DIN-Verbraucherrat

Studie

Untersuchung zum Thema „Verbrauchersicherheitswissen und -verhalten im Digitalen Raum“

Impressum

Herausgeber:

DIN-Verbraucherrat
DIN e.V.

Am DIN Platz
Burggrafenstraße 6
10787 Berlin

E-Mail: verbraucherrat@din.de
Web: http://www.din.de/go/verbraucherrat
Twitter: https://twitter.com/verbraucherrat

Gefördert durch:

Bundesministerium
für Umwelt, Naturschutz, nukleare Sicherheit
und Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Autoren:

Dr. Sara Elisa Kettner
s.e.kettner@conpolicy.de

Dr. Otmar Lell
o.lell@conpolicy.de

ConPolicy GmbH
Institut für Verbraucherpolitik
Crellestr. 37
10827 Berlin

www.conpolicy.de

Berlin, Dezember 2022

ConPolicy
Institut für Verbraucherpolitik

2. Dezember 2022

Untersuchung zum Thema „Verbrauchersicherheitswissen und -verhalten im Digitalen Raum“

Studie

vorgelegt bei:
DIN e. V.
DIN-Verbraucherrat
Herrn Dr. Alexander Goschew
Am DIN-Platz
Burggrafenstraße 6
10787 Berlin

durch:
ConPolicy GmbH
Institut für Verbraucherpolitik
Crellestr. 37
10827 Berlin
www.conpolicy.de

Autor:innen:
Dr. Sara Elisa Kettner
s.e.kettner@conpolicy.de
Dr. Otmar Lell
o.lell@conpolicy.de

Zusammenfassung

Mit Fortschreiten der Digitalisierung haben auch Sicherheitsrisiken für Verbraucher:innen zugenommen. Vor diesem Hintergrund wurde eine **online-repräsentative Bevölkerungsbefragung zur Sicherheit von IoT-Produkten** durchgeführt.

Die Befragung hat zu folgenden Ergebnissen geführt:

- **Kennzeichen für IT-Sicherheit helfen Verbraucher:innen grundsätzlich beim Kauf von IoT-Produkten.** Der statische Bestandteil des IT-Sicherheitskennzeichen des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist mit Blick auf seine Verständlichkeit verbesserungsfähig. Verbraucher:innen entnehmen dem statischen Bestandteil des BSI-Sicherheitskennzeichens teilweise eine Sicherheitsgarantie, die das Zeichen tatsächlich nicht gibt. Nicht untersucht wurde im Rahmen der Studie die dynamische Komponente des BSI-IT-Sicherheitskennzeichens .
- **Verbraucher:innen sind bereit, ein hohes Maß an Eigenverantwortung für die Sicherheit ihrer IoT-Geräte zu übernehmen.** Allerdings fällt es manchen schwer, diese Eigenverantwortung in die Tat umzusetzen, weil sie die Geräte als unverständlich und Einstellungen als zu kompliziert wahrnehmen.
- **Verbraucher:innen wünschen sich striktere Regeln bei der Zulassung von Produkten oder im Hinblick auf Verbote von unsicheren Produkten.**
  Ferner wünschen sie sich mehr Transparenz zur Sicherheit digitaler Geräte.

Im Abgleich der Befragungsergebnisse mit der zuvor durchgeführten Analyse von gesetzlichen und normativen Anforderungen an die IT-Sicherheit ergeben sich folgende **Handlungsempfehlungen für die Verbraucherpolitik:**

- **Der Vorschlag der EU-Kommission für einen Cyber Resilience-Act** verspricht, erstmalig ein durchgängig hohes Sicherheitsniveau bei verbrauchernahen IT-Produkten zu schaffen und **ist insofern sehr zu begrüßen**.
- Das durch den Cyber Security-Act der EU vorgegebene **Cybersecurity-Zertifikat** ermöglicht mit einer abgestuften Bewertung von IT-Sicherheit ein **hohes Maß an Transparenz und sollte daher alsbald praktisch eingeführt werden**.

Für die Normung ergeben sich folgende Handlungsempfehlungen:

- Ein **hohes Verbraucherschutzniveau in IT-Sicherheitsnormen wird mit dem Cyber Resilience Act noch wichtiger,** da Normen das Gesetz konkretisieren.
- Um **Security by Design** zu gewährleisten, müssen **Verbraucherinteressen bei IT-technischen Normungsvorhaben durchgängig vertreten werden.**
- **Normung sollte Usable Security befördern**, indem die **Verständlichkeit von Gebrauchsanweisungen und Sicherheitshinweisen** gewährleistet wird, indem ein hohes **Sicherheitsniveau voreingestellt** wird und indem **technische Sicherheitslösungen** entwickelt werden.

Abstract

As digitalisation has progressed, security risks for consumers have also increased. Against this background, an **online representative population survey** was conducted on the security of IoT products.

The survey led to the following results:

- **IT security labels generally help consumers when purchasing IoT products.** The static component of the IT security label issued by the German Federal Office for Information Security (BSI) could be improved with regard to its comprehensibility. Consumers sometimes take the static component of the BSI security label to mean a security guarantee that the label does not actually provide. Because of the limited scope of the study, the dynamic component of the German IT-Security Label was not included in the survey.
- **Consumers are willing to assume a high degree of personal responsibility for the security of their IoT devices.** However, some find it difficult to put this personal responsibility into practice because they perceive the devices as incomprehensible and the settings as too complicated.
- **Consumers would like to see stricter rules in the approval of products or with regard to bans on unsafe products.** They also want more transparency about the safety of digital devices.

Comparing the survey results with the preceding analysis of legal and normative requirements for IT security, the **following recommendations for consumer policy** emerge:

- The EU Commission's proposal for a **Cyber Resilience Act promises to create a consistently high level of security for consumer-related IT products** for the first time and **is therefore very welcome.**
- The **cybersecurity certificate specified by the EU's Cyber Security Act** enables a high degree of transparency with a graduated assessment of IT security. It should, therefore, be **practically implemented in the near future**.

The following recommendations result for standardisation:

- **A high level of consumer protection in IT security standards becomes even more important with the Cyber Resilience Act, as standards concretize the law.**
- **To ensure security by design, consumer interests must be consistently represented in IT standardisation projects.**
- **Standardisation should promote usable security** by ensuring that **instructions for use and security information are comprehensible**, by setting the **default for a high level of security** and by **developing technical security solutions**.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

1.1. Hintergrund

Digitale Technologien und Anwendungen ziehen immer weiter in den Konsumalltag der Verbraucher:innen ein. Die Effekte dieser Verbreitung sind ambivalent: Auf der einen Seite profitieren Verbraucher:innen von neuen Produkten, Diensten, Anwendungen und Komfortsteigerungen. Auf der anderen Seite sehen sie sich mit neuen Herausforderungen und Risiken insbesondere hinsichtlich der IT-Sicherheit ihrer Geräte und des Schutzes ihrer Privatsphäre konfrontiert. Fragen der Privatsphäre und des Datenschutzes werden hierbei gesellschaftlich intensiv diskutiert, Fragen der IT-Sicherheit bislang jedoch weniger. Wissen, Verhalten und Einstellungen der Verbraucher:innen zu Fragen der IT-Sicherheit sind daher Thema der vorliegenden Studie.

Um Verbraucher:innen vor Sicherheitsrisiken zu schützen und sie zu befähigen, selbst für IT-Sicherheit zu sorgen, hat sich ein Instrumentenmix auf drei Ebenen herausgebildet: *Rechtliche Regelungen* geben Mindeststandards und Leitplanken gesetzlich vor, untergesetzliche Konkretisierungen durch *Normen und Standards* zeigen den Herstellern und Anbietern auf, wie sie den rechtlichen Regelungen genügen können, und *Verbraucherbildungs- und Verbraucherinformationsaktivitäten* fördern ein informiertes Verbraucherverhalten.

Allerdings lassen die beschriebenen Instrumente derzeit in der Praxis noch große Lücken bei der Gewährleistung von IT-Sicherheit. Laut der aktuellen Erhebung des gemeinnützigen Vereins Deutschland sicher im Netz e. V. hat sich die Sicherheitslage der Verbraucher:innen verschlechtert: Einer wachsenden Zahl und Intensität von Bedrohungen steht eine Stagnation bei den Themen Sicherheitswissen und Sicherheitsverhalten gegenüber. Die Folge ist, dass der Sicherheitsindex aktuell auf dem niedrigsten Wert seiner Messungen liegt.[1]

Besonders relevant ist hier der Wachstumsmarkt des Internet of Things (IoT). Während im Jahr 2015 erst 2,3 Prozent der befragten Verbraucher:innen vernetzte Haustechnik nutzten, waren dies im Jahr 2022 bereits 11,0 Prozent. Vernetzte Unterhaltungselektronik nutzen aktuell 15,4 Prozent der Verbraucher:innen. Dies geht mit einem erheblichen Gefühl von Verunsicherung einher: 31,1 Prozent der befragten Verbraucher:innen halten laut derselben Erhebung vernetzte Haustechnik für gefährlich oder sehr gefährlich; bei vernetzter Unterhaltungselektronik haben 25,4 Prozent diese Sorge.[2]

[1] Deutschland sicher im Netz e.V. (Hrsg.) (2022), DsiN Sicherheitsindex 2022: Digitale Sicherheitslage von Verbraucher:innen in Deutschland. Abgerufen von https://www.sicher-im-netz.de/dsin-sicherheitsindex-2022 (11.07.2022).

[2] Deutschland sicher im Netz e.V. (Hrsg.) (2022), a. a. O. (Fn. 1).

Der effektive Schutz von Verbraucher:innen bleibt daher eine Aufgabe, die in der Praxis noch zu lösen ist. Auf den drei beschriebenen Maßnahmenebenen im Bereich der IT-Sicherheit kommt es darauf an, die Maßnahmen von den Verbraucher:innen her zu denken. Nur so können die Maßnahmen die Verbraucher:innen vor IT-Sicherheitsrisiken schützen und sie befähigen, informiert und kompetent mit digitalen Produkten und Anwendungen umzugehen.

1.2. Zielsetzung und Fragestellungen

Vor diesem Hintergrund verfolgt die vorliegende Studie im Auftrag des DIN-Verbraucherrat (DIN-VR) das Ziel, das **Verbraucherwissen und -verhalten in Bezug auf IT-Sicherheit sowie Anforderungen und Wünsche an eine Weiterentwicklung der Rahmenbedingungen und Unterstützungsmaßnahmen** zu erheben.

Im Fokus stehen hierbei Sicherheitsaspekte von Geräten im **Internet der Dinge** (Internet of Things – IoT). Mit dem „Internet der Dinge“ sind hierbei **Alltagsgegenstände gemeint, die herkömmlich nicht als Computer angesehen werden, aber mit Netzkonnektivität und Rechenkapazität ausgestattet werden und dadurch ins Internet integriert** werden.[3] Während manche IoT-Anwendungen wie smarte Türschließungsanlagen oder smarte Heizungssteuerung derzeit nur in besonders technikaffinen Haushalten Verwendung finden, sind andere weitverbreitet, etwa der Router als Zugangspunkt des Heimnetzwerks zum Internet, das Smartphone als internetfähige Fortentwicklung des Telefons oder der Smart TV als internetfähiger Fernseher (vgl. hierzu die Umfrageergebnisse in Abschnitt 4.3, S. 40 ff.).

1.2.1. Begriff der IT-Sicherheit

Der Begriff der **IT-Sicherheit** oder – gleichbedeutend – der Cybersicherheit wird im Folgenden entsprechend der Definition im BSI-Gesetz so verstanden, dass es um die **Verhinderung von Datenmanipulationen und von nicht autorisierter Preisgabe von Informationen** geht (vgl. § 2 Abs. 2 S. 2 BSI-Gesetz[4]).

Insofern wird **IT-Sicherheit** als prinzipiell verschieden vom **Datenschutz** und von der **Funktionssicherheit** verstanden. Schnittmengen zwischen den drei Themenfeldern gibt es allerdings, soweit Datenschutz auch den Schutz personenbezogener Daten vor unkontrolliertem Datenabfluss bezweckt und soweit die Funktionssicherheit durch Datenmanipulationen beeinträchtigt wird.

[3] Defnition angelehnt an Rose, K., Eldridge, S., Chapin, L. (2015), The Internet of Things: An Overview, S. 16 f.. Abgerufen von https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf (1.12.2023)

[4] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist.

1.2.2. Leitfragen

Die Studie ist an den folgenden Leitfragen ausgerichtet:

1. **Bestandsaufnahme:** Welche „blinden“ empirischen Flecken existieren hinsichtlich des Verbraucher*wissens* und *-verhaltens* über IT-Sicherheit bei IoT-Geräten derzeit und welche *Erwartungen und Anforderungen* haben Verbraucher:innen hinsichtlich der Rahmenbedingungen und möglicher Unterstützungsmaßnahmen?
2. **Verbraucherumfrage:** Welche Aussagen lassen sich aufgrund einer repräsentativen Verbraucherumfrage über das Wissen, Verhalten und die Einstellungen von Verbraucher:innen zur Sicherheit von IoT-Geräten treffen, soweit hierzu bislang noch keine Erkenntnisse vorlagen? Konkret:
   - Wie ist es um das *Wissen von Verbraucher:innen* hinsichtlich der Sicherheit von IoT-Geräten bestellt?
   - Wie *verhalten* sich Verbraucher:innen hinsichtlich der IT-Sicherheit bei IoT-Geräten heute?
   - Welche *Anforderungen und Erwartungen* haben Verbraucher:innen heute hinsichtlich der Rahmenbedingungen und möglicher Unterstützungsmaßnahmen hinsichtlich der IT-Sicherheit bei IoT-Geräten?
3. **Schlussfolgerungen und Handlungsempfehlungen:** Welche Schlussfolgerungen lassen sich aus den Ergebnissen für die Verbraucherpolitik ziehen? Wie kann *usable security*[5] (im Sinne von gebrauchstauglicher, die Nutzbarkeit nicht einschränkender Sicherheit) verwirklicht werden? Welche Handlungsempfehlungen leiten sich hieraus konkret für die Arbeit des DIN-Verbraucherrats in der Normung ab?

1.3. Methodik und Struktur des Berichts

Um den unterschiedlichen Fragestellungen gerecht zu werden, wurden in dem Vorhaben **drei unterschiedliche Methoden** kombiniert:

Für die Bestandsaufnahme wurde eine **Literaturrecherche** durchgeführt, um einen Überblick über die maßgeblichen Regelungen (vgl. Kapitel 2) und die relevanten Normen sowie über den Forschungsstand zu Wissen und Verhalten der Verbraucher:innen (vgl. Kapitel 3) zu geben. Auf diese Weise wurde die durch die Befragung zu schließende Forschungslücke konkretisiert.

Um eigene empirische Erkenntnisse zu Wissen, Verhalten und Erwartungen von Verbraucher:innen an die Sicherheit von IoT-Produkten zu generieren, wurde eine

[5] Brockhaus, A. (2021), Sicherheit darf kein Hindernis sein – Was ist „Usable Security & Privacy“? Zuletzt abgerufen am 2.08.2022 von https://www.is-its.org/it-security-blog/sicherheit-darf-kein-hindernis-sein-was-ist-usable-security-und-privacy

repräsentative Online-Befragung durchgeführt (vgl. Kapitel 4). Der hierfür verwendete Fragebogen wurde zuvor zwei Pretest unterzogen, zum einen auf die fachliche Richtigkeit hin mit Expert:innen, zum anderen auf die Verständlichkeit hin mit Verbraucher:innen. Details der Methodik zur Verbraucherbefragung werden im Zusammenhang mit den einzelnen Schritten der Erhebung dargestellt.

Im Anschluss an die Befragung wurde eine **Gap-Analyse** durchgeführt, welche die Erwartungen der Verbraucher:innen mit dem festgestellten Status Quo vergleicht. Hieraus werden **Handlungsempfehlungen für die Verbraucherpolitik und für die Normung** abgeleitet (vgl. Kapitel 5).

2. Grundlagen der IT-Sicherheit in Recht und Normung

IT-Sicherheit bezeichnet die Sicherheit bzw. den Schutz informationstechnologischer Infrastruktur vor Gefahren oder Schäden jedweder Art, seien es Bedrohungen von außen, beispielsweise durch Viren und Cyberangriffe oder Risiken von innen, insbesondere durch menschliche Versäumnisse im Umgang mit der Technik.[6]

Die Gewährleistung der IT-Sicherheit in diesem Sinne ist Aufgabe der Rechtsordnung, die einerseits durch das Gesetzesrecht umgesetzt wird, andererseits auch durch Normen und Standards, die technische Anforderungen an die IT-Sicherheit konkretisieren. Über beides wird nachfolgend ein Überblick gegeben.

2.1. Gesetzliche Grundlagen der IT-Sicherheit

2.1.1. BSI-Gesetz

In Deutschland ist das durch das IT-Sicherheitsgesetz 2.0[7] novellierte **Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)**[8] die zentrale normative Grundlage des IT-Sicherheitsrechts[9].

Betreiberpflichten

Die Verpflichtungen von Betreibern informationstechnischer Infrastrukturen unterscheiden sich danach, ob diese **kritische Infrastrukturen** betreiben (**KRITIS**), bei denen Störungen der IT-Sicherheit besonderes Schadenspotential haben wie etwa in den Bereichen Energie, Verkehr, Gesundheit, Wasser, Ernährung oder Finanzen, oder ob es sich um weniger schadensgeneigte **digitale Dienste** handelt.

KRITIS-Betreiber sind verpflichtet, die von ihnen betriebenen Kritischen Infrastrukturen beim Bundesamt für die Sicherheit in der Informationstechnik (BSI) zu registrieren und eine Kontaktstelle zu benennen. Sie sind verpflichtet, die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der verwendeten IT-Systeme zu gewährleisten – wobei das Gesetz keine konkret umzusetzenden Schutzmaßnahmen benennt, sondern die konkreten Sicherheitsmaßnahmen den Unterneh-

---

[6] Bussche, A. v. d., Schelinski, T. (2021), Rechtsgrundlagen der IT-Sicherheit, in: Leupold, A., Wiebe, A., Glossner, S. (Hrsg.), IT-Recht, 4. Aufl., 2021, S. 736 ff. (Rdnr. 2).

[7] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18.05.2021 (BGBl. I S. 1122).

[8] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist.

[9] Daneben ergeben sich IT-sicherheitsrechtliche Pflichten auch aus allgemeinen Rechtsvorschriften wie dem Gesellschafts- und Handelsrecht, da die dort niedergelegten unternehmerischen Sorgfaltspflichten auch Auswirkungen auf die IT-Sicherheit haben, vgl. dazu Bussche, A. v. d., Schelinski, T. a. a. O. (vgl. Fn. 6), Rdnr. 12.

men überlässt. Die Schutzmaßnahmen müssen dem Stand der Technik entsprechen – wodurch ein Anreiz geschaffen wird, branchenspezifische Sicherheitsstandards zu entwickeln, die dann vom BSI als sichere Systemarchitektur anerkannt werden können. Im Falle von Störungen müssen KRITIS-Betreiber diese dem BSI melden. Pflichtverstöße ziehen regelmäßig zivilrechtliche Haftungsansprüche nach sich.

Digitale Dienste im Sinne des BSI-Gesetzes sind **Online-Marktplätze, Online-Suchmaschinen sowie Cloud-Computing-Dienste**. Die Anbieter dieser digitalen Dienste sind verpflichtet, Risiken für die Sicherheit der Netz- und Informationsdienste, welche sie zur Bereitstellung ihrer digitalen Dienste in der EU nutzen, abzuwenden. Ebenso wie bei Betreibern kritischer Infrastrukturen werden die Schutzmaßnahmen auch hier nicht weiter spezifiziert, müssen aber dem Stand der Technik entsprechen. Auch hier gibt es Meldepflichten gegenüber dem BSI sowie mögliche Haftungsfolgen, allerdings in abgeschwächter Form gegenüber KRITIS-Betreibern.

Aufgaben des BSI

Das **Bundesamt für die Sicherheit in der Informationstechnik (BSI)** ist nach dem BSI-Gesetz die **zentrale Stelle für die Informationssicherheit auf nationaler Ebene**. Zu diesem Zweck nimmt das BSI eine Fülle von Aufgaben im Bereich der IT-Sicherheit wahr, etwa im Bereich der Untersuchung von Sicherheitsrisiken und der Entwicklung von informationstechnischen Verfahren für die Sicherheit in der Informationstechnik.

Das BSI hat auch Aufgaben im Bereich des Verbraucherschutze und der Verbraucherinformation zu Fragen der IT-Sicherheit. Die Ziele des BSI im digitalen Verbraucherschutz sind:

- das Schaffen der technischen Grundlagen und Rahmenbedingungen für Anbieter und Hersteller, um sichere und vertrauenswürdige Produkte und Dienste zu gestalten,
- die Information, Beratung und Warnung von Verbraucherinnen und Ver-brauchern, damit sie digitale Produkte und Dienste sicher nutzen können,
- die Unterstützung von Verbraucherinnen und Verbraucher bei der Steige-rung ihrer Resilienz, damit sie IT-Sicherheitsvorfälle bewältigen können.

In diesem Kontext steht auch die Entwicklung eines **freiwilligen IT-Sicherheitskennzeichens** (§ 9c BSI-Gesetz). Dieses IT-Sicherheitskennzeichen besteht aus einer statischen und einer dynamischen Komponente. Die statische Komponente bildet die Zusicherung des Herstellers oder Diensteanbieters ab, dass das Produkt für eine festgelegte Dauer bestimmte, vom BSI anerkannte IT-Sicherheitsanforderungen erfüllt (Herstellererklärung) und leitet Verbraucher:innen über einen Link und QR-Code zur dynamische Komponente des Kennzeichens auf der Website des BSI (Sicherheitsinformation). Den Schwerpunkt legt das Kennzeichen dabei auf

die dynamische Komponente, die aus einer individuellen Produktinformationsseite besteht, die Verbraucher:innen das IT-Sicherheitskennzeichen erklärt und Informationen wie Laufzeit und Herstellerpflichten bereitstellt. Als besonderes Element befindet sich dort eine aktuelle Sicherheitsinformation zum Produkt, über die das BSI z.B. zu notwendigen Updates oder aktuellen Sicherheitslücken informieren kann. Zusätzlich werden für Verbraucher:innen aufbereitete Informationen zu den Anforderungen des zugrundeliegenden Standards bereitgestellt.

