliches Layout, eine integrierte Hilfe-Funktion und Optionen für Nutzer mit eingeschränkter Wahrnehmung.

Die TrutzBox ist das erste Gerät für die „Techniker“ und erreicht bei der Untersuchung 39 von 58 möglichen Punkten. Das Ergebnis von 67% entspricht dabei einer *fast guten* Usabili-

ty (vgl. Spalte „TrutzBox“ in Tabelle 12). Kritisiert wurden das Fehlen von Funktionen für „Rückgängig“ oder „Wiederherstellen“ bei Änderungen, sowie inkonsistente Darstellung bei Überschriften, Expansion-Tiles und Links im UI. Neben fehlenden Optionen für Favoriten oder zuletzt verwendete Funktionen wirken Informationen teilweise redundant, bzw. die Zusammenhänge und Unterschiede werden nicht sofort ersichtlich (z.B. „TrutzBrowse-Blacklists“ und „Filtergruppen“).

Des Weiteren sind Beschreibungstexte zu lang bzw. nicht optional darstellbar und die Auswahl sich ausschließender Optionen ist möglich (z.B. Auswahl von „Alle Filter“ und „Keine Filter“ bei *Slider-Definitionen*). Zusätzlich führten komplizierte Fehlermeldungen und das Ignorieren von Falscheingaben in Suche oder Formularfeldern zu weiteren Abzügen. Zuletzt fehlen Hilfe-Optionen, Möglichkeiten zur Personalisierung und die Unterstützung für sehschwache Nutzer. Zuletzt werden das häufig auftretende, zufällige Abmelden aus dem Admin-Bereich und das Ausbleiben einer Aktion beim manuellen „Ausloggen“ kritisiert.

Als letztes Gerät in der Usability-Evaluation erreicht der eBlocker mit 50,5 von 59 bewertbaren Punkten ein Ergebnis von 86%, was einer *sehr guten* Usability entspricht (vgl. Spalte „eBlocker“ in Tabelle 12). Abzüge gab es lediglich für das Fehlen von Favoriten, zuletzt verwendeten Funktionen und Optionen für „Rückgängig“ sowie „Wiederherstellen“. Das Ignorieren von Rechtschreibfehlern in der Suche und mangelnde Unterstützung für Nutzer mit geringer Sehkraft wurden ebenfalls bemängelt.

Nach der Usability-Bewertung der untersuchten Privacy-Boxen fehlt zuletzt noch die Auswertung der Privacy-Scores auf Grundlage der ermittelten Privacy-Nudges. Da für die Bewertung von Privacy-Nudges jedoch noch eine Bewertungs-Skala fehlt, wird diese zunächst erarbeitet.

Privacy-Score

Zur Ermittlung der Privacy-Scores wurde die Häufigkeit von unterschiedlichen Privacy-Nudges bei Privacy-Boxen untersucht. Das Ranking von Schöbel et al. entspricht einer Wertung von 1 bis 8 (siehe Anhang B.6), wobei 1 die höchste und 8 die niedrigsten Akzeptanz durch Nutzer bedeutet [151, S. 3924]. Um eine aussagekräftigere Bewertung für die Umsetzung von Usable-Privacy daraus abzuleiten, wird eine Gewichtung aus den Angaben „Best“ und „Worst“ der Untersuchung von Schöbel et al. berechnet. Dazu lässt sich der bereits vorhandene Mittelwert verwenden und auf einen positiven Bereich zwischen Werten von 0 und 1 skalieren (die Berechnung kann in Anhang C.3 nachvollzogen werden).

Mit dieser Gewichtung bekommen von Nutzern präferierte Privacy-Nudges höhere Werte für das Ergebnis. Durch die Multiplikation der Gewichte mit der Anzahl an gefundenen Privacy-Nudges, lassen sich so Bewertungen (Scores) für die einzelnen Privacy-Nudge-Kategorien bestimmen. Die Summe aller Bewertungen spiegelt neben der Anzahl an gefundenen Privacy-Nudges zusätzlich deren Akzeptanz beim Nutzer wider. Eine höhere Anzahl an von Nutzern akzeptierten Privacy-Nudges kann somit als Gütekriterium für Usable-Privacy gesehen werden: Es handelt sich dabei um „Nudges“, die gute Datenschutz-Entscheidungen vorgeben, welche vom Nutzer auch akzeptiert werden.

In Tabelle 13 sind auf der linken Seite neben den jeweiligen Kategorien der Privacy-Nugdes der entsprechende Rang von Schöbel et al. und die berechneten Gewichte zu finden:

Nutzertyp			Bemühter Amateur				Techniker			
Security & Privacy-Box			**BOX**		**SENSE**		**TrutzBox**		**eBlocker**	
Privacy-Nudge	Rang	Gew.	Anz.	Score	Anz.	Score	Anz.	Score	Anz.	Score
Standard	1	0,9	1	0,9	2	1,8	4	3,6	4	3,6
Farbelem. Rot	2	0,7	–	0,0	–	0,0	1	0,7	1	0,7
Farbelem. Grün	3	0,6	–	0,0	–	0,0	1	0,6	6	3,6
Feedback	4	0,5	–	0,0	–	0,0	1	0,5	1	0,5
Information	5	0,4	1	0,4	1	0,4	3	1,2	2	0,8
Soziale Norm	6	0,3	–	0,0	–	0,0	–	0,0	–	0,0
Zeitverzögerung	7	0,3	1	0,3	–	0,0	–	0,0	1	0,3
Fortschrittsanz.	8	0,3	1	0,3	1	0,3	3	0,9	1	0,3
Nudges | Privacy-Score			**4**	**1,9**	**4**	**2,5**	**13**	**7,5**	**16**	**9,8**

Tabelle 13: Bewertung der identifizierten Privacy-Nudges bei Privacy-Boxen

Die vollständige Liste an ermittelten Privacy-Nudges kann in Anhang C.4 nachgeschlagen werden. Um aus den berechneten Privacy-Scores aussagekräftige Bewertungen abzuleiten wird in Tabelle 14 folgende Skala zur Beurteilung von Privacy-Nudges definiert:

Punkte	Bewertung
10+	Sehr Gut
8	Gut
6	Ausreichend
4	Mangelhaft
2	Ungenügend

Tabelle 14: Skala zur Bewertung von Privacy-Nudges

Bei der BOX konnten insgesamt vier Privacy-Nudges aus verschiedenen Kategorien entdeckt werden (die eher in den Security-Kontext passen). Die vier Privacy-Nudges entsprechen dabei einem Privacy-Score von 1,9 Punkten, was einer *ungenügenden* Usable-Privacy entspricht (vgl. Spalte „BOX“ in Tabelle 13). Beim SENSE wurden ebenfalls vier Privacy-Nudges gefunden, jedoch nur in drei unterschiedlichen Kategorien. Damit wird ein Privacy-Score von 2,5 Punkten erreicht, was ebenfalls noch als *ungenügende* Berücksichtigung von Usable-Privacy gewertet wird (vgl. Spalte „SENSE“ in Tabelle 13).

Bei der TrutzBox konnten insgesamt 13 Privacy-Nudges in sechs unterschiedlichen Kategorien gefunden werden. Elemente mit doppelter Einordnung („Farbelemente“ beim *Security-Slider*) werden nur einfach bewertet (in der Kategorie mit höherem Gewicht). Somit erreicht die TrutzBox mit 13 Privacy-Nudges einen Privacy-Score von 7,5 Punkten, was eine *fast gute* Umsetzung von Usable-Privacy bedeutet (vgl. Spalte „TrutzBox“ in Tabelle 13). Der eBlocker erreicht bei der Bewertung von 16 Privacy-Nudges, bei denen nur die Kategorie „Soziale Norm“ nicht vorkommt, einen Privacy-Score von 9,8 Punkten, was insgesamt einer *sehr guten* Berücksichtigung von Usable-Privacy entspricht.

6.2.2 Diskussion und Interpretation der Ergebnisse

Nach Auswertung der Untersuchungs-Ergebnisse können die ermittelten Bewertungen der Privacy-Boxen interpretiert und miteinander verglichen werden. Zu diesem Zweck werden die Bewertungen der untersuchten Geräte bezüglich OOBE, Nutzeraufgaben, Usability und Usable-Privacy in Tabelle 15 nochmal übersichtlich zusammengefasst:

Nutzertyp	Bemühter Amateur		Techniker	
Privacy-Box	**Bitdefender BOX 2**	**F-Secure SENSE**	**TrutzBox Home**	**eBlocker 2**
OOBE-Bewertung	Sehr Gut	Fast Perfekt	Fast Gut[1]	Fast Sehr Gut
OOBE Zeit-Bewert.	Ausreichend	Fast Gut	Ausreichend[2]	Gut
Aufgaben-Lösbarkeit	30%	30%	80%	100%
Aufgaben-Zeit (Std.)	01:02	00:45	03:15	02:35
Usability-Bewertung	Ausreichend[3]	Fast Sehr Gut	Fast Gut	Sehr Gut
Probleme/Showstop.	2 / 1	– / –	15+ / 2	3 / –
Privacy-Bewertung	Ungenügend	Ungenügend	Fast Gut	Sehr Gut

[1] Die abschließende Bewertung wird aufgrund von zwei „Showstoppern“ auf *Mangelhaft* angepasst
[2] Das Ergebnis wurde mit einem USB3-Stick erzielt, ansonsten gilt die Bewertung als *Ungenügend*
[3] Die abschließende Bewertung wird aufgrund eines „Showstoppers“ auf *Mangelhaft* angepasst

Tabelle 15: Übersicht und Vergleich der Untersuchungs-Ergebnisse von Privacy-Boxen

Zu den Ergebnissen in Tabelle 15 muss erwähnt werden, dass für eine bessere Vergleichbarkeit die ursprünglichen Bewertungen ohne Abzüge durch aufgetretene „Showstopper“ verwendet werden (markiert durch Hochzahlen). So werden die betreffenden Privacy-Boxen beim Vergleich nicht aufgrund von Problemen benachteiligt, die möglicherweise nur zufällig aufgetreten sind. Nichtsdestotrotz zeigt jeder „Showstopper“, dass dieses Problem eintreten kann und wird deshalb in der Diskussion mit berücksichtigt.

Zusätzlich sind die ermittelten Usability-Probleme und „Showstopper“ in Tabelle 15 aufgelistet, die ausführlich in Anhang C.5 beschrieben werden. Wie sich bereits erkennen lässt, wurden beim SENSE keine, bei BOX und eBlocker zwei bis drei und bei der TrutzBox mehr als 15 Usability-Probleme entdeckt. Im Anschluss werden die Untersuchungs-Ergebnisse der Privacy-Boxen beider Nutzertypen miteinander verglichen und interpretiert.

Bitdefender BOX 2 vs. F-Secure SENSE

Die *sehr gute* bis *fast perfekte* OOBE von *Bitdefender BOX 2* (BOX) und *F-Secure SENSE* (SENSE) zeigt, dass von den Herstellern viel Aufwand für die Optimierung dieses Prozesses betrieben wurde. Dies kann als Bestätigung für die Einordnung der Geräte zur Nutzergruppe „Bemühte Amateure“ gesehen werden: Aufgrund ihrer geringen Motivation darf bei der Einrichtung nichts schief laufen, damit das Gerät anschließend genutzt wird. Auch die geringe Anzahl an Funktionen und Einstellungen deutet auf diese Zielgruppe hin.

Bei der Durchführung typischer Anwendunsszenarien gab es bei beiden Geräten Schwierigkeiten, die sich in 30% Lösbarkeit der Nutzeraufgaben widerspiegeln. Insgesamt entstand der Eindruck, dass die Hersteller versprochene Funktionen zum Schutz der Privatsphäre nicht ausreichend implementiert haben. Viele der Selbstdatenschutz-Funktionen sind nur über weitere Apps oder zusätzliche Software-Abos verfügbar und damit losgelöst vom Nutzungskontext der jeweiligen Privacy-Box.

Neben dieser Problematik führt die starke Ausprägung von Funktionen im Bereich „Sicherheit“ (siehe Tabelle 4 in „Überprüfung der Geräte-Vorauswahl“) dazu, dass sowohl BOX als auch SENSE eher als „Security-Boxen“ kategorisiert werden sollten, mit einem geringen Anteil an Privatsphäre-Schutz. Auch bei der Untersuchung von Privacy-Nudges konnten nur wenige Ansätze entdeckt werden, um Nutzer zu besseren Datenschutz-Entscheidungen zu motivieren. Die meisten Nudges ließen sich im Security-Kontext finden, was den Schwerpunkt der Geräte als „Security-Boxen“ nochmal bestätigt.

Bei der Bewertung der Usability werden zwei unterschiedliche Ansätze der Hersteller deutlich: Die nur als *ausreichend* bewertete Usability der BOX lässt sich auf die Integration von Funktionen in eine bestehende App zurückführen. Da Einrichtung und Konfiguration der BOX über die „Bitdefender Central App“ stattfinden, sind die Funktionen weder prominent platziert noch für die Nutzung optimiert. Beim SENSE hingegen wurde eine eigene App für Einrichtung und Konfiguration entwickelt. Das Ergebnis einer *fast sehr guten* Usability macht deutlich, dass die App speziell auf die Nutzung des SENSE zugeschnitten ist.

Auch ohne Berücksichtigung des „Showstoppers“, der das Ergebnis der BOX deutlich verschlechtert, erzielt der SENSE in allen Kategorien die besseren Ergbnisse (vgl. Spalten „BOX“ und „SENSE“ in Tabelle 15). Damit geht er als Gewinner aus dem Vergleich von Privacy-Boxen für „Bemühte Amateure“ hervor[177].

TrutzBox Home vs. eBlocker 2

Beim Vergleich von *TrutzBox Home* (TrutzBox) und *eBlocker 2* (eBlocker), erreicht der eBlocker bei der OOBE das bessere Ergebnis, obwohl die benötigten Komponenten einzeln gekauft werden müssen. Bei beiden Privacy-Boxen lässt sich in diesem Zusammenhang das mangelnde Feedback für die Konfigurations-Bereitschaft kritisieren. Die TrutzBox hat bereits Lautsprecher und LEDs eingebaut, die dafür genutzt werden können, der eBlocker müsste beim Zusammenbau zusätzliche Hardware berücksichtigten (z.B. Lautsprecher oder LEDs). So ließe sich die Angabe einer Wartezeit in Minuten vermeiden.

Das Auftreten von „Showstoppern“ ist bei Nutzern vom Typ „Techniker“ aufgrund ihrer höheren Motivation nicht so gravierend wie bei den „Bemühten Amateuren“. Allerdings müssen zwei „Showstopper“ bei Einrichtung der TrutzBox als eine grenzwertige Hürde bewertet werden, auch für „Techniker“. Zusätzlich macht die Benutzung der TrutzBox an vielen Stellen Schwierigkeiten, wie durch die Anzahl gefundener Usability-Probleme deutlich wird. Die Komplexität der Funktionsweise und die Menge an dargestellten Informationen kann sogar für „Techniker“ eine Herausforderung darstellen.

177 Da der Vertrieb des SENSE eingestellt wurde, gibt es keine Empfehlung für „Bemühte Amateure“

Aufgrund der Menge und feinen Granularität von Einstellungs-Möglichkeiten ist es denkbar, dass die TrutzBox für Nutzer vom Typ „Fundamentalist“ besser geeignet ist (siehe „Zielgruppe für Privacy-Boxen“ in Abschnitt 5.2.2). Mit Optionen wie dem Versand verschlüsselter Emails zeigt die TrutzBox zusätzlich einen etwas anderen Schwerpunkt, den sonst keine andere Privacy-Box bietet.

Der eBlocker bietet den Nutzern im Gegensatz zur TrutzBox genau die richtige Menge an Informationen an, was sich an einer besseren Usability erkennen lässt. Standardmäßig sind für Nutzer nur die notwendigen Informationen verfügbar, die zusätzlich kurz und einfach formuliert sind. Bei Bedarf lassen sich jederzeit zusätzliche Informationen darstellen, die ins Detail gehen und eine höhere Komplexität aufweisen.

Bei der Durchführung von typischen Anwendungsszenarien wurde deutlich, dass sowohl die TrutzBox als auch der eBlocker die Bezeichnung als „Privacy-Box“ verdient haben. Die hohe Lösbarkeit der untersuchten Nutzeraufgaben mit 80% bzw. 100% zeigt, dass die Hersteller ihre Versprechen über die implementierten Selbstdatenschutz-Funktionen in den Privacy-Boxen größtenteils einhalten.

In der Untersuchung zur Umsetzung von Usable-Privacy zeigte sich, dass die TrutzBox bereits viele Privacy-Nudges berücksichtigt. Den Nutzern werden beim eBlocker allerdings noch deutlich mehr Entscheidungen in Form von Standard-Einstellungen zum Schutz der Privatsphäre abgenommen. Damit wird deutlich, dass der eBlocker die Nutzer besser dazu motiviert, gute Entscheidungen für den Schutz ihrer Privatsphäre zu treffen.

Im direkten Vergleich aller untersuchten Kriterien ist der eBlocker der TrutzBox in jeder Kategorie überlegen: Somit gewinnt er bei dieser Gegenüberstellung und geht als Sieger aus dem Vergleich von Privacy-Boxen für „Techniker“ hervor (vgl. Spalten „TrutzBox“ und „eBlocker“ in Tabelle 15).

6.2.3 Gültigkeit der Ergebnisse

Nach Abschluss der Ergebnis-Interpretation und dem Vergleich von je zwei untersuchten Privacy-Boxen für beide definierten Nutzertypen wird die Gültigkeit der Ergebnisse überprüft, indem auf mögliche, gefährdende Faktoren hingewiesen wird.

Während der Durchführung der Untersuchung wurde darauf geachtet, die Rolle des entsprechenden Nutzertyps anzunehmen. Die Adaption des entsprechenden Wissens- und Motivations-Niveaus ist jedoch schwierig, sodass die gewünschte Nutzerrolle möglicherweise nicht ausreichend berücksichtigt wurde. Zusätzlich führte das spezielle Test-Setup (ein zusätzlicher Router zur Absicherung der Internetverfügbarkeit) dazu, dass bestimmte Aufgaben in der Untersuchung nicht wie geplant funktionierten.

Da die Dokumentation der Ergebnisse zeitgleich bzw. kurz nach der Evaluation durchgeführt wurde, ist es möglich, dass die gemessenen Zeiten durch die Notation verzerrt wurden. Die Fragen konnten nicht immer chronologisch beantwortet werden, daher wurden die Zeiten für die einzelnen Aufgaben durch notierte Zeitmarker zurückgerechnet. Auch wenn die Summe der Gesamtzeit stimmt, können die Zeiten der einzelnen Aufgaben ungenau sein.