Die Verwendung des Sicherheitskennzeichens ist nur nach Freigabe durch das BSI gestattet. Allerdings prüft das BSI bei Erteilung nicht, ob die versprochenen Sicherheitseigenschaften im Rahmen der Herstellererklärung tatsächlich technisch umgesetzt sind, sondern nur, ob die Angaben des Herstellers plausibel und durch Unterlagen hinreichend belegt sind. Die Plausibilitätsprüfung umfasst unter anderem die Prüfung, ob dem BSI zum Zeitpunkt des Antrags Schwachstellen zum Produkt bekannt sind. Darüber hinaus müssen Hersteller im Rahmen der Antragsstellung darlegen, wie sie bei der Eigenprüfung vorgegangen sind und erklären, wie sie zu dem Ergebnis gekommen sind, das ihr Produkt den Anforderungen entspricht. Sofern der Hersteller von optionalen Anforderungen des Sicherheitsstandards abweicht, muss er dies ausführlich begründen. Die Angaben des Herstellers werden durch das BSI nachvollzogen und auf Widersprüche zu den zugrundeliegenden Sicherheitsanforderungen geprüft.

Nach der Erteilung des IT-Sicherheitskennzeichens prüft die BSI-Marktaufsicht die Produkte stichprobenartig anlasslos und anlassbezogen bei Bekanntwerden von Schwachstellen. Im Rahmen der Aufsicht können Antragsunterlagen, technische Unterlagen und Herstellerdokumente herangezogen oder technische Überprüfungen veranlasst werden. Dabei kann sowohl die Konformität zur Herstellererklärung als auch die Einhaltung der mit dem IT-Sicherheitskennzeichen einhergehenden Pflichten der Hersteller geprüft werden.

Mit der Einführung einer dynamischen Komponente und der nachgelagerten Überwachung durch die BSI-Marktaufsicht hebt sich das BSI mit dem IT-Sicherheitskennzeichen von anderen Kennzeichen für IoT-Produkte ab.

2.1.2. EU-rechtliche Grundlagen der IT-Sicherheit

EU-rechtlicher Hintergrund der deutschen IT-Sicherheitsgesetzgebung sind verschiedene Richtlinien der Europäischen Union[10], insbesondere die **Datenschutzgrundverordnung**[11], die **NIS-RL**[12], die **Funkgeräterichtlinie**[13] und der **Rechtsakt zur Cybersicherheit**[14]. Darüber hinaus plant die EU-Kommission weitere Maßnahmen für die Verbesserung der IT-Sicherheit, insbesondere ein **Gesetz zur Cyberwiderstandsfähigkeit**[15]. Das BSI-Gesetz setzt viele der EU-rechtlichen Vorgaben um; gleichzeitig behalten die EU-rechtlichen Grundlagen der IT-Sicherheit in mancher Hinsicht eigenständige Relevanz, wie nachfolgend ausgeführt wird.

Datenschutzgrundverordnung

Die **Datenschutzgrundverordnung** (DSGVO) enthält mit Blick auf den Schutz der Vertraulichkeit personenbezogener Daten Verpflichtungen zur Gewährleistung der Datensicherheit (Art. 32 DSGVO). Diese Verpflichtungen sind inhaltlich ähnlich den eben beschriebenen Vorschriften nach dem BSI-Gesetz und verpflichten Datenverarbeiter:innen zu geeigneten technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Verpflichtungen zur Datensicherheit nach der DSGVO gehen aber insoweit über das BSI-Gesetz hinaus, als sie nicht nur für die im BSI-Gesetz genannten Anbieter digitaler Dienste gelten, sondern für alle Verarbeiter:innen personenbezogener Daten – also auch für die Anbieter von IoT-Produkten, die personenbezogene Daten verarbeiten. Die DSGVO nennt unter den Schutzmaßnahmen im Bereich der Datensicherheit unter anderem auch die **Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen**. Da die DSGVO in Deutschland unmittelbar geltendes Recht ist, sind ihre Vorgaben auch ohne weiteren Umsetzungsakt im nationalen Recht direkt anzuwenden.

---

[10] Auch auf der EU-Ebene gibt es neben den hier beschriebenen Rechtsakten noch weitere Vorgaben zur IT-Sicherheit, so etwa die Richtlinie 2001/95/EG zur allgemeinen Produktsicherheit oder die Richtlinie 2019/771 über den Warenkauf – letztere schreibt vor, dass Updates für IoT-Geräte solange zur Verfügung gestellt werden müssen, wie Verbraucher:innen das vernünftigerweise erwarten können.

[11] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. (EU) L 119 vom 4.05.2016 (Datenschutz-Grundverordnung)

[12] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. (EU) L 194 vom 19.07.2016 (NIS-Richtlinie)

[13] Richtlinie (EU) 2014/53 vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG, ABl. (EU) L 153 vom 22.05.2014 (Funkgeräterichtlinie)

[14] Verordnung (EU) 2019/881 vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit)

[15] EU-Kommission (2022), Aufforderung zur Stellungnahme zu einer Folgenabschätzung zum Gesetz zur Cyberwiderstandsfähigkeit. Zuletzt abgerufen am 3.08.2022 von https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Gesetz-uber-Cyberresilienz-neue-Cybersicherheitsvorschriften-fur-digitale-Produkte-und-Nebendienstleistungen_de

Funkgeräterichtlinie

Ziel der Funkgeräterichtlinie ist es, die freie Verkehrsfähigkeit von Funkgeräten im Binnenmarkt sicherzustellen. Funkanlagen im Sinne der Richtlinie sind alle elektrischen oder elektronischen Erzeugnisse, die zum Zwecke der Funkkommunikation und/oder der Funkortung bestimmungsgemäß Funkwellen ausstrahlen oder empfangen, also auch IoT-Geräte, die über W-LAN mit dem Internet verbunden sind. Die Verkehrsfähigkeit dieser Funkanlagen steht unter der Voraussetzung, dass sie grundlegende Sicherheitsanforderungen erfüllen. Darunter fällt zunächst der Schutz der Gesundheit und Sicherheit von Menschen, Haus- und Nutztieren sowie elektromagnetische Verträglichkeit. Funkanlagen müssen aber auch die Gewähr bieten, dass sie **keine schädlichen Auswirkungen auf das Netz oder seinen Betrieb verursachen**, dass sie über Sicherheitsvorkehrungen verfügen, die **sicherstellen, dass personenbezogene Daten und die Privatsphäre der Nutzer:innen geschützt werden**, und dass sie bestimmte **Funktionen zum Schutz vor Betrug** unterstützen.

Eine **delegierte Verordnung der EU-Kommission**[16] legt in verbindlicher Weise einen weiten Anwendungsbereich dieser Verpflichtungen fest. Auf diese Weise aktiviert sie die entsprechenden Verpflichtungen der Funkgeräterichtlinie im Bereich der **Cybersicherheit**. In der Folge müssen insbesondere alle Funkanlagen, die personenbezogene Daten, Verkehrsdaten oder Standortdaten verarbeiten können, über Sicherheitsvorrichtungen verfügen, die sicherstellen, dass personenbezogene Daten und die Privatsphäre des Nutzers und des Teilnehmers geschützt werden. Die entsprechenden Verpflichtungen gelten ab dem 1.08.2024.

Rechtsakt zur Cybersicherheit (Cybersecurity Act)

Der **Rechtsakt zur Cybersicherheit** regelt zum einen die Zuständigkeiten der **Agentur der Europäischen Union für Cybersicherheit (ENISA)** sowie **der nationalen IT-Sicherheitsbehörden** und trifft zum anderen Vorgaben für eine **europäische Cybersicherheitszertifizierung**[17].

Der Rechtsakt für Cybersicherheit etabliert die europäische Cybersicherheitszertifizierung allerdings nicht direkt, sondern schafft nur die rechtliche Grundlage hierfür. Sobald eine Cybersicherheitszertifizierung auf dieser Grundlage beschlossen und angenommen ist, wird sie **nationale Schemata für die Cybersicherheitszertifizierung unwirksam** machen (Art. 57).

Für das europäische Cybersicherheitszertifikat sind **drei verschiedene Stufen der Sicherheitsbewertung** vorgesehen (niedrig, mittel und hoch, Art. 52). Die **Anforderungen des IT-Sicherheitskennzeichens des BSI** an das Sicherheitsniveau **gehen über die Stufe "niedrig" hinaus, liegen jedoch unter der Stufe "mittel"**.

---

[16] Delegierte Verordnung (EU) 2022/30 vom 29. Oktober 2021zur Ergänzung der Richtlinie 2014/53/EU im Hinblick auf die Anwendung der grundlegenden Anforderungen, auf die in Artikel 3 Absatz 3 Buchstaben d, e und f der Richtlinie Bezug genommen wird, ABl. (EU) L 7 vom 12.01.2022

[17] vgl. dazu auch unten Abschnitt 0, , S. 63.

Eine **Selbstbewertung der Konformität** ist nur für die Vertrauenswürdigkeitsstufe **„niedrig“** zulässig (Art. 53). Für eine Zertifizierung mit den Vertrauenswürdigkeitsstufen „mittel“ und „hoch“ muss die Einhaltung der Voraussetzungen für die Vergabe des Cybersicherheitszertifikats von einer unabhängigen **Konformitätsbewertungsstelle** geprüft werden.

2.2. Grundlagen der IT-Sicherheit in Normung und Standardisierung

Die eben beschriebenen gesetzlichen Grundlagen der IT-Sicherheit legen meist nur grundsätzliche Wertungen fest, aber keine technischen Maßnahmen oder Verfahren. Insofern sind die Gesetze auf **Ausfüllung durch technische Standards und Regelwerke** angelegt.

So wird regelmäßig auf Normen zurückgegriffen, wenn rechtliche Anforderungen die **Einhaltung des Standes der Technik** verlangen - so etwa, wenn das BSI-Gesetz von den Betreibern informationstechnischer Infrastrukturen oder den Anbietern von IT-Diensten verlangt, dass sie bei ihren Sicherheitsmaßnahmen den jeweils aktuellen Stand der Technik anwenden.

Noch stärker ist die Relevanz von Normen im Zusammenhang mit der **Kennzeichen für IoT-Produkte**: Die Vorschriften des BSI-Gesetzes zum Sicherheitskennzeichen werden ebenso wie die EU-Regelungen zur Cybersicherheitszertifizierung erst dann praktisch wirksam, wenn die **einzuhaltenden Sicherheitsmaßnahmen durch technische Regelwerke konkret definiert** werden und diese Regelwerke für die Zwecke der Kennzeichnung behördlich anerkannt worden sind.

Dementsprechend gibt es **zahlreiche Normen sowie laufende Normungsvorhaben im Bereich der IT-Sicherheit**. Nachfolgend wird ein kurzer Überblick über die wichtigsten Normenwerke und Normungsvorhaben gegeben.

2.2.1. Normen und Standards: Begriffsklärung und Wirkungsweise

Normen und Standards sind Dokumente, die Anforderungen an Produkte, Dienstleistungen oder Verfahren festlegen. Ihr Ziel ist es, Klarheit über deren Eigenschaften zu erzielen und damit Rationalisierung und Qualitätssicherung zu unterstützen.

In Deutschland wird der Normungsprozess vom **Deutschen Institut für Normung e.V. (DIN)** organisiert. DIN ist ein eingetragener Verein und wird privatwirtschaftlich getragen.

DIN gewährleistet durch die **Beteiligung aller interessierten Kreise**, unabhängig von ihrer wirtschaftlichen Leistungsfähigkeit, faire Verfahrensrichtlinien. Diese sind in den Normen der Reihe DIN 820 „Normungsarbeit“ festgelegt und öffentlich einsehbar.

Je nach dem Konsensgrad, d. h. nach der Breite der Beteiligung interessierter Kreise, lassen sich **verschiedene Arten von Normen und Standards** unterscheiden.

Je höher der Konsensgrad, desto höher ist die gesellschaftliche Anerkennung eines Normungsdokuments. Allerdings steigt mit dem Konsensgrad auch die Zeit, die für die Erarbeitung des Normungsdokuments erforderlich ist.

Im Einzelnen veröffentlicht DIN folgende **Typen von Dokumenten:**

1. **Normen:**

   Normen entstehen im Konsens. Das bedeutet, die Expert:innen verständigen sich unter Berücksichtigung des Standes der Technik auf eine gemeinsame Version der Inhalte, die versucht, alle Interessen der Beteiligten zu berücksichtigen und Gegenargumente auszuräumen.

   DIN-Normen werden spätestens alle fünf Jahre auf Aktualität überprüft. Entspricht eine Norm nicht mehr dem Stand der Technik, so wird ihr Inhalt überarbeitet oder die Norm zurückgezogen.

2. **Standards**

- **Technische Spezifikationen (TS)**: Eine TS ist das Ergebnis einer Normungsarbeit, das wegen bestimmter Vorbehalte zum Inhalt, wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens oder mit Rücksicht auf die europäischen Rahmenbedingungen vom DIN nicht als Norm herausgegeben wird.
- **Technischer Report (TR)**: Ein TR ist ein Sachstandsbericht, der Erkenntnisse, Daten usw. aus Normungsvorhaben enthält, die der Information über den Stand der Normung – auch anderer internationaler und regionaler Normungsorganisationen – dient und der bei späteren Normungsarbeiten als Grundlage herangezogen werden kann.
- **DIN SPEC**: Eine DIN SPEC lässt sich innerhalb weniger Monate erstellen und veröffentlichen. Nicht alle Kreise müssen beteiligt werden und sie muss auch nicht unbedingt im Konsens erstellt werden. Nach dem PAS-Verfahren (PAS=Publicly available Specification) erstellte DIN SPEC werden kostenlos als Download über die Homepage des Beuth-Verlags zur Verfügung gestellt.

Alle diese normativen Dokumente haben gemein, dass ihre **Anwendung freiwillig** ist. Sie sind nur dann verpflichtend einzuhalten, wenn sie vertraglich vereinbart wurden oder vom Gesetzgeber unter Bezug genommen werden. Sie können **geltende Rechtsvorschriften nicht ändern, ersetzen oder aushebeln**. Eine Norm kann damit auch keine Rechtsfrage klären in dem Sinne, dass sie verbindlich über die Zulässigkeit einer rechtlich umstrittenen Unternehmenspraxis entscheidet. Dies zu entscheiden, ist Aufgabe von Gesetzgeber und Rechtsprechung.

Allerdings können Normen und Standards **unbestimmte Rechtsbegriffe untergesetzlich definieren**. Normen konkretisieren den Stand der Technik und schreiben ihn flexibel fort. Da Normen eindeutige (anerkannte) Regeln sind, bietet der Bezug auf Normen in Verträgen Rechtssicherheit. Im Rechtsstreit billigt ein Richter der

DIN-Norm regelmäßig den **„Beweis des ersten Anscheins“** zu. Dies ist eine widerlegbare Rechtsvermutung, die im Streitfall eine **Beweislastumkehr** bewirkt.

Wird eine Norm oder ein Standard verwendet, so müssen die entsprechenden Anforderungen auch in Gänze eingehalten werden. Dafür kann dann in der Außendarstellung eine Aussage darüber getroffen werden, dass das **jeweilige Produkt einer bestimmten Norm oder einem bestimmten Standard entspricht**. Eine entsprechende, kostenpflichtige **Bestätigung durch Dritte in Form einer Zertifizierung** ist ebenso möglich.

2.2.2. Normung auf deutscher, europäischer und internationaler Ebene

Die Normungsarbeit findet **auf deutscher, europäischer und internationaler Ebene** statt. Weil IT-Sicherheit und die Sicherheit von IoT-Produkten nur in grenzüberschreitender Zusammenarbeit sinnvoll gewährleistet werden kann, sind die europäische und die internationale Ebene hier besonders wichtig.

Die **europäischen Normungsorganisationen** sind das **Europäische Komitee für Normung (CEN)**, das **Europäische Komitee für elektrotechnische Normung (CENELEC)** und das **Europäische Institut für Telekommunikationsnormen (ETSI**).[18]

Auf internationaler Ebene sind die **Internationale Organisation für Normung (ISO)** und die **Internationale Elektrotechnische Kommission (IEC)** in den hier relevanten Bereichen aktiv.[19]

Das **Deutsche Institut für Normung (DIN)** bringt sich in die Verhandlungen über Normen auf europäischer und internationaler Ebene als **nationales Spiegelgremium** ein. Europäische Normen sind nach ihrer Ratifikation als nationale Normen unverändert anzuwenden. Internationale Normen können nach ihrer Veröffentlichung von nationalen Normungsorganisationen in das nationale Normenwerk übernommen werden. Eine Verpflichtung hierzu besteht aber – im Unterschied zu den europäischen Normen – nicht.

2.2.3. Normen und Normungsvorhaben mit Relevanz für die Sicherheit von IoT-Produkten

Die nachfolgende Tabelle enthält einen Überblick über die für die Sicherheit von IoT-Produkten relevantesten Normen und laufende Normungsvorhaben (vgl, S. 20).

Besonders bedeutsam ist hier die **europäische Norm ETSI EN 303 645**. Diese trifft **grundlegende Anforderungen an die Cybersicherheit von IoT-Produkten für Endverbraucher:innen**. Zu den erfassten Themenbereichen zählen insbesondere

[18] DIN (2022), DIN in Europa. Abgerufen von https://www.din.de/de/din-und-seine-partner/din-in-der-welt/din-in-europa (13.07.2022)
[19] DIN (2022), Internationale Normung. Abgerufen von https://www.din.de/de/din-und-seine-partner/din-in-der-welt/internationale-normung (13.07.2022)

Passwortschutz und Authentisierung, die Offenlegung von Sicherheitslücken, Sicherheitsupdates, die sichere Speicherung von essentiellen Sicherheitsdaten, Kommunikationssicherheit, der Schutz vor Angriffen sowie diverse Anforderungen für eine leichte Installation und Wartung der Geräte. Die zugehörige Konformitätsbewertung richtet sich nach der Norm ETSI TS 103 701.

Relevant ist im hier untersuchten Zusammenhang auch das **Normungsvorhaben ISO 27404.**[20] Ziel dieses Normungsvorhabens ist es, einen **Rahmen für Cybersicherheitslabel für Endverbraucher-IoT-Geräte** zu bestimmen. Hierbei wird von vier Vertrauenswürdigkeitsstufen ausgegangen. Die ersten beiden Vertrauenswürdigkeitsstufen bleiben hierbei nach dem gegenwärtigen Stand der Beratungen im Anspruch hinter den Anforderungen des EU-Rechtsakts zur Cybersicherheit zurück; die dritte und vierte Stufe sehen ebenso wie der EU-Rechtsakt zur Cybersicherheit eine externe Zertifizierung vor.

Standard	Titel	Status
ETSI EN 303 645	Cyber Security for Consumer Internet of Things: Baseline Requirements	veröffentlicht
ISO 15408-1	Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model	veröffentlicht
ISO 15408-2	Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components	veröffentlicht
ISO 15408-3	Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components	veröffentlicht
ISO 24760-1	IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts	veröffentlicht
ISO 27400	Cybersecurity — IoT security and privacy — Guidelines	veröffentlicht
ISO 27402	Cybersecurity – IoT Security and Privacy- Device baseline requirements	in Bearbeitung
ISO 27403	Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics	in Bearbeitung
ISO 27404	Information technology — Security techniques — Universal cybersecurity labelling framework for consumer IoT	in Bearbeitung
ISO 29100	Information technology — Security techniques — Privacy framework	veröffentlicht
ISO 31700	Consumer protection — Privacy by design for consumer goods and services	in Bearbeitung
ISO AWI TR 31700-2	Privacy-by-design for Consumer Goods and Services — use cases	in Bearbeitung
DIN SPEC 27072	Informationstechnik – IoT-fähige Geräte – Mindestanforderungen zur Informationssicherheit	zurückgezogen

Tabelle 1: veröffentlichte Normen und in Bearbeitung befindliche Normungsvorhaben mit Bedeutung für die Sicherheit von IoT-Produkten. Quelle: DIN Verbraucherrat; eigene Darstellung (ConPolicy)

[20] ISO/IEC, Dokument vom 31.05.2022, Dokument-Nr. ISO/IEC JTC 1/SC 27/WG 4 N 5805, Text for ISO/IEC end PWI 27404, Information technology — Security techniques — Universal cybersecurity labelling framework for consumer IoT.

2.3. Zusammenfassung der Grundlagen der IT-Sicherheit in Recht und Normung

Die Rechtsanalyse hat die **Vielzahl von punktuellen Rechtsgrundlagen im Bereich der IT-Sicherheit auf deutscher und europäischer Ebene** aufgezeigt. Es fehlt aber derzeit noch an einer **durchgängigen Anforderung zur Gewährleistung eines hohen Sicherheitsniveaus bei verbrauchernahen IT-Produkten.**

Die Anforderungen dieser Rechtsvorschriften sind **allgemein formuliert** und geben keine bestimmten technischen Maßnahmen vor. Insofern sind für eine effektive Gewährleistung von IT-Sicherheit **anspruchsvolle und praktisch relevante Normen und Standards unverzichtbar**.

Bei konkreten Fragen **konkurrieren unterschiedliche regulatorische Ansätze.** Das resultierende Niveau des Verbraucherschutzes im Bereich der IT-Sicherheit hängt daher davon ab**, welches Regulierungskonzept sich durchsetzt**. Als Beispiel hierfür werden nachfolgend die **Anforderungen an ein IT-Sicherheitskennzeichen nach dem deutschen BSI-Gesetz, nach dem EU-Rechtsakt zur Cybersicherheit und nach dem Normentwurf der ISO 27404 verglichen** (vgl. Tabelle 2).