Bei der Bewertung der einzelnen Fragen wurde zusätzlich auf Objektivität geachtet, dennoch können die Ergebnisse durch subjektive Eindrücke beeinflusst sein. Auch die Auswertung der Untersuchungs-Ergebnisse mithilfe der Bewertungsskala einer anderen Methode (SUS-Skala) und die Festlegung weiterer Bewertungsskalen nach eigenem Ermessen können als Beeinflussung der Ergebnisse gesehen werden.

6.3 Beantwortung der Forschungsfragen

Nachdem die Ergebnisse ausgewertet, interpretiert und verglichen wurden, folgt die Beantwortung der Forschungsfragen aus Abschnitt 4.1.2, bevor überprüft wird, ob sich die zu Beginn der Arbeit gestellten Annahmen bewahrheitet haben.

Die grundlegende Forschungsfrage hatte zum Inhalt, wie die Usability von Privacy-Boxen zu bewerten ist, wenn Nutzer sich vor ungewollter Verwendung ihrer Daten sowie Eingriffen in die Privatsphäre schützen möchten (F). Zur weiteren Präzisierung wurde die Forschungsfrage in zwei Unterfragen aufgeteilt. Dabei wurde untersucht, ob es Nutzern möglich ist, Privacy-Boxen zum Schutz ihrer Daten und Privatsphäre korrekt anzuschließen und einzurichten (F1) und ob sie bei typischen Anwendungsszenarien zum Selbstdatenschutz durch das UI von Privacy-Boxen entsprechend unterstützt werden (F2). Zur Beantwortung der Forschungsfragen werden die Ergebnisse der durchgeführten Untersuchungen aus Tabelle 15 verwendet.

Forschungsfrage 1

Das Anschließen und Einrichten von Privacy-Boxen zum Schutz von Daten und Privatsphäre ist für Nutzer *gut* bis *sehr gut* möglich, sofern dabei keine „Showstopper“ auftreten. Die Motivation der entsprechenden Zielgruppe wird von den Herstellern entsprechend berücksichtigt: Der Aufbau und die Einrichtung von Privacy-Boxen, die für „Bemühte Amateure“ geeignet sind, ist einfacher und schneller möglich, als dies bei Geräten für „Techniker“ der Fall ist. Beim Auftreten von „Showstoppern“ während der Einrichtung, hängt der Erfolg einer Privacy-Boxen von der Motivation des Nutzers ab. Die Bereitschaft, den Prozess zu Wiederholen oder nach Lösungen für das Problem zu suchen, ist beim Nutzertyp „Techniker“ höher und somit der Erfolg wahrscheinlicher.

Forschungsfrage 2

Die Unterstützung bei typischen Anwendungsszenarien zum Selbstdatenschutz durch das UI von Privacy-Boxen lässt sich nicht für alle Nutzer der Zielgruppe einheitlich beantworten. Es gehören sowohl die Berücksichtigung einer guten Usability als auch einer guten Umsetzung von Usable-Privacy zur Beantwortung dieser Frage. Dazu muss zwischen den beiden Nutzertypen „Bemühter Amateur“ und „Techniker“ unterschieden werden.

„Bemühte Amateure“ werden durch die UIs von Privacy-Boxen *ausreichend* bis *fast sehr gut* unterstützt, sofern keine „Showstopper“ auftreten. Dies gilt allerdings nur für generelle Aufgaben und nicht für typische Anwendungsszenarien zum Selbstdatenschutz. Zum einen bieten die Privacy-Boxen nur wenig relevante Selbstdatenschutz-Funktionen an und zum anderen motivieren sie die Nutzer nicht ausreichend dazu, gute Privatsphäre-Entscheidungen

zu treffen. Das Auftreten eines „Showstoppers“ während der Nutzung wird bei den „Bemühten Amateuren“ als K.O.-Kriterium gesehen.

„Techniker“ hingegen werden durch die UIs von Privacy-Boxen *fast gut* bis *sehr gut* bei typischen Anwendungsszenarien zum Selbstdatenschutz unterstützt. Es stehen ihnen eine große Auswahl an relevanten Selbstdatenschutz-Funktionen zur Verfügung, deren Einrichtung und Konfiguration sie größtenteils effektiv, effizient und zufriedenstellend durchführen können. Dabei werden sie von den Geräten in *fast hohem* bis *sehr hohem* Maß dazu motiviert, gute Entscheidungen im Bezug auf ihre Privatsphäre zu treffen.

Generelle Forschungsfrage

Um die generelle Forschungsfrage abschließend zu beantworten: Die Bewertung der Usability von Privacy-Boxen, wenn Nutzer sich vor ungewollter Verwendung ihrer Daten sowie Eingriffen in die Privatsphäre schützen möchten, hängt vom jeweiligen Nutzertyp ab:

Für die „Bemühten Amateure“ ist die Einrichtung und Nutzung von Privacy-Boxen möglich, solange dabei keine gravierenden Fehler auftreten, die den weiteren Prozess verhindern. Die von ihnen benutzbaren Geräte bieten allerdings keine ausreichende Funktionalität zum Schutz der Privatsphäre an. Dadurch ist ein effektiver Selbstdatenschutz mit Privacy-Boxen für diese Nutzergruppe, trotz einer durchschnittlich guten Usability, nur schwer möglich.

Für „Techniker“ ist der Aufbau und die Verwendung von Privacy-Boxen möglich, auch wenn größere Fehler dabei auftreten. Die ihnen zur Verfügung stehenden Geräte bieten eine Vielzahl an Privatsphäre-Funktionen, sodass ein effektiver Selbstdatenschutz mit Privacy-Boxen möglich ist. Nutzer dieser Gruppe werden bei typischen Anwendungsszenarien von den Geräten mit einer durchschnittlich mehr als guten Usability unterstützt.

Die Anzahl der implementierten Privacy-Funktionen ist damit ebenso ein entscheidender Faktor für erfolgreichen Selbstdatenschutz mit Privacy-Boxen wie eine gute UX/Usability.

Überprüfung der Anfangs-Annahmen

Zu Beginn der Arbeit wurde angenommenen, dass es grundlegende Unterschiede in Leistungs- und Funktionsumfang der betrachteten Privacy-Boxen geben wird. Mit Blick auf den sehr unterschiedlichen Funktionsumfang bei der Markt-Übersicht (vgl. Tabelle 3) oder der Geräte-Vorauswahl (vgl. Tabelle 4) lässt sich diese Vermutung bestätigen.

Des Weiteren wurden Gegensätze in der intuitiven Benutzbarkeit der im Vergleich stehenden Produkte, vor allem bei der Einrichtung und der Verwaltung von Einstellungen, zur Verbesserung des Selbstdatenschutzes erwartet. Beim Vergleich der Untersuchungs-Ergebnisse (vgl. Tabelle 15) lassen sich zwar keine Gegensätze, aber deutliche Unterschiede in UX und Usability der verglichenen Privacy-Boxen feststellen.

Zuletzt wurde vermutet, dass in vielen Fällen das erforderliche Know-how des Endanwenders über das Grundwissen der Zielgruppe hinaus geht, um ein Gerät den Bedürfnissen entsprechend zu konfigurieren. Diese Vermutung bewahrheitet sich für den Fall, dass Nutzer Privacy-Boxen verwenden, die nicht ihrem Nutzertyp entsprechen (z.B. wäre ein „Bemühter Amateur“ bei der Nutzung einer TrutzBox überfordert).

7 Fazit und Ausblick

Abschließend werden in einem Rückblick die Vorgehensweise und Ergebnisse der gesamten Arbeit zusammengefasst, sowie aufgetretene Probleme und Herausforderungen aufgezeigt. Im anschließenden Ausblick werden Punkte genannt, die im Rahmen dieser Arbeit nicht betrachtet werden konnten, sich aber in künftigen Arbeiten anschließen können.

7.1 Rückblick und Zusammenfassung

Das Ziel dieser Arbeit war eine Betrachtung zum Selbstdatenschutz mit Fokus auf die Benutzbarkeit von Security & Privacy-Boxen (Privacy-Boxen). Die zugrundeliegende Fragestellung zielte darauf ab herauszufinden, ob die Usability für Nutzer ein Entscheidungskriterium darstellt, um Selbstdatenschutz mithilfe von Privacy-Boxen realisieren zu können.

Zu Beginn der Arbeit wurden Grundlagen zu Sicherheit und Privatheit erarbeitet und darauf aufbauend das Thema Selbstdatenschutz eingeführt. Anschließend konnte der Nutzer, als Urheber von Daten, in den Mittelpunkt der Betrachtung gestellt und auf Gefahren durch die Sammlung, Auswertung und Neuverknüpfung seiner personenbezogenen Daten hingewiesen werden. Die für Nutzer verfügbaren Schutzmaßnahmen, vor ungewollter Verfolgung im Internet, wurden in Form von rechtlichen, organisatorischen und technischen Maßnahmen vorgestellt.

Mit der Einführung von Usability-Grundlagen, wurden die Begriffe „Benutzbarkeit“ (Usability) und „Benutzererfahrung“ (UX) definiert und Methoden für deren Untersuchung vorgestellt. Die Betrachtung des aktuellen Forschungsstandes (Related Work) adressierte die Frage, ob es bereits Arbeiten mit ähnlichen Zielen gibt, deren Methodik verwendet oder auf denen aufgebaut werden kann. Das Ergebnis zeigte, dass lediglich verwandte Arbeiten mit Schnittmengen zu relevanten Themen existieren. Es konnte allerdings keine Methodik gefunden werden, die sich adaptieren oder anwenden ließ.

Damit wurde die Erarbeitung einer eigenen Methodik zur Bewertung der Usability von Privacy-Boxen notwendig. Anhand von Einrichtungs-Schritten und typischen Anwendungsszenarien sollte untersucht werden, ob Nutzer in der Lage sind, Selbstdatenschutz mithilfe von Privacy-Boxen zu realisieren. Die Grundlage der Methodik stellte die Erarbeitung eines Werkzeug-Katalogs dar, in dem alle bekannten Maßnahmen zum Selbstdatenschutz gesammelt und ihrer zeitlichen Anwendung entsprechend kategorisiert wurden.

Mit einer Marktübersicht konnte gezeigt werden, welche Bandbreite an Privacy-Boxen in den unterschiedlichen Markt-Segmenten existiert. Bei den identifizierten Privacy-Boxen wurden anschließend die implementierten Funktionen zum Selbstdatenschutz recherchiert. Durch einen Vergleich des Funktionsumfangs konnte aus dem Marktangebot eine repräsentative Vorauswahl von acht „interessanten“ Privacy-Boxen ermittelt werden. Alle Geräte dieser Vorauswahl wurden anschließend für die geplante Untersuchung bestellt.

Auf Grundlage der zuvor recherchierten Selbstdatenschutz-Funktionen von Privacy-Boxen wurde ein Feature-Modell entwickelt. Anhand gemeinsamer Selbstdatenschutz-Ziele gruppiert es Funktionen und Eigenschaften von Privacy-Boxen in folgende zusammengehöri-

ge Bereiche: IT-Schutz, Anonymität, Vertraulichkeit und Autonomie. Mithilfe des Modells ließ sich überprüfen, welche der zuvor definierten Privacy-Werkzeuge, mithilfe von Privacy-Boxen realisiert werden können. Diese Schnittmenge von Werkzeugen und Funktionen wurde als „maximal erreichbarer Schutz“ für Nutzer durch den Einsatz von Privacy-Boxen definiert.

Mithilfe einer Zielgruppen-Analyse ließen sich „Bemühte Amateure“ und „Techniker“ als relevante Nutzertypen für Privacy-Boxen identifizieren. Anschließend wurden die bestellten Geräte der Vorauswahl den Nutzertypen zugeordnet und so in zwei Gruppen aufgeteilt. Durch eine Analyse von häufig genutzten Internetaktivitäten und Schutzmaßnahmen konnten die unterschiedlichen Selbstdatenschutz-Bereiche von Privacy-Boxen nach Relevanz gewichtet werden. Auf dieser Grundlage war es möglich, für jeden Nutzertyp zwei relevante Geräte und fünf Nutzeraufgaben für die Untersuchung zu bestimmen.

Den „Bemühten Amateuren“ wurden die Geräte *Bitdefender BOX 2* und *F-Secure SENSE* zur Untersuchung zugeteilt. Als typische Nutzerszenarien ließen sich die Verwendung eines VPN-Tunnels, das Aktivieren von Inhaltsfiltern, die Konfiguration einer Netzwerk-Firewall, die Einrichtung von Anti-Virus-Maßnahmen und das Einstellen eines IoT-Monitors definieren. Für „Techniker“ wurde die Untersuchung der Privacy-Boxen *TrutzBox Home* und *eBlocker 2* festgelegt. Die Einrichtung von Anti-Tracking-Maßnahmen, das Aktivieren eines DNS-Schutzes, die Verwendung eines VPN-Tunnels, die Konfiguration von Ad-Blockern und das Aktivieren von Inhaltsfiltern stellten die typischen Nutzerszenarien dar.

Nach der Festlegung auf eine expertenorientierte (analytische) Untersuchung von Privacy-Boxen konnte durch einen Vergleich von gängigen Evaluations-Methoden eine Mischform als die vielversprechendste Variante bestimmt werden: der „Heuristic Walkthrough“ (HW). Als benötigte Usability-Heuristik wurde eine aktuelle Arbeit gewählt (Granollers), welche die Stärken zweier bereits bewährter Heuristiken miteinander vereint (Nielsen und Tognazzini). Zur Untersuchung der Nutzer-Erfahrung (UX) bei Aufbau und Einrichtung der Privacy-Boxen ließ sich eine bestehende nutzerorientierte (empirische) Methode als Grundlage verwenden (Serif und Ghinea) und für eine analytische Untersuchung anpassen.

Um bei der Untersuchung von Privacy-Boxen neben UX und Usability auch die Privacy zu berücksichtigen, wurden drei Ansätze von Privacy-Heuristiken auf Schnittmengen mit Privacy-Boxen analysiert. Bei den auf der DSGVO basierenden Heuristiken ließ sich in Privacy-Nudges der größte Mehrwert für eine Untersuchung von Privacy-Boxen identifizieren. Zusätzlich konnte eine Arbeit ermittelt werden, die anhand aktueller Forschungen die wichtigsten Privacy-Nudges extrahiert und auf Nutzerakzeptanz bewertet (Schöbel et al.). Somit wurden UX und benötigte Zeit beim Aufbau sowie Usability und Usable-Privacy bei der Nutzung von Privacy-Boxen als Metriken für die Untersuchung festgelegt.

Durch Einrichten einer Testumgebung konnte die Untersuchungs-Methodik in mehreren Pilot-Durchläufen überprüft und optimiert werden. Anschließend folgte die Untersuchung der vier ausgewählten Privacy-Boxen. Dabei wurde zuerst die UX bei der Einrichtung, anschließend die Usability bei der Benutzung und zuletzt die Usable-Privacy evaluiert. Nach Abschluss der Untersuchung folgte die Auswertung der Ergebnisse. Dazu wurde eine bereits

etablierte Skala (Bangor et al.) verwendet und es wurden nach Bedarf eigene Skalen zur Bewertung definiert.

Nach der Auswertung konnten die Ergebnisse von UX, Usability und Usable-Privacy vorgestellt und zusätzlich die Lösbarkeit der typischen Anwendungsszenarien bewertet werden. Die Ergebnisse von Privacy-Boxen aus der selben Nutzergruppe wurden anschließend miteinander verglichen und interpretiert. Dabei ließen sich deutliche Unterschiede sowohl bei den Privacy-Boxen der „Bemühten Amateure“ (Bitdefender BOX 2 und F-Secure SENSE) als auch bei den Geräten für die „Techniker“ (TrutzBox Home und eBlocker 2) feststellen.

Im Anschluss wurde die Gültigkeit der ermittelten Ergebnisse überprüft und auf mögliche Fehlerquellen hingewiesen. Abschließend konnten die Forschungsfragen beantwortet und festgehalten werden, das effektiver Selbstdatenschutz mit Privacy-Boxen für „Bemühte Amateure“ nur schwer möglich ist. Als Grund ließ sich weniger die Usability, als die fehlenden Privatsphäre-Funktionen und -Voreinstellungen identifizieren. Für „Techniker“ hingegen ist der erfolgreiche Einsatz von Selbstdatenschutz mit Privacy-Boxen gut möglich, da viele Optionen zum Privatsphäre-Schutz von einer guten Usability unterstützt werden. Zuletzt ließen sich die zu Beginn der Arbeit gestellten Annahmen größtenteils bestätigen.

7.2 Kritische Reflexion

Im Folgenden wird die Vorgehensweise der Arbeit kritisch reflektiert, indem bereits bekannte Schwächen und Angriffsvektoren aufgezählt werden, welche die Gültigkeit der Arbeit gefährden können.

Die Grundlage der Methodik wurde durch die Entwicklung eines Katalogs für Selbstdatenschutz-Werkzeuge erarbeitet (siehe „Werkzeuge zum Selbstdatenschutz“ in Abschnitt 4.2). Dabei wurden Selbstdatenschutz-Maßnahmen aus verschiedenen Quellen aktueller Literatur und des Internets zusammengefasst, um den Katalog so umfassend wie möglich zu gestalten. Dennoch ist es denkbar, dass der Werkzeug-Katalog nicht alle existierenden Maßnahmen zum Selbstdatenschutz abdeckt und somit Lücken in der Methoden-Grundlage verbleiben.

Eine weitere Gefahr ist bei der durchgeführten Marktanalyse erkennbar (siehe „Marktanalyse und Geräteübersicht“ in Abschnitt 4.3). Hier ist es möglich, dass trotz intensiver Recherche wichtige oder relevante Privacy-Boxen nicht gefunden wurden, die im Rahmen dieser Arbeit hätten betrachtet werden können. Gleiches gilt für neue Privacy-Boxen, die in der Zeit zwischen Marktanalyse und Untersuchung entwickelt wurden.

Anhand der vorgestellten Privacy-Boxen wurde eine Liste mit Selbstdatenschutz-Funktionen erstellt, die sich auf Informationen und Angaben von Herstellern stützt (siehe Tabelle 3 „Funktionen, Eigenschaften und Preise von Privacy-Boxen im Vergleich“). Es wurde (mit Ausnahme der vier untersuchten Privacy-Boxen) nicht überprüft, ob die angegebenen Funktionen wirklich implementiert sind und dem Nutzer den versprochenen Schutz bieten. Um eventuelle Falschangaben sowie Lücken und Fehler bei der Recherche auszuschließen, hätte eine Überprüfung der Funktionen bei jeder Privacy-Box stattfinden müssen.

Im Rahmen der Methodik-Entwicklung wurde ein Feature-Modell erstellt, welches Selbstdatenschutz mit Privacy-Boxen anhand ihrer Eigenschaften und Funktionen beschreibt (siehe „Feature-Modell von Privacy-Boxen“ in Abschnitt 5.1.1). Dabei wurde eine Unterteilung in fünf Bereiche vorgenommen, von denen vier Bereiche im Rahmen einer UX-/Usability-Evaluation auf ihre Ausprägung untersucht werden können. Der fünfte Bereiche stellt das Ergebnis dieser Untersuchungen dar. Die Auslegung und Einordnung von Eigenschaften und Funktionen ist hierbei nicht immer eindeutig, wodurch das Modell auch in anderen Ausprägungen gültig sein kann.

Bei der Ermittlung typischer Anwendungsszenarien mit Privacy-Boxen wurden Statistiken über häufige Aktivitäten und häufig eingesetzte Schutzmaßnahmen bei der Internetnutzung verwendet (siehe „Anwendungsszenarien“ in Abschnitt 5.3). Diese wurden den ermittelten Bereichen des Feature-Modells zugeordnet, um anschließend Gewichte für deren Relevanz daraus abzuleiten. Die Art der Aggregierung von Statistik-Daten kann hierbei verzerrte Ergebnisse liefern: Neben der Häufigkeit sind keine zusätzlichen Informationen z.B. über den Zeitraum der genutzten Tätigkeiten o.Ä. vorhanden. Dadurch kann die Gewichtung eines Bereichs durch sich überschneidende Aktivitäten stärker ausfallen. Zusätzlich kann nicht sichergestellt werden, dass bei der Erhebung der Statistik-Daten die abgefragten Tätigkeiten und Schutzmaßnahmen hinreichend sind. Es ist möglich, dass relevante Bereiche nicht abgefragt wurden.

Zur Bestätigung der Annahme über interessante Geräte für einen Vergleich wurde eine Berechnung der Vergleichbarkeit durchgeführt (siehe „Geräteauswahl und Nutzerszenarien“ in Abschnitt 5.3.3). Diese bewertet die Anzahl an vergleichbaren Funktionen mit einer hohen Gewichtung, basierend auf den häufigen Internetaktivitäten und Schutzmaßnahmen der zuvor ausgewerteten Statistiken. Das Ergebnis dieser Berechnung führte anschließend zur Auswahl typischer Anwendungsszenarien, die sich bei beiden im Vergleich stehenden Geräten untersuchen lassen. Diese Vorgehensweise ist jedoch anfällig für Folgefehler in dem Fall, dass bereits bei der Statistik-Auswertung falsche Annahmen gemacht wurden.

Bei der Wahl einer geeigneten Evaluationsmethode wurde zunächst die Entscheidung für eine analytische Vorgehensweise getroffen (siehe „Art und Weise der Evaluation“ in Abschnitt 5.4.1). Diese Entscheidung wurde durch den Mangel existierender Arbeiten zum Thema „Privacy-Boxen“ und den erhöhten Aufwand bei der Durchführung einer empirischen Evaluation begründet. In der Zeit zwischen Recherche zu „Related Work“ und Durchführung der Untersuchung ist es jedoch möglich, dass ähnliche oder vergleichbare Arbeiten veröffentlicht wurden. Zusätzlich wären bei der Durchführung einer empirischen Evaluation, trotz des höheren Aufwands, aussagekräftigere Ergebnisse und eine größere Anzahl an aufgedeckten Usability-Problemen möglich.

Beim Vergleich der analytischen Evaluationsmethoden wurden Bewertungen unterschiedlicher Autoren miteinander verglichen (siehe „Vergleich von Evaluationsmethoden“ in Abschnitt 5.4.3). Bei der Zusammenfassung ähnlicher Gütebegriffe und der Normalisierung unterschiedlicher Bewertungs-Skalen sind Fehler denkbar. Zusätzlich können die ungleichmäßige Abdeckung von bewerteten Methoden und Kriterien sowie das Schätzen eines fehlenden Werts, das Ergebnis verzerren.

Bei der Übersetzung der verwendeten Heuristiken vom Englischen ins Deutsche können Übersetzungsfehler aufgetreten sein, wodurch die Bedeutung von Aussagen variieren kann. Zudem ist die Verwendung einer empirischen Methodik als Grundlage für eine analytische Untersuchung der OOBE kritisierbar (siehe „Die Out-of-Box Experience“ in Abschnitt 5.4.2). Aus Mangel an analytischen Grundlagen wurde die empirische Methodik einer analytische Evaluation angepasst, durch mehrere Testdurchläufe verbessert und schließlich als geeignet bewertet. Zusätzlich gelten die in Abschnitt 6.2.3 (Gültigkeit der Ergebnisse) genannten Faktoren für mögliche Fehler bei der Auswertung von Ergebnissen.

Es wurden alle vorgestellten Gefahren nach bestem Wissen und Gewissen abgewogen und die entsprechenden Entscheidungen und Vorgehensweisen als nachvollziehbar und vertretbar bewertet.

7.3 Ausblick und Future Work

Im Rahmen dieser Arbeit gab es einige Aspekte, die bei der Betrachtung aufgrund ihres Umfangs oder ihrer geringen Relevanz ausgelassen wurden. Da sie jedoch für zukünftige Arbeiten mit anderem Schwerpunkt von Interesse sein können, folgt im Anschluss eine Aufzählung der Punkte, um das Fortführen dieser Arbeit zu vereinfachen. Zu Beginn wird dazu motiviert, das mit dieser Arbeit neu erschlossene Forschungsgebiet über Security & Privacy-Boxen auszuweiten und weiter zu erforschen.

Dazu könnte mit der Durchführung von empirischen Nutzerstudien überprüft werden, ob die Zielgruppe von Privacy-Boxen tatsächlich den in dieser Arbeit ermittelten Nutzertypen entspricht. Des Weiteren ließe sich verifizieren, ob die Häufigkeiten der genutzten Internetaktivitäten und eingesetzten Schutzmaßnahmen von Nutzern den in dieser Arbeit verwendeten Grundlagen entsprechen. Ferner ließe sich bestimmen, ob die analytisch ermittelten Ergebnisse über UX, Usability und Usable-Privacy bei der Einrichtung und Nutzung von Privacy-Boxen mit echten Nutzern bestätigt werden können.

Des Weiteren wurden bei der Untersuchung der Out-of-Box Experience (OOBE) die Phasen 1 und 4 des Produkt-Lebenszyklus von Privacy-Boxen nicht betrachtet. Dabei könnte untersucht werden, wie sich z.B. Recherche, Kaufentscheidung und Vorfreude bei Anschaffung einer Privacy-Box auf die Nutzung auswirken. Noch interessanter wäre allerdings die Frage nach dem Austausch oder der Stilllegung von Privacy-Boxen und dem Verbleib der darauf gespeicherten personenbezogenen Daten.

Ein weiterer Punkt, der im Rahmen dieser Arbeit nicht betrachtet werden konnte, betrifft die Usable-Privacy-Heuristiken von Johansen und Fischer-Hübner (siehe Anhang B.5). Denkbar sind Untersuchungen von Privacy-Boxen, deren Evaluation die Nutzung von Alternativ-Diensten (z.B. Cloud-Speicher) oder verschlüsselter Kommunikation (z.B. Emails oder Chats) als typische Anwendungsszenarien berücksichtigt. Dabei ließe sich untersuchen, ob und in welchem Maß Usable-Privacy-Heuristiken von Privacy-Boxen berücksichtigt werden.

Zuletzt fällt rückblickend auf, dass ein großer Teil dieser Arbeit die Entwicklung der Evaluations-Methodik zum Inhalt hat. Dieser Teil wird allerdings von den Forschungsfragen nicht entsprechend berücksichtigt bzw. aufgegriffen. Der Umfang für die Methodik-Entwicklung stellte sich erst im Verlauf der Arbeit heraus. Daher wäre es in folgenden Arbeiten denkbar und wünschenswert, die in dieser Arbeit entwickelte Evaluations-Methode für Privacy-Boxen anhand verschiedener Gütekriterien zu untersuchen und zu bewerten.

Dabei ließe sich die Nachvollziehbarkeit der Methodik untersuchen, also ob alle Evaluations- bzw. Berechnungsschritte gut dokumentiert wurden. Es könnte mit der Korrektheit von Ergebnissen fortgefahren werden, um zu überprüfen, ob die ermittelten Punktwerte mit der eigentlich zu bewertenden Nutzbarkeit korrelieren (z.B. anhand einer empirischen Evaluation). Zusätzlich ließe sich die Methodik auf Vollständigkeit überprüfen, indem untersucht wird, ob alle wichtigen Aspekte von Privacy-Boxen abgedeckt werden. Die Reproduzierbarkeit und die Effizienz der Methodik könnten als weitere Punkte folgen.

Damit sind hinreichend Punkte für zukünftige Arbeiten genannt, um dem Thema von Security & Privacy-Boxen durch weitere Forschungen eine stärkere Präsenz zu ermöglichen. Jede Arbeit in diesem Gebiet trägt dazu bei, dass Nutzer in Zukunft Selbstdatenschutz mit Security & Privacy-Boxen effektiv, effizient und zufriedenstellend durchführen können.

Danksagung

An dieser Stelle möchte ich mich bei all denjenigen bedanken, die mich während der Anfertigung dieser Masterarbeit unterstützt und motiviert haben.

Zuerst gebührt mein Dank den Professoren Luigi Lo Iacono und Andreas Heinemann, die meine Masterarbeit betreut und mit hilfreichen Anregungen und konstruktiver Kritik bei der Erstellung geholfen haben.

An zweiter Stelle gebührt mein Dank Hannah und Andy, für die unermüdlichen Korrekturen, fortwährend gute Ideen und natürlich die Unterstützung in allen Lebenslagen!

Ebenfalls möchte ich meinem Kommilitonen Michael danken, für die organisatorische Hilfe bei den teilweise komplizierten Bestellungen der Privacy-Boxen.

Zusätzlich geht ein Dank an meine ehemaligen Arbeitskollegen Peter und Stephan, für die Hilfe bei der Beschaffung von schwer zu findender Literatur.

Ich danke zusätzlich Herrmann Sauer von der Comidio GmbH für das großzügige Bereitstellen der TrutzBox und die ausführlichen Informationen über Grundlagen und Marktanalyse.

Des Weiteren gebührt Gisela Strangmüller ein Dank für das Bereitstellen einer Lizenz für das Premium-Sicherheitspaket F-Secure TOTAL.

Zuletzt danke ich Boris für die nie endende Energie.

Abbildungsverzeichnis

Tabellenverzeichnis

Literatur

[1] Christian Ächter. *Datenschutzgesetze im Überblick - welche Gesetze relevant sind*. Juni 2017. URL: https://datenschutzfachmann.eu/datenschutzgesetze/ (besucht am 08. 09. 2020).

[2] Alessandro Acquisti et al. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online". In: *ACM Computing Surveys* 50.3 (Aug. 2017), 44:1–44:41. ISSN: 0360-0300. DOI: 10.1145/3054926.

[3] International Trade Administration. *Privacy Shield Program Overview*. 2020. URL: https://www.privacyshield.gov/Program-Overview (besucht am 09. 09. 2020).

[4] Akita. *AKITA Amazon Shop | Instant WiFi Privacy Protection for Smart Home Devices*. 2020. URL: https://www.amazon.com/stores/AKITA/AKITA/page/B4C14F79-CBAC-409E-B237-258837C0C6E8 (besucht am 07. 10. 2020).

[5] Sascha Alpers, Maria Pieper und Manuela Wagner. *Herausforderungen bei der Entwicklung von Anwendungen zum Selbstdatenschutz*. Gesellschaft für Informatik, Bonn, 2017. ISBN: 978-3-88579-669-5. DOI: 10.18420/in2017_108.

[6] Arne Arnold. *Sicherheitsboxen im Test: Schutz oder Augenwischerei?* Okt. 2016. URL: https://www.pcwelt.de/ratgeber/Sicherheitsboxen-im-Test-10059814.html (besucht am 22. 06. 2020).

[7] Andrés Arrieta et al. *Privacy Badger Is Changing to Protect You Better*. Okt. 2020. URL: https://www.eff.org/deeplinks/2020/10/privacy-badger-changing-protect-you-better (besucht am 20. 10. 2020).

[8] Aaron Bangor, Philip T. Kortum und James T. Miller. "An Empirical Evaluation of the System Usability Scale". In: *International Journal of Human–Computer Interaction* 24.6 (Juli 2008), S. 574–594. ISSN: 1044-7318. DOI: 10.1080/10447310802205776.

[9] Maximilian Batz. *pi3g - Anonymebox 3 Plus*. 2020. URL: https://buyzero.de/products/anonymebox-anonym-frei-einfach (besucht am 08. 10. 2020).

[10] §3 BDSG. Erster Abschnitt - Allgemeine und gemeinsame Bestimmungen (§§ 1 - 11). *Weitere Begriffsbestimmungen*. Jan. 2009.

[11] Jennifer Bendery. *Woman Fired For Flipping Off Trump's Motorcade*. Juli 2017. URL: https://www.huffpost.com/entry/woman-flips-off-donald-trump-fired_n_59fe0ab4e4b0c9652fffa484 (besucht am 17. 07. 2020).

[12] Patrick Beuth. Digital. "Snowden-Enthüllungen: Alles Wichtige zum NSA-Skandal". In: *Die Zeit* (Jan. 2016). ISSN: 0044-2070. URL: https://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal (besucht am 17. 07. 2020).

[13] BGBL. "Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG)". In: *Bundesgesetzblatt Teil I* 7 (Jan. 1977), S. 14.

[14] Paul Bischoff. *Data Privacy Laws & Government Surveillance by Country*. Okt. 2019. URL: https://www.comparitech.com/blog/vpn-privacy/surveillance-states/ (besucht am 20. 07. 2020).

[15] Bitdefender. *BOX - Heimnetzwerksicherheit für alle Ihre vernetzten Geräte*. 2020. URL: https://www.bitdefender.de/box/ (besucht am 06. 10. 2020).

[16] BITKOM. *Big Data im Praxiseinsatz – Szenarien, Beispiele, Effekte*. Techn. Ber. Berlin: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., 2012, S. 103.

[17] Internetredaktion BMBF. *Bekanntmachung „Ökonomische Aspekte von IT-Sicherheit und Privatheit“*. Juli 2019. URL: https://www.bmbf.de/foerderungen/bekanntmachung-2547.html (besucht am 13. 07. 2020).

[18] Emily Brandon. *How Sadness Can Turn You Into a Shopaholic*. Nov. 2008. URL: https://money.usnews.com/money/personal-finance/articles/2008/02/11/how-sadness-can-turn-you-into-a-shopaholic (besucht am 14. 07. 2020).

[19] Brave. *What's Brave Done For My Privacy Lately? Episode #3: Fingerprint Randomization*. März 2020. URL: https://brave.com/whats-brave-done-for-my-privacy-lately-episode3/ (besucht am 29. 07. 2020).

[20] Matthew Brocker und Stephen Checkoway. “iSeeYou: Disabling the MacBook Webcam Indicator LED” (Dez. 2013). (Besucht am 10. 08. 2020).

[21] Carol Brown. “Online Reputation in a Connected World”. In: *cross-tab transforming market research* (Jan. 2010), S. 23.

[22] BSI. *Sichere Passwörter erstellen - BSI für Bürger*. 2020. URL: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html (besucht am 28. 07. 2020).

[23] BSI. *Was ist Anonymität?* 2020. URL: https://www.bsi.bund.de/DE/Publikationen/Studien/Anonym/wasistanonymitaet.html (besucht am 13. 07. 2020).

[24] Peter Buxmann. *Der Preis des Kostenlosen – Was sind unsere Daten wert? – Prof. Dr. Peter Buxmann*. Aug. 2016. URL: https://www.peterbuxmann.de/2016/08/15/preis-des-kostenlosen/ (besucht am 14. 07. 2020).

[25] BVDW. *Browsercookies und alternative Tracking-Technologien: Technische und datenschutzrechtliche Aspekte*. Whitepaper. Berlin: Bundesverband Digitale Wirtschaft (BVDW) e.V., Aug. 2015, S. 27.

[26] BVDW. *Digitale Nutzung in Deutschland 2018*. Marktforschung. Düsseldorf: Bundesverband Digitale Wirtschaft (BVDW) e.V., 2018, S. 100.

[27] BVerfG. *Beschluss vom 27. Mai 2020 - 1 BvR 1873/13, 1 BvR 2618/13 (Bestandsdatenauskunft II)*. Mai 2020.

[28] BVerfG. *Regelungen zur Bestandsdatenauskunft verfassungswidrig | Pressemitteilung Nr. 61/2020*. Juli 2020. URL: https://www.bverfg.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-061.html (besucht am 09. 09. 2020).

[29] Farah Chanchary und Sonia Chiasson. “User perceptions of sharing, advertising, and tracking”. In: *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*. SOUPS ’15. Ottawa, Canada: USENIX Association, Juli 2015, S. 53–67. ISBN: 978-1-931971-24-9.

[30] Comidio. *Trutzbox - Ihre Privacy Box. Mehr Schutz im Internet.* 2020. URL: `https://trutzbox.de/trutzbox/` (besucht am 06. 10. 2020).

[31] Kovila P. L. Coopamootoo und Thomas Groß. “Why Privacy Is All But Forgotten: An Empirical Study of Privacy & Sharing Attitude”. In: *Proceedings on Privacy Enhancing Technologies* 2017.4 (Okt. 2017), S. 97–118. DOI: `10.1515/popets-2017-0040`.

[32] Matthew Corner et al. “A Usability Evaluation of Privacy Add-ons for Web Browsers”. In: *Design, User Experience, and Usability. Practice and Case Studies*. Hrsg. von Aaron Marcus und Wentao Wang. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2019, S. 442–458. ISBN: 978-3-030-23535-2. DOI: `10.1007/978-3-030-23535-2_33`.

[33] Lorrie Faith Cranor. *Web Privacy with P3p*. 1st Edition. Beijing ; Sebastopol, Calif: O’Reilly Media, Okt. 2002. ISBN: 978-0-596-00371-5.

[34] Lorrie Faith Cranor und Simson Garfinkel. “Security and Usability: Designing Secure Systems that People Can Use - Chapter 4”. O’Reilly Media, 2005, S. 401–414. ISBN: 978-0-596-00827-7.

[35] Lorrie Faith Cranor, Praveen Guduru und Manjula Arjula. “User interfaces for privacy agents”. In: *ACM Transactions on Computer-Human Interaction* 13.2 (Juni 2006), S. 135–178. ISSN: 1073-0516. DOI: `10.1145/1165734.1165735`.

[36] Der Sächsische Datenschutzbeauftragte. *Selbstdatenschutz*. Jan. 2012. URL: `https://web.archive.org/web/20120105070747/http://www.saechsdsb.de:80/datenschutz-fuer-buerger/112-selbstdatenschutz` (besucht am 21. 07. 2020).

[37] IoT Defense. *RATtrap - Technology*. 2020. URL: `https://www.myrattrap.com/technology/` (besucht am 06. 10. 2020).

[38] Markus Donko-Huber. *Usable Privacy Box - Privatsphäre im Internet*. 2020. URL: `https://upribox.org/` (besucht am 08. 10. 2020).