Grundlage	BSI-Gesetz (ergänzt durch Normen und Branchenstandards)	EU-Rechtsakt zur Cybersicherheit	Normentwurf ISO 27404[21]
Sicherheitsanforderungen	Definiert durch Normen oder branchenabhängige IT-Sicherheitsstandards, die vom BSI anerkannt werden.	Grundlegende Mindestanforderungen an IT-Sicherheit Weitere Anforderungen je nach Schutzniveau	Keine allgemeinen Anforderungen; Schutzniveau je nach Sicherheitsniveau unterschiedlich definiert
Sicherheitsniveaus	Keine Unterscheidung unterschiedlicher Sicherheitsniveaus	Drei Sicherheitsniveaus	Vier Sicherheitsniveaus
Externe Zertifizierung	Plausibilitätsprüfung	Teilweise: Stufe 1 nein, Stufen 2, 3 ja.	Teilweise: Stufen 1, 2 nein, Stufen 3, 4 ja.
Optische Gestaltung		(noch) keine Vorgaben	

Tabelle 2: Regulierungskonzepte für IT-Sicherheitskennzeichen. Quelle der optischen Gestaltung der IT-Sicherheitskennzeichen: BSI[22], ISO/IEC[23]; eigene Darstellung (ConPolicy).

[21] Darstellung nach dem Entwurfsstand der Norm gem. ISO/IEC, a. a. O. (vgl. Fn. 20) – die Darstellung kann sich im weiteren Verlauf der Beratungen über die Norm noch ändern.

[22] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/IT-Sicherheitskennzeichen/it-sicherheitskennzeichen_node.html

[23] ISO/IEC, a. a. O. (vgl. Fn. 20)

3. Der bisherige Forschungsstand: Wissen, Verhalten und Einstellungen von Verbraucher:innen zur Sicherheit von IoT-Geräten

Es gibt bereits einen umfassenden Forschungsstand zu Wissen, Verhalten und Einstellungen von Verbraucher:innen zur IT-Sicherheit. Einige der vorhandenen Erhebungen beziehen sich explizit auf die Sicherheit von IoT-Geräten, andere auf IT-Sicherheit im Allgemeinen. Auch aus den letztgenannten, allgemeinen Erhebungen ergeben sich relevante Erkenntnisse für die Sicherheit von IoT-Geräten im Speziellen.

Nachstehend wird der Forschungsstand zum Wissen, Verhalten und zu den Einstellungen von Verbraucher:innen zur Sicherheit von IoT-Geräten und zur IT-Sicherheit im Allgemeinen dargestellt, wie er sich aufgrund einer Literaturrecherche im Rahmen dieses Projekts darstellt.

3.1. Verbraucherwissen und -verhalten

3.1.1. Passwortnutzung

Erkenntnisse zum Verbraucherwissen zur IT-Sicherheit liegen insbesondere anhand der Frage der **Passwortnutzung** vor.

Zahlreiche Untersuchungen belegen, dass die überwiegende Mehrheit von Verbraucher:innen **elementare Kenntnisse zu den Sicherheitsanforderungen** an Passwörter besitzen. So wissen 92 Prozent der Verbraucher:innen weltweit, dass es ein Risiko ist, das gleiche oder ein ähnliches Passwort zu benutzen.[24] Wenn es um konkrete Sicherheitsanforderungen geht, scheint das Wissen von Verbraucher:innen allerdings an Grenzen zu stoßen.[25] Die befragten Verbraucher:innen glaubten auch eher nicht, dass sie sich selbst durch Passwörter wirksam vor Hackern schützen können. Ebenfalls wussten sie eher nicht, ab wann ein Passwort sicher ist. [26]

Dennoch nimmt die Nutzung von sicheren Passwörtern in der Bevölkerung allmählich zu. Laut Digitalbarometer 2021 des Bundesamt für Sicherheit in der Informa-

[24] LastPass (Hrsg.) (2021), Psychology of Passwords. Zuletzt abgerufen am 12.07.2022: https://www.lastpass.com//-/media/9fe0bf5dc473413b8ab4df3bd8688295.pdf
[25] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2020), Die Lage der IT-Sicherheit in Deutschland 2020. Bonn. Zuletzt abgerufen am 12.07.2022: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2
[26] BSI (2020), a. a. O. (Fn. 25)

tionstechnik (BSI) nutzen 60% der deutschen Bevölkerung (14 bis 69 Jahren) sichere Passwörter. Im Vergleich zum Vorjahr ist hier ein Anstieg zu erkennen, 2020 nutzten nur 48% der Befragten sichere Passwörter.[27]

Weiterhin nutzen Verbraucher:innen **viele unterschiedliche Accounts**, wodurch die Menge an Passwörtern tendenziell zunimmt. 78% nutzen bis zu 20 Accounts.[28] Im Zuge dessen lassen sich viele einfache oder ähnliche Passwörter besser merken. Ein schwieriges Passwort, welches den Sicherheitsempfehlungen entsprechen würde, zu merken, erfordert deutlich mehr kognitive Kapazität, welche ungern aufgebracht wird. Nichtsdestotrotz nutzen 63 % der Befragten unterschiedliche Passwörter für unterschiedliche Dienste laut Initiative D21 (2021).[29]

Eine Erleichterung bei der Vergabe von sicheren Passwörtern und beim praktischen Umgang mit diesen können **Passwortmanager** schaffen. 39 Prozent der Verbraucher:innen kennen Passwortmanager, 27 Prozent der Verbraucher:innen nutzen diese auch.[30] Die Diskrepanz zwischen Kenntnis und praktischer Nutzung könnte sich damit erklären lassen, dass eine große Mehrheit der Verbraucher:innen **Vorbehalte gegenüber Passwortmanagern** haben. So haben 78 Prozent der Verbraucher:innen in Deutschland etwa die Sorge, dass ein Hacker mit einem Schlag auf alle Passwörter zugreifen könne[31].

Interessant zu beobachten ist, dass 45% der Befragten einer weltweiten Studie selbst nach einem Sicherheitsvorfall im vergangenen Jahr ihr **Passwort nicht geändert** haben.[32]

3.1.2. Zwei-Faktor-Authentisierung

Aufschlussreich auch für andere Fragen der IT-Sicherheit ist das Verhältnis von Wissen und Verhalten beim Thema **Zwei-Faktor-Authentisierung**. Der **Begriff** selbst ist laut einer repräsentativen Befragung im Auftrag des Verbraucherzentrale Bundesverband (vzbv)[33] ohne weitere Erklärung **nur 43 Prozent der Befragten** bekannt. Allerdings **kennen 75 Prozent das Prinzip der zweistufigen Anmeldung**.

---

[27] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2021), Digitalbarometer 2021: Bürgerbefragung zur Cyber-Sicherheit. Bonn. Zuletzt abgerufen am 12.07.2022: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2021.pdf?__blob=publicationFile&v=2

[28] BSI (2020), a. a. O. (Fn. 25)

[29] Initiative D21 (2021). Digitalpolitik: Digital Skills Gap. https://initiatived21.de/app/uploads/2021/08/digital-skills-gap_so-unterschiedlich-digital-kompetent-ist-die-deutsche-bevlkerung.pdf; ähnlich BSI – Bundesamt für Sicherheit in der Informationstechnik (2020). Die Lage der IT-Sicherheit in Deutschland 2020. Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2 – hiernach nutzen 67 Prozent der Befragten unterschiedliche Passwörter.

[30] BSI (2020), a. a. O. (Fn. 25)

[31] BSI (2020), a. a. O. (Fn. 25)

[32] LastPass (Hrsg.) (2021), a. a. O. (Fn. 24)

[33] Verbraucherzentrale Bundesverband (vzbv) (2021), Zwei-Faktor-Authentisierung. Zuletzt abgerufen am 12.07.2022: https://www.vzbv.de/sites/default/files/2022-03/21-08-31_2FA-Chartbericht_freigegeben_0.pdf

Das lässt erkennen, dass die praktische Erfahrung mit sicherheitstechnischen Verfahren, etwa bei der Tätigung von Bankgeschäften, auch zu einem praktischen sicherheitstechnischen Erfahrungswissen beiträgt.

Darüber hinaus haben in derselben Umfrage **50 Prozent der Befragten** erklärt, dass sie es akzeptieren würden, wenn man sich bei einem Dienst **nur noch mit einer „Zwei-Faktor-Authentisierung“** anmelden könnte.

Für die Nutzung von vernetzten Geräten/Smart Home Technologien (**IoT-Geräten**) bedienen sich 5% der deutschen Internetnutzenden (ab 16 Jahren) der **Zwei-Faktor-Authentisierung als Sicherheitsmaßnahme**.[34]

3.1.3. Relevante Entscheidungsfaktoren beim Kauf von IoT-Geräten

Eine Befragung von IoT-Verbraucher:innen ergab, dass diese **Datenschutz und Sicherheit zu den wichtigsten Faktoren zählen, die beim Kauf von IoT-Geräten zu berücksichtigen** sind.[35]

Trotzdem geben die meisten Befragten an, dass sie vor dem Kauf eines IoT-Geräts **Aspekte von Datenschutz und IT-Sicherheit tatsächlich nicht beachtet** hätten.[36]

Eine Untersuchung zu den Verbraucherpräferenzen belegt, dass Verbraucher:innen bei Smart-Home-Geräten dazu neigen, die **potenziellen Risiken zu ignorieren** und sich mehr auf die potenziellen Vorteile zu konzentrieren, die sich aus der Nutzung ergeben.[37]

3.1.4. Bewusstsein für Datensicherheit

Mit 83% ist sich ein Großteil der Verbraucher:innen bewusst, dass **Dienste und Anwendungen persönliche Daten weitergeben**.[38] Darüber hinaus interessiert sich wiederum **nur jede:r zweite Verbraucher:in für Informationen über Sicherheit im Internet**. 22 Prozent der Verbraucher:innen geben sogar an, sich nie zu informieren.[39]
Bezogen auf das Thema der **Cyberkriminalität** ist allerdings ein deutlicher Wunsch nach mehr Informationen festzustellen: Einer repräsentativen Umfrage

---

[34] vzbv (2021), a. a. O. (Fn. 33)
[35] Emami-Naeini, P., Dixon, H., Agarwal, Y. und Cranor, L. F (2019), *Exploring How Privacy and Security Factor into IoT Device Purchase Behavior.* In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 534, S. 1–12. https://doi.org/10.1145/3290605.3300764
[36] Emami-Naeini, P., et. al. (2019), a. a. O. (Fn. 35)
[37] Wang, X., McGill, T. J. und Klobas, J. E (2020), *I Want It Anyway: Consumer Perceptions of Smart Home Devices*. Journal of Computer Information Systems. 60:5. S. 437-447. doi: 10.1080/08874417.2018.1528486
[38] Initiative D21 (2021), *Digitalpolitik: Digital Skills Gap.* Zuletzt abgerufen am 12.07.2022: https://initiative21.de/app/uploads/2021/08/digital-skills-gap_so-unterschiedlich-digital-kompetent-ist-die-deutsche-bevlkerung.pdf
[39] BSI und ProPK (2021), a. a. O. (Fn. 27)

zufolge wünschen sich zwei Drittel der Befragten mehr Informationen bezüglich des Schutzes vor Datendiebstahl.[40]

3.2. Diskrepanz zwischen Wissen und Verhalten: Privacy Paradox

Zusammenfassend lässt sich sagen, dass das Wissen von Verbraucher:innen zu Fragen der IT-Sicherheit weithin lückenhaft ist. Das Handeln von Verbraucher:innen bleibt aber selbst hinter diesem elementaren Wissen noch deutlich zurück. Diese Diskrepanz zwischen Wissen und Handeln ist durch viele Studien als **Privacy Paradox** belegt. So kannten etwa in einer Studie 67 Prozent der Verbraucher:innen Sicherheitsempfehlungen zum Schutz vor Kriminalität im Internet, nur 37 Prozent setzten diese aber zumindest teilweise um, und nur 12 Prozent vollständig.[41]

Unter anderem folgende **Gründe** sind hierfür zu nennen: Verbraucher:innen **kennen grundlegende IT-Sicherheitsstandards nicht**. Sie sind ferner **zu optimistisch** hinsichtlich der Risiken des Internet und können sich nicht vorstellen, dass ausgerechnet sie betroffen sein werden. Die Umsetzung von Maßnahmen zur IT-Sicherheit **nimmt Zeit ein, welche Nutzende eher für ihre eigentlichen Aufgaben oder Interessen nutzen wollen**.[42]

Als positive Entwicklung sollte demgegenüber aber festgehalten werden, dass laut Digitalbarometer 2021 immerhin **60 Prozent der Befragten sichere Passwörter, 62 Prozent ein aktuelles Virenprogramm, 53 Prozent eine aktuelle Firewall, 40 Prozent die Zwei-Faktor-Authentisierung und 32 Prozent die automatische Installation von Updates nutzen**. Im Vergleich zum Vorjahr (Digitalbarometer 2020) wurden Schutzmaßnahmen vermehrt umgesetzt. Pro Maßnahme gab es einen durchschnittlichen Anstieg von 6,5%.[43] (vgl. Tabelle 3).

[40] Bundeskanzleramt & Bundesamt für Sicherheit in der Informationstechnik (2020), Schutz von Online-Konten. https://www.bundesregierung.de/resource/blob/975272/1732446/4c4377ce98f697a94011955fdc9a1f62/de-passwort-download-zwischenbericht-data.pdf?download=1

[41] BSI und ProPK (2021), a. a. O. (Fn. 39)

[42] Tam, L., Glassman, M., & Vandenwauver, M. (2010), The psychology of password management: a tradeoff between security and convenience. Behaviour & Information Technology, 29(3), 233-244.

[43] BSI und ProPK (2021), a. a. O. (Fn. 39)

Wie schützen Sie sich vor Gefahren im Internet?	2020	2021
Aktuelles Virenschutzprogramm	57%	62%
Sichere Passwörter	48%	60%
Aktuelle Firewall	47%	53%
Sichere https-Verbindung bei der Übertragung persönlicher Daten	31%	41%
Zwei Faktor-Authentisierung	33%	40%
Einstellung der automatischen Installation von Updates	25%	32%
Regelmäßiges Anlegen von Sicherheitskopien	20%	28%
Verschlüsselte E-Mail-Kommunikation	18%	23%
Verzicht auf soziale Medien	10%	13%
Verzicht auf Online-Banking	10%	9%

Tabelle 3: Maßnahmen zum Schutz vor Gefahren im Internet. Quelle: BSI (2021), Digitalbarometer 2021[44], 2021 n = 2025, 2020 n = 2000, Mehrfachnennungen möglich.

3.3. Einstellungen und politische Forderungen

Wenn die Verbraucher:innen selbst nach ihren Forderungen und Wünschen befragt werden, zeigen sich **Unterschiede nach dem Grad der digitalen Affinität**: **Digital affine Bevölkerungsgruppen** (v.a. jüngere Generationen zwischen 26 und 55 Jahren) wünschen sich **mehr Befähigung im Sinne von Wissenserweiterung und Qualifizierungen**. Ältere Generationen (ab 56 Jahren), die **wenig eigene praktische Erfahrung** damit haben, wünschen sich neben der Befähigung **in erster Linie Schutz durch die Politik**.[45]

Generell befürworten Verbraucher:innen die Idee, **Sicherheits- und Datenschutzbewertungen von vertrauenswürdigen und unabhängigen Organisationen auf Sicherheitsetiketten** zu haben. [46] IoT-Verbraucher:innen nehmen Labels als zugänglich und nützlich für Kaufentscheidungen wahr.[47]

In der aktuellen Kauflandschaft ist es für IoT-Verbraucher:innen jedoch **schwierig bis unmöglich, vor dem Kauf Informationen zum Datenschutz und zur Sicherheit**

[44] BSI (2021), a. a. O. (vgl. Fn. 27).
[45] Initiative D21 (2021), Digitalpolitik: Diese Themen dürfen aus Sicht der BürgerInnen in den Koalitionsverhandlungen nicht fehlen. Berlin. Zuletzt abgerufen am 12.07.2022: https://initiatived21.de/app/uploads/2021/10/d21_kurzexpertise_digitalpolitik.pdf
[46] Emami-Naeini, P., Agarwal, Y., Cranor, L. F. und Hibshi, H. 2020. *Ask the Experts: What Should Be on an IoT Privacy and Security Label?*. IEEE Symposium on Security and Privacy (SP) 2020. S. 447-464. doi: 10.1109/SP40000.2020.00043. Zuletzt abgerufen am 12.07.2022: https://ieeexplore.ieee.org/abstract/document/9152770
[47] Emami-Naeini, P., et. al. (2019), a. a. O. (Fn. 35)

zu finden.[48] Datenschutz- und Sicherheitsmerkmale auf einem IoT-Label können die Risikowahrnehmung und die Kaufbereitschaft beeinflussen.[49] 43% der deutschen Internetbevölkerung wünschte sich darüber hinaus verständliche Informationen zu allen wichtigen Themen der privaten IT-Anwendung. [50] Informationen bezüglich des Schutzes vor Datendiebstahl, praktische Tipps zur Handhabung von Online-Konten und weitere Sicherheitsinformationen sollten am ehesten von staatlichen Stellen zur Verfügung gestellt werden.[51]

3.4. Zusammenfassung zum Forschungsstand und Schlussfolgerungen für die Erhebung

Nach den dargestellten Erkenntnissen der Forschung lassen sich **Unterschiede zwischen Sicherheitsbewusstsein und Sicherheitsverhalten** feststellen. Es gibt auch Ansätze zur Erklärung dieser Unterschiede, aber weiterhin auch **Unklarheiten für die Motivation des Verbraucherverhaltens.**

Damit lassen sich folgende **Fragestellungen für die empirische Erhebung** im Rahmen des vorliegenden Projekts festhalten, die durch die bisherige Literatur noch nicht zureichend beantwortet werden:

- Welche Rolle spielen Sicherheitsaspekte in der Motivation der Verbraucher:innen beim Kauf von IT-Produkten?
- Welche Rolle spielen Sicherheitsaspekte bei der Inbetriebnahme von IT-Produkten und während der Nutzungsphase, etwa bei Updates?
- Wie schätzen Verbraucher:innen ihre eigene Verantwortung für IT-Sicherheit ein, und welche Erwartungen haben sie insoweit an die Politik?
- Wie bewerten Verbraucher:innen konkret das in Deutschland seit kurzem etablierte IT-Sicherheitskennzeichen des Bundesamts für Sicherheit in der Informationstechnik (BSI)?

.

[48] Emami-Naeini, P., et. al. (2019), a. a. O. (Fn. 35)
[49] Emami-Naeini, P., Dheenadhayalan, J., Agarwal, Y. und Cranor, L. F. 2021. *Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices?* IEEE Symposium on Security and Privacy (SP) 2021. S. 519-536, doi: 10.1109/SP40001.2021.00112.
[50] Bundeskanzleramt & BSI (2020), a. a. O. (Fn. 40)
[51] Bundeskanzleramt & BSI (2020), a. a. O. (Fn. 40)

4. Ergebnisse der Bevölkerungsbefragung im Rahmen des Projekts

Die Verbraucherbefragung zielte darauf ab, die **blinden Flecken bzgl. des Verbraucherwissens und -verhaltens sowie Erwartungen an IoT-Sicherheitsaspekte zu schließen**, da diese noch nicht oder nur ungenügend in der Literatur und in weiteren Studien abgedeckt wurden.

4.1. Überblick und Vorgehensweise

Die Befragung untergliederte sich in fünf unterschiedliche Teile, die die **gesamte Customer Journey eines digitalen IoT-Produkts** bzw. einer Anwendung abdeckten und hierbei alle IT-sicherheitsrelevanten Aspekte untersuchten:

1. Im ersten Teil der Befragung wurde analysiert, welche **Attribute bei der Auswahl eines digitalen Produkts** eine Rolle spielen. Der Hauptfokus lag dabei auf sicherheitsrelevanten Attributen wie der Prüfinstanz, dem objektiven Sicherheitsniveau sowie dem Updatezeitraum. Darüber hinaus wurde beleuchtet, welche Rolle die Kosten bzw. der Preis des Produkts spielen.
2. Im zweiten Teil wurde untersucht, wie sich Verbraucher:innen bei der **Inbetriebnahme** von digitalen Produkten und Anwendungen verhalten. Der Fokus lag dabei auf den Sicherheitseinstellungen vor der ersten Nutzung von IoT-Geräten.
3. Anschließend wurden im dritten Teil der Befragung die **Nutzungsphase** des Geräts und der Umgang mit **Sicherheitsaktualisierungen** untersucht.
4. Im vierten Teil wurde die allgemeine Bereitschaft der Verbraucher:innen **Verantwortung** für die eigene IT-Sicherheit zu übernehmen sowie **Erwartungen** an den Gesetzgeber beleuchtet.
5. Der fünfte und letzte Teil behandelte **IT-Sicherheitskennzeichen im Allgemeinen** sowie im konkreten Fall den statischen Bestandteil des IT-Sicherheitskennzeichens des Bundesamts für Sicherheit in der Informationstechnik. Der dynamische Bestandteil, der den Schwerpunkt des Kennzeichens bildet, wurde nicht betrachtet.

Der Fragebogen deckte neben diesen Aspekten auch Fragen zu sozio-demografischen Attributen ab. Diese werden im Folgenden nicht gesondert ausgewertet, sondern in den jeweiligen Hauptabschnitten mitberücksichtigt, falls sie für das Antwortverhalten eine systematische Rolle spielen.

4.1.1. Stichprobe und Hinweise zum Datensatz

Die **Gesamtstichprobe** umfasst **N=995 Teilnehmer:innen**, die im September 2022 den Fragebogen absolvierten. Die Rekrutierung erfolgte über ein aktiv-gemanagtes Online-Panel und die Teilnehmer:innen wurden online-repräsentativ für die Studie ausgewählt (Quotierung nach Alter, Geschlecht und Wohnort).[52]

Das Durchschnittsalter der Proband:innen lag bei 48,7 Jahren, die jüngste Person war 16 und die älteste 83 Jahre alt. 49% der Proband:innen waren männlich, 51% weiblich und ‹1% divers. 22% der Proband:innen hatten einen niedrigen, 29% einen mittleren und 51% einen hohen Bildungsabschluss. Im Durchschnitt benötigten die Proband:innen knapp 19 Minuten zur Fertigstellung des Fragebogens (Median = 17 Minuten).

4.1.2. Aufbau der Abschnitte zu den Ergebnissen

Da die einzelnen Teile der Verbraucherbefragung **unterschiedliche Schritte** im Rahmen der **Customer Journey** behandeln, werden diese separat voneinander, d.h. in getrennten Abschnitten, berichtet. In jedem Befragungsteil werden zuerst die **Zielsetzung** und die behandelten **Forschungsfragen** präsentiert. Danach folgt die konkrete **Methodik**, d.h. die Vehikel, die gewählt wurden, um die Forschungsfragen optimal zu beantworten. Dann werden die **Ergebnisse** entlang der Forschungsfragen präsentiert. Übergeordnete Ergebnisse werden jeweils in gelben Ergebnis-Boxen präsentiert. Im Text darunter werden zusätzliche Daten und Fakten sowie Abbildungen vorgestellt.[53]

In der statistischen Auswertung des Datensatzes wurden die Hauptvariablen auch systematisch im Hinblick auf **Zusammenhänge mit sozio-demografischen Attributen** untersucht. Hierzu zählen das Alter der Teilnehmer:innen in Jahren, das Geschlecht sowie die digitale Affinität. Letztere umfasst wiederum drei einzelne Befragungsbatterien, die jeweils zu einer Summe zusammengefasst wurden: (1) die Anzahl der IoT-Geräte, die Teilnehmer:innen besitzen, (2) die Kenntnis unterschiedlicher digitaler Begriffe, wie bspw. Fake News, Biometrie oder Blockchain, und (3) die Nutzung unterschiedlicher Schutzmaßnahmen für die eigene Datensicherheit, wie bspw. getrennte WLAN-Netzwerke, Updates oder Offline-Modus.[54]

Im letzten Abschnitt der einzelnen Kapitel findet sich eine **Gesamtzusammenfassung** der Ergebnisse sowie ein **Fazit**.

---

[52] Insgesamt absolvierten N=1.000 Personen die Befragung. Aus Qualitätssicherungsgründen wurden jedoch 5 Personen ausgeschlossen, da diese entweder eine auffällig schnelle Bearbeitungszeit aufwiesen oder den Fragebogen nicht vollständig beantworteten.

[53] Hierbei sollte angemerkt werden, dass zur besseren Lesbarkeit numerische Ergebnisse, wie bspw. Anteile, als ganze Zahlen präsentiert werden. Hierdurch ist es auch möglich, dass durch das Runden auf ganze Zahlen die Summe von Antwortoptionen nicht immer 100% entspricht.

[54] Der vollständige Fragebogen steht als separates Dokument zur Verfügung.

4.2. Teil 1: Kauf von vernetzten Geräten und IT-Sicherheitskennzeichen

Ziel des ersten Befragungsteils war es, das **Verhalten von Nutzer:innen beim Kauf von IoT-Geräten** zu untersuchen und zu prüfen, welche Faktoren bei der Auswahl eines vernetzten Produkts eine Rolle spielen.

Die konkreten Forschungsfragen waren:

- Spielen Kennzeichen zur IT-Sicherheit eine Rolle für den Kauf von smarten Produkten? Interpretieren Nutzer:innen die Informationen auf solchen Kennzeichen korrekt und kaufen mit Hilfe der Kennzeichen eher das sicherste Produkt?
- Macht es einen Unterschied ob die Produkte extern überprüft werden oder die Sicherheit vom Hersteller bescheinigt wird?
- Spielt der Preis der Produkte eine Rolle für die Kaufwahrscheinlichkeit?
- Macht es einen Unterschied, ob zusätzliche Informationen zur Updategarantie der Produkte zur Verfügung stehen?

4.2.1. Methodik

Um die Forschungsfragen systematisch zu untersuchen, wurde ein **Experimental-Design im Vignetten Stil**[55] entwickelt, bei dem die Teilnehmer:innen ihre **Kaufwahrscheinlichkeit** für ein Produkt in unterschiedlichen Ausprägungen angeben sollten.

Produkt: Das Produkt, das gekauft werden sollte, war ein handelsüblicher Router, der mit einem Marken-neutralen Bild angezeigt wurde und einen fiktiven, neutralen Produktnahmen trug. Außerdem wurde in jeder Produkt-Vignette der Preis sowie Informationen zur IT-Sicherheit angezeigt. Abbildung 1 zeigt beispielhaft eine Produkt-Vignette.

Abbildung 1: Produkt-Vignette – mehrstufiges Label im höchsten Sicherheitsniveau (3*).

[55] Eine Vignette ist eine aus systematisch variierten Merkmalen bestehende Produktbeschreibung. Sie fasst somit die für die Entscheidungssituation relevanten Merkmale auf einen Blick zusammen und präsentiert sie den Proband:innen.

Rangreihenfolge von fünf unterschiedlichen Produkten: Die Teilnehmer:innen wurden gebeten, sich in jeder Entscheidungssituation in eine realistische Kaufsituation zu versetzen und anzugeben, welches Produkt sie am ehesten kaufen würden (Rang 1), welches Produkt sie mit der zweithöchsten Wahrscheinlichkeit kaufen würden (Rang 2), welches mit der dritthöchsten Wahrscheinlichkeit (Rang 3) usw. Dabei wurden ihnen fünf unterschiedliche Produkte angezeigt, die sich im Hinblick auf ihre IT-Sicherheit sowie z.T. im Hinblick auf den Preis unterschieden. Es gab also jeweils fünf Ränge, vom ersten bis zum fünften, die von den Proband:innen nach eigenem Ermessen, beeinflusst durch die Produktmerkmale vergeben wurden.

Produkte mit unterschiedlichen Sicherheitsniveaus: Tabelle 4 gibt einen Überblick über die fünf Produkte und Informationen zu ihrer Ausgestaltung. Dabei gab es jeweils unterschiedliche Sicherheitsniveaus, die sich an den Anforderungen des IT-Sicherheitskennzeichens des BSI, den Überlegungen zum EU-Rechtsakt zur Cybersicherheit sowie dem Normentwurf ISO 27404 orientierten und gestalterisch ableiteten.

Produkt und Bezeichnung	Beschreibung	Abbildung in der Produkt-Vignette
Produkt 1: Kein Label	• Kontrollgruppe • Produkt erfüllt keine Anforderungen an IT-Sicherheit und trägt somit auch kein Label • Objektiv das unsicherste Produkt	
Produkt 2: Binäres Label	• Produkt erfüllt die minimalen Anforderungen an IT-Sicherheit • IT-Sicherheit wird durch ein einfaches Label ausgezeichnet • Die Anforderungen werden vom Hersteller bescheinigt • Das Sicherheitsniveau ist identisch zum folgenden Label • Optische Gestaltung orientiert sich an der statischen Komponente des IT-Sicherheitskennzeichen des BSI	
Produkt 3: Mehrstufiges Label (1*)	• Produkt erfüllt die minimalen Anforderungen an IT-Sicherheit • IT-Sicherheit wird durch ein mehrstufiges Label ausgezeichnet • Das Produkt erreicht eine von drei Sicherheitsstufen • Die Anforderungen werden vom Hersteller bescheinigt • Das Sicherheitsniveau ist identisch zum vorhergehenden Label • Optische Gestaltung orientiert sich am EU-Rechtsakt zur Cybersicherheit sowie dem Normentwurf ISO 27404	
Produkt 4: Mehrstufiges Label (2*)	• Produkt erfüllt mittlere Anforderungen an IT-Sicherheit • IT-Sicherheit wird durch ein mehrstufiges Label ausgezeichnet • Das Produkt erreicht zwei von drei Sicherheitsstufen • Die Anforderungen werden von unabhängiger Stelle geprüft • Optische Gestaltung orientiert sich am EU-Rechtsakt zur Cybersicherheit sowie dem Normentwurf ISO 27404	
Produkt 5: Mehrstufiges Label (3*)	• Produkt erfüllt die maximalen Anforderungen an IT-Sicherheit • IT-Sicherheit wird durch ein mehrstufiges Label ausgezeichnet • Das Produkt erreicht drei von drei Sicherheitsstufen • Die Anforderungen werden von unabhängiger Stelle geprüft • Objektiv das sicherste Produkt • Optische Gestaltung orientiert sich am EU-Rechtsakt zur Cybersicherheit sowie dem Normentwurf ISO 27404	

Tabelle 4: Übersicht der Produkte und Sicherheitskennzeichen in der Befragung.

Statische Kennzeichnung: Bei allen Kennzeichen wurden lediglich die statischen Aspekte berücksichtigt, d.h. das Kennzeichen, wie es sich für den Verbraucher in der optischen Gestaltung unmittelbar darstellt.

Unberücksichtigt bleibt im Rahmen dieser Studie das hybride Konzept, das dem IT-Sicherheitskennzeichen des BSI zugrunde liegt. Dieses relativ neue Konzept bietet durch die Verbindung mit einer produkteigenen Internetseite via QR-Code oder Link speziell für die Verbraucher:innen aufbereitete Informationen über das Kennzeichen selbst, die zugrundeliegenden Sicherheitsanforderungen, den Update-Stand, aktuelle Sicherheitslücken und die Gültigkeit des konkreten Kennzeichens.

Dieses Konzept bietet daher eine Fülle weiterer Informationen, die aufgrund ihrer Aktualität und ihrem Umfang bei einem rein statischen Kennzeichen nicht bereitgestellt werden kann. Zugleich müssen die Verbraucher:innen selbst aktiv werden (z.B. durch Scannen des QR-Codes), um an die Informationen zu gelangen.

Das auf die statische Komponente des IT-Sicherheitskennzeichens beschränkte Untersuchungsdesign legt insofern eine Situation zugrunde, in der diese zusätzlichen Informationsangebote praktisch nicht genutzt werden. Vergleichbare andere Fallkonstellationen, etwa bei der Chemikalienkennzeichnung lassen erwarten, dass dies eine praktisch häufige Situation ist.

Weiterführende Studien sollten allerdings durchgeführt werden, um zu untersuchen, inwieweit die zusätzlichen Informationsangebote in der Praxis tatsächlich durch die Verbraucher:innen angenommen werden und wie sich die zusätzliche Information auf das Verbraucherverhalten auswirkt.

Vier Experimentalbedingungen: Insgesamt ermöglichte das Design die Testung von vier Experimentalbedingungen, die sich im Hinblick auf die integrierten Sicherheitskennzeichen sowie die Preise der Produkte unterschieden. Die erste Experimentalgruppe („einfach konstant“) erhielt die bereits vorgestellte, einfache Ausführung des Sicherheitslabels. In der Produkt-Vignette wurden also nur der Produktname, das Bild, Informationen zum Sicherheitsniveau an sich sowie zur ausstellenden Instanz (Hersteller oder unabhängige Stelle) angezeigt. Des Weiteren war der Preis für alle fünf Produkte konstant und betrug 99 Euro.

Die zweite Experimentalbedingung („einfach ansteigend“) wurde entworfen, um die Forschungsfrage zur Rolle des Preises bzw. zum Einfluss der Produktkosten auf die Kaufwahrscheinlichkeit zu untersuchen. Der Preis pro Sicherheitsstufe stieg somit an. Das Produkt ohne Label kostete weiterhin 99 Euro. Das Produkt mit binärem Label sowie das Produkt mit mehrstufigem Label und einem Stern erfüllte das minimale Anforderungsniveau an IT-Sicherheit und war in beiden Fällen identisch. Somit kosteten beide Produkte jeweils 109 Euro. Das Produkt, das das mittlere Sicherheitsniveau erfüllte und somit das mehrstufige Label mit zwei Sternen trug, kostete entsprechend 119 Euro. Das objektiv sicherste Produkt, zertifiziert durch das mehrstufige Label mit drei Sternen, kostete 129 Euro.

Die dritte Experimentalbedingung („erweitert konstant“) wurde konzipiert, um zu untersuchen, ob zusätzliche Informationen zur Updategarantie eine Rolle für die Kaufwahrscheinlich spielten. Hierfür wurden die Label der Produkte entsprechend ihrem Sicherheitsniveau um Informationen zur Updategarantie erweitert. Wie in Abbildung 2 zu sehen, wurde auf dem Label der beiden Produkte mit minimaler IT-Sicherheit vermerkt, dass Updates noch zwei weitere Jahre zur Verfügung stünden. Beim Produkt mit mittlerem Sicherheitsniveau waren Updates noch fünf Jahre verfügbar und bei dem Angebot mit der maximalen Sicherheit zehn Jahre. Alle Produkte in der dritten Experimentalgruppe hatten einen konstanten Preis von 99 Euro.

Abbildung 2: Erweitertes Label mit Informationen zur Updategarantie.

Die vierte Experimentalbedingung („erweitert ansteigend“) wurde ergänzt, um das erweiterte Label ebenfalls im Hinblick auf steigende Kosten bzw. Preise zu untersuchen. Somit wurden die erweiterten Kennzeichen mit Informationen zur Verfügbarkeit der Sicherheitsupdates abgebildet (vgl. Abbildung 2) und die Preise stiegen von 99 Euro (unsicherstes Produkt) schrittweise auf 129 Euro (sicherstes Produkt), analog zur zweiten Experimentalbedingung, an.

Zufällige Anordnung der Produkte und Reihenfolge: In jeder Entscheidungssituation wurden auf dem Bildschirm der Teilnehmer:innen alle fünf unterschiedlichen Produkte gleichzeitig angezeigt. Die Reihenfolge der fünf Produkte untereinander wurde dabei voll randomisiert, d.h. es wurde zufällig ausgewählt, welches Produkt an oberster Stelle angezeigt wurde und welches darunter.

Jede:r Teilnehmer:in traf seine Kaufentscheidung (Bewertung der Kaufwahrscheinlichkeit) zweimal. Es wurde dabei zufällig ausgewählt welche Experimentalbedingung zuerst präsentiert wurde und welche danach. Somit gab es vier mögliche Konstellationen:

1. Konstellation: zuerst „einfach konstant“, danach „einfach ansteigend“
2. Konstellation: zuerst „einfach ansteigend“, danach „einfach konstant“
3. Konstellation: zuerst „erweitert konstant“, danach „erweitert ansteigend“
4. Konstellation: zuerst „erweitert ansteigend“, danach „erweitert konstant“

Dieses Design wurde so gewählt, um sowohl mögliche Reihenfolgeeffekte der Anzeige zu vermeiden als auch die Anzahl an Observationen pro Experimentalbedingung zu maximieren. In der Auswertung zur Vorbereitung des finalen Datensatzes wurde auf einen Reihenfolgeeffekt untersucht und die statistischen Analysen ergaben, dass es keine systematischen Unterschiede in der Präsentation der Reihenfolge gab. Somit können die Observationen aus den einzelnen Experimentalbedingungen, unabhängig davon, ob sie in der ersten oder zweiten Entscheidungsstufe präsentiert wurden, zusammen betrachtet werden.

Observationen je Experimentalbedingung: Soweit nicht anders vermerkt, basieren die Ergebnisse auf den folgenden Observationszahlen pro Experimentalbedingung:

- Einfach konstant N=498
- Einfach ansteigend N=498
- Erweitert konstant N=497
- Erweitert ansteigend N=497

4.2.2. Ergebnisse

Ergebnis 1: Nutzer:innen interpretieren die unterschiedlichen Sicherheitsniveaus, die durch die Label abgebildet werden, scheinbar korrekt. Produkte mit (objektiv) höherem Sicherheitsstandard werden eher gekauft als solche mit niedrigerem Standard.

Abbildung 3 zeigt die Bewertung der Produkte als Anteile der Rangbewertung in der Experimentalbedingung „einfach konstant“. Betrachtet man die Median-Ränge der unterschiedlichen Labels ergibt sich ein klares Bild. Das mehrstufige Label mit drei Sternen, das heißt die höchste Sicherheitsstufe mit externer Prüfung, landet auf dem ersten Rang, gefolgt vom mehrstufigen Label mit zwei Sternen und externer Prüfung. Auf dem dritten Rang verorten die Nutzer:innen das binäre Label, bei dem der Hersteller die Sicherheit bescheinigt. Das objektiv gleich ausgestaltete Produkt, das das mehrstufige Label mit einem Stern trägt und ebenfalls vom Hersteller bescheinigt wird, landet auf dem vierten Rang.

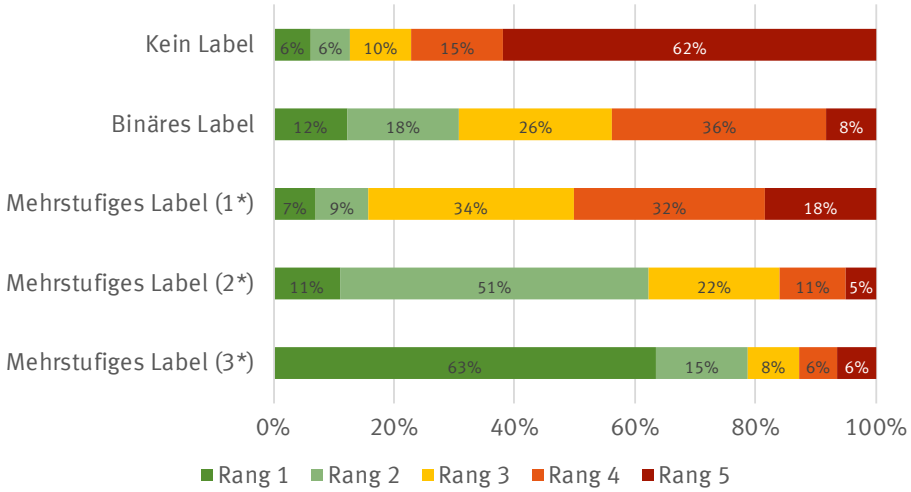

Abbildung 3: Bewertung IT-Sicherheitslabel: Einfache Ausführung – Konstanter Preis.[56]

Die Ergebnisse deuten also darauf hin, dass Verbraucher:innen in einer Kaufsituation mit Hilfe der Informationen, die auf den Sicherheitskennzeichen enthalten sind, in der Lage sind, das sicherste Produkt auszuwählen.

Ergebnis 2: Produkte ohne Label werden seltener gekauft als Produkte mit Label.

Auf dem fünften und letzten Platz landet das Produkt ohne Label. Es wird durchschnittlich schlechter bewertet als die anderen Produkte, die ein Sicherheitskennzeichen tragen bzw. deren IT-Sicherheit zumindest in Teilen zertifiziert ist. Fast zwei Drittel der Verbrauer: innen verorten das Produkt auf dem letzten Rang und drücken damit die im Vergleich geringste Kaufabsicht aus.

Ergebnis 3: Produkte mit extern überprüfter Sicherheit werden eher gekauft als solche, deren Sicherheit lediglich von Hersteller bescheinigt wird.

Die Sicherheitskennzeichen unterscheiden sich auch im Hinblick auf die Prüfinstanz, die das Sicherheitsniveau bescheinigt. Zum einen gibt es die Gruppe der Produkte, deren Sicherheit vom Hersteller bescheinigt wird und dies auch auf dem Label an sich vermerkt haben. Hierzu zählen das binäre Label und das mehrstufige Label, mit einer Wertung von einem von einem Stern hinsichtlich des Sicherheitsniveaus. Zum anderen gibt es die Gruppe der Produkte, deren Sicherheit von unabhängiger Stelle geprüft wurde. Hierzu zählen die mehrstufigen Label mit einer Sicherheitswertung von zwei und drei Sternen. Vergleicht man die beiden Gruppen, so kann festgestellt werden, dass Produkte mit unabhängiger Prüfung

[56] Die Durchschnittsbewertung als Rang zwischen 1 (bester Rang und höchste Kaufwahrscheinlichkeit) und 5 (schlechtester Rang und somit niedrigste Kaufwahrscheinlichkeit) der einzelnen Produkte bzw. Labels war: Kein Label 4,2, binäres Label 3,1, mehrstufiges Label (1*) 3,5, mehrstufiges Laben (2*) 2,5 und mehrstufiges Label (3*) 1,8.

eher gekauft werden als solche, die nur vom Hersteller zertifiziert sind. Sie landen in der durchschnittlichen Bewertung durch die Nutzer:innen auf einem besseren Rang.

Interessant ist auch, dass die beiden Produkte, deren Sicherheit lediglich vom Hersteller geprüft wurde, sich ebenfalls in der Bewertung unterscheiden. So ist die Kaufwahrscheinlichkeit für das Produkt mit dem binären Label durchschnittlich höher als die Kaufwahrscheinlichkeit für das Produkt, das das mehrstufige Label trägt und mit einem Stern für das Sicherheitsniveau ausgezeichnet ist. Die erdachten Produkte sind allerdings im Hinblick auf die Prüfung sowie das Sicherheitsniveau identisch angelegt und unterscheiden sich lediglich im Hinblick auf ihr Aussehen und die Produktnamen.

Ergebnis 4: Der Preis spielt für die Kaufpräferenzen der Nutzer:innen keine systematische Rolle.

Abbildung 4 zeigt die Bewertung der Kaufwahrscheinlichkeit (Rangreihenfolge) für die Produkte mit einfachem Label und einem ansteigenden Preis. Wie im Abschnitt zur Methodik bereits beschrieben, hatte das Produkt ohne Sicherheitskennzeichen (unsicherstes Produkt) den geringsten Preis und das Produkt mit dem höchsten Sicherheitsniveau (3 Sterne, sicherstes Produkt) den höchsten Preis. Mit jeder höheren Sicherheitsstufe stieg der Preis also an.

Bei den Median-Rängen der unterschiedlichen Produkte und Label bleibt die Reihenfolge, bis auf eine Ausnahme, bestehen. In der Experimentalgruppe mit ansteigendem Preis teilen sich das binäre Label und das mehrstufige Label mit einem Stern den dritten Rang. Dennoch wird auch hier das binäre Label durchschnittlich besser bewertet.