[39] Art. 17 DSGVO. Kapitel III - Rechte der betroffenen Person (Art. 12 - 23), Abschnitt 3 - Berichtigung und Löschung (Art. 16 - 20). *Recht auf Löschung (”Recht auf Vergessenwerden”)*. Mai 2018.

[40] Art. 25 DSGVO. Kapitel IV - Verantwortlicher und Auftragsverarbeiter (Art. 24 - 43), Abschnitt 1 - Allgemeine Pflichten (Art. 24 - 31). *Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen*. Mai 2018.

[41] Art. 4 DSGVO. Kapitel I - Allgemeine Bestimmungen (Art. 1 - 4). *Begriffsbestimmungen*. Mai 2018.

[42] Art. 5 DSGVO. Kapitel II - Grundsätze (Art. 5 - 11). *Grundsätze für die Verarbeitung personenbezogener Daten*. Mai 2018.

[43] Janna Lynn Dupree et al. “Privacy Personas: Clustering Users via Attitudes and Behaviors toward Security Practices”. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. San Jose California USA: ACM, Mai 2016, S. 5228–5239. ISBN: 978-1-4503-3362-7. DOI: 10.1145/2858036.2858214.

[44] W. Dzida, S. Herda und W.D. Itzfeldt. “User-Perceived Quality of Interactive Systems”. In: *IEEE Transactions on Software Engineering* SE-4.4 (Juli 1978), S. 270–276. ISSN: 1939-3520. DOI: 10.1109/TSE.1978.231511.

[45] DIN e.V. *2016-12:DIN EN ISO 6385, Grundsätze der Ergonomie für die Gestaltung von Arbeitssystemen; Deutsche Fassung*. Norm. Beuth Verlag GmbH, Dez. 2016, S. 26. DOI: 10.31030/2429191.

[46] DIN e.V. *2018-11:DIN EN ISO 9241-11, Ergonomie der Mensch-System-Interaktion - Teil 11: Gebrauchstauglichkeit: Begriffe und Konzepte; Deutsche Fassung*. Norm. Beuth Verlag GmbH, Nov. 2018, S. 46. DOI: 10.31030/2757945.

[47] DIN e.V. *2020-03:DIN EN ISO 9241-210, Ergonomie der Mensch-System-Interaktion - Teil 210: Menschzentrierte Gestaltung interaktiver Systeme; Deutsche Fassung*. Norm. Beuth Verlag GmbH, März 2020, S. 47. DOI: 10.31030/3104744.

[48] DIN e.V. *2020-09:DIN EN ISO/IEC 29100, Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutz; Deutsche Fassung*. Norm. Beuth Verlag GmbH, Sep. 2020, S. 34. DOI: 10.31030/3174636.

[49] DIN e.V. *2020-10:DIN EN ISO 9241-110, Ergonomie der Mensch-System-Interaktion - Teil 110: Interaktionsprinzipien; Deutsche Fassung*. Norm. Beuth Verlag GmbH, Okt. 2020, S. 47. DOI: 10.31030/3147467.

[50] eBlocker. *eBlocker Open Source: Kostenlos anonym surfen. Plus Ad-Blocker. Schützt alle Geräte.* 2020. URL: https://eblocker.org (besucht am 07. 10. 2020).

[51] eBlocker UG. *eBlocker: Do It Yourself – Selbstbau*. 2020. URL: https://eblocker.org/eblockeros-download/ (besucht am 03. 12. 2020).

[52] EDAA. *YourOnlineChoices.eu - Präferenzmanagement*. 2020. URL: https://www.youronlinechoices.com/de/praferenzmanagement/ (besucht am 28. 07. 2020).

[53] EFF. *Secure Messaging Scorecard*. Okt. 2019. URL: https://www.eff.org/pages/secure-messaging-scorecard (besucht am 31. 07. 2020).

[54] EFF. *Upstream vs. PRISM*. Okt. 2017. URL: https://www.eff.org/de/pages/upstream-prism (besucht am 10. 09. 2020).

[55] Jasmine Enberg. *Global Digital Ad Spending 2019*. 2020. URL: https://www.emarketer.com/content/global-digital-ad-spending-2019 (besucht am 07. 07. 2020).

[56] Christian Endreß und Nils Petersen. *Die Dimensionen des Sicherheitsbegriffs | bpb*. Juni 2012. URL: https://www.bpb.de/politik/innenpolitik/innere-sicherheit/76634/dimensionen-des-sicherheitsbegriffs (besucht am 13. 07. 2020).

[57] ENISA. *Privacy and data protection by design - from policy to engineering*. LU: Publications Office, Jan. 2015.

[58] EP. *Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)*. Dez. 2002.

[59] EP. *Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz (Text von Bedeutung für den EWR)*. Dez. 2009.

[60] EP. *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*. Nov. 1995.

[61] EP. *Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation*. Dez. 1997.

[62] EP. *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)*. Okt. 2017.

[63] EuGH. *Urteil vom 16.07.2020 - C-311/18 (Privacy-Shield-Vereinbarung)*. Juli 2020.

[64] F-Secure. *SENSE - Sicherer Router und sichere App*. 2020. URL: `https://www.f-secure.com/de/home/products/sense` (besucht am 06. 10. 2020).

[65] Alexander Fanta. *Ob Nutzer oder nicht: Facebook legt Schattenprofile über alle an*. März 2018. URL: `https://netzpolitik.org/2018/ob-nutzer-oder-nicht-facebook-legt-schattenprofile-ueber-alle-an/` (besucht am 08. 07. 2020).

[66] Frederic Filloux. *The ARPUs of the Big Four Dwarf Everybody Else*. Feb. 2019. URL: `https://mondaynote.com/the-arpus-of-the-big-four-dwarf-everybody-else-e5b02a579ed3` (besucht am 10. 07. 2020).

[67] Dimitris Geneiatakis et al. "Security and privacy issues for an IoT based smart home". In: *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. Opatija, Croatia: IEEE, Mai 2017, S. 1292–1297. ISBN: 978-953-233-090-8. DOI: `10.23919/MIPRO.2017.7973622`.

[68] Art. 1 GG. Kapitel I - Die Grundrechte (Art. 1 - 19). *Die Grundrechte*. Mai 1949.

[69] Hauke Gierow. *Privacy-Boxen im Test: Trügerische Privatheit - Golem.de*. Apr. 2016. URL: `https://www.golem.de/news/privacy-boxen-im-test-truegerische-privatheit-1604-120250.html` (besucht am 22. 06. 2020).

[70] IGI Global. *What is Social Web | IGI Global*. 2020. URL: `https://www.igi-global.com/dictionary/mobile-social-web/27518` (besucht am 07. 07. 2020).

[71] Datum Network GmbH. *Data Calculator - How much are companies making from your data?* 2020. URL: https://calc.datum.org/ (besucht am 28. 07. 2020).

[72] JonDos GmbH. *Anonym Bezahlen mit Paysafecard oder Bitcoin*. 2020. URL: https://www.anonym-surfen.de/help/premium_jondo4.html (besucht am 04. 08. 2020).

[73] PROLIANCE GmbH. *ePrivacy Verordnung*. 2020. URL: https://www.datenschutzexperte.de/eprivacy-verordnung/ (besucht am 08. 09. 2020).

[74] PROLIANCE GmbH. *Neue ePrivacy Verordnung*. Nov. 2019. URL: https://www.datenschutzexperte.de/blog/datenschutz-und-eu-dsgvo/review-was-bringt-die-neue-eprivacy-verordnung/ (besucht am 08. 09. 2020).

[75] Google. *Ersuchen um Entfernung von Inhalten gemäß europäischem Datenschutzrecht*. Mai 2020. URL: https://transparencyreport.google.com/eu-privacy/overview (besucht am 15. 07. 2020).

[76] Toni Granollers. "Usability Evaluation with Heuristics, Beyond Nielsen's List". März 2018, S. 60–65. ISBN: 978-1-61208-616-3.

[77] Shane Green. *About Shane*. Sep. 2010. URL: https://shanegreen.org/shanegreenbio/ (besucht am 17. 07. 2020).

[78] Shane Green. *Revisiting a crowdsourced Digital Bill of Rights "by the people, for the people" from SXSW 2012*. Dez. 2018. URL: https://shanegreen.org/2018/12/20/revisiting-a-crowdsourced-digital-bill-of-rights-by-the-people-for-the-people-from-sxsw-2012/ (besucht am 16. 07. 2020).

[79] Seda Gürses, Carmela Troncoso und Claudia Diaz. "Engineering Privacy by Design" (Jan. 2011), S. 25.

[80] Seda Gürses, Carmela Troncoso und Claudia Diaz. "Engineering Privacy by Design Reloaded" (Sep. 2015), S. 21.

[81] Kai Haller. "Sicherheitsbewusstsein bei der Nutzung von Apps". In: *mediaTest digital* (Sep. 2013).

[82] David Harborth et al. "Integrating Privacy-Enhancing Technologies into the Internet Infrastructure". In: *arXiv:1711.07220 [cs]* (Nov. 2017).

[83] Andreas Heinemann. *Sicherheitslösungen müssen benutzbar sein*. 2020. URL: http://manager-wissen.com/heinemann (besucht am 27. 07. 2020).

[84] Dominik Herrmann. "Notwehr oder notwendiger Ungehorsam? Wirksamer Selbstdatenschutz geht manchmal zulasten anderer". In: *digma: Zeitschrift für Datenrecht und Informationssicherheit* (Sep. 2014), S. 148–152.

[85] Dominik Herrmann und Jens Lindemann. "Obtaining personal data and asking for erasure: Do app vendors and website owners honour your privacy rights?" In: *arXiv:1602.01804 [cs]* (Apr. 2016).

[86] Dominik Herrmann et al. “Behavior-based tracking of Internet users with semi-supervised learning”. In: *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. Auckland, New Zealand: IEEE, Dez. 2016, S. 596–599. ISBN: 978-1-5090-4379-8. DOI: 10.1109/PST.2016.7906992.

[87] Steffan Heuer. *Mich kriegt ihr nicht!: Die wichtigsten Schritte zur digitalen Selbstverteidigung*. 1. Aufl. Murmann Publishers GmbH, 2019.

[88] Christian Hildebrandt und René Arnold. *Wirtschaftliche Auswirkungen der Regelungen der ePrivacy-Verordnung auf die Online-Werbung und werbefinanzierte digitale Geschäftsmodelle*. Studie für das Bundesministerium für Wirtschaft und Energie. Bad Honnef: WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, Nov. 2017, S. 29.

[89] Jaap-Henk Hoepman. “Privacy Design Strategies”. In: *ICT Systems Security and Privacy Protection*. Hrsg. von Nora Cuppens-Boulahia et al. IFIP Advances in Information and Communication Technology. Berlin, Heidelberg: Springer, 2014, S. 446–459. ISBN: 978-3-642-55415-5. DOI: 10.1007/978-3-642-55415-5_38.

[90] Martin Holland. *NSA-Überwachungsskandal: PRISM, Tempora und Co. - was bisher geschah*. Okt. 2013. URL: https://www.heise.de/newsticker/meldung/NSA-Ueberwachungsskandal-PRISM-Tempora-und-Co-was-bisher-geschah-1909702.html (besucht am 22. 07. 2020).

[91] Marvin Hubert, Joachim Griesbaum und Christa Womser-Hacker. “Usability von Browsererweiterungen zum Schutz vor Tracking”. In: *Information - Wissenschaft & Praxis* 71.2-3 (Apr. 2020), S. 95–106. ISSN: 1619-4292, 1434-4653. DOI: 10.1515/iwp-2020-2075.

[92] Simon Hurtz. *”Hey Google, wie viele Menschen hören mir zu?”*. Juli 2019. URL: https://www.sueddeutsche.de/digital/alexa-google-datenschutz-1.4535355 (besucht am 10. 08. 2020).

[93] Simon Hurtz. *Alexa, Siri und Google: Sprachassistent ohne Ohren*. Apr. 2019. URL: https://www.sueddeutsche.de/digital/alexa-siri-google-datenschutz-1.4552480 (besucht am 10. 08. 2020).

[94] Simon Hurtz. *Cambridge Analytica: Neues Jahr, neuer Skandal?* Juli 2020. URL: https://www.sueddeutsche.de/digital/cambridge-analytica-facebook-brittany-kaiser-1.4747594 (besucht am 17. 07. 2020).

[95] InvizBox. *InvizBox Go | Award winning portable VPN Router*. 2020. URL: https://www.invizbox.com/products/invizbox-go/ (besucht am 07. 10. 2020).

[96] IONOS. *Was sind Cookies?* Mai 2020. URL: https://www.ionos.de/digitalguide/hosting/hosting-technik/was-sind-cookies/ (besucht am 21. 07. 2020).

[97] Autorenteam iRights.Lab. *Das Recht auf informationelle Selbstbestimmung | bpb*. Okt. 2017. URL: https://www.bpb.de/gesellschaft/digitales/persoenlichkeitsrechte/244837/informationelle-selbstbestimmung (besucht am 16. 07. 2020).

[98] Johanna Johansen und Simone Fischer-Hübner. “Making GDPR Usable: A Model to Support Usability Evaluations of Privacy”. In: *arXiv:1908.03503 [cs]* 576 (2020), S. 275–291. DOI: 10.1007/978-3-030-42504-3_18.

[99] Christian Johner. *User Experience ungleich Usability*. Juli 2015. URL: https://www.johner-institut.de/blog/iec-62366-usability/user-experience/ (besucht am 24. 07. 2020).

[100] Philipp Jordan. “Auswahl einer geeigneten Methode zur Usability Evaluation”. In: *KTD* (2008). DOI: 10.13140/RG.2.1.2956.9448.

[101] Ruogu Kang et al. “’My Data Just Goes Everywhere:’ User Mental Models of the Internet and Implications for Privacy and Security”. 2015, S. 39–52. ISBN: 978-1-931971-24-9.

[102] Murat Karaboga et al. “White Paper - Selbstdatenschutz”. In: *Forum Privatheit* (Nov. 2014), S. 44. ISSN: 2199-8914.

[103] Keezel. *Keezel – Online Security for Everyone*. 2020. URL: https://eu.keezel.co/ (besucht am 06. 10. 2020).

[104] Kickstarter. *RelaxBox - a box to thouroughly secure your internet access*. Okt. 2015. URL: https://www.kickstarter.com/projects/470304262/relaxbox-a-box-to-thouroughly-secure-you-internet (besucht am 07. 10. 2020).

[105] Matthias Kirchler et al. “Tracked Without a Trace: Linking Sessions of Users by Unsupervised Learning of Patterns in Their DNS Traffic”. In: *Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security - ALSec ’16*. Vienna, Austria: ACM Press, 2016, S. 23–34. ISBN: 978-1-4503-4573-6. DOI: 10.1145/2996758.2996770.

[106] klicksafe. *Privatshphäre und Big Data*. Lern-Baustein. Medienanstalt Rheinland-Pfalz (LMK) und Landesanstalt für Medien NRW, Mai 2015, S. 52.

[107] Erik Krempel. *Privacy by Design - Die 7 Grundprinzipen*. 2020. URL: https://www.iosb.fraunhofer.de/servlet/is/69348/ (besucht am 11. 08. 2020).

[108] KUM. *Methodenhandbuch zur nutzerzentrierten Entwicklung*. Handbuch. Kompetenzzentrum Usability für den Mittelstand, Juli 2015, S. 59.

[109] Ponnurangam Kumaraguru und Lorrie Faith Cranor. “Privacy Indexes: A Survey of Westin’s Studies” (Dez. 2005), S. 22.

[110] Prof. Dr. Richard Lackes. *Definition: Benutzerfreundlichkeit*. Text. Feb. 2018. URL: https://wirtschaftslexikon.gabler.de/definition/benutzerfreundlichkeit-29898/version-253494 (besucht am 23. 07. 2020).

[111] Pedro Leon et al. “Why Johnny can’t opt out: a usability evaluation of tools to limit online behavioral advertising”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’12. New York, NY, USA: Association for Computing Machinery, Mai 2012, S. 589–598. ISBN: 978-1-4503-1015-4. DOI: 10.1145/2207676.2207759.

[112] Andrew Lewis. *blue_beetle - User-driven discontent - MetaFilter*. Aug. 2010. URL: https://www.metafilter.com/95152/Userdriven-discontent#3256046 (besucht am 07. 07. 2020).

[113] Hans Leyendecker und Ralf Wiegand. *Bettina Wulff wehrt sich gegen Verleumdungen*. Aug. 2012. URL: https://www.sueddeutsche.de/politik/klage-gegen-google-und-jauch-bettina-wulff-wehrt-sich-gegen-verleumdungen-1.1462439 (besucht am 17. 07. 2020).

[114] Markus Lippodl. *Wie China seine Bürger überwachen will*. Okt. 2019. URL: https://www.n-tv.de/politik/Wie-China-seine-Buerger-ueberwachen-will-article21359017.html (besucht am 17. 07. 2020).

[115] Anonabox LLC. *Anonabox | Privacy Protected | Tor Router | VPN Router | Access Deep Web*. 2020. URL: https://www.anonabox.com/ (besucht am 07. 10. 2020).

[116] Pi-hole LLC. *Pi-hole - Network-wide Ad Blocking*. 2020. URL: https://pi-hole.net (besucht am 08. 10. 2020).

[117] Luigi Lo Iacono. *Mensch-Computer-Interaktion Kapitel 1: Definitionen und Standards*. TH Köln, März 2019. (Besucht am 20. 03. 2019).

[118] Syncloud Ltd. *Syncloud - Ihr persönlicher Server*. 2020. URL: https://syncloud.org/ (besucht am 21. 10. 2020).

[119] Max Maass et al. "PrivacyScore: Improving Privacy and Security via Crowd-Sourced Benchmarks of Websites". In: *arXiv:1705.05139 [cs]* 10518 (2017), S. 178–191. DOI: 10.1007/978-3-319-67280-9_10.

[120] Markus Mandalka. *Datenspuren und Datenschmutz*. 2020. URL: https://www.selbstdatenschutz.info/datenspuren (besucht am 07. 07. 2020).

[121] Markus Mandalka. *Digitale Selbstverteidigung für Eilige*. 2020. URL: https://www.selbstdatenschutz.info/digitale_selbstverteidigung (besucht am 03. 07. 2020).

[122] Markus Mandalka. *Staatliche Überwachung*. 2020. URL: https://www.selbstdatenschutz.info/staatliche_ueberwachung/ (besucht am 29. 06. 2020).

[123] Philipp K. Masur. "How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information". In: *Media and Communication* 8.2 (Juni 2020), S. 258–269. ISSN: 2183-2439. DOI: 10.17645/mac.v8i2.2855.