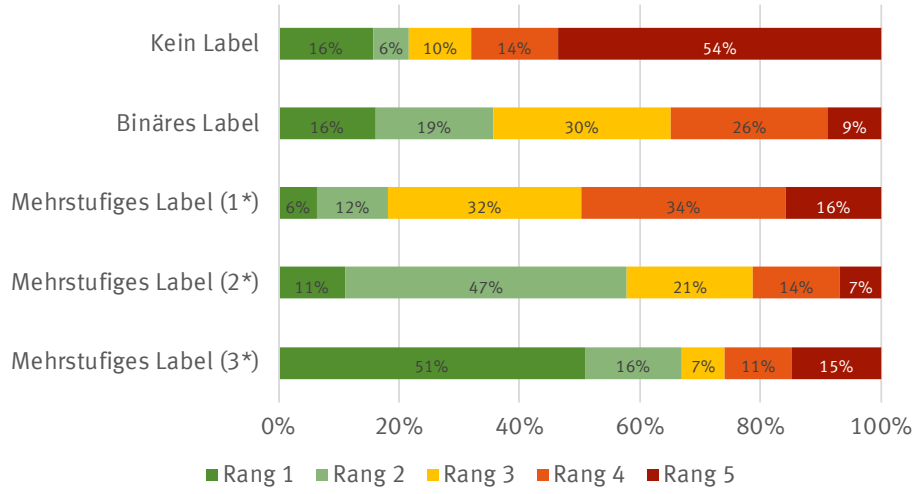

Abbildung 4: Bewertung IT-Sicherheitslabel: Einfache Ausführung – Ansteigender Preis.[57]

[57] Die Durchschnittsbewertung als Rang zwischen 1 (bester Rang und höchste Kaufwahrscheinlichkeit) und 5 (schlechtester Rang und somit niedrigste Kaufwahrscheinlichkeit) der einzelnen Produkte bzw. Labels war: Kein Label 3,8, binäres Label 2,9, mehrstufiges Label (1*) 3,4, mehrstufiges Laben (2*) 2,6 und mehrstufiges Label (3*) 2,2.

Interessant ist, dass sich die Reihenfolge der objektiv sichereren Produkte nicht verändert, obwohl diese teurer werden. Zwar kann man hieraus nicht ableiten, dass Verbraucher:innen in der Realität zwingend mehr für Sicherheit zahlen würden, aber die Analyse weist auf diese begrüßenswerten Tendenzen hin.

Dieses Ergebnis bestätigt sich auch, wenn man die Mittelwerte der einzelnen Produkte mit konstantem Preis und ansteigendem Preis vergleicht. Zwar deuten vereinzelte Tests auf signifikante Unterschiede hin, aber die Effektstärken sind maximal klein. Folglich lässt sich nicht stützen, dass der Preis die Bewertung / Rangreihenfolge systematisch beeinflusst.[58]

Ergebnis 5: Die Präferenzen der Nutzer:innen sind stabil, wenn ein erweitertes Label mit Informationen zur Verfügbarkeit von Sicherheitsupdates präsentiert wird.

Abbildung 5 zeigt die Bewertung der Kaufwahrscheinlichkeit für die Produkte, die mit einem erweiterten Label ausgestattet wurden. Zusätzlich zu den Informationen zum Sicherheitsniveau und der Prüfinstanz wurden Angaben zur Verfügbarkeit von Sicherheitsupdates angezeigt. Je sicherer das Produkt selbst war, desto länger standen auch Sicherheitsupdates zur Verfügung.

Auch in diesem Fall zeigen die Auswertungen, dass die Bewertung der Kaufwahrscheinlichkeit durch die Nutzer:innen unverändert ist. Je sicherer ein Produkt ist, desto höher ist auch die Kaufwahrscheinlichkeit (Durchschnitt und Median-Rang). Das binäre Label sowie das mehrstufige Label mit einem Stern teilen sich weiterhin den dritten Rang (Median), wobei die durchschnittliche Bewertung des binären Labels besser ist. Auf dem letzten Rang befindet sich weiterhin das unsicherste Produkt ohne Label.

[58] Bei den Tests (t Tests) wurde verglichen: Mehrstufiges Label mit drei Sternen für 99 EUR und mehrstufiges Label mit drei Sternen für 129 EUR, Mehrstufiges Label mit zwei Sternen für 99 EUR und mehrstufiges Label mit zwei Sternen für 119 EUR usw.

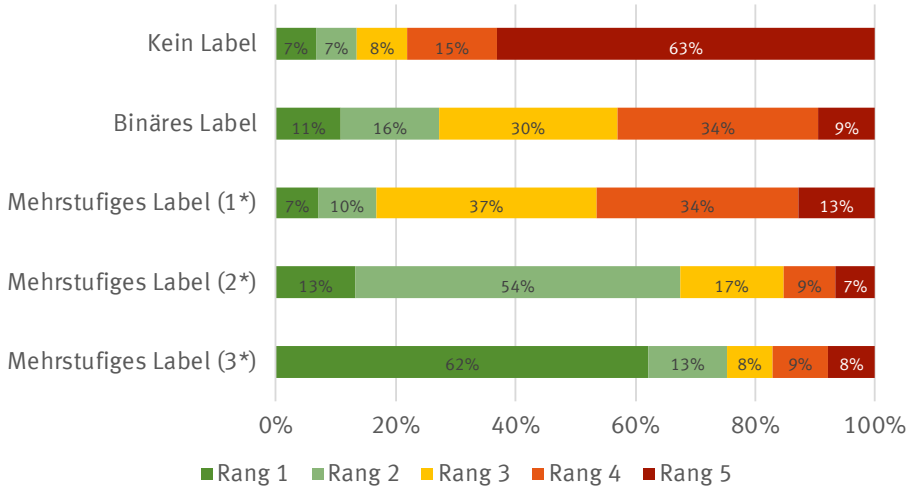

Abbildung 5: Bewertung IT-Sicherheitslabel: Erweiterte Ausführung – Konstanter Preis.[59]

Ergebnis 6: Auch beim erweiterten Label scheint der Preis keinen systematischen Einfluss auf die Kaufpräferenzen der Nutzer:innen zu haben.

Abbildung 6 zeigt die Ergebnisse der Bewertung der Kaufwahrscheinlichkeit (Rang) für das erweiterte Label mit ansteigendem Preis. Wie auch zuvor ist das unsicherste Produkt das günstigste und die Preise erhöhen sich schrittweise bis hin zum sichersten Produkt.

Auch hier sind die Bewertung und Reihenfolge der Produkte wie zuvor. Die durchschnittliche Kaufwahrscheinlichkeit des sichersten Produkts mit mehrstufigem Label und drei Sternen ist am höchsten. Hiernach folgt das mehrstufige Label mit zwei Sternen, das binäre Label und das mehrstufige Label mit einem Stern. Auf dem letzten Platz und somit das Produkt mit der geringsten Kaufwahrscheinlichkeit, ist das Produkt ohne Label.

Im Vergleich zur Experimentalbedingung mit konstantem Preis sind die Unterschiede in der Bewertung nicht systematisch.[60] Das heißt, dass auch in diesem Fall der Preis der Produkte keinen Einfluss auf die Kaufwahrscheinlichkeit der Nutzer:innen hat.

[59] Die Durchschnittsbewertung als Rang zwischen 1 (bester Rang und höchste Kaufwahrscheinlichkeit) und 5 (schlechtester Rang und somit niedrigste Kaufwahrscheinlichkeit) der einzelnen Produkte bzw. Labels war: Kein Label 4,2, binäres Label 3,1, mehrstufiges Label (1*) 3,4, mehrstufiges Laben (2*) 2,4 und mehrstufiges Label (3*) 1,9.

[60] In der Analyse können zwar vereinzelte signifikante Unterschiede festgestellt werden, aber diese sind nicht systematisch. Weiterhin sind die Effektstärken bei den vereinzelten, signifikanten Unterschieden sehr klein.

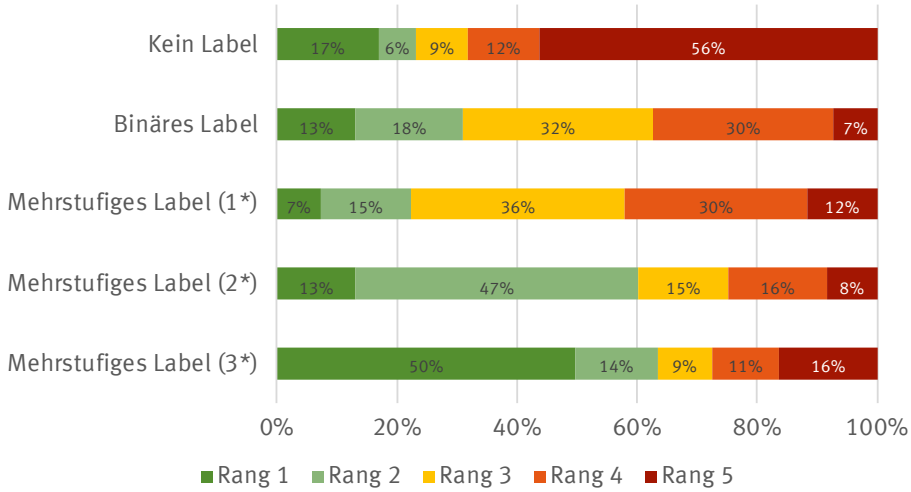

Abbildung 6: Bewertung IT-Sicherheitslabel: Erweiterte Ausführung – Ansteigender Preis.[61]

4.2.3. Zusammenhänge mit sozio-demografischen Attributen

Zusätzlich zur übergeordneten Auswertung der Daten wurden die Ergebnisse auch im Hinblick auf etwaige Zusammenhänge mit sozio-demografischen Attributen der Befragten überprüft.[62] Dabei ist festzustellen, dass die Kenntnis von unterschiedlichen Technologiebegriffen, als Indikator für die digitale Affinität der Befragten, positiv mit der Bewertung des sichersten Produkts zusammenhängt. Das bedeutet, **je besser sich Verbraucher:innen mit der Digitalisierung** an sich **auskennen, desto wahrscheinlicher ist es** auch**, dass sie das sicherste Produkt kaufen würden.** Einen ähnlichen Zusammenhang kann man auch für die Anzahl der genutzten, smarten Geräte feststellen. Je mehr IoT-Geräte Befragte besitzen, desto eher würden sie auch das sicherste Produkt kaufen.

4.2.4. Fazit: Kennzeichen, die Informationen zur Sicherheit von IoT-Geräten enthalten, haben die gewünschte Wirkung

Die Ergebnisse der Befragung zeigen, dass **Label bzw. Sicherheitskennzeichen**, die Nutzer:innen über die Sicherheit von digitalen Geräten informieren, scheinbar die **gewünschte Wirkung haben**: Bei konstantem Preis präferieren Verbraucher:innen Produkte, die einen höheren Sicherheitsstandard erfüllen gegenüber unsicheren Produkten. Produkte, deren Sicherheit nicht geprüft wurde – die somit auch kein Sicherheitskennzeichen tragen – werden am schlechtesten bewertet. Außerdem werden Produkte, deren Sicherheit von unabhängiger Stelle zertifiziert wird,

[61] Die Durchschnittsbewertung als Rang zwischen 1 (bester Rang und höchste Kaufwahrscheinlichkeit) und 5 (schlechtester Rang und somit niedrigste Kaufwahrscheinlichkeit) der einzelnen Produkte bzw. Labels war: Kein Label 3,8, binäres Label 3,0, mehrstufiges Label (1*) 3,2, mehrstufiges Laben (2*) 2,6 und mehrstufiges Label (3*) 2,3.

[62] Es werden lediglich statistisch signifikante Ergebnisse (mind. $p<5\%$) präsentiert. Bei Gruppenvergleichen basieren die Ergebnisse auf Chi^2-Tests und bei metrischen Variablen wurden Logistische Regressionsanalysen verwendet.

Produkten vorgezogen, deren Sicherheit durch den Hersteller bescheinigt wird. Positiv hervorzuheben ist außerdem, dass die **Präferenzen der Verbraucher:innen stabil** sind, wenn der **Preis für Sicherheit höher ist**.[63]

Zusätzlich konnte die Befragung zeigen, dass die **Kaufpräferenzen** der Verbraucher:innen auch **stabil** sind, wenn **erweiterte Informationen zur Verfügbarkeit von Updates** auf dem Label **aufgenommen** werden. Sie schaden also nicht, haben aber auch keine bessere Wirkung auf die Kaufentscheidung der Verbraucher:innen. Weiterhin wurden sichere Produkte unsicheren Produkten vorgezogen und dies unabhängig von Preis der Produkte.

Insgesamt ist beim Einsatz von Labeln wichtig eine **einfache und intuitive Botschaft zur Sicherheit**, bspw. „ja oder nein“ bzw. auf einer Skala (in Sternen), zu transportieren. Dies erleichtert es Verbraucher:innen Produkte zu wählen, die sicher sind. Dabei sollte auch auf die Menge der Information geachtet werden und darauf, dass auch Verbraucher:innen unterstützt werden, die weniger digital-affin sind. Darüber hinaus ist es nicht notwendig, das Kennzeichen mit überbordenden Informationen vollzupacken.

4.3. Teil 2: Inbetriebnahme von IoT-Geräten

Im zweiten Teil der Befragung wurden die Proband:innen gebeten, Angaben zu ihrem **Verhalten vor der ersten Nutzung bzw. der Inbetriebnahme** eines digitalen Geräts zu machen.

Die konkreten Forschungsfragen waren:

- Wer richtet digitale Geräte vor der ersten Nutzung ein? Setzen Nutzer:innen dies selbst um oder übergeben sie die Inbetriebnahme an Dritte, wie Personen in ihrem persönlichen Umfeld oder externe Dienstleister?
- Nehmen Nutzer:innen vor der Nutzung besondere Sicherheitseinstellungen vor? Wenn ja, welche sind dies?
- Welche Gründe gibt es, die Inbetriebnahme Dritten zu überlassen?
- Spielt es für das Verhalten der Nutzer:innen eine Rolle, um welches digitale Gerät es sich handelt?

[63] Hier muss jedoch angemerkt werden, dass die Ergebnisse der Befragung lediglich auf hypothetischen Entscheidungen fußen, d.h. die Kaufentscheidung wurde nicht in der Praxis tatsächlich vollzogen. Durch das Befragungsdesign wurde allerdings die Kaufsituation sehr realistisch simuliert . Diese Methode hat sich in der Forschung bewährt und entspricht wissenschaftlichen Standards.

4.3.1. Methodik

Aus den vorangegangen formulierten Forschungsfragen wurden mehrere **geschlossene Fragen** abgeleitet und den Teilnehmer:innen gestellt. Um etwaige **Unterschiede im Hinblick auf Produktarten** zu untersuchen, wurden die Teilnehmer:innen in drei Gruppen eingeteilt, jeweils mit einer Zufallswahrscheinlichkeit von einem Drittel. Die erste Gruppe beantwortete die Fragen zur Inbetriebnahme eines **Routers**, die zweite Gruppe mit Fokus auf ein **Smartphone** und die dritte Gruppe im Hinblick auf einen **Smart TV**.

Darüber hinaus wurden die Befragten nach ihrer **persönlichen und konkreten Erfahrung** mit der Inbetriebnahme eines solchen Gerätes gefiltert. So wurde zu Beginn des Fragekomplexes danach gefiltert, ob die Befragten in den vergangenen fünf Jahren ein digitales Gerät gekauft oder gemietet haben und somit bei den anschließenden Fragen über ihr reales Verhalten berichten konnten.[64]

Die Ergebnisse, die im Folgenden berichtet werden, umfassen N=205 Observationen bei der Inbetriebnahme eines Routers, N=260 Observationen bei der Inbetriebnahme eines Smartphones und N=159 Observationen bei der Inbetriebnahme eines Smart TVs.

4.3.2. Ergebnisse

Ergebnis 7: Die Mehrheit der Nutzer:innen richtet ihr vernetztes Gerät vor der ersten Nutzung selbst ein, gefolgt von einer Einrichtung von Personen aus dem persönlichen Umfeld. Externe werden dabei eher selten beauftragt.

Abbildung 7 zeigt die Verantwortlichkeit bei der Inbetriebnahme nach Produkt. Für alle drei Produkte gilt, dass die Mehrheit der Nutzer:innen das Gerät vor der ersten Nutzung selbst in Betrieb nimmt. Der Anteil ist beim Router mit 62% etwas geringer als beim Smartphone (75%) und Smart TV (72%). Umgekehrt fällt auf, dass der Router häufiger vom Anbieter bzw. Händler eingerichtet wird (12%). Bei Smartphone (3%) und Smart TV (5%) sind die Anteile geringer. Über alle Produkte hinweg übernehmen in gut einem Fünftel der Fälle Familienangehörige oder Bekannte die Einrichtung. Der summierte Anteil für den Router liegt bei 22%, für das Smartphone bei 21% und für den Smart TV bei 22%. In den seltensten Fällen werden externe Dienstleister mit der Einrichtung beauftragt. Beim Router sind dies 3%, beim Smart TV 1% und beim Smartphone ‹1%.

[64] Der Zeitraum von fünf Jahren wurde gewählt, um zu gewährleisten, dass sich die Befragten noch konkret an den Vorgang bei der Inbetriebnahme erinnern konnten. Weiterhin sollte der Zeitraum zumindest so breit gewählt sein, dass eine Neuanschaffung bzw. der Ersatz eines vorhandenen Geräts realistisch ist. Um zu vermeiden, dass zu wenige Befragte aus ihrer persönlichen und konkreten Erfahrung berichten konnten, wurde außerdem ein hypothetisches Szenario parallel zum realen Szenario formuliert. Da die Anzahl der Observationen in den drei Produktkategorien jedoch ausreichend ist, wird im Folgenden nur das tatsächliche Verhalten berichtet.

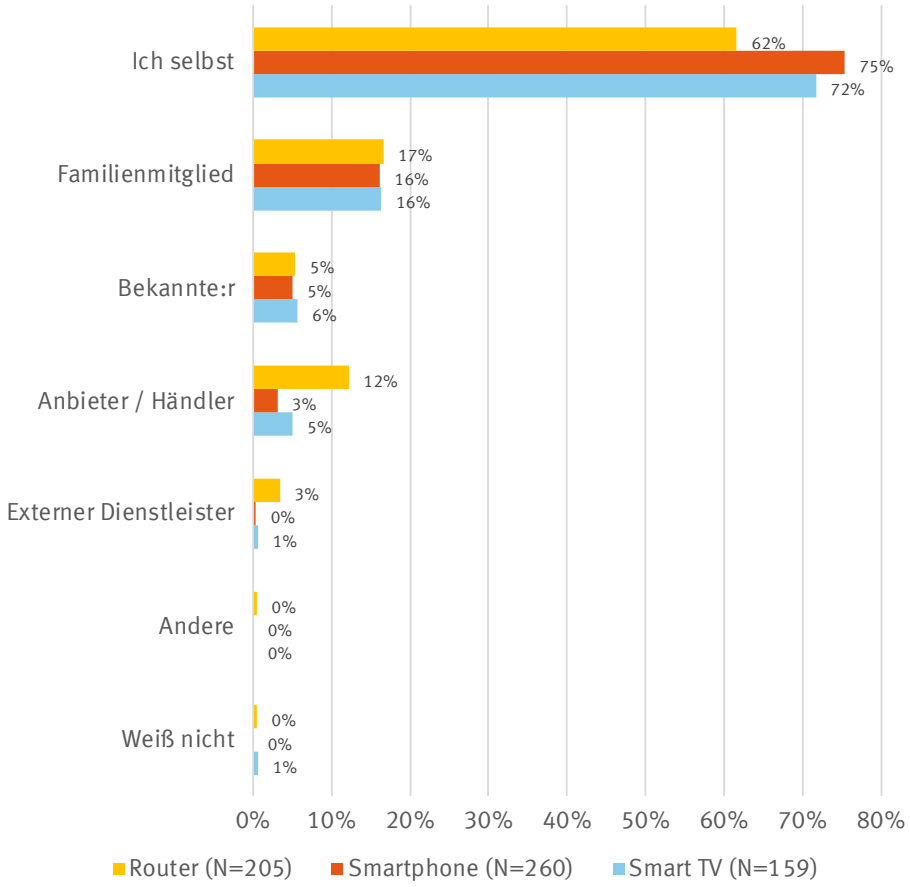

Abbildung 7: Verantwortung für die Inbetriebnahme.

Ergebnis 8: Die Mehrheit der selbständig-einrichtenden Nutzer:innen nimmt zusätzliche Sicherheitsanpassungen vor der ersten Nutzung vor. Die Häufigkeit unterscheidet sich dabei von Produkt zu Produkt.

Abbildung 8 zeigt den Anteil der Nutzer:innen, die selbst Sicherheitsanpassungen vor der ersten Nutzung vornehmen, nach Produktkategorie. Über alle drei Produkte hinweg gibt die Mehrheit an, dass sie solche Sicherheitsanpassungen vornimmt, jedoch sind die Anteile je nach Produktkategorie unterschiedlich. Der Anteil an Sicherheitsanpassungen bei Smartphone-Besitzer:innen liegt bei 84%, gefolgt von 73% beim Smart TV und 62% beim Router.

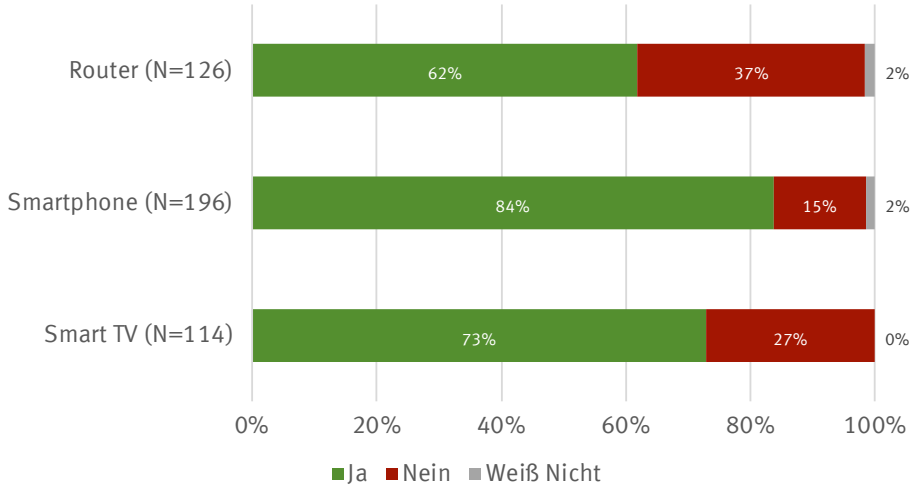

Abbildung 8: Sicherheitsanpassung vor der ersten Nutzung.

Zusätzlich wurden die Befragten, die angaben, persönliche Sicherheitsanpassungen vor der ersten Nutzung vorzunehmen, gebeten diese in einem offenen Textfeld zu benennen. Beim Router gaben 34% dieser Befragten an, das Passwort ihres Routers angepasst zu haben, weitere 30% benannten zusätzliche Sicherheitsvorkehrungen wie bspw. die Änderung des Verschlüsselungsverfahrens oder individuelle Einstellungen für den Zugang der Geräte, die im Haushalt von Kindern genutzt werden. 49% machten uneindeutige oder unkonkrete Angaben. Beim Smartphone gaben 27% der Nutzer:innen an, dass sie einen zusätzlichen Virenschutz auf ihrem Gerät installiert haben, 20% erwähnten einen gesonderten PIN-Schutz des Gerätes, 13% biometrische Sicherheitsverfahren zum Entsperren der Geräte und 12% sonstige Anpassungen, wie 2-Faktor-Authentisierung oder Updateeinstellungen. 40% machten wiederum uneindeutige oder unkonkrete Angaben. Beim Smart TV gaben 13% der Nutzer:innen an, dass sie eine Passwort- oder PIN-Sicherung für ihr Gerät eingerichtet haben. 33% nannten weitere Aspekte, wie eine Kindersicherung des Geräts oder die Einstellung, dass sonstige mobile Geräte im Haushalt sich nicht mit dem Smart TV koppeln dürfen. 54% der Befragten machten uneindeutige oder unkonkrete Angaben.

Ergebnis 9: Insbesondere Unverständlichkeit und eine hohe Komplexität hindern Nutzer:innen daran, Geräte nicht alleinständig einzurichten. Auch Sorgen vor Fehlern bei der Einrichtung zählen zu häufigen Hinderungsgründen.

Wie in Abbildung 9 dargestellt, übergeben 30% der Nutzer:innen die Einrichtung ihrer smarten Geräte an Dritte, wie Personen in ihrem direkten Umfeld oder den Anbieter / Dienstleister. Abbildung 9 zeigt die Begründungen der Befragten, ihre digitalen Geräte nicht selbstständig einzurichten. Über alle drei Produkte hinweg geben 31% der Nutzer:innen an, dass sie nicht verstehen, was sie bei einer Einrichtung tun müssen. 28% geben an, dass die Einrichtung ihnen zu kompliziert sei, wobei diese Begründung für das Smartphone und den Smart TV mit 33% bzw. 34% häufiger genannt wird als für den Router mit 22%. Weitere 26% geben an,

dass sie Angst haben, die Einstellungen des Geräts bei der Einrichtung zu verändern, so dass dieses nicht mehr funktioniert. Für das Smartphone liegt dieser Anteil sogar bei 39%, beim Router im Vergleich dazu nur bei 21% und beim Smart TV bei 18%. Immerhin 22% der Nutzer:innen geben über alle drei Produkte hinweg an, dass sie die Einrichtung nerve, so dass sie diese an eine dritte Person abtreten. Weitere Gründe spielen eine untergeordnete Rolle und können der Abbildung entnommen werden.

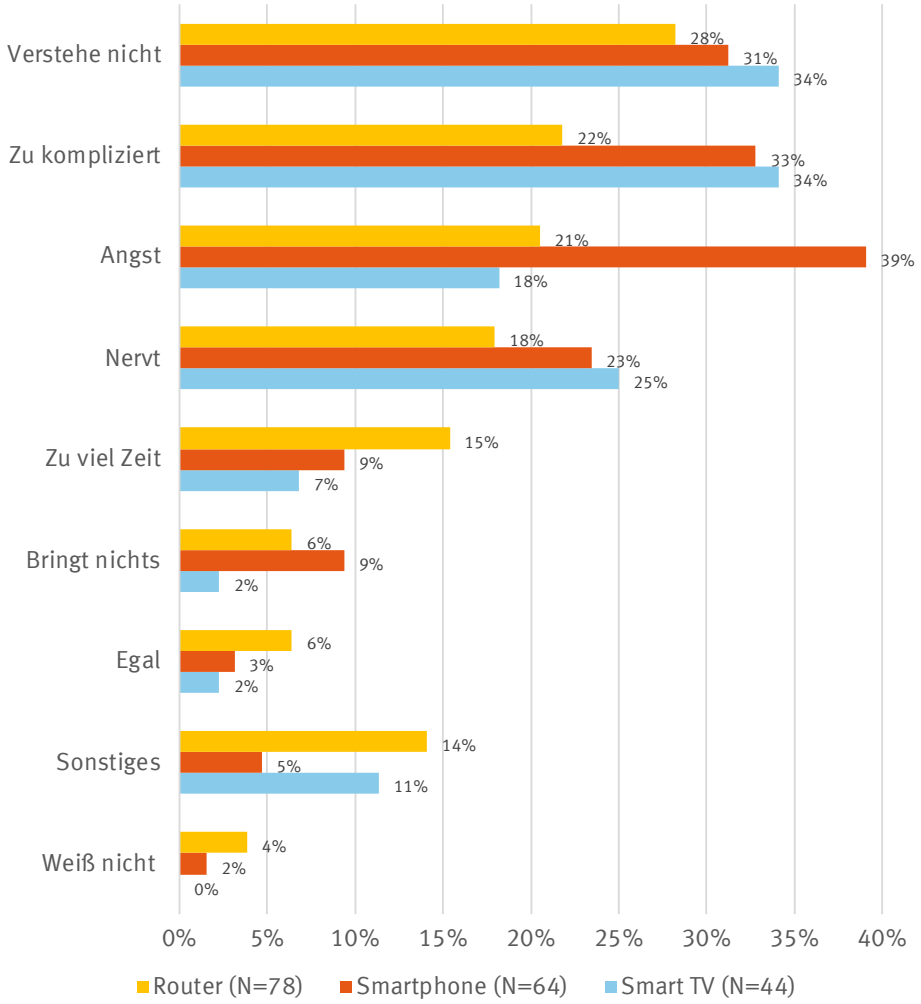

Abbildung 9: Gründe, ein IoT-Gerät nicht selbst einzurichten.

4.3.3. Zusammenhänge mit sozio-demografischen Attributen

Eine weitergehende Analyse im Hinblick auf Zusammenhänge mit den erhobenen sozio-demografischen Variablen, ergibt zusätzlich spannende Erkenntnisse.[65] So richten **männliche Nutzer ihre Geräte häufiger selbst** ein als weibliche Nutzerin-

[65] Es werden lediglich statistisch signifikante Ergebnisse (mind. p<5%) präsentiert. Bei Gruppenvergleichen basieren die Ergebnisse auf Chi ²-Tests und bei metrischen Variablen wurden logistische Regressionsanalysen verwendet.

nen (79% versus 60%). Darüber hinaus steht das Alter in Jahren in einem negativen Zusammenhang mit der Wahrscheinlichkeit, das eigene digitale Gerät selbst einzurichten, d.h. **je höher das Alter, desto unwahrscheinlicher ist eine selbstständige Einrichtung**. Im Hinblick auf die **digitale Affinität**, die sich in der Anzahl der smarten Geräte im Zuhause, der Kenntnis unterschiedlicher Technologien und Technikbegriffe sowie der Nutzung von bestimmten Schutzmaßnahmen widerspiegelt, ist ein **positiver Zusammenhang mit der Wahrscheinlichkeit das eigene Gerät selbst einzurichten** festzustellen. Das bedeutet, (1) je mehr Geräte Nutzer:innen besitzen, (2) je besser der Kenntnisstand von Nutzer:innen im Hinblick auf diverse Technologien ist, und (3) je häufiger Nutzer:innen Schutzmaßnahmen zur Datensicherheit ergreifen, desto wahrscheinlicher ist es, dass sie ein digitales Gerät selbst einrichten.

4.3.4. Fazit: Die Inbetriebnahme erfolgt mehrheitlich selbstständig und zusätzliche Sicherheitseinstellungen werden vor der ersten Nutzung häufig vorgenommen

Die Befragung konnte zeigen, dass die **Mehrheit der Nutzer:innen die Einrichtung ihrer IoT-Geräte selbst in die Hand nimmt und auch zusätzliche Sicherheitseinstellungen vornimmt**. Dies trifft insbesondere auf digitale Produkte wie das Smartphone zu, das einen präsenten Begleiter für viele Nutzer:innen darstellt und sich in vielen Fällen auch durch nutzerfreundliche Bedienoberflächen (Betriebssysteme wie Android oder iOS) auszeichnet. Aber auch Router werden mehrheitlich selbst eingerichtet.

Während die Einrichtung durch Dienstleister oder den Hersteller sehr selten vorkommt, übergeben Verbraucher:innen die Einrichtung teilweise auch an **Personen in** ihrem **persönlichen Umfeld**. Dies trifft insbesondere auf **ältere Verbraucher:innen** zu und auf solche, die **weniger digital-affin** sind. Die Gründe für die Übergabe an Familie, Freunde oder Bekannte sind dabei insbesondere **Unverständlichkeit und eine hohe Komplexität** der Einrichtung. Teilweise sorgen sich Verbraucher:innen auch davor, Fehler bei der Einrichtung zu machen.

4.4. Teil 3: Nutzung und Updates von IoT-Geräten

Im dritten Teil der Befragung wurden die Teilnehmer:innen gebeten, Angaben zu ihrem **Sicherheitsverhalten während der Nutzung** zu machen. Dies umfasste insbesondere **Sicherheitsupdates**, die die Sicherheit während der Nutzung des Gerätes gewährleisten sollen.

Die konkreten Forschungsfragen waren:

- Werden digitale Geräte regelmäßig durch Nutzer:innen geupdatet? Wer übernimmt die Verantwortung für Updates?
- Empfinden Nutzer:innen, die ihre IoT-Geräte selbst updaten, diese Aufgabe als einfach oder schwer?

- Welche Gründe gibt es, dass Updates an Dritte übergeben werden? Welche Gründe gibt es, dass Updates überhaupt nicht durchgeführt werden?
- Spielt es für das Verhalten der Nutzer:innen eine Rolle, um welches digitale Gerät es sich handelt?

4.4.1. Methodik

Zur Beantwortung der formulierten Forschungsfragen wurden ebenfalls **geschlossene Fragen** entwickelt und an die Teilnehmer:innen gerichtet. So wie bereits im zweiten Teil der Befragung wurden die Teilnehmer:innen **drei unterschiedlichen Produktgruppen**, nämlich Router, Smartphone und Smart TV zugeteilt, um etwaige Produktunterschiede untersuchen zu können. Die Befragten verblieben im dritten Teil also den Produktgruppen, denen sie bereits zufällig im zweiten Teil zugeordnet wurden.

Weiterhin wurden die Befragten nach ihren **persönlichen und konkreten Erfahrungen** in der Nutzung der digitalen Geräte befragt. Die Filterfrage war, ob die Teilnehmer:innen das digitale Produkt besitzen.

Die Ergebnisse, die im Folgenden berichtet werden, umfassen N=305 Observationen bei der Inbetriebnahme eines Routers, N=313 Observationen bei der Inbetriebnahme eines Smartphones und N=242 Observationen bei der Inbetriebnahme eines Smart TVs.

4.4.2. Ergebnisse

Ergebnis 10: Digitale Geräte werden regelmäßig von Nutzer:innen geupdatet. Dies geschieht entweder in Eigenregie oder wird vom Gerät automatisch durchgeführt.

Abbildung 10 zeigt das Updateverhalten der Nutzer:innen im Gebrauch. Unabhängig vom Produkt geben 90% der Befragten an, dass ihr Gerät regelmäßig ein Update erhält. Beim Smartphone übernimmt die Mehrheit von 55% der Nutzer:innen das Update selbst, beim Smart TV sind es immerhin 42% und beim Router mit 30% knapp ein Drittel. Automatische Geräte-Updates finden im Falle des Routers in 45% der Fälle statt, beim Smart TV liegt der Anteil bei 36% und beim Smartphone bei 33%. Sehr selten, d.h. über alle Produkte hinweg in knapp 10% der Fälle, wird das Update von einer anderen Person übernommen.

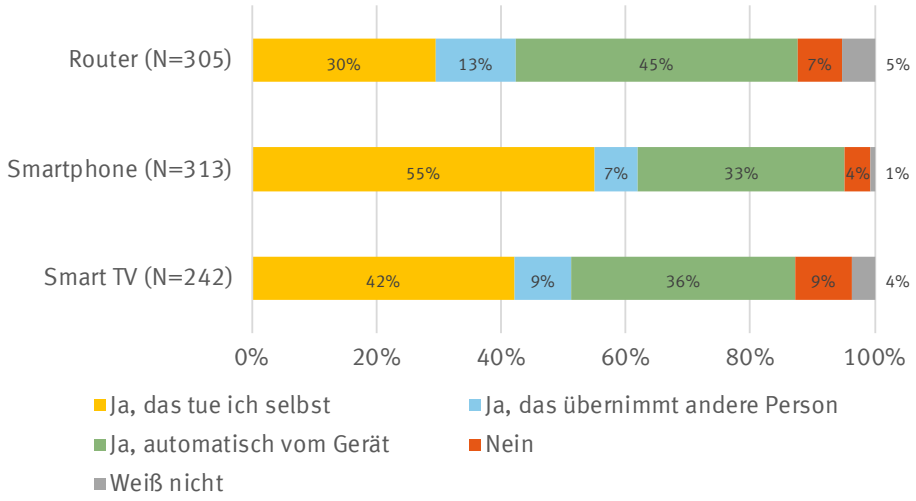

Abbildung 10: Durchführung und Verantwortung für Updates.

Ergebnis 11: Im Durchschnitt empfinden Nutzer:innen die Umsetzung von Updates als eher einfach.

Nutzer:innen, die angaben, dass sie Updates an ihrem Gerät selbstständig durchführen, wurden gebeten, die Umsetzung zu bewerten. Dies erfolgte auf einer 5er-Skala von 1 „sehr schwer“ bis 5 „sehr einfach“. Der Median für alle Produkte lag dabei bei 4 („eher einfach“).[66]

Ergebnis 12: Updates, die von Dritten übernommen werden, entfallen am häufigsten auf persönliche Kontakte und weniger auf Externe.

Wie bereits angegeben, werden lediglich 10% der Updates von Dritten übernommen. Abbildung 11 zeigt, welche Anteile hierbei auf unterschiedliche Personengruppen entfallen und dass es Unterschiede in den Produktgruppen gibt. 95% der Stellvertreter-Updates von Smart TVs werden von Personen im persönlichen Umfeld (Familie, Bekannte) übernommen, bei Routern sind es 82% und beim Smartphone 68%. Umgekehrt liegt der Anteil der Smart TV-Updates zu 5% bei externen Personen (Anbieter oder externe Dienstleister), bei Routern sind es 15% und bei Smartphones 32%.

Wichtig ist hierbei jedoch anzumerken, dass die Ergebnisse auf sehr wenigen Observationen basieren und entsprechend Einzelmeinungen stärker ins Gewicht fallen. Die Ergebnisse decken sich jedoch mit den Zahlen zur Inbetriebnahme, so dass davon ausgegangen werden kann, dass insbesondere Dritte aus dem persönlichen Umfeld die Sicherheitseinstellungen während der Nutzungsphase übernehmen und nicht externe Personen.

[66] Der Mittelwert für den Router lag bei 3,63, für den Smart TV bei 3,9 und für das Smartphone bei 4,0.

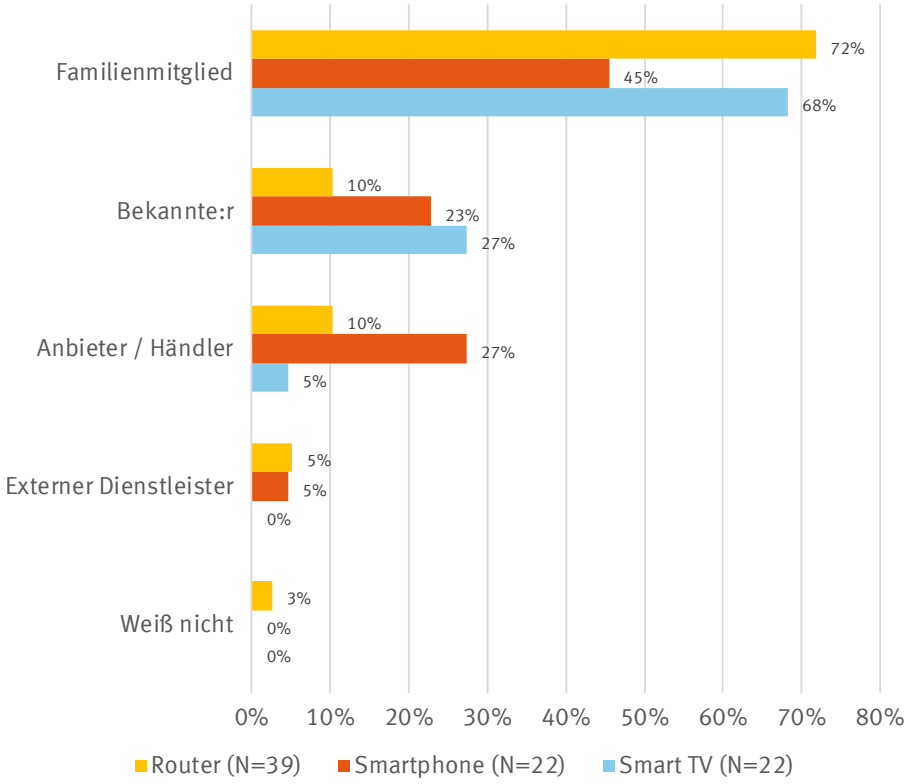

Abbildung 11: Übernahme der Updates durch eine andere Person.

Ergebnis 13: Insbesondere Unverständlichkeit, Angst und hohe Komplexität sorgen dafür, dass Nutzer:innen Updates an Dritte auslagern.

Abbildung 12 zeigt die Gründe, die Nutzer:innen angeben, wenn sie Updates an Dritte abgeben. Auch hier ist wichtig zu betonen, dass die Ergebnisse auf einer geringen Anzahl von Observationen basieren, da nur sehr wenige Befragte diese Aufgabe überhaupt an Dritte abtreten. Somit fallen vereinzelte Angaben stärker ins Gewicht, jedoch deckt sich das Bild mit den Gründen, die auch bei der Inbetriebnahme angegeben wurden.

Über alle drei Produkte hinweg geben 33% der Befragten an, dass sie nicht verstehen, was bei einem Update zu tun sei und sie die Aufgabe deshalb übergeben würden. 30% geben außerdem an, dass sie besorgt seien, dass sie durch die Updates die Einstellungen des Geräts so verändern, dass es nicht mehr funktioniere. Weitere 22% geben an, dass ihnen Updates zu kompliziert sein.

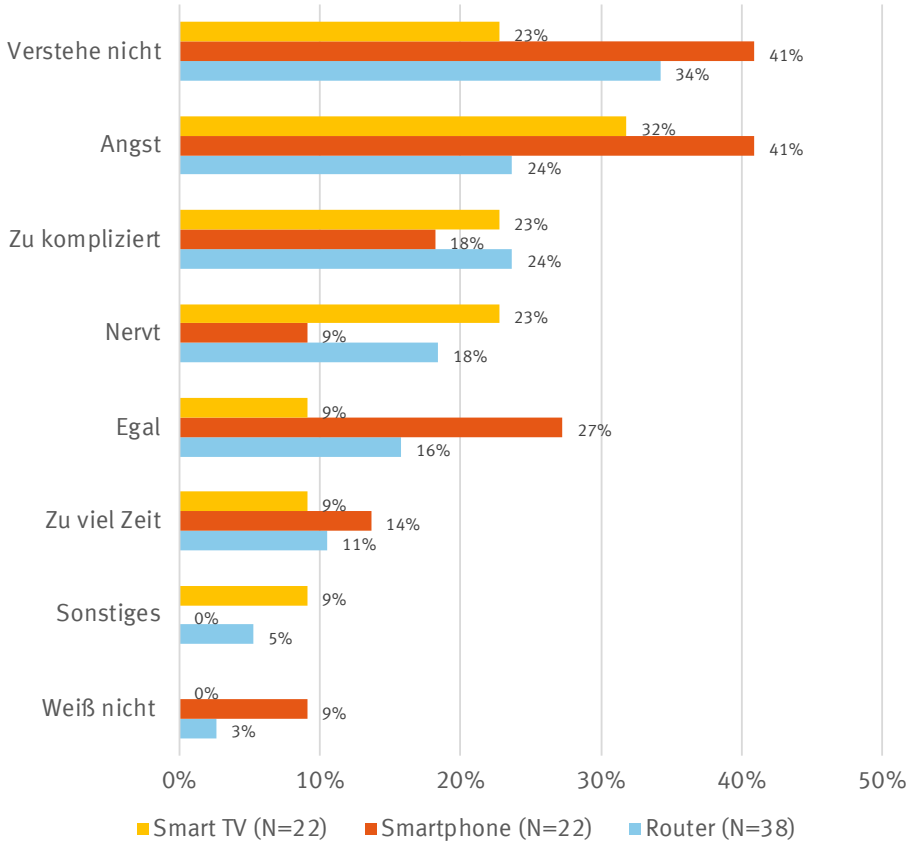

Abbildung 12: Gründe für die Auslagerung der Updates an eine andere Person.

Ergebnis 14: Ähnliche Gründe werden dafür genannt, dass Nutzer:innen gar keine Updates umsetzen.

Abbildung 13 zeigt Begründungen dafür, dass Nutzer:innen keine Updates durchführen, d.h. weder selbstständig noch durch Dritte. Zuerst ist zu beachten, dass der Anteil der Nutzer:innen, die gar keine Updates durchführen, mit 7% über alle Produkte hinweg sehr gering ist (vgl. Ergebnis 10).