[124] Philipp K. Masur. "Mehr als Bewusstsein für Privatheitsrisiken. Eine Rekonzeptualisierung der Online- Privatheitskompetenz als Kombination aus Wissen, Fähig- und Fertigkeiten". In: *M&K Medien & Kommunikationswissenschaft* 66.4 (2018), S. 446–465. ISSN: 1615-634X. DOI: 10.5771/1615-634X-2018-4-446.

[125] Arunesh Mathur et al. "Characterizing the use of browser-based blocking extensions to prevent online tracking". In: *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*. SOUPS '18. Baltimore, MD, USA: USENIX Association, Aug. 2018, S. 103–116. ISBN: 978-1-931971-45-4.

[126] Tim Mocan. *Was ist der beste Browser für den Datenschutz?* Dez. 2019. URL: https://www.cactusvpn.com/de/privacy/was-ist-der-sicherste-und-beste-browser-fur-den-datenschutz/ (besucht am 30. 07. 2020).

[127] Eben Moglen. *FreedomBox - Personal Server at Home*. 2020. URL: https://freedombox.org/ (besucht am 08. 10. 2020).

[128] Melvin Mohokum und Rolf Ellegast. "Ergonomie am Büroarbeitsplatz". In: *Prävention und Gesundheitsförderung* (Mai 2019), S. 1–17. DOI: 10.1007/978-3-662-55793-8_100-1.

[129] Christian Moser. "Informationsarchitektur". *User Experience Design: Mit erlebniszentrierter Softwareentwicklung zu Produkten, die begeistern*. Hrsg. von Christian Moser. X.media.press. Berlin, Heidelberg: Springer, 2012, S. 105–120. ISBN: 978-3-642-13363-3. DOI: 10.1007/978-3-642-13363-3_6.

[130] Christian Moser. "Usability Testing". *User Experience Design: Mit erlebniszentrierter Softwareentwicklung zu Produkten, die begeistern*. Hrsg. von Christian Moser. X.media.press. Berlin, Heidelberg: Springer, 2012, S. 219–242. ISBN: 978-3-642-13363-3. DOI: 10.1007/978-3-642-13363-3_10.

[131] Cathy Moya und Susan Burgess. "Out of Box and First Time User Experiences" (2011), S. 45.

[132] mozilla. *Ein Einblick in Deutschlands Kampf gegen Hassrede*. März 2019. URL: https://internethealthreport.org/2019/ein-einblick-in-deutschlands-kampf-gegen-hassrede/?lang=de (besucht am 15. 07. 2020).

[133] Timofey Neshitov. *Warum ein Berliner Amazon mit Suizid drohte - DER SPIEGEL - Netzwelt*. Juli 2020. URL: https://www.spiegel.de/netzwelt/amazon-warum-ein-berliner-dem-unternehmen-mit-suizid-drohte-a-00000000-0002-0001-0000-000172071824 (besucht am 21. 07. 2020).

[134] Jakob Nielsen. *10 Heuristics for User Interface Design: Article by Jakob Nielsen*. Apr. 1994. URL: https://www.nngroup.com/articles/ten-usability-heuristics/ (besucht am 07. 11. 2020).

[135] Jakob Nielsen. *Heuristic Evaluation: How-To: Article by Jakob Nielsen*. Jan. 1994. URL: https://www.nngroup.com/articles/how-to-conduct-a-heuristic-evaluation/ (besucht am 03. 11. 2020).

[136] Jakob Nielsen. *Why You Only Need to Test with 5 Users*. März 2000. URL: https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/ (besucht am 03. 11. 2020).

[137] Łukasz Olejnik, Claude Castelluccia und Artur Janc. "Why Johnny Can't Browse in Peace: On the Uniqueness of Web Browsing History Patterns" (Feb. 2012), S. 16.

[138] PricewaterhouseCoopers. *Datenkonsum - German Entertainment & Media Outlook 2018-2022*. Okt. 2018. URL: https://www.pwc.de/de/technologie-medien-und-telekommunikation/german-entertainment-and-media-outlook-2018-2022/datenkonsum.html (besucht am 17. 07. 2020).

[139] PrimSEO. *Reputationsmanagement: Nachhaltig und effektiv mit PrimSEO*. 2020. URL: https://www.primseo.de/reputationsmanagement (besucht am 15. 07. 2020).

[140] privacytools.io. *PrivacyTools - Encryption Against Global Mass Surveillance*. 2020. URL: https://www.privacytools.io (besucht am 17. 07. 2020).

[141] Fahimeh Raja, Kirstie Hawkey und Konstantin Beznosov. "Revealing hidden context: improving mental models of personal firewall users". In: *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*. Mountain View, California: ACM Press, 2009, S. 1. ISBN: 978-1-60558-736-3. DOI: 10.1145/1572532.1572534.

[142] Jeff Roberts. *Lawsuit Says Hacked Address Book Contacts Worth 60 Cents To $3 Each*. März 2012. URL: https://gigaom.com/2012/03/15/419-lawsuit-says-hacked-address-book-contacts-worth-60-cents-to-3-each/ (besucht am 10. 07. 2020).

[143] Manuel Polst Rudolph, Svenja Polst und Denis Feth. "Usable Specification of Security and Privacy Demands: Matching User Types to Specification Paradigms". In: *Proceedings of the Mensch und Computer 2019 Workshop on Usable Security und Privacy*. Hamburg: Gesellschaft für Informatik e.V., 2019, S. 248–255. DOI: 10.18420/MUC2019-WS-302-05.

[144] Manuel Rudolph, Denis Feth und Svenja Polst. "Why Users Ignore Privacy Policies – A Survey and Intention Model for Explaining User Privacy Behavior". In: *Human-Computer Interaction. Theories, Methods, and Human Issues*. Hrsg. von Masaaki Kurosu. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018, S. 587–598. ISBN: 978-3-319-91238-7. DOI: 10.1007/978-3-319-91238-7_45.

[145] Scott Ruoti et al. "Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client". In: *arXiv:1510.08555 [cs]* (Jan. 2016).

[146] J.H. Saltzer und M.D. Schroeder. "The protection of information in computer systems". In: *Proceedings of the IEEE* 63.9 (Sep. 1975), S. 1278–1308. ISSN: 1558-2256. DOI: 10.1109/PROC.1975.9939.

[147] Florian Sarodnick und Henning Brau. *Methoden der Usability Evalution: Wissenschaftliche Grundlagen und praktische Anwendung*. 3. unveränd. Bern: Hogrefe AG, 2015. ISBN: 978-3-456-85597-4.

[148] Hermann Sauer. "TrutzBox Kompendium Version 6.3". In: *Comidio GmbH* (Aug. 2020), S. 213. URL: https://trutzbox.de/trutzbox/#support (besucht am 28. 09. 2020).

[149] Florian Schaub et al. "Watching Them Watching Me: Browser Extensions Impact on User Privacy Awareness and Concern". In: *Proceedings 2016 Workshop on Usable Security*. San Diego, CA: Internet Society, 2016. ISBN: 978-1-891562-42-6. DOI: 10.14722/usec.2016.23017.

[150] Mattias Schlenker. *Privacy-Boxen im Test: Trutzbox, Eblocker und Co. - PC Magazin*. Mai 2017. URL: https://www.pc-magazin.de/testbericht/privacy-boxen-test-trutzbox-eblocker-pihole-upribox-3197771.html (besucht am 22. 06. 2020).

[151] Sofia Schöbel et al. "Understanding User Preferences of Digital Privacy Nudges – A Best-Worst Scaling Approach". Maui, Hawaii, USA., Jan. 2020, S. 3918–3927. DOI: 10/1/JML_769.pdf.

[152] Sabrina Schomberg et al. "Ansatz zur Umsetzung von Datenschutz nach der DSGVO im Arbeitsumfeld: Datenschutz durch Nudging". In: *Datenschutz und Datensicherheit - DuD* 43.12 (Dez. 2019), S. 774–780. ISSN: 1862-2607. DOI: 10.1007/s11623-019-1204-5.

[153] Andrew Sears. "Heuristic Walkthroughs: Finding the Problems Without the Noise". In: *International Journal of Human-Computer Interaction* (Nov. 2009). DOI: 10.1207/s15327590ijhc0903_2.

[154] Awanthika Senarath und Nalin A. G. Arachchilage. "Why developers cannot embed privacy into software systems?: An empirical investigation". In: *Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018 - EASE'18*. Christchurch, New Zealand: ACM Press, 2018, S. 211–216. ISBN: 978-1-4503-6403-4. DOI: 10.1145/3210459.3210484.

[155] T Serif und G Ghinea. "HMD vs. PDA: A Comparative Study of the User Out-of-Box Experience" (Sep. 2009), S. 27.

[156] Steve Sheng, Levi Broderick und Colleen Alison Koranda. "Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software" (2006), S. 2.

[157] Sören Siebert. *Weitreichendes Urteil: EuGH erklärt Privacy-Shield-Abkommen für ungültig*. Juli 2020. URL: https://www.e-recht24.de/artikel/datenschutz/12236-eugh-erklaert-privacy-shield-fuer-ungueltig.html (besucht am 10. 09. 2020).

[158] SonicWall. *Content Filtering Service und Content Filtering Client*. Techn. Ber. 2018. URL: https://www.sonicwall.com/de-de/products/firewalls/security-services/content-filtering-client/ (besucht am 02. 10. 2020).

[159] Ole Reißmann SPIEGEL DER. *Anonabox-Kickstarter gestoppt: Geld zurück statt Tor-Router - DER SPIEGEL - Netzwelt*. Okt. 2014. URL: https://www.spiegel.de/netzwelt/web/anonabox-kickstarter-gestoppt-geld-zurueck-statt-tor-router-a-997934.html (besucht am 07. 10. 2020).

[160] Milan Stanojevic. *The 14 best firewall devices to protect your home network*. Juli 2019. URL: https://web.archive.org/web/20190720210401/https://windowsreport.com/firewall-device-for-home/ (besucht am 22. 06. 2020).

[161] Statista. *Einsatz von Maßnahmen zum Schutz vor Datenmissbrauch im Internet 2017*. 2017. URL: https://de.statista.com/statistik/daten/studie/28771/umfrage/haltung-zu-sicherheitsrisiken-im-internet/ (besucht am 10. 11. 2020).

[162] Statista. *Social networks: value per active user 2014*. 2014. URL: https://www.statista.com/statistics/289505/social-networks-value-per-active-user/ (besucht am 10. 07. 2020).

[163] Christian Stöcker und Konrad Lischka. *XKeyscore: Wie die NSA-Überwachung funktioniert - DER SPIEGEL - Netzwelt*. Juli 2013. URL: https://www.spiegel.de/netzwelt/netzpolitik/xkeyscore-wie-die-nsa-ueberwachung-funktioniert-a-914187.html (besucht am 22. 07. 2020).

[164] Tarnomat. *Wechselangebot für Relaxbox-Kunden*. 2020. URL: https://www.tarnomat.com/relaxbox/ (besucht am 07. 10. 2020).

[165] Isabell Thiele. *Was sind meine Daten eigentlich wert?* Feb. 2018. URL: https://blog.to.com/was-sind-meine-daten-eigentlich-wert/ (besucht am 11. 08. 2020).

[166] Laura F. Thies et al. "Anforderungs- und Entwurfsmuster als Instrumente des Privacy by Design". *Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung*. Hrsg. von Alexander Roßnagel, Michael Friedewald und Marit Hansen. DuD-Fachbeiträge. Wiesbaden: Springer Fachmedien, 2018, S. 175–191. ISBN: 978-3-658-23727-1. DOI: 10.1007/978-3-658-23727-1_10.

[167] Bruce Tognazzini. *First Principles of Interaction Design (Revised & Expanded)*. März 2014. URL: https://asktog.com/atc/principles-of-interaction-design/ (besucht am 07. 11. 2020).

[168] Ioanna Topa und Maria Karyda. "Usability Characteristics of Security and Privacy Tools: The User's Perspective". In: *ICT Systems Security and Privacy Protection*. Hrsg. von Lech Jan Janczewski und Mirosław Kutyłowski. IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing, 2018, S. 231–244. ISBN: 978-3-319-99828-2. DOI: 10.1007/978-3-319-99828-2_17.

[169] Sabine Trepte et al. "Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS)". *Reforming European Data Protection Law*. Hrsg. von Serge Gutwirth, Ronald Leenes und Paul de Hert. Law, Governance and Technology Series. Dordrecht: Springer Netherlands, 2015, S. 333–365. ISBN: 978-94-017-9385-8. DOI: 10.1007/978-94-017-9385-8_14.

[170] Michael Trusov, Liye Ma und Zainab Jamal. "Crumbs of the Cookie: User Profiling in Customer-Base Analysis and Behavioral Targeting". In: *Marketing Science* 35.3 (Apr. 2016), S. 405–426. ISSN: 0732-2399. DOI: 10.1287/mksc.2015.0956.

[171] W3C. *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*. Apr. 2002. URL: https://www.w3.org/TR/P3P/ (besucht am 07. 09. 2020).

[172] Stephanie Weinhardt und Doreen St Pierre. "Lessons learned – Conducting a User Experience evaluation of a Trust Policy Authoring Tool". In: *Proceedings 2019 Open Identity Summit*. Bonn, DE: Gesellschaft für Informatik, 2019, S. 6. ISBN: 978-3-88579-687-9.

[173] Wertgarantie. *Privacy Boxen – Zusatzschutz für Zuhause?* 2020. URL: https://www.wertgarantie.de/ratgeber/datensicherheit/privacy-boxen-zusatzschutz-fuer-zuhause (besucht am 21. 09. 2020).

[174] Alma Whitten und J. D. Tygar. "Why Johnny can't encrypt: a usability evaluation of PGP 5.0". In: *Proceedings of the 8th conference on USENIX Security Symposium - Volume 8*. SSYM'99. USA: USENIX Association, Aug. 1999, S. 14.

[175] Winston. *Privacy Filter | Online privacy protection for your entire home.* 2020. URL: https://winstonprivacy.com/pages/technology (besucht am 06. 10. 2020).

[176] Quanzeng You, Sumit Bhatia und Jiebo Luo. "A picture tells a thousand words-About you! User interest profiling from user generated visual content". In: *Signal Processing* 124.C (Juli 2016), S. 45–53. ISSN: 0165-1684. DOI: 10.1016/j.sigpro.2015.10.032.

[177] Zhonghao Yu et al. "Tracking the Trackers". In: *Proceedings of the 25th International Conference on World Wide Web - WWW '16*. Montréal, Québec, Canada: ACM Press, 2016, S. 121–132. ISBN: 978-1-4503-4143-1. DOI: 10.1145/2872427.2883028.

[178] Eric Zeng, Shrirang Mare und Franziska Roesner. "End user security & privacy concerns with smart homes". In: *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*. SOUPS '17. Santa Clara, CA, USA: USENIX Association, Juli 2017, S. 65–80. ISBN: 978-1-931971-39-3.

[179] Serena Zheng et al. "User Perceptions of Smart Home IoT Privacy". In: *Proceedings of the ACM on Human-Computer Interaction* 2.CSCW (Nov. 2018), S. 1–20. ISSN: 2573-0142, 2573-0142. DOI: 10.1145/3274469.

[180] Jan Henrik Ziegeldorf, Oscar Garcia Morchon und Klaus Wehrle. "Privacy in the Internet of Things: threats and challenges: Privacy in the Internet of Things: threats and challenges". In: *Security and Communication Networks* 7.12 (Dez. 2014), S. 2728–2742. ISSN: 19390114. DOI: 10.1002/sec.795.

[181] Mary Ellen Zurko und Richard T. Simon. "User-centered security". In: *Proceedings of the 1996 workshop on New security paradigms*. NSPW '96. Lake Arrowhead, California, USA: Association for Computing Machinery, Sep. 1996, S. 27–33. ISBN: 978-0-89791-944-9. DOI: 10.1145/304851.304859.

Anhang

A Methodik (Szenarien)

A.1 Kategorisierung und Gewichtung häufiger Internetaktivitäten

Häufigkeit	*Internetaktivität*	*Gewicht*
Bereich	**Surfen im Internet** (Anonymität)	**7,7**
97%	Suchmaschinen nutzen	
96%	Online-Shopping	
86%	Nutzung von Apps	
84%	Online News lesen	
82%	Online-Banking	
77%	Musikvideos, Videos, Videopodcasts schauen	
76%	Bewertungen von Produkten lesen	
73%	Nutzung von Social Netzworks	
64%	Herunterladen von Musik, Apps, Spielen	
62%	Filme, Fernsehsendungen über Mediatheken schauen	
57%	Nutzung von Smart-TV	
54%	Filme, Fernsehserien über Streaming Dienste schauen	
48%	Musik über Webradio oder Live-Streams hören	
48%	Live-Streams schauen	
42%	Musik über Musikstreaming-Portale hören	
35%	Nutzung von E-Books/E-Readern	
25%	Bezahlen mit der App/dem Handy	
22%	Online-Dating	
21%	Nutzung einer Smartwatch/eines Fitnessarmbandes	
Bereich	**Kommunikation** (Vertraulichkeit)	**1,7**
98%	E-Mails senden und empfangen	
82%	Instant Messaging	
68%	Telefonieren über das Internet	
Bereich	**Cloud-Dienste** (Autonomie)	**0,3**
48%	Nutzung von Cloud-Diensten	
Bereich	**Sonstiges**	**0,4**
55%	News auf öffentlichen Screens lesen	

Die Zahlen entsprechen den Prozent befragter Personen, welche diese Tätigkeit ausüben

Formeln:

- Gewicht Max = 10
- Gewicht eines Bereichs = $\frac{\text{Summe von Häufigkeiten eines Bereichs}}{\text{Summe von allen Häufigkeiten}}$ * Gewicht Max

Daten aus:

- BVDW: „Digitale Nutzung in Deutschland 2018“ [26, S. 20-21]

A.2 Kategorisierung und Gewichtung häufiger Schutzmaßnahmen

Häufigkeit	*Schutzmaßnahme*	*Gewicht*
Bereich	**Schutz vor Tracking/Tracing** (Anonymität)	**3,4**
47%	Regelmäßiges Löschen von Cookies und Browserverlauf	
38%	Schutz vor Schnüffelsoftware (Anti-Spyware)	
36%	Popup-Blocker/Werbeblocker	
35%	Abschalten von Cookies im Internetbrowser	
33%	Achten auf Gütesiegel beim Online-Einkauf	
17%	Angabe von Fake-Benutzernamen bei sozialen Netzwerken	
9%	Software zum anonymen Surfen	
4%	Verwendung besonderer Suchmaschinen wie ixquick	
Bereich	**Schutz der Kommunikation** (Vertraulichkeit)	**2,3**
66%	E-Mails von unbekannten Absendern nicht öffnen/sofort lösch.	
49%	Spam-Filter	
23%	Separate Email für Spiele/Gewinnspiele	
9%	Verschlüsselungsprogramme für E-Mails	
Bereich	**IT-Sicherheitsmanagement** (IT-Schutz)	**3,7**
62%	Virenschutzprogramme/Virenscanner	
59%	Firewall	
43%	Nutzung komplizierter Passwörter	
43%	Passwörter, PINs oder TAN-Listen nicht auf Festplatte speich.	
36%	Regelmäßiges Ändern von Passwörtern	
Bereich	**Sonstiges**	**0,6**
31%	Keine Nutzung fremder PCs (z.B. Internetcafé)	
7%	Bewusst wenig Nutzung des Internets	
4%	Nichts davon	

Die Zahlen entsprechen den Prozent befragter Personen, welche diese Tätigkeit ausüben

Formeln:

- Gewicht Max = 10
- Gewicht eines Bereichs = $\frac{\text{Summe von Häufigkeiten eines Bereichs}}{\text{Summe von allen Häufigkeiten}}$ * Gewicht Max

Daten aus:

- Statista: „Einsatz von Maßnahmen zum Schutz vor Datenmissbrauch im Internet 2017“ [161]

A.3 Verhältnis von Internetaktivitäten zu Schutzmaßnahmen

Gewicht (absolut)	**Aktivität/Schutzmaßnahme**
7,7	Surfen im Internet
3,3	Schutz vor Tracking/Tracing
1,7	Web-Kommunikation
2,3	Schutz der Kommunikation

Aufteilung (relativ)	**Aktivität/Aktivität mit Schutzmaßnahme**
(10 − 3,3 =) 6,7	Surfen im Internet
3,3	Surfen im Internet mit Schutz vor Tracking/Tracing
(10 − 2,3 =) 7,7	Web-Kommunikation
2,3	Web-Kommunikation mit Schutz der Kommunikation

Verhältnis (absolut)	**Aktivität ohne/Aktivität mit Schutzmaßnahme**
(7,7 * 6,7 / 10 =) 5,2	Surfen im Internet ohne Schutz vor Tracking/Tracing
(7,7 * 3,3 / 10 =) 2,5	Surfen im Internet mit Schutz vor Tracking/Tracing
(1,7 * 7,7 / 10 =) 1,3	Web-Kommunikation ohne Schutz der Kommunikation
(1,7 * 2,3 / 10 =) 0,4	Web-Kommunikation mit Schutz der Kommunikation

Formeln:

- Gewicht Max = 10
- Aufteilung (Aktivität) = Gewicht Max − Gewicht Maßnahme
- Verhältnis (Aktivität) = $\frac{\text{Gewicht Aktivität * Aufteilung Aktivität}}{\text{Gewicht Max}}$
- Verhältnis (Maßnahme) = $\frac{\text{Gewicht Aktivität * Aufteilung Maßnahme}}{\text{Gewicht Max}}$

Daten aus:

- Anhang A.1: Gewichte Aktivitäten
- Anhang A.2: Gewichte Schutzmaßnahmen

A.4 Berechnung der Vergleichbarkeit von Privacy-Boxen

Nutzertyp	**Bemühter Amateur**						**Techniker**						Gewichtungsfaktor	Anwendungsbereich
Funktion	BOX/SENSE	BOX/RAT	BOX/Keezel	SENSE/RAT	SENSE/Keezel	RAT/Keezel	Trutz/eBlock	Trutz/Syncl	Trutz/FreeBox	eBlock/Syncl	eBlock/FreeBox	Syncl/FreeBox		
Anti-Virus	**4**	–	–	–	–	–	–	–	–	–	–	–	4	IT-Sicherheit
Firewall	**4**	4	4	4	4	4	–	–	–	–	–	–		
IoT-Monitor	**4**	–	–	–	–	–	–	–	–	–	–	–		
Passwort-Manager	–	–	–	–	–	–	–	–	–	–	–	–		
Open Source Code	–	–	–	–	–	–	4	4	4	4	4	4		
Inhaltsfilter	**8**	8	–	8	–	–	**8**	–	–	–	–	–	8	Surfen im Internet
Ad-Blocker	–	–	–	–	–	8	**8**	8	8	8	8	8		
Anti-Tracking	–	–	–	8	–	–	**8**	8	–	8	–	–		
DNS-Schutz	–	–	–	–	–	–	**8**	8	8	8	8	8		
VPN-Tunnel	**8**	–	8	–	8	–	**8**	8	8	8	8	8		
Mesh/TOR	–	–	–	–	–	–	–	–	–	–	8	–		
Sichere Email	–	–	–	–	–	–	–	–	–	–	–	–	2	Kommunikation
Sichere Chats	–	–	–	–	–	–	–	2	2	–	–	2		
Web-Meetings	–	–	–	–	–	–	–	2	2	–	–	2		
Private Telefonie	–	–	–	–	–	–	–	2	2	–	–	2		
Soziales Netzwerk	–	–	–	–	–	–	–	–	–	–	–	–		
Notizen	–	–	–	–	–	–	–	–	–	–	–	–	0	Cloud-Dienste nutzen
Kalender	–	–	–	–	–	–	–	–	–	–	–	–		
Adressbuch	–	–	–	–	–	–	–	–	–	–	–	–		
Cloudspeicher	–	–	–	–	–	–	–	–	–	–	–	0		
Web-Hosting	–	–	–	–	–	–	–	–	–	–	–	0		
Email-Server	–	–	–	–	–	–	–	0	0	–	–	0		
Git-Server	–	–	–	–	–	–	–	–	–	–	–	–		
Mobiler Schutz	–	–	–	–	–	–	0	0	–	0	–	–		
Web Dashboard	–	–	–	–	–	–	6	6	6	6	6	6	6	Interfaces
Smartphone App	6	6	6	6	6	6	–	–	–	6	–	–		
Router-Funktion	6	–	–	–	–	–	6	6	–	6	–	–		
WLAN-Netzwerk	6	–	6	–	6	–	–	–	6	–	–	–		
Ber. IT-Sicherheit	**12**	4	4	4	4	4	4	4	4	4	4	4	0,1	Skalierungsfaktor
Ber. Surfen im Int.	16	8	8	16	8	8	**40**	32	24	32	32	24		
Ber. Kommunikat.	–	–	–	–	–	–	–	6	6	–	–	6		
Ber. Cloud-Dienste	–	–	–	–	–	–	0	0	0	0	–	0		
Ber. Interfaces	18	6	12	6	12	6	12	12	12	18	6	6		
Bereiche Gesamt	**46**	18	24	26	24	18	**56**	54	46	54	42	40		
Ergebnis (0–10)	**5**	2	2	3	2	2	**6**	5	5	5	4	4		

Formeln:

- Funktion für Vergleich (siehe Tabelle 4):

```
WENN ( (Funktion Gerät A UND Funktion Gerät B)
    GLEICH (Checkmark ODER (Checkmark)) )
DANN (1) SONST (-)
```

- Summe Bereich:

$$\texttt{Max} = \texttt{Oberste Funktion Bereich X}$$

$$\texttt{Min} = \texttt{Unterste Funktion Bereich X}$$

$$\texttt{Wert} = \texttt{Vergleich}(\texttt{Gerät A}/\texttt{Gerät B})$$

$$\texttt{Summe Bereich X} = \sum_{\texttt{Min}}^{\texttt{Max}} (\texttt{Wert} * \texttt{Gewichtungsfaktor})$$

- Summe Gesamt:

$$\texttt{Max} = \texttt{Oberste Summe Bereich X}$$

$$\texttt{Min} = \texttt{Unterste Summe Bereich X}$$

$$\texttt{Summe Gesamt} = \sum_{\texttt{Min}}^{\texttt{Max}} (\texttt{Summe Bereich X})$$

- Berechnung Ergebnis:

$$\texttt{Ergebnis} = \lfloor \texttt{Summe Gesamt} * \texttt{Skalierungsfaktor} \rceil$$

Bedeutungen:

- Funktion (N): Die Funktion wird von beiden Geräten unterstützt und ist vergleichbar
- Funktion (–): Die Funktion wird von mindestens einem Gerät nicht unterstützt
- Gewichtung (0): Keine Anzahl häufiger Aktivitäten in diesem Bereich
- Gewichtung (10): Sehr hohe Anzahl häufiger Aktivitäten in diesem Bereich
- Ergebnis (0): Keine vergleichbaren Funktionen mit hoher Relevanz
- Ergebnis (10): Totale Übereinstimmung vergleichbarer Funktionen hoher Relevanz
- Skalierung (0,1): Der Faktor skaliert das Ergebnis-Maximum auf den Wert 10

Markierungen:

- Ausgewählte Funktionen für die Evaluation im oberen Bereich sind **fett** markiert
- Eindeutige Maxima von Anwendungsbereichen im unteren Bereich sind **fett** markiert

Daten aus:

- Tabelle 4: Funktionen der Geräte
- Abbildung 22: Gewichtungsfaktoren

A.5 Berechnung des Vergleichs analytischer Evaluationsmethoden

Autoren/**Methoden**	*Praktische Relevanz*	Aufwand	Expertenwissen	Effizienz	Detailgrad	Flexibilität	Individualität	*Wissensch. Relevanz*	Validität	Objektivität	Reliabilität	**Ergebnis**
Christian Moser		–	–	–	–	–	–		–	–	–	
KUM-Handbuch		1	2	3	–	–	–		2	–	–	
Philipp Jordan		–	–	–	–	–	–		–	–	–	
Sarodnick & Brau		2,5	3	1	1	2	–		2	2	3	
Guideline-Review	*1,7*	1,8	2,5	2,0	1,0	2,0	(1,0)	*2,3*	2,0	2,0	3,0	**1,9**
Christian Moser		2	2	1	–	–	–		2	3	3	
KUM-Handbuch		2	2	2	–	–	–		2	–	–	
Philipp Jordan		3	1	1	3	1	1		1	2	3	
Sarodnick & Brau		2	3	1	3	1	–		2	2	3	
GOMS	*1,8*	2,3	2,0	1,3	3,0	1,0	1,0	*2,4*	1,8	2,3	3,0	**2,0**
Christian Moser		–	–	–	–	–	–		–	–	–	
KUM-Handbuch		2	2	3	–	–	–		3	–	–	
Philipp Jordan		2	2	2	2	3	2		2	1	2	
Sarodnick & Brau		2	2	2	2	3	–		2	1	2	
Cogn. Walkthr.	*2,2*	2,0	2,0	2,3	2,0	3,0	2,0	*1,8*	2,3	1,0	2,0	**2,1**
Christian Moser		3	3	3	–	–	–		2	1	3	
KUM-Handbuch		2	3	3	–	–	–		3	–	–	
Philipp Jordan		2,5	2	3	3	3	2		2	2	1	
Sarodnick & Brau		2,5	2	3	3	3	–		2	2	1	
Heur. Evaluation	*2,7*	2,5	2,5	3,0	3,0	3,0	2,0	*1,9*	2,3	1,7	1,7	**2,4**

Bewertungen:

- 1,0 für Bewertungen mit ● / ∗ / •
- 2,0 für Bewertungen mit ● / ∗ ∗ / • •
- 3,0 für Bewertungen mit ● / ∗ ∗ ∗ / • • •

Formeln:

- Berechnung Aufwand (Invertierung und Mittelwert):

$$\texttt{Z} = \texttt{Zeitlicher Aufwand}$$

$$\texttt{M} = \texttt{Materieller Aufwand}$$

$$\texttt{Aufwand} = 3,0 - (\tfrac{\texttt{Z}+\texttt{M}}{2}) + 1,0$$

- Berechnung Kategorie:

  $$\texttt{A}_1 = \texttt{Oberster Autor Kategorie X}$$

  $$\texttt{A}_\texttt{n} = \texttt{Unterster Autor Kategorie X}$$

  $$\texttt{Mittelwert Kategorie X} = \frac{\texttt{A}_1+\texttt{A}_2+...+\texttt{A}_\texttt{n}}{\texttt{n}}$$

- Berechnung Relevanz (praktisch/wissenschaftlich):

  $$\texttt{K}_1 = \texttt{Erste Kategorie Bereich X}$$

  $$\texttt{K}_\texttt{n} = \texttt{Letzte Kategorie Bereich X}$$

  $$\texttt{Mittelwert Bereich X} = \frac{\texttt{K}_1+\texttt{K}_2+...+\texttt{K}_\texttt{n}}{\texttt{n}}$$

- Berechnung Ergebnis:

  $$\texttt{K}_1 = \texttt{Erste Kategorie Gesamt}$$

  $$\texttt{K}_\texttt{n} = \texttt{Letzte Kategorie Gesamt}$$

  $$\texttt{Mittelwert Ergebnis} = \frac{\texttt{K}_1+\texttt{K}_2+...+\texttt{K}_\texttt{n}}{\texttt{n}}$$

Bedeutungen:

- Wert (1-3): Normierte Bewertung des Autors nach Bewertungs-Schema
- Wert (–): Keine Bewertung für diese Kategorie vom Autor verfügbar
- Bewertungen (1): Entspricht einer schlechten/geringen Ausprägung der Kategorie
- Bewertungen (2): Entspricht einer mittleren Ausprägung der Kategorie
- Bewertungen (3): Entspricht einer guten/hohen Ausprägung der Kategorie
- Ergebnis (1): Entspricht einer geringen Relevanz der Methode
- Ergebnis (2): Entspricht einer mittleren Relevanz der Methode
- Ergebnis (3): Entspricht einer hohen Relevanz der Methode

Markierungen:

- Ein Wert (in Klammern) wurde bei *Individualität* auf „niedrig“ geschätzt

Daten aus:

- Moser: „User Experience Design“ (Kapitel 10) [130, S. 225]
- KUM: „Methodenhandbuch zur nutzerzentrierten Entwicklung“ [108, S. 5-6]
- Jordan: „Auswahl einer geeigneten Methode zur Usability Evaluation“ [100, S. 76-77]
- Sarodnick & Brau: „Methoden der Usability-Evaluation“ (Kapitel 4) [147, S. 201-202]

B Methodik (Evaluation)

B.1 UX-Leitfaden für Out-of-Box Experience

Die folgenden Heuristiken werden als Leitfaden zur Ermittlung der OOBE verwendet:

H1 Das Öffnen der Verpackung sollte intuitiv sein und das Auspacken muss Informationen und Komponenten auf logische Weise offenbaren.

H2 Dem Nutzer müssen einfache Entscheidungen, durch das Festlegen sinnvoller Standardeinstellungen, ermöglicht werden (ggfs. mit Hinweisen).

H3 Die verständliche Kombinationen von Text und Bildern erzielt die besten Ergebnisse.

H4 Es müssen Sicherheitsvorkehrungen für häufig auftretende Fehler getroffen werden.

H5 Nach dem erfolgreichem Abschluss, muss der Nutzer deutliches Feedback erhalten.

H6 Der Nutzer muss beim Übergang von Installation zu Nutzung unterstützt werden (Erfahrung bei Erstbenutzung).

H7 Dem Nutzer darf bei der Einrichtung nichts in die Quere kommen.

H8 Die Einrichtung darf nicht zu lange dauern.

Übersetzt nach:

- Moya und Burgess: „Out of Box and First Time User Experiences“ [131, S. 43]

B.2 UX-Heuristiken für Out-of-Box Experience

Die folgenden Fragen werden zur Ermittlung der OOBE verwendet:

O1 Verpackung

- O1.1 Sind die Kisten leicht genug, dass ihr Inhalt herumgetragen werden kann?
- O1.2 Lassen sich alle zusammengehörenden Kisten auf einmal transportieren?
- O1.3 Ist es leicht, den Inhalt der Kisten anhand ihrer Verpackung zu identifizieren?
- O1.4 Ist die Verpackung ansprechend gestaltet und weckt Vorfreude auf das Produkt?
- O1.5 Sind die Kisten so konstruiert, dass das Öffnen erleichtert wird? (z.B. Laschen)

O2 Auspacken

- O2.1 Ist es einfach, an den Inhalt der Box und das Handbuch zu gelangen?
- O2.2 Ist es leicht, die innere Organisation der Box zu verstehen?
- O2.3 Ist es einfach, den Inhalt des Kartons zu inventarisieren? (Inventar-Liste)
- O2.4 Ist es leicht, die Funktionalität und die Beziehung zwischen den Komponenten zu verstehen?
- O2.5 Ist es einfach, die Geräte wieder in ihre Originalverpackung zurückzupacken?

O3 Aufbau und Anschluss

- O3.1 Gibt es einen Quickstart-Guide zur schnellen Einrichtung?
- O3.2 Ist das Handbuch leicht verständlich und klar strukturiert?
- O3.3 Werden die Anschluss-Optionen des Geräts eindeutig erklärt?
- O3.4 Ist es leicht, die physikalische Anordnung der Komponenten zu verstehen?
- O3.5 Lassen sich die Komponenten einfach anschließen? (Symbole/Farben)
- O3.6 Sind alle notwendigen Komponenten beigelegt? (Adapter/Kabel)

O3t Zusammenbau und Installation (nur Nutzergruppe „Techniker“)

- O3t.1 Wird der Zusammenbau von Komponenten gut erklärt?
- O3t.2 Ist der Zusammenbau von Komponenten leicht durchzuführen?
- O3t.3 Ist es einfach, die aktuelle Firmware im Internet zu finden?
- O3t.4 Wird standardmäßig, die aktuellste Version zum Download angeboten?
- O3t.5 Werden zusätzlich benötigte Komponenten vorher genannt? (USB-Stick)
- O3t.6 Ist die Installation von neuer Firmware gut dokumentiert?
- O3t.7 Gibt es Feedback über den Abschluss der Installation? (Erfolg/Fehler)

O4 Einschalten

- O4.1 Sind Instruktionen zum Einschalten des Geräts eindeutig formuliert? (Position des Einschaltknopfes)

O4.2 Ist es leicht zu sehen, ob das Gerät funktioniert? (LEDs/Batteriestand)

O4.3 Sind die Zustände des Systemstatus im Handbuch dokumentiert?

O4.4 Ist es leicht zu erkennen, ob das Gerät bereit zur Konfiguration ist? (LEDs/Audiosignale)

O5 Konfiguration

O5.1 Geht aus dem Handbuch hervor, wie sich das Gerät konfigurieren lässt?

O5.2 Ist die Einrichtung mit gängigen Geräten/Betriebssystemen möglich? (*Bemühte Amateure*: iOS/Android, *Techniker*: Windows/macOS/Linux)

O5.3 Lässt sich das User-Interface des Geräts einfach aufrufen? (Link/QR-Code)

O5.4 Macht der Startbildschirm deutlich, ob das Gerät ordnungsgemäß funktioniert?

O5.5 Werden alle nötigen Schritte zur Einrichtung klar formuliert/visualisiert?

O5.6 Werden unterschiedliche Betriebsmodi des Geräts vorgestellt?

O5.7 Wird der erfolgreiche Abschluss der Einrichtung klar angezeigt?

O6 Registrierung

O6.1 Kann ein Nutzer-Account (wenn nötig) schnell eingerichtet werden?

O6.2 Lässt sich die Lizenz für die Cloud-Services einfach finden/aktivieren?