26% der Nutzer:innen geben an, dass Angst, dass das Gerät nach dem Update nicht mehr funktionieren könnte, ein Hinderungsgrund für sie sei. 25% geben an, dass sie nicht verstehen, was bei einem Update zu tun sei.

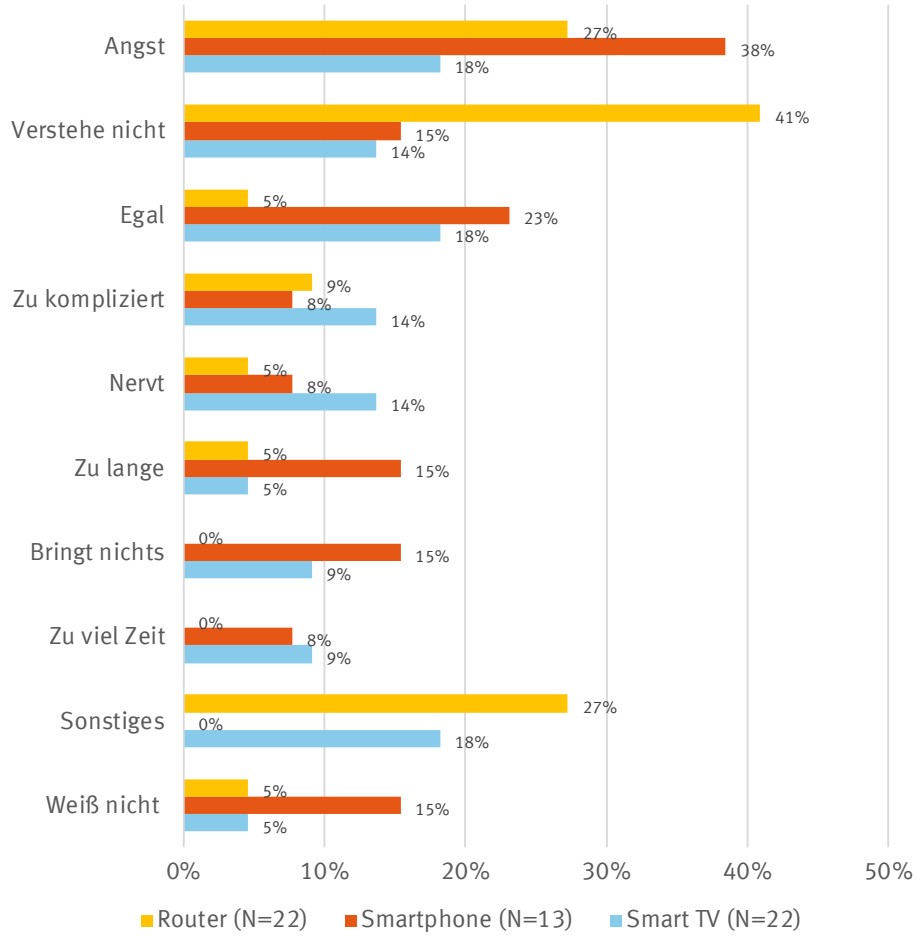

Abbildung 13: Gründe keine Updates durchzuführen.

4.4.3. Zusammenhänge mit sozio-demografischen Attributen

Auch im Hinblick auf die zusätzliche erhobenen sozio-demografischen Attribute der Befragten, ergeben sich spannende Erkenntnisse.[67] Diese decken sich stark mit den Ergebnissen zum Verhalten bei der Inbetriebnahme und zeichnen ein klares Bild, welche Nutzer:innen die Sicherheit bei der Nutzung digitaler Geräte mehr oder weniger in die eigene Hand nehmen.

Zum einen kann ein negativer Zusammenhang zwischen Alter und Updatewahrscheinlichkeit festgestellt werden, d.h. **je älter die Nutzer:innen, desto unwahrscheinlicher ist es, dass ihre Geräte Sicherheitsaktualisierungen erhalten**. Zum anderen gibt es einen **positiven Zusammenhang zwischen der digitalen Affinität**, d.h. Anzahl der Geräte, Kenntnis von Technologien sowie ergriffene Schutzmaßnahmen, und der **Wahrscheinlichkeit Sicherheitsupdates durchzuführen**. Konkret bedeutet dies, (1) je mehr Geräte Verbraucher:innen zuhause besitzen, (2) je bes-

[67] Es werden lediglich statistisch signifikante Ergebnisse (mind. p<5%) präsentiert. Bei Gruppenvergleichen basieren die Ergebnisse auf Chi ^{2}-Tests und bei metrischen Variablen wurden logistische Regressionsanalysen verwendet.

ser sie sich mit digitalen Technologien auskennen und (3) je mehr Schutzmaßnahmen sie in ihrem digitalen Privatleben nutzen, desto wahrscheinlicher ist es auch, dass sie Updates an ihren digitalen Geräten, d.h. Router, Smartphone und Smart TV, durchführen.

4.4.4. Fazit: Das Updateverhalten bei der Nutzung von digitalen Geräten ist insgesamt positiv. Die Mehrheit der Geräte erhält regelmäßig Sicherheitsaktualisierungen.

Insgesamt zeigt die Befragung, dass der Großteil der **Nutzer:innen IoT-Geräte regelmäßig updatet und Sicherheitsaktualisierungen während der Nutzung installiert.** Dies geschieht entweder in Eigenregie oder wird ohnehin automatisch vom Gerät übernommen.

Nur selten werden Updates **an Dritte ausgelagert**. Häufig handelt es sich bei Nutzer:innen, die Updates nicht selbst durchführen, um **ältere Verbraucher:innen und solche, die weniger digital-affin sind**. Als **Gründe** werden, wie auch bei der Inbetriebnahme von IoT-Geräten, **Unverständlichkeit**, **Angst** vor Fehlern und **hohe Komplexität** genannt. Positiv ist außerdem hervorzuheben, dass Nutzer:innen nur sehr selten Updates explizit nicht installieren.

4.5. Teil 4: Verantwortung für die Sicherheit und Erwartungen an den Gesetzgeber

Der vierte Befragungsteil befasste sich mit der **Verantwortung für die Sicherheit digitaler Geräte** und **Erwartungen** der Nutzer:innen **an die Gesetzgebung** und Transparenz bei der Kommunikation von Sicherheitsaspekten digitaler Produkte.

Die konkreten Forschungsfragen waren:

- Sind Nutzer:innen bereit etwas für die Sicherheit ihrer digitalen Produkte zu tun?
- Wer trägt aus Sicht der Nutzer:innen die Verantwortung im Hinblick auf die Sicherheit ihrer digitalen Geräte? Wie viel Verantwortung sehen sie bei sich selbst, wie viel bei den Herstellern und wie viel beim Gesetzgeber?
- Welche Erwartungen haben Nutzer:innen bzgl. stärkerer Anforderungen, d.h. Gesetze oder Normen, an digitale Geräte sowie der Transparenz von IT-Sicherheitsaspekten.

4.5.1. Methodik

Um die Forschungsfragen zu beantworten, wurden **geschlossene Fragen** konzeptioniert und von den Teilnehmer:innen beantwortet. Im vierten Teil der Befragung gab es **keine zusätzliche Filterung** der Befragten, so dass zu allen Fragen N=995 Observationen vorliegen.

4.5.2. Ergebnisse

Ergebnis 15: Nutzer:innen sind grundsätzlich bereit ihre Passwörter regelmäßig zu ändern – aber nicht unter jeder Bedingung.

Zuerst wurden die Teilnehmer:innen zu ihrer grundsätzlichen Bereitschaft befragt, alle ihre Passwörter, bspw. für Konten wie E-Mail, Social Media, Online-Shopping, regelmäßig zu ändern. 44% der Verbraucher:innen gaben an, dass sie (sozusagen uneingeschränkt) bereit seien, ihre Passwörter regelmäßig zu ändern. Weitere 39% gaben an, dass sie dies nur tun würden, wenn sie vom Anbieter bzw. System hierzu gezwungen würden. Lediglich 13% gaben an, dass sie nicht hierzu bereit wären und 3% machten keine Angabe.

Die Analysen zeigen insgesamt eine hohe Bereitschaft der Eigenverantwortung und spiegeln sich ebenfalls im bereits berichteten tatsächlichen Verhalten der Nutzer:innen wider. So gaben 90% der Nutzer:innen an, dass entweder sie selbst oder eine von ihnen beauftragte Person Updates durchführe oder Updates automatisch installiert werden (vgl. Abbildung 10).

Ergebnis 16: Nutzer:innen sehen die Hauptverantwortung für die Sicherheit ihrer Geräte bei sich selbst.

Im Hinblick auf die Sicherheit von digitalen Geräten und Diensten gibt es unterschiedliche Verantwortliche. Zum einen tragen Nutzer:innen die Verantwortung für die Gerätesicherheit selbst, bspw. indem sie unsichere Verhaltensweisen vermeiden. Zum anderen liegt die Verantwortung beim Hersteller oder Anbieter des Geräts, indem bspw. Sicherheitslücken, die von externen Angreifern genutzt werden können, vermieden werden. Außerdem existiert eine externe, auf Regulierung basierende Verantwortung beim Gesetzgeber, der dafür sorgt, dass bspw. konkrete Sicherheitsanforderungen an Produkte eingehalten werden oder unsichere Produkte vom Markt ausgeschlossen werden. Um die Frage zu beantworten, zu welchem Anteil diese drei Gruppen aus Sicht der Nutzer:innen Verantwortung tragen, wurden die Befragten gebeten, die Gesamtverantwortung (in 100%) über die drei Gruppen aufzuteilen. Sie gaben also an, welcher Anteil der Verantwortung bei der Sicherheit ihrer digitalen Geräte auf sie selbst, den Anbieter sowie den Gesetzgeber entfällt.

Abbildung 14 zeigt die durchschnittlichen Verantwortungsanteile für die Sicherheit der genutzten Geräte und Services. Mit 52% wird durchschnittlich über die Hälfte der Gesamtverantwortung bei den Nutzer:innen selbst gesehen. 30% der Verantwortung entfällt auf Anbieter bzw. Hersteller der Geräte und Services und 18% auf den Gesetzgeber.

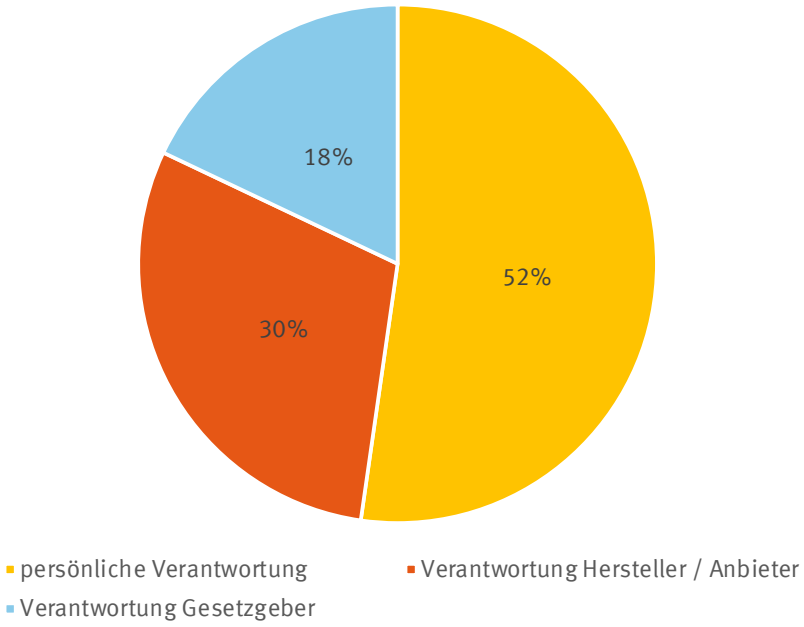

Abbildung 14: Verantwortung für Sicherheit von IoT-Geräten.

Ergebnis 17: Nutzer:innen wünschen sich grundsätzlich stärkere Anforderungen, d.h. Gesetze oder Normen bezüglich digitaler Geräte sowie mehr Transparenz zu den IT-Sicherheitsaspekten von Produkten.

Darüber hinaus wurden die Befragten nach ihren Erwartungen an die Zulassung von Produkten sowie die Transparenz von IT-Sicherheitsaspekten befragt. Die erste Frage bezog sich dabei auf den Wunsch nach stärkeren Anforderungen hinsichtlich der Sicherheit von digitalen Produkten, bspw. durch Normen oder Gesetze. 63% der Verbraucher:innen bejahten den Wunsch nach stärkeren Anforderungen an die IT-Sicherheit von Produkten, 28% verneinten dies und 9% waren sich unsicher.

Die zweite Frage bezog sich auf den Wunsch nach mehr Transparenz zu IT-Sicherheitsaspekten von Produkten oder Anwendungen. Auch hier gab die Mehrheit (74%) der Nutzer:innen an, dass sie sich mehr Transparenz wünschen. 19% teilten diesen Wunsch nicht und 7% machten keine Angabe hierzu.

4.5.3. Zusammenhänge mit sozio-demografischen Attributen

Auch im Hinblick auf den Zusammenhang zwischen der Verantwortungsübernahme sowie den Erwartungen und den sozio-demografischen Attributen der Verbraucher:innen lassen sich interessante Ergebnisse feststellen.[68]

[68] Es werden lediglich statistisch signifikante Ergebnisse (mind. $p<5\%$) präsentiert. Bei Gruppenvergleichen basieren die Ergebnisse auf Chi^2-Tests und bei metrischen Variablen wurden Logistische Regressionsanalysen verwendet.

So findet sich zwischen der **digitalen Affinität** der Verbraucher:innen, d.h. Anzahl der genutzten Geräte im Zuhause, Kenntnis unterschiedlicher Technologiebegriffe sowie ausgeübter Schutzmaßnahmen, ein **positiver Zusammenhang mit der grundsätzlichen Bereitschaft,** regelmäßig die Passwörter der genutzten Dienste zu ändern. Konkret bedeutet dies: (1) Je mehr digitale Geräte eine Person nutzt, (2) je besser eine Person sich mit digitalen Technologiebegriffen auskennt und (3) je mehr Schutzmaßnahmen eine Person bei der Nutzung ihrer digitalen Geräte ergreift, desto höher ist die Bereitschaft regelmäßig Passwörter zu ändern.

Im Hinblick auf die Verantwortungsanteile, die den unterschiedlichen Gruppen zugeschrieben werden, finden sich hingegen keine systematischen Unterschiede bei den sozio-demografischen Attributen.

Interessanterweise steht der **Wunsch nach einer stärkeren Regulierung mit der Kenntnis digitaler Technologien und dem eigenen Schutzverhalten in einem positiven Zusammenhang**. Das bedeutet, dass Personen mit besserer Kenntnis digitaler Technologiebegriffe und Personen mit einem ausgeprägterem Schutzverhalten häufiger stärkere Anforderungen, d.h. Gesetze oder Normen, an Geräte fordern. Ein **ähnlicher Zusammenhang** kann auch zwischen der digitalen Affinität der Verbraucher:innen und ihrem **Wunsch nach mehr Transparenz** über IT-Sicherheitsaspekte festgestellt werden. Auch hier gilt konkret, (1) je mehr digitale Geräte eine Person nutzt, (2) je besser sie sich mit digitalen Technologien auskennt und (3) je mehr Schutzmaßnahmen sie nutzt, desto wahrscheinlicher ist es auch, dass sie sich mehr Transparenz zu IT-Sicherheitsaspekten von Produkten oder Anwendungen wünscht. Ähnlich verhält es sich auch mit dem Alter der Verbraucher:innen. Je älter diese sind, desto mehr Transparenz wünschen sie sich.

4.5.4. Fazit: Nutzer:innen sind bereit etwas für ihre IT-Sicherheit zu tun und sehen sich selbst auch in der Verantwortung. Der Gesetzgeber kann jedoch die Bedingungen im Hinblick auf Anforderungen und Transparenz verbessern.

Die Befragung zeigt, dass **Verbraucher:innen nicht nur** Sicherheit für ihre IoT-Geräte **fordern**, **sondern auch selbst bereit sind**, **etwas für ihre Sicherheit zu tun.** So wälzen sie die Hauptverantwortung nicht nur auf Hersteller oder den Gesetzgeber ab. Darüber hinaus sind sie grundsätzlich bereit ihre Passwörter zu ändern. Dies deckt sich auch mit der Eigenverantwortung, die Nutzer:innen bei der Inbetriebnahme ihrer Geräte und deren Nutzung übernehmen (vgl. Teil 2 und 3).

Unabhängig davon, kann der **Gesetzgeber** Verbraucher:innen jedoch **zusätzlich unterstützen**. So wünschen sich Verbraucher:innen grundsätzlich **stärkere Anforderungen**, d.h. Gesetze oder Normen, an digitale Geräte sowie **mehr Transparenz** zu den IT-Sicherheitsaspekten von Produkten.

Positiv hervorzuheben ist auch, dass nicht nur Personen, die ggf. aufgrund ihrer geringeren digitalen Affinität Hilfe vom Gesetzgeber nötig haben, solche auch for-

dern. Im Gegenteil, gerade Personen mit einer hohen digitalen Affinität und solche, die sich schon zu hohen Anteilen selbst schützen, fordern striktere Anforderungen an Geräte und mehr Transparenz.

4.6. Teil 5: IT-Sicherheitskennzeichen im Allgemeinen und BSI-Sicherheitskennzeichen

Der fünfte und letzte Teil der Befragung beschäftigte sich tiefergehend mit der **Transparenz von Sicherheitsaspekten**, nämlich in Form von sog. IT-Sicherheitskennzeichen, die Verbraucher:innen beim Kauf von Produkten unterstützen können. Dabei wurde auch ein **konkretes Sicherheitskennzeichen, das sog. IT-Sicherheitskennzeichen des Bundesamts für Sicherheit in der Informationstechnik** (im Folgenden: BSI-Kennzeichen), untersucht.

Die konkreten Forschungsfragen waren:

- Inwieweit finden Verbraucher:innen ein Sicherheitskennzeichen hilfreich?
- Wie ist die objektive Verständlichkeit des BSI-Kennzeichens? Wie schneidet dieses in der subjektiven Bewertung der Verbraucher:innen ab?

4.6.1. Methodik

Zur Beantwortung der Forschungsfragen wurden auch in diesem Teil **geschlossene Fragen** formuliert und an die Teilnehmer:innen des Fragebogens gerichtet. Es gab dabei **keine Filterung** der Teilnehmer:innen in unterschiedliche Gruppen. Soweit nicht anders vermerkt, beziehen sich die Statistiken somit auf die Gesamtstichprobe von N=995.

Bei den Fragen, die sich konkret auf das BSI-Kennzeichen bezogen, wurde die statische Komponente des **originalen IT-Sicherheitskennzeichens des BSI immer gleichzeitig zu den Fragetexten abgebildet** (vgl. Abbildung 15). Die Teilnehmer konnten somit nur den Informationsgehalt der statischen Komponente bei der Beantwortung berücksichtigen. Durch die Verwendung der originalen Abbildung der statischen Komponente des Kennzeichens konnte gewährleistet werden, dass auch Teilnehmer:innen, die sich bisher nicht mit dem BSI-Kennzeichen befasst hatten, einen realen Eindruck bekamen.

Abbildung 15: IT-Sicherheitskennzeichen des BSI.

4.6.2. Ergebnisse

Ergebnis 18: Grundsätzlich finden Nutzer:innen ein IT-Sicherheitssiegel oder Kennzeichen beim Kauf hilfreich.

Zuerst wurden die Proband:innen gebeten anzugeben, ob ein IT-Sicherheitssiegel oder Kennzeichen, das über die IT-Sicherheit eines Geräts informiert und auf der Verpackung des Produkts abgedruckt wird oder bei einem Kauf im Online-Shop angezeigt wird, hilfreich sei. Die Mehrheit von 75% bejahte dies, 18% gaben an, dass dies nicht hilfreich sei und 7% machten keine Angabe.

Ergebnis 19: Das objektive Verständnis im Hinblick auf das BSI-Sicherheitskennzeichen ist insgesamt ausbaufähig.

Im nächsten Schritt wurde den Teilnehmer:innen das BSI-Kennzeichen angezeigt und eine Frage zur objektiven Verständlichkeit gestellt. Die Ergebnisse sind in Abbildung 16 dargestellt. Die Frage wurde im Quiz-Format gestellt und Befragte sollten auswählen, welche Aussagen bzw. Eigenschaften korrekterweise auf das BSI-Kennzeichen zutrifft. Es wurden sechs unterschiedliche Aussagen als Antwortoptionen präsentiert, zwei davon waren korrekt und vier inkorrekt.

Insgesamt 7% der Befragten beantworteten die Frage vollständig korrekt.[69,70] Positiv hervorzuheben ist, dass 59% der Befragten korrekterweise aus dem Kennzeichen ableiteten, dass der Hersteller die Sicherheit des Gerätes zusichert. Jedoch interpretierten 44% der Befragten das Kennzeichen fälschlicherweise so, dass das BSI die Anforderungen vor Erteilung des Kennzeichens überprüft. 43% erkannten korrekterweise, dass mit Hilfe des Kennzeichens aktuelle Informationen über das Produkt abrufbar seien (vgl. QR-Code auf dem Kennzeichen sowie Weblink).

Darüber hinaus schätzten fast ein Drittel der Befragten die Sicherheit des Geräts falsch, d.h. zu hoch ein. So gaben 30% an, dass das Kennzeichen anzeige, dass das Produkt sicherer als andere Produkte auf dem Markt sei und 29% interpretierten das Kennzeichen als Beleg dafür, dass das Produkt an sich den höchsten Sicherheitsstandard erfülle.

[69] Das heißt, sie wählten die beiden korrekten Aspekte aus und keinen der inkorrekten Aspekte.
[70] 90% beantworteten die Frage nicht korrekt und 2% antworteten „weiß nicht“.