O7 Erstbenutzung

O7.1 Wird die Betriebsbereitschaft des Geräts deutlich angezeigt?

O7.2 Werden die wichtigsten Funktionen zu Beginn einmal vorgestellt? (Tutorial/Erste Schritte)

O7.3 Wird eine Übersicht des aktuellen System/Netzwerk-Status gezeigt?

O7.4 Sind die Funktionsbereiche klar und übersichtlich strukturiert?

O8 Arbeiten

- Untersuchung von typischen Anwendungsszenarien mit Heuristic Walkthrough (siehe Anhang B.4)

O9 Hilfe

O9.1 Gibt es Richtlinien zur Vorgehensweise, falls Fehler auftreten?

O9.2 Sind Informationen in unterschiedlichen Sprachen verfügbar? (Handbuch)

O9.3 Wird umfassendere Hilfe über die Website des Herstellers angeboten? (FAQ)

O9.4 Verfügt der Hersteller über andere Möglichkeiten der Hilfeleistung? (z.B. E-Mail, Telefon)

Quelle:

- Serif und Ghinea: „HMD vs. PDA: A Comparative Study of the User Out-of-Box Experience“ [131, S. 19-21]

B.3 Gedanken-fokussierende Fragen für Heuristic Walkthrough

Die folgenden Fragen werden als Leitfaden zur Ermittlung der Usability verwendet:

G1 Werden die Nutzer wissen, was sie als nächstes tun müssen?

Es ist möglich, dass Nutzer einfach nicht wissen, was sie als Nächstes tun sollen.

G2 Werden die Nutzer bemerken, dass es ein Steuerelement (z.B. Schaltfläche, Menü) gibt, mit dem sie den nächsten Teil ihrer Aufgabe erledigen können?

Es ist möglich, dass die Aktion versteckt ist oder dass die Terminologie nicht mit dem übereinstimmt, was die Benutzer suchen. In beiden Fällen ist das richtige Steuerelement vorhanden, aber die Benutzer können es nicht finden. Das Vorhandensein und die Qualität von Beschriftungen auf Steuerelementen und die Anzahl der Steuerelemente auf dem Bildschirm beeinflussen die Fähigkeit des Benutzers, ein geeignetes Steuerelement zu finden.

G3 Wenn die Nutzer das Steuerelement gefunden haben, werden sie dann wissen, wie es zu benutzen ist (z.B. Anklicken, Doppelklick, Pulldown-Menü)?

Wenn es sich bei dem Steuerelement beispielsweise um ein Pulldown-Menü handelt, es aber wie eine normale Schaltfläche aussieht, verstehen die Nutzer möglicherweise nicht, wie es zu verwenden ist. Nutzer finden vielleicht das Symbol, das der gewünschten Aktion entspricht, aber wenn es ein Dreifach-Klick erfordert, werden sie vielleicht nie herausfinden, wie man es benutzt.

G4 Wenn die Nutzer die richtige Aktion ausführen, werden sie dann sehen, dass Fortschritte bei der Erledigung der Aufgabe gemacht werden?

Bietet das System eine angemessene Rückmeldung? Wenn nicht, sind die Nutzer möglicherweise nicht sicher, dass die gerade durchgeführte Aktion korrekt war.

Übersetzt nach:

- Sears: „Heuristic Walkthroughs: Finding the Problems Without the Noise“ [153, S. 220-221]

B.4 Usability-Heuristiken für Heuristic Walkthrough

Die folgenden Fragen werden zur Ermittlung der Usability mittels HW verwendet:

U1 Sichtbarkeit und Systemstatus

- U1.1 Enthält die Anwendung eine sichtbare Seite oder einen Bereich für den Titel?
- U1.2 Weiß der Nutzer immer, wo er sich befindet?
- U1.3 Weiß der Nutzer immer, was das System oder die Anwendung gerade macht?
- U1.4 Sind die Links klar definiert?
- U1.5 Können alle Funktionen direkt dargestellt werden? (Ohne dass weiteren Aktionen erforderlich sind)

U2 Verbindung zwischen System und realer Welt, Metaphorik und menschliche Objekte

- U2.1 Erscheinen Informationen für den Nutzer in einer logischen Reihenfolge?
- U2.2 Entspricht die Gestaltung von Symbolen Gegenständen aus dem Alltag?
- U2.3 Führt jedes Symbol die Aktion aus, die vom Nutzer erwartet wird?
- U2.4 Verwendet das System Ausdrücke und Konzepte, die dem Nutzer vertraut sind?

U3 Kontrolle und Freiheit des Nutzers

- U3.1 Gibt es einen Link, um zum Ausgangszustand / zur Startseite zurückzukehren?
- U3.2 Sind die Funktionen „Rückgängig“ und „Wiederherstellen“ implementiert?
- U3.3 Ist es einfach, zu einem früheren Zustand der Anwendung zurückzukehren?

U4 Konsistenz und Standards

- U4.1 Haben Links die gleichen Bezeichnungen wie ihre Ziele?
- U4.2 Führen die gleichen Aktionen immer zu gleichen Ergebnissen?
- U4.3 Haben die Symbole überall die gleiche Bedeutung?
- U4.4 Werden Informationen auf jeder Seite einheitlich dargestellt?
- U4.5 Sind die Farben der Links einheitlich? Wenn nicht, sind sie für ihre Verwendung geeignet?
- U4.6 Folgen die Navigationselemente den Standards? (Schaltflächen, Kontrollkästchen, ...)

U5 Erkennen statt Erinnern, Lernen und Vorhersehen

- U5.1 Ist es einfach, das System zum ersten Mal zu benutzen?
- U5.2 Ist es einfach, Informationen zu finden, nach denen bereits vorher gesucht wurde?
- U5.3 Kann das System jederzeit benutzt werden, ohne sich an frühere Bildschirme zu erinnern?

U5.4 Sind alle Inhalte, die für die Navigation oder Aufgabe benötigt werden, auf dem „aktuellen Bildschirm“ zu finden?

U5.5 Sind die Informationen nach einer dem Nutzer vertrauten Logik organisiert?

U6 Flexibilität und Effizienz der Nutzung

U6.1 Gibt es Tastaturkürzel für häufige Aktionen?

U6.2 Wenn ja, ist es offensichtlich, wie sie zu verwenden sind?

U6.3 Ist es möglich, eine früher durchgeführte Aktion einfach auszuführen?

U6.4 Passt sich das Design den Änderungen der Bildschirmauflösung an?

U6.5 Ist die Verwendung von Beschleunigungsmechanismen für den normalen Nutzer sichtbar?

U6.6 Wird der Nutzer vom System konstant gefordert? (ohne unnötige Wartezeiten)

U7 Nutzern helfen, Fehler zu erkennen, zu diagnostizieren und zu beheben

U7.1 Gibt es eine Warnung, bevor unwiderrufliche Maßnahmen ausgeführt werden?

U7.2 Werden Fehler in Echtzeit angezeigt?

U7.3 Ist die erscheinende Fehlermeldung leicht zu verstehen?

U7.4 Wird ein bestimmter Code verwendet, um den Fehler zu referenzieren?

U8 Fehler vermeiden

U8.1 Wird eine fehlerhafte Eingabe erkannt und die folgende Aktion verweigert?

U8.2 Ist es deutlich, welche Informationen in Formularfelder einzutragen sind?

U8.3 Toleriert die Suche Tipp- und Rechtschreibfehler?

U9 Ästhetische und minimalistische Gestaltung

U9.1 Wird ein Design ohne Informationsredundanz verwendet?

U9.2 Sind die Informationen kurz, prägnant und genau?

U9.3 Unterscheidet sich jede Information von den anderen und ist nicht verwirrend?

U9.4 Ist der Text gut organisiert, mit kurzen Sätzen und schnell zu verstehen?

U10 Hilfe und Dokumentation

U10.1 Gibt es die Option „Hilfe“?

U10.2 Wenn ja, ist sie sichtbar und leicht zugänglich?

U10.3 Ist der Hilfeabschnitt auf die Lösung von Problemen ausgerichtet?

U10.4 Gibt es einen Abschnitt mit häufig gestellten Fragen (FAQ)?

U10.5 Ist die Hilfedokumentation übersichtlich und mit Beispielen versehen?

U11 Speichern des Zustands und Sichern der Arbeit

U11.1 Können Nutzer von einem früheren Zustand aus fortfahren (wo sie zuvor waren, oder von einem anderen Gerät aus)?

U11.2 Ist „Automatische Speicherung“ implementiert?

U11.3 Reagiert das System gut auf externe Störungen? (Stromausfall, Internet funktioniert nicht, ...)

U12 Farbe und Lesbarkeit

U12.1 Haben die Schriften eine angemessene Größe?

U12.2 Verwenden die Schriften Farben mit ausreichendem Kontrast zum Hintergrund?

U12.3 Erlauben Hintergrundbilder oder -muster das Lesen des Inhalts?

U12.4 Werden Menschen mit eingeschränkter Sehkraft berücksichtigt?

U13 Autonomie

U13.1 Wird der Benutzer über den Systemstatus informiert?

U13.2 Ist der Systemstatus zudem sichtbar und wird aktualisiert?

U13.3 Kann der Benutzer seine eigenen Einstellungen vornehmen? (Personalisierung)

U14 Standardeinstellungen

U14.1 Bietet das System oder Gerät die Möglichkeit, die Werkseinstellungen wiederherzustellen?

U14.2 Wenn ja, werden die Konsequenzen der Aktion deutlich vermittelt?

U14.3 Wird der Begriff „Standard“ verwendet?

U15 Reduzieren der Wartezeit

U15.1 Ist die Ausführung intensiver Aufgaben für den Nutzer erkennbar?

U15.2 Wird während der Ausführung intensiver Aufgaben die verbleibende Zeit oder eine Animation angezeigt?

Übersetzt und optimiert nach:

- Granollers: „Usability Evaluation with Heuristics, Beyond Nielsen’s List“ [76, S. 62]

B.5 Usable Privacy-Heuristiken nach DSGVO

UPC.1 Wie hoch ist der Grad der Kontrolle, den die betroffenen Personen über ihre Daten haben?

UPC.2 Sind alle an die Öffentlichkeit oder an die betroffenen Personen gerichteten Informationen und Mitteilungen im Zusammenhang mit der Verarbeitung personenbezogener Daten prägnant, leicht zugänglich und leicht zu verstehen?

UPC.3 Werden die Informationen über die beabsichtigte Verarbeitung auf leicht sichtbare, verständliche und klar lesbare Weise bereitgestellt?

UPC.4 Bezieht sich jede Information und Kommunikation, die an die Öffentlichkeit oder an die betroffenen Personen gerichtet ist, auf die Verarbeitung personenbezogener Daten, wobei eine klare und deutliche Sprache verwendet wird?

UPC.5 Werden die Informationen und die Kommunikation welche an die Öffentlichkeit oder an die betroffenen Personen gerichtet sind, bei Bedarf visualisiert?

UPC.6 Wird den betroffenen Personen ein aussagekräftiger Überblick über die beabsichtigte Verarbeitung gegeben?

UPC.7 Haben die betroffenen Personen vom Datenverantwortlichen aussagekräftige Informationen erhalten über «die involvierte Logik sowie die Bedeutung und die voraussichtlichen Folgen der automatisierten Entscheidungsfindung, einschließlich der Erstellung von Profilen, gegen die sie Einwände haben können»?

UPC.8 Wird die Einwilligung durch eine klare Zustimmungserklärung erteilt, die einen frei gegebenen, spezifischen, informierten und eindeutigen Hinweis auf die Zustimmung der betroffenen Personen zur Verarbeitung sie betreffender persönlicher Daten enthält?

UPC.9 Werden die Einwilligungen der betroffenen Personen erteilt, indem sie einem Antrag auf elektronischem Wege folgen? Wenn ja, ist der Antrag klar, prägnant und stört die Nutzung der Dienstleistung, für die er gestellt wird, nicht unnötig?

UPC.10 Sind im Zusammenhang mit einer schriftlichen Erklärung zu einer anderen Angelegenheit Schutzvorkehrungen gewährleistet, so dass die betroffenen Personen sich der Tatsache bewusst sind, ob und in welchem Umfang die Einwilligung erteilt wird?

UPC.11 Wird die vom Datenverantwortlichen vorformulierte Einverständniserklärung in einer verständlichen und leicht zugänglichen Form, in klarer und verständlicher Sprache und ohne mißbräuchliche Klauseln abgegeben?

UPC.12 Wird der Antrag auf Einwilligung in einer Weise gestellt, die sich deutlich von anderen Angelegenheiten unterscheidet?

UPC.13 Haben die betroffenen Personen eine freie und echte Wahl bei der Erteilung ihrer Einwilligung?

UPC.14 Können die betroffenen Personen ihre Einwilligung ohne Schaden verweigern oder zurückziehen?

UPC.15 Ist es so einfach, die Einwilligung zu widerrufen, wie sie zu erteilen?

UPC.16 Werden die Rechte der betroffenen Personen gemäß Artikel 15 bis 22 (d.h. Auskunftsrecht, Recht auf Berichtigung, Recht auf Löschung, Recht auf Einschränkung der Verarbeitung, Recht auf Datenübertragbarkeit, Widerspruchsrecht und Rechte im Zusammenhang mit der automatisierten individuellen Entscheidungsfindung) erleichtert?

UPC.17 Sind sich die betroffenen Personen darüber im Klaren, wie sie ihre Rechte in Bezug auf die Verarbeitung personenbezogener Daten ausüben können?

UPC.18 Haben die betroffenen Personen das Recht auf Zugang zu persönlichen Daten, die über sie gesammelt wurden, und können sie dieses Recht leicht und in angemessenen Abständen ausüben, um sich über die Rechtmäßigkeit der Verarbeitung zu informieren und diese zu überprüfen?

UPC.19 Wird das Widerspruchsrecht den betroffenen Personen spätestens bei der ersten Kommunikation mit den betroffenen Personen ausdrücklich zur Kenntnis gebracht und klar und getrennt von allen anderen Informationen dargestellt?

UPC.20 Sind sich die betroffenen Personen der Risiken, Regeln, Schutzmaßnahmen und Rechte im Zusammenhang mit der Verarbeitung ihrer persönlichen Daten bewusst?

UPC.21 Ist der spezifische Zweck, zu dem persönliche Daten verarbeitet werden, explizit angegeben?

UPC.22 Sind die persönlichen Daten angemessen, relevant und auf das beschränkt, was für die Zwecke, für die sie verarbeitet werden, notwendig ist?

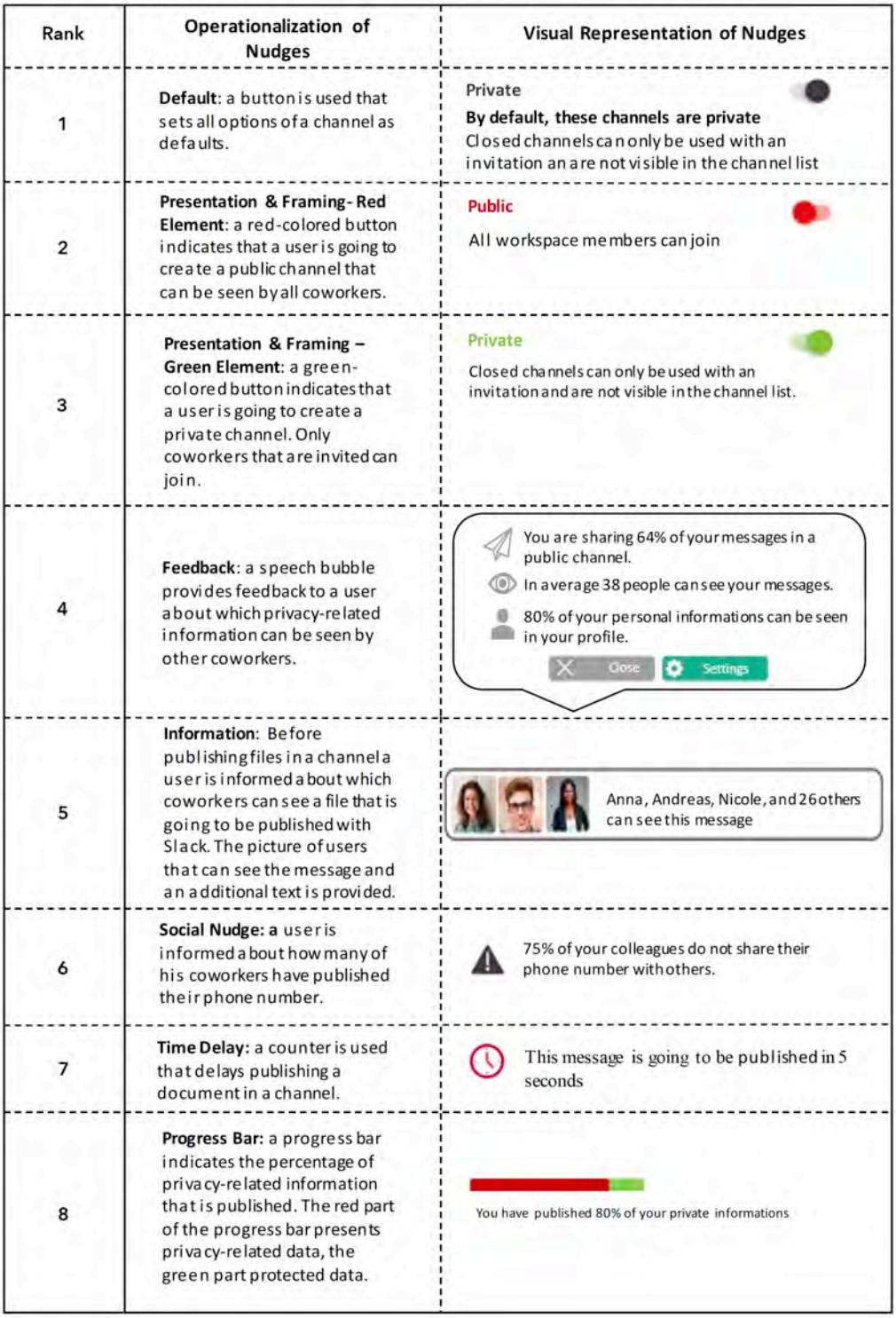
UPC.23 Wird das Vorliegen eines berechtigten Interesses eines Datenverantwortlichen sorgfältig geprüft, wobei die angemessenen Erwartungen der betroffenen Personen aufgrund ihrer Beziehung zu dem Datenverantwortlichen berücksichtigt werden?

UPC.24 Ist geprüft worden, ob die Interessen und Grundrechte der betroffenen Personen das Interesse der Datenverantwortlichen überwiegen könnten, wenn personenbezogene Daten unter Umständen verarbeitet werden, bei denen die betroffenen Personen eine weitere Verarbeitung nicht angemessen erwarten können?

Übersetzt nach:

- Johansen und Fischer-Hübner: „Making GDPR Usable: A Model to Support Usability Evaluations of Privacy“ [98, S. 21-31]

B.6 Privacy-Heuristiken als Digital Privacy Nudges



Modifiziert nach:

- Schöbel et al.: „Understanding User Preferences of Digital Privacy Nudges – A Best-Worst Scaling Approach“ [151, S. 3922]

C Auswertung (Ergebnisse)

C.1 Vollständige Auswertung der OOBE-Untersuchung

Nutzertyp		Bemühter Amateur				Techniker			
Security & Privacy-Box		**BOX**		**SENSE**		**TrutzBox**		**eBlocker**	
Kategorie	Max.	Punk.	Zeit	Punk.	Zeit	Punk.	Zeit	Punk.	Zeit
O1 Verpackung	**5**	**3,0**	01:30	**4,0**	01:00	**1,5**	01:30	**4,5**	01:30
O1.1 Gewicht	1	1,0		1,0		1,0		1,0	
O1.2 Transport	1	–		–		–		1,0	
O1.3 Gestaltung	1	1,0		1,0		0,0		1,0	
O1.4 Vorfreude	1	1,0		1,0		0,0		1,0	
O1.5 Öffnungshilfe	1	0,0		1,0		0,5		0,5	
O2 Auspacken	**5**	**4,5**	04:30	**5,0**	03:00	**4,5**	03:30	**2,0**	03:00
O2.1 Aufwand	1	1,0		1,0		1,0		0,5	
O2.2 Organisation	1	1,0		1,0		1,0		–	
O2.3 Inventar	1	0,5		1,0		1,0		–	
O2.4 Beziehungen	1	1,0		1,0		1,0		1,0	
O2.5 Zurückpacken	1	1,0		1,0		0,5		0,5	
O3 Aufbau	**6**	**5,5**	03:30	**6,0**	03:45	**5,5**	03:00	**4,5**	01:00
O3.1 Quickstart	1	1,0		1,0		1,0		0,5	
O3.2 Handbuch	1	1,0		1,0		1,0		1,0	
O3.3 Optionen	1	1,0		1,0		1,0		1,0	
O3.4 Anordnung	1	1,0		1,0		1,0		1,0	
O3.5 Anschluss	1	0,5		1,0		0,5		1,0	
O3.6 Komponenten	1	1,0		1,0		1,0		–	
O3t Installation	**7**	–	–	–	–	**5,5**	40:30	**5,0**	16:00
O3t.1 Erklärung	1					1,0		0,0	
O3t.2 Zusammenbau	1					0,5		1,0	
O3t.3 Download	1					0,0		1,0	
O3t.4 Version	1							0,5	
O3t.5 Komponenten	1					1,0		1,0	
O3t.6 Installation	1					1,0		0,5	
O3t.7 Abschluss	1					0,5		1,0	
O4 Einschalten	**4**	**4,0**	03:00	**4,0**	02:30	**2,0**	03:00	**2,0**	05:30
O4.1 Anweisung	1	1,0		1,0		1,0		1,0	
O4.2 Feedback	1	1,0		1,0		0,5		1,0	
O4.3 Zustände	1	1,0		1,0		0,5		0,0	
O4.4 Bereitschaft	1	1,0		1,0		0,0		0,0	
O5 Konfiguration	**7**	**6,0**	07:00	**7,0**	14:45	**5,5**	07:00	**6,0**	13:00
O5.1 Handbuch	1	1,0		1,0		1,0		1,0	

O5.2 Geräte	1	1,0		1,0		1,0		1,0	
O5.3 Übergang	1	1,0		1,0		1,0		1,0	
O5.4 Start-Screen	1	0,5		1,0		1,0		1,0	
O5.5 Anleitung	1	1,0		1,0		0,5		1,0	
O5.6 Betriebsmodi	1	0,5		1,0		0,0		0,0	
O5.7 Abschluss	1	1,0		1,0		1,0		1,0	
O6 Registrierung	**2**	**2,0**	06:00	–	–	**2,0**	03:00	**1,0**	–
O6.1 Account	1	1,0		–		1,0		–	
O6.6 Lizenzierung	1	1,0		–		1,0		1,0	
O7 Erstbenutzung	**4**	**3,0**	02:00	**3,0**	01:15	**2,5**	01:30	**3,5**	02:00
O7.1 Bereitschaft	1	1,0		1,0		0,5		1,0	
O7.2 Erste Schritte	1	0,0		0,0		0,0		0,5	
O7.3 System-Status	1	1,0		1,0		1,0		1,0	
O7.4 Übersicht	1	1,0		1,0		1,0		1,0	
O9 Hilfe	**4**	**3,0**	–	**4,0**	–	**2,0**	–	**3,5**	–
O9.1 Richtlinien	1	1,0		1,0		0,0		1,0	
O9.2 Sprachauswahl	1	0,0		1,0		0,0		1,0	
O9.3 FAQ/Webseite	1	1,0		1,0		1,0		1,0	
O9.4 Email/Support	1	1,0		1,0		1,0		0,5	
Erreichte Punkte	37 | 44	31,0		33,0		29,5		32,0	
Bewertbares Max.	37 | 44	36,0		34,0		42,0		40,0	
Ergebnis	100%	**86%**	**27:30**	**97%**	**26:15**	**70%**	**63:00**	**80%**	**42:00**

Bewertungen:

Antwort	Bewertung
Ja	1 Punkt
Weder noch	0,5 Punkte
Nein	0 Punkte
Nicht anwendbar	–

Formeln:

- Kategorie-Punkte = Summe von Punkten einer Kategorie
- Erreichte Punkte = Summe von Punkten aller Kategorien
- Bewertbares Maximum = Anzahl an bewerteten Fragen
- Ergebnis (Prozent) = $\frac{\text{Erreichte Punkte}}{\text{Bewertbares Maximum}}$
- Ergebnis (Zeit) = Summe von Zeiten aller Kategorien

C.2 Vollständige Auswertung der Usability-Untersuchung

Nutzertyp		Bemühter Amateur		Techniker	
Security & Privacy-Box		**BOX**	**SENSE**	**TrutzBox**	**eBlocker**
Kategorie	Max.	Punkte	Punkte	Punkte	Punkte
U1 Systemstatus	**5**	**3,0**	**4,0**	**4,5**	**5,0**
U1.1 Titelbereich	1	1,0	1,0	1,0	1,0
U1.2 Orientierung	1	0,5	1,0	1,0	1,0
U1.3 System-Aktivität	1	1,0	1,0	1,0	1,0
U1.4 Link-Definition	1	0,5	1,0	1,0	1,0
01.5 Darstellbarkeit	1	0,0	0,0	0,0	1,0
U2 Metaphorik	**4**	**4,0**	**4,0**	**4,0**	**4,0**
U2.1 Hierarchie	1	1,0	1,0	1,0	1,0
U2.2 Symbolik	1	1,0	1,0	1,0	1,0
U2.3 Erwartungen	1	1,0	1,0	1,0	1,0
U2.4 Konzepte	1	1,0	1,0	1,0	1,0
U3 Kontrolle	**3**	**1,0**	**1,0**	**2,0**	**2,0**
U3.1 Startseite	1	1,0	1,0	1,0	1,0
U3.2 Steuerung	1	0,0	0,0	0,0	0,0
U3.3 Zustände	1	0,0	0,0	1,0	1,0
U4 Konsistenz	**6**	**5,5**	**5,0**	**5,0**	**6,0**
U4.1 Links und Ziele	1	1,0	1,0	1,0	1,0
U4.2 Wiederholbarkeit	1	0,5	1,0	1,0	1,0
U4.3 Symbolik	1	1,0	1,0	1,0	1,0
U4.4 Einheitlichkeit	1	1,0	0,0	0,5	1,0
U4.5 Link-Farben	1	1,0	1,0	0,5	1,0
U4.6 Standardelemente	1	1,0	1,0	1,0	1,0
U5 Erlernbarkeit	**5**	**2,5**	**3,5**	**3,0**	**4,0**
U5.1 Erstbenutzung	1	0,5	1,0	0,5	1,0
U5.2 Wiederholungen	1	0,0	0,0	0,0	0,0
U5.3 Eigenständigkeit	1	1,0	1,0	0,5	1,0
U5.4 Vollständigkeit	1	0,0	1,0	1,0	1,0
U5.5 Vertrautheit	1	1,0	0,5	1,0	1,0
U6 Flexibilität	**6**	**1,0**	**1,0**	**2,0**	**3,0**
U6.1 Tastaturkürzel	1	–	–	0,0	0,0
U6.2 Intuition	1	–	–	–	–
U6.3 Wiederverwendung	1	0,0	0,0	0,0	0,0
U6.4 Adaptivität	1	–	–	1,0	1,0
U6.5 Beschleuniger	1	0,0	0,0	0,0	1,0
U6.6 Wartezeiten	1	1,0	1,0	1,0	1,0

U7 Warnungen	**4**	**3,0**	**3,0**	**1,0**	**3,5**
U7.1 Auswirkungen	1	1,0	1,0	0,5	1,0
U7.2 Echtzeit	1	0,5	1,0	0,5	1,0
U7.3 Verständlichkeit	1	1,0	1,0	0,0	1,0
U7.4 Fehler-Codes	1	0,5	0,5	0,0	0,5
U8 Toleranz	**3**	**2,0**	**2,0**	**0,5**	**2,0**
U8.1 Fehleingaben	1	1,0	1,0	0,0	1,0
U8.2 Formularfelder	1	1,0	1,0	0,5	1,0
U8.3 Rechtschreibung	1	0,0	–	0,0	0,0
U9 Gestaltung	**4**	**3,5**	**4,0**	**3,0**	**4,0**
U9.1 Redundanz	1	0,5	1,0	1,0	1,0
U9.2 Präzision	1	1,0	1,0	1,0	1,0
U9.3 Verwirrung	1	1,0	1,0	0,5	1,0
U9.4 Textlogik	1	1,0	1,0	0,5	1,0
U10 Hilfe/Doku.	**5**	**2,0**	**4,0**	**2,0**	**4,5**
U10.1 Verfügbarkeit	1	0,0	1,0	0,0	1,0
U10.2 Sichtbarkeit	1	–	1,0	–	1,0
U10.3 Problemlösung	1	0,5	1,0	0,5	0,5
U10.4 FAQ-Bereich	1	0,5	1,0	0,5	1,0
U10.5 Dokumentation	1	1,0	0,0	1,0	1,0
U11 Zustände	**3**	**1,5**	**1,0**	**2,0**	**2,0**
U11.1 Fortsetzen	1	0,5	0,0	1,0	1,0
U11.2 Auto-Speichern	1	0,0	0,0	0,0	0,0
U11.3 Externe Störungen	1	1,0	1,0	1,0	1,0
U12 Lesbarkeit	**4**	**2,5**	**3,0**	**3,0**	**3,0**
U12.1 Schriftgröße	1	0,5	1,0	1,0	1,0
U12.2 Kontraste	1	1,0	1,0	1,0	1,0
U12.3 Hintergründe	1	1,0	1,0	1,0	1,0
U12.4 Unterstützung	1	0,0	0,0	0,0	0,0
U13 Autonomie	**3**	**2,0**	**2,5**	**2,5**	**3,0**
U13.1 Systemstatus	1	1,0	1,0	1,0	1,0
U13.2 Aktualisierung	1	1,0	1,0	1,0	1,0
U13.3 Personalisierung	1	0,0	0,5	0,5	1,0
U14 Standards	**3**	**1,5**	**3,0**	**3,0**	**2,5**
U14.1 Werkseinstellungen	1	1,0	1,0	1,0	1,0
U14.2 Konsequenzen	1	0,0	1,0	1,0	1,0
U14.3 Standard-Begriff	1	0,5	1,0	1,0	0,5
U15 Wartezeit	**2**	**2,0**	**2,0**	**1,5**	**2,0**
U15.1 System-Auslastung	1	1,0	1,0	1,0	1,0

U15.2 Animationen	1	1,0	1,0	0,5	1,0
Erreichte Punkte	60	37,0	43,0	39,0	50,5
Bewertbares Maximum	60	56,0	56,0	58,0	59,0
Ergebnis	100%	**66%**	**77%**	**67%**	**86%**

Bewertungen:

Antwort	Bewertung
Ja	1 Punkt
Weder noch	0,5 Punkte
Nein	0 Punkte
Nicht anwendbar	–

Formeln:

- Kategorie-Punkte = Summe von Punkten einer Kategorie
- Erreichte Punkte = Summe von Punkten aller Kategorien
- Bewertbares Maximum = Anzahl an bewerteten Fragen
- $\text{Ergebnis} = \dfrac{\text{Erreichte Punkte}}{\text{Bewertbares Maximum}}$

C.3 Gewichtung von Privacy-Nudges zur Bewertung

Privacy-Nudge	Rang	„Best“	„Worst“	„Mean“	Gewicht
Standard	1	570	123	0,36	0,9
Farbelement Rot	2	392	204	0,15	0,7
Farbelement Grün	3	326	202	0,10	0,6
Feedback	4	320	343	-0,01	0,5
Information	5	289	351	-0,05	0,4
Soziale Norm	6	156	348	-0,15	0,3
Zeitverzögerung	7	230	436	-0,16	0,3
Fortschrittsanzeige	8	195	471	-0,22	0,3

Formeln:

- Gewicht = $\lfloor 0{,}5 + \text{Mean} \rceil$

Bemerkungen:

- Die Werte für „Best“, „Worst“ und „Mean“ wurden von Schöbel et al. übernommen.

Quelle:

- Schöbel et al.: „Understanding User Preferences of Digital Privacy Nudges – A Best-Worst Scaling Approach“ [151, S. 3924]

C.4 Bei der Untersuchung ermittelte Privacy-Nudges

Bitdefender BOX 2

- **Standard:** Verwendung eines sicheren WLAN-Passworts
- **Information:** Systemstatus der BOX in der Central App
- **Zeitverzögerung:** Countdown bei Geräte-Neustart
- **Fortschrittsanzeige:** Passwort-Komplexität bei Registrierung

F-Secure SENSE:

- **Standard:** 1. Schutz von Geräten, 2. Schutz beim Surfen
- **Information:** Systemstatus des SENSE in der Router App
- **Fortschrittsanzeige:** Fortschritt beim Einrichtungs-Prozess

TrutzBox Home

- **Standard:** 1. Wirkungsweise des Security-Sliders, 2. Konfiguration wichtiger Webseiten, 3. Filterlisten, 4. Filtergruppen
- **Farbelement rot:** 1. Security-Slider: „Keine Anonymität“, 2. Inaktive Netzwerk-Anschlüsse
- **Farbelement grün:** 1. Security-Slider: „Höchste Anonymität“, 2. Aktive Netzwerk-Anschlüsse
- **Feedback:** TrutzBurg-Symbol mit Anzahl an Server-Verbindungen
- **Information:** 1. Status-Übersicht der TrutzBox, 2. Verbindungsprotokoll, 3. Filter-Level des Security-Sliders
- **Fortschrittsanzeige:** 1. Fortschritt bei Einrichtung, 2. Fortschritt bei Updates, 3. Passwort-Komplexität bei Registrierung

eBlocker 2

- **Standard:** 1. Content-Filter beim Nutzertyp „Kind“, 2. Vertrauenswürdige Apps und Webseiten, 3. DNS-Firewall 4. Blocker für Werbung, Tracker und Malware
- **Farbelement rot:** Inaktive Lizenz bei Einrichtung
- **Farbelement grün:** 1. Systemstatus bei Einrichtung, 2. Geräteschutz, 3. Content-Filter, 4. Dashboard-Status für Schutz vor Trackern und Werbung, 5. HTTPS-Modus 6. VPN-Modus (eBlocker Mobile)
- **Feedback:** „Confirmation-Toast“ bei Erfolg oder Fehler
- **Information:** 1. eBlocker-Dashboard, 2. Statusbar Details
- **Zeitverzögerung:** Automatisches Schließen der Willkommenseite
- **Fortschrittsanzeige:** 3. Passwort-Komplexität bei Registrierung

C.5 Bei der Untersuchung ermittelte Probleme

Bei der Untersuchung aufgetretene Usability-Probleme:

Bitdefender BOX 2

1. iOS/Android: Fehlen einer „Zurück“-Option im Einrichtungsprozess
2. Android: Viel zu große Schrift für „Anzahl geschützter Tage“ in „Aktivität“

F-Secure SENSE

–

TrutzBox Home

1. Ausblenden des „Security-Slider“-Overlays nur über „TrutzBurg Schild“ möglich
2. Häufiges und zufälliges Abmelden aus dem Administrations-Bereich
3. Fehlende Button-Funktionen („Abmelden“, „Download der VPN-Konfiguration“)
4. Suchfeld-Problem (weißes UI durch Texteingabe in Suche bei „Filter-Listen“)
5. Gegensätzliche Optionen (Auswahl „Alle Filter“ und „Keine Filter“ möglich)
6. Fehlende Funktion „Bearbeiten“ bei selbst angelegten Filterlisten
7. Fehlende Information über Art der Filterliste („Whitelist“ oder „Blacklist“)
8. Nicht auswählbare Buttons („WLAN-Einstellungen“, „Rechtliche Hinweise“)
9. Fehlender Text in Info-Overlay „Zertifikat Aktivieren“ bei „Fernzugriff“
10. Probleme mit Text-Darstellung (Überlagerungen, fehlende Abstände)
11. Inkonsistente Darstellung (Seiten-Überschriften, Expansion-Tiles, Buttons)
12. Keine einheitliche Link-Definition (Farben, Links, Nicht-Links)
13. Unklare Funktion für „Überschriften gruppieren“ per Drag-und-Drop
14. Keine Überprüfung auf Fehleingaben (Video-Konferenz, PGP-Schlüssel)
15. Schlüssel-Management (keine Gültigkeitsprüfung, keine manuelle Verwaltung)
16. Und weitere ...

eBlocker 2

1. Neue Filter-Kategorien werden erst nach „Reload“ der Seite angezeigt
2. Die Anzahl zugewiesener Filter-Kategorien ist „absolut“ und nicht „aktuell“
3. Fehlender Hinweis über Nicht-Löschbarkeit zugewiesener Filter-Kategorien

Bei der Untersuchung aufgetretene „Showstopper“:

Bitdefender BOX 2

1. Verschwinden der Geräte-Funktionen aus der Konfigurations-App, Werks-Reset und Neu-Einrichtung notwendig

F-Secure SENSE

–

TrutzBox Home

1. Beigelegtes LAN-Kabel ohne Funktion, Einrichtung ist nicht möglich, Austausch von LAN-Kabel notwendig
2. Gewähltes Passwort *„4qzhhAxZ!FTacEF%“* verweigert Login zum Admin-Bereich, Neu-Installation und -Einrichtung notwendig

eBlocker 2

–

„Personal data is the new oil of the internet and the new currency of the digital world.“ — Meglena Kuneva