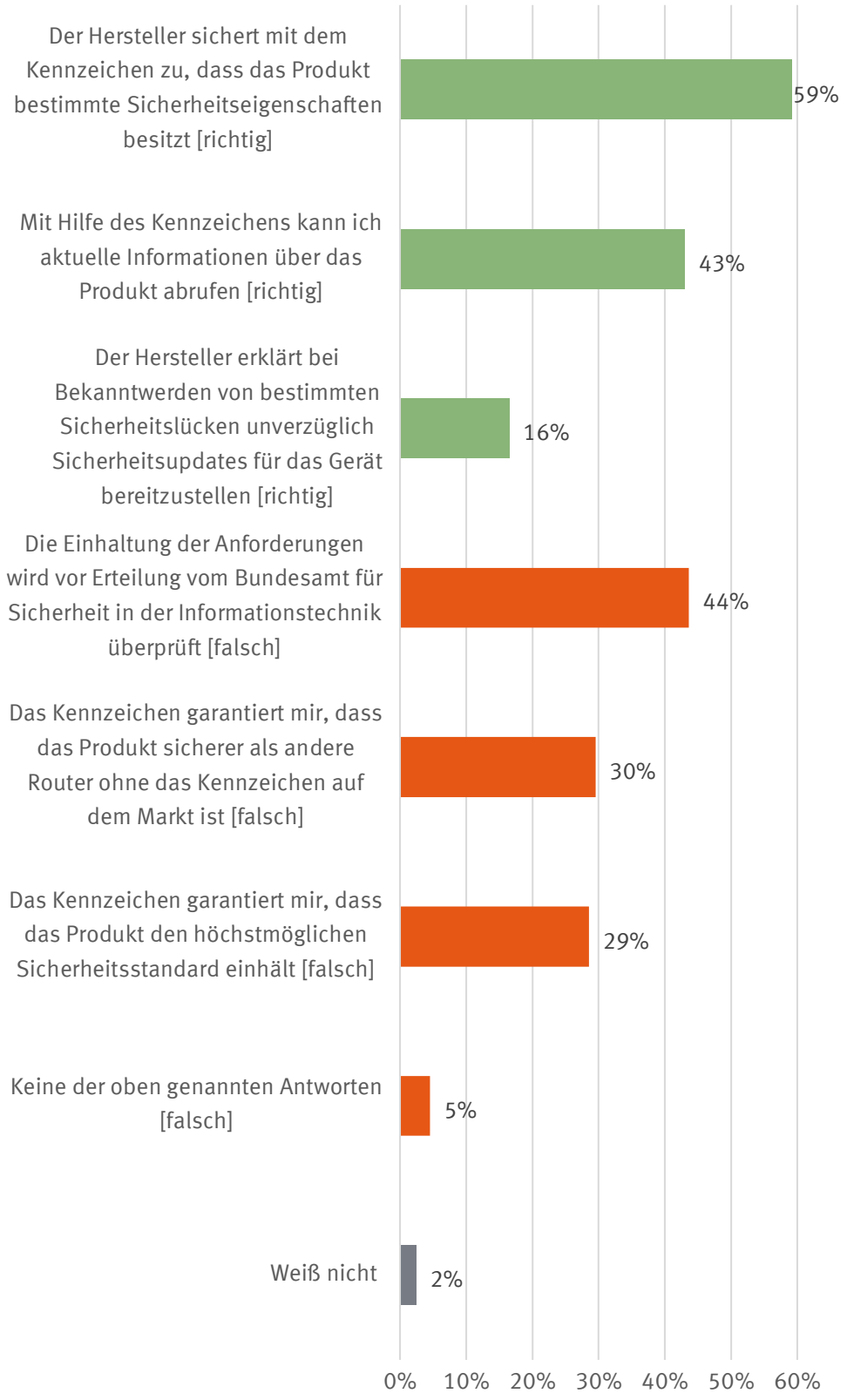

Abbildung 16: Objektives Verständnis des IT-Sicherheitskennzeichen des BSI.

Ergebnis 20: Das BSI-Kennzeichen wird insgesamt eher positiv von den Verbraucher:innen bewertet.

Abbildung 17 zeigt die Ergebnisse der beiden Fragen zur subjektiven Bewertung des BSI-Kennzeichens. Zum einen wurden die Befragten gebeten, die (subjektive) Verständlichkeit zu bewerten. 16% gaben dabei an, dass das BSI-Kennzeichen „voll und ganz verständlich“ sei und weitere 44% gaben an, dass es „eher verständlich“ sei. 23% wählten als Antwort „weder noch“, 12% empfanden das Kennzeichen als „eher nicht verständlich“ und 3% empfanden es als „ganz und gar nicht verständlich“.[71]

Die zweite Frage bezog sich auf die Vertrauenswürdigkeit des BSI-Kennzeichens. Auch hier schneidet das Kennzeichen insgesamt sehr positiv ab. 18% der Befragten gaben an, dass das BSI-Kennzeichen aus ihrer Sicht „voll und ganz vertrauenswürdig“ sei, 45% bewerteten es als „eher vertrauenswürdig“, 26% als „weder noch“ und 7% als „eher nicht vertrauenswürdig“. Lediglich 2% gaben an, dass das Kennzeichen „ganz und gar nicht vertrauenswürdig“ sei.[72]

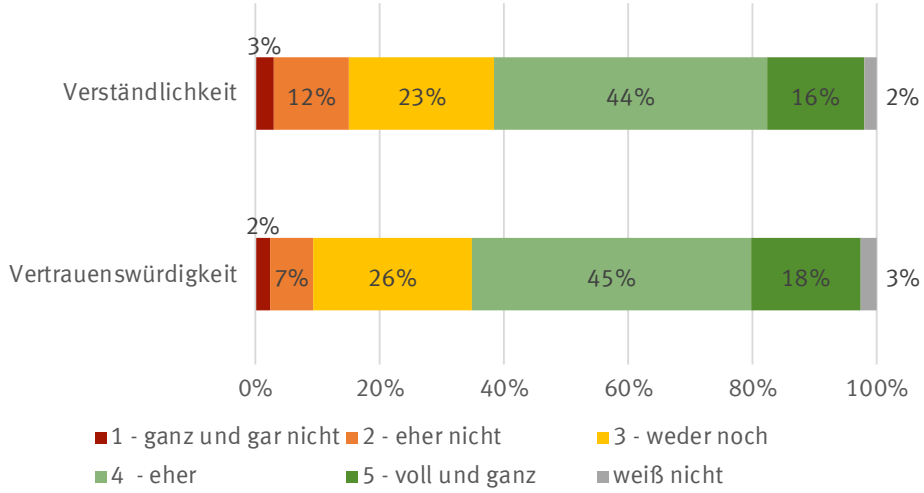

Abbildung 17: Subjektive Bewertung des IT-Sicherheitskennzeichens des BSI.

Ergebnis 21: In einer Folgestudie sollte untersucht werden, inwieweit die dynamische Komponente des IT-Sicherheitskennzeichens des BSI (aktuelle Zusatzinformationen per Link abrufbar) von Verbraucher:innen angenommen wird und wie sich diese Zusatzinformationen auf das Verbraucherverhalten auswirken.

Wie bereits unter 4.2.1. ausgeführt, vermittelt das IT-Sicherheitskennzeichen des BSI seine Informationen schwerpunktmäßig durch die dynamische Komponente zu der die Teilnehmer:innen im Rahmen der Befragung keinen Zugang hatten. Im

[71] 2% keine Angabe / weiß nicht.
[72] 3% keine Angabe / weiß nicht.

Rahmen einer Folgestudie sollte das IT-Sicherheitskennzeichen des BSI daher unter Einbeziehung der dynamischen Komponente untersucht werden.

4.6.3. Zusammenhänge mit sozio-demografischen Attributen

Auch im Hinblick auf die Bewertung von Sicherheitskennzeichen lassen sich einige Zusammenhänge mit den sozio-demografischen Attributen der Befragten beobachten.[73] So stehen Alter und **digitale Affinität in einem Zusammenhang mit der Bewertung der Hilfestellung durch ein IT-Sicherheitskennzeichen**. Je älter die Verbraucher:innen, desto hilfreicher bewerten sie eine Siegel. Außerdem kann beobachtet werden, (1) je mehr digitale Geräte eine Person nutzt, (2) je besser ihre Kenntnis im Bereich digitaler Technologiebegriffe ist und (3) je mehr Schutzmaßnahmen sie kennt und nutzt, desto hilfreicher bewertet sie auch ein IT-Sicherheitskennzeichen.

Interessanterweise sind im Hinblick auf die objektive Verständlichkeit nur vereinzelte Zusammenhänge mit sozio-demografischen Attributen zu beobachten. Lediglich **Alter und die Kenntnis von digitalen Technologiebegriffen** stehen mit der **korrekten Interpretation des BSI-Kennzeichens** in einem Zusammenhang. Je älter die Befragten und je besser ihre Kenntnis unterschiedlicher Technologiebegriffe ist, desto wahrscheinlicher ist es, dass sie die Frage zum objektiven Wissen korrekt beantworten.

Bei der subjektiven Verständlichkeit kann man außerdem einen Unterschied zwischen den Geschlechtern feststellen. So bewerten **Männer** das BSI-Kennzeichen durchschnittlich als **verständlicher als Frauen** – obwohl im Hinblick auf die objektive Verständlichkeit kein Unterschied besteht. Im Hinblick auf die **digitale Affinität** können sowohl bei der **subjektiven Verständlichkeit** als auch bei der **Bewertung der Vertrauenswürdigkeit** des BSI-Kennzeichens, **positive Zusammenhänge** festgestellt werden. Das bedeutet konkret: (1) Je mehr Geräte die Verbraucher:innen nutzen, (2) je besser ihre Kenntnis unterschiedlicher digitaler Technologien und (3) je mehr Schutzmaßnahmen sie ergreifen, desto verständlicher bzw. vertrauenswürdiger bewerten sie das BSI-Kennzeichen.

4.6.4. Fazit: Verbraucher:innen fordern mehr Transparenz durch Siegel. Das BSI-Kennzeichen ist jedoch ausbaufähig.

Wie Teil 4 der Befragung aufzeigen konnte, wünschen sich Verbraucher:innen insgesamt mehr Transparenz zur Sicherheit ihrer IoT-Geräte. Eine solche Ausgestaltung könnte bspw. ein Kennzeichen sein, das Verbraucher:innen beim Kauf von Produkten zur Verfügung gestellt wird. Die **Mehrheit der Verbraucher:innen findet** ein solches **Kennzeichen als hilfreich** und auch im ersten Teil der Befragung zum

[73] Es werden lediglich statistisch signifikante Ergebnisse (mind. $p<5\%$) präsentiert. Bei Gruppenvergleichen basieren die Ergebnisse auf Chi^2-Tests und bei metrischen Variablen wurden logistische Regressionsanalysen verwendet.

Kauf von digitalen Produkten konnte gezeigt werden, dass Sicherheitskennzeichen tatsächlich die gewünschte Wirkung haben. Sichere Produkte werden mit Hilfe der Kennzeichen auch eher gekauft als unsichere.

Eine mögliche Ausgestaltung eines Labels könnte das **IT-Sicherheitskennzeichen des Bundesamts für Sicherheit in der Informationstechnik** sein. Die Befragung zeigt dabei, dass Verbraucher:innen das Kennzeichen **insgesamt positiv bewerten**, d.h. als eher verständlich und eher vertrauenswürdig. Jedoch ist hieran problematisch, dass die subjektive Verständlichkeit von der objektiven Verständlichkeit abweicht. So **versteht** die **Mehrheit** der Verbraucher:innen die statischen **Inhalte des BSI-Kennzeichens nicht korrekt**. Eine Mehrheit von Befragten rechnete dem BSI-Kennzeichen auch Attribute zu, die es nicht erfüllt. Solange Produkte insgesamt sicher sind, ist dies auch kein Problem. Wenn jedoch Sicherheitslücken entstehen, die die Nutzung der gekennzeichneten Produkte unsicher machen, kann das BSI-Kennzeichen auch dafür sorgen, dass sich die Verbraucher:innen fälschlicherweise in Sicherheit wiegen , sofern sie nicht die detaillierten Hinweise verfolgen, die über den QR-Code und über den Link zur BSI-Webseite abrufbar sind.

Ein weiterer Aspekt, den die Befragung aufzeigen konnte, ist, dass insbesondere Personen mit hoher digitaler Affinität das BSI-Kennzeichen subjektiv als verständlich bewerten. Prinzipiell ist dies wenig überraschend, zeigt aber auch auf, dass gerade für Personen, die Unterstützung in der digitalen Welt nötig haben, die Inhalte des Kennzeichen im Hinblick auf die Verständlichkeit ausbaufähig sind.

4.7. Zusammenfassung der Befragungsergebnisse

Ziel der Verbraucherbefragung war es, die **blinden Flecken bzgl. des Verbraucherwissens und -verhaltens sowie Erwartungen an IoT-Sicherheitsaspekte zu schließen**, da diese noch nicht oder nur ungenügend in der Literatur und in weiteren Studien abgedeckt wurden. Hierzu wurden online insgesamt N=995 Teilnehmer:innen befragt, die online-repräsentativ für die deutsche Bevölkerung sind.

Die Ergebnisse der Befragung zeigen, dass **Kennzeichen für IT-Sicherheit Verbraucher:innen grundsätzlich beim Kauf von IoT-Produkten helfen**. Wichtig ist dabei die Ausgestaltung der Label bzw. Kennzeichen und so ist es unabdingbar, diese verständlich und einfach zu gestalten. Eine mögliche Umsetzung eines Sicherheitslabels, das in der Befragung untersucht wurde, ist das IT-Sicherheitskennzeichen des Bundesamts für Sicherheit in der Informationstechnik. Dieses wird im Hinblick auf die subjektive Verständlichkeit und die Vertrauenswürdigkeit positiv bewertet, im Hinblick auf die objektive Verständlichkeit ist es bezogen auf die hier untersuchten statischen Elemente jedoch ausbaufähig. Verbraucher:innen schreiben dem BSI-Kennzeichen Eigenschaften zu, die es eigentlich nicht erfüllt. Bei Produkten, die insgesamt sicher sind, ist dies prinzipiell unproblematisch. Wenn jedoch Sicherheitslücken entstehen, die für die Nutzung der Produkte problematisch sind, kann das Sicherheitskennzeichen im schlechtesten Fall dazu verleiten,

dass sich Nutzer:innen fälschlicherweise in Sicherheit wiegen, sofern diese nicht das Informationsangebot des BSI-Kennzeichens über die dynamische Komponente in Form der Produktinformationsseite über den abgedruckten Link und QR-Code wahrnehmen. Zusammenfassend zeigt die Befragung jedoch, dass Kennzeichen für IT-Sicherheit Verbraucher:innen helfen und die Einführung grundsätzlich begrüßenswert ist. Hier kann der Gesetzgeber zusätzlich unterstützend wirken und die Gestaltung der Kennzeichnung sowie die zugrundeliegenden Anforderungen optimieren.

Ein weiterer Schwerpunkt der Befragung lag auf dem Verhalten der Verbraucher:innen und dem Umgang mit den eigenen IoT-Geräten. Insgesamt ist positiv hervorzuheben, dass **Nutzer:innen bereit** sind**, ein hohes Maß an Eigenverantwortung für die Sicherheit ihrer IoT-Geräte zu übernehmen** – und dies auch schon tun. So richten sich ihre Geräte oftmals selbstständig ein und kümmern sich um die Installation von Sicherheitsaktualisierungen. Interessant wäre vor diesem Hintergrund die Bereitschaft von Verbraucher:innen zu untersuchen, auf ein Informationsangebot zurückzugreifen, wie es z.B. durch die dynamische Komponente des IT-Sicherheitskennzeichens des BSI bereitgestellt wird. Das Verhalten hängt dabei jedoch auch von der Produktart und von der digitalen Affinität der Verbraucher:innen ab. So übergeben Verbraucher:innen teilweise die Einrichtung und Aktualisierung ihrer Geräte an Dritte im persönlichen Umfeld und begründen dies insbesondere mit der Unverständlichkeit und hohen Komplexität der Einrichtung. Außerdem sorgen sie sich zum Teil, die Geräte fehlerhaft einzustellen, so dass sie nicht mehr funktionieren. Aus diesem Grund ist es gerade im Hinblick auf die Nutzerfreundlichkeit und Gestaltung der Produkte bei der Inbetriebnahme und Updates unabdingbar, auch die Bedürfnisse von Verbraucher:innen zu berücksichtigen, die weniger digital-affin sind.

Darüber hinaus entbindet das hohe Maß an Eigenverantwortung weder Hersteller noch Gesetzgeber aus der Mitverantwortung für die Sicherheit von IoT-Geräten. Die befragten Verbraucher:innen stellen hier **klare Forderungen an die Politik** und wünschen sich **striktere Regeln**, bspw. bei der Zulassung von Produkten oder im Hinblick auf Verbote von unsicheren Produkten. Außerdem wünschen sie sich **mehr Transparenz** über die Sicherheit ihrer digitalen Geräte.

5. Schlussfolgerungen und Handlungsempfehlungen

Auf der Grundlage der Literaturauswertung sowie der neuen Erkenntnisse aus der im Rahmen der Studie durchgeführten empirischen Erhebung wird abschließend der Frage nachgegangen, welche Schlussfolgerungen hieraus mit Blick auf die verbraucherpolitische Wahrnehmung des Themas IT-Sicherheit sowie hinsichtlich der weiteren Rolle der Normung in diesem Kontext zu ziehen sind.

Hierfür werden zunächst die im Laufe des Projekts gewonnenen Erkenntnisse über Wahrnehmung und Verhalten von Verbraucher:innen zu Fragen der IT-Sicherheit mit dem Status Quo in Recht und Normung abgeglichen (Abschnitt 5.1). Aus diesem Abgleich werden Schlussfolgerungen für die Verbraucherpolitik generell (Abschnitt 5.2) und für die Normung im Speziellen (Abschnitt 5.3) gezogen.

5.1. Abgleich der empirischen Erkenntnisse mit dem Status Quo in Recht und Normung

Die **Verbraucherumfrage** hat folgende Kernpunkte deutlich gemacht:

- Verbraucher:innen wünschen sich **stärkere Anforderungen, d.h. Gesetze oder Normen, an digitale Geräte**.
- Verbraucher:innen sind bereit, **Eigenverantwortung für die Sicherheit von IT-Produkten** zu übernehmen. Ihnen fällt es aber teilweise schwer, diese Eigenverantwortung in die Tat umzusetzen, weil sie die **Geräte als unverständlich und die Einstellungen als kompliziert** wahrnehmen.
- Verbraucher:innen legen großen Wert darauf, dass **Transparenz über IT-Sicherheit beim Kauf von IoT-Geräten** geschaffen wird.

Ein Abgleich des **gesetzlichen und normativen Rahmens** mit Blick auf diese Anforderungen führt zu folgendem Ergebnis:

- Die **gesetzlichen Regelungen zur IT-Sicherheit sind bislang lückenhaft und sehr allgemein**; für die meisten verbraucherrelevanten IT-Sicherheitsfragen gibt es derzeit keine spezifischen rechtlichen Anforderungen. Die **Normung** stellt zwar konkretere Anforderungen, diese werden aber **in der Praxis nicht durchgängig umgesetzt.**
- Derzeit fällt es Verbraucher:innen schwer, eigenverantwortlich für die Sicherheit von IT-Produkten zu sorgen, weil das Konzept der **„Usable Security“**, d. h. die leichte, möglichst intuitive Handhabung von Sicherheitsaspekten durch Verbraucher:innen, gegenwärtig **praktisch noch wenig umgesetzt** wird.
- Mit dem **IT-Sicherheitskennzeichen des BSI** wurde ein neuartiges hybrides Kennzeichen geschaffen, das Verbraucher:innen ein Instrument zur Schaffung

von Transparenz über IT-Sicherheit bei Kaufentscheidungen zur Verfügung stellt. Das BSI-Kennzeichen trifft auf einen Bedarf bei Verbraucher:innen und wird dementsprechend insgesamt **positiv aufgenommen**. Allerdings kann das BSI-Sicherheitskennzeichen teilweise **unzutreffende und zu weitreichende Erwartungen** hinsichtlich der Sicherheit der ausgezeichneten Produkte wecken, wenn die Verbraucher:innen lediglich auf das statische Element zurückgreifen und nicht das Informationsangebot des BSI-Kennzeichens über die dynamische Komponente in Form der Produktinformationsseite nutzen, die über den abgedruckten Link und QR-Code zugänglich ist.. Daher sind **andere, mehrstufige Konzepte von Sicherheitskennzeichen** wie das vom **EU-Rechtsakt für Cybersicherheit** anvisierte Sicherheitszertifikat als Alternativen in Betracht zu ziehen.

5.2. Handlungsempfehlungen für die Verbraucherpolitik

Aus dem Abgleich der Befragungsergebnisse mit dem Status Quo in Recht und Normung lassen sich folgende Schlussfolgerungen ableiten:

- **Ein hohes Niveau an IT-Sicherheit für verbrauchernahe IT-Produkte** muss durch Gesetz und Normung konsequent, lückenlos und spezifisch vorgegeben und durchgesetzt werden.
- **Usable Security** im Sinne einer leichten, intuitiven Handhabung von Sicherheitsaspekten durch Verbraucher:innen sollte durch Gesetzgebung und Normung durchgängig verwirklicht werden.
- Oberhalb eines gesetzlich definierten Standards sollte das **Niveau an IT-Sicherheit für Verbraucher:innen beim Kauf von IoT-Produkten transparent** gemacht werden.

Ergebnis 22: Ein durchgängig hohes Niveau an IT-Sicherheit für verbrauchernahe IT-Produkte, Usable Security sowie Transparenz über IT-Sicherheitsaspekte beim Kauf sind zentrale Zielsetzungen für die Verbraucherpolitik.

Auch wenn der derzeitige Rechtsrahmen diese Zielsetzungen noch nicht abdeckt, so gibt es doch **rechtspolitische Vorschläge**, die diese Zielsetzungen adressieren. Zwei zentrale Vorschläge werden im Folgenden wiedergegeben.

5.2.1. Vorschlag der EU-Kommission für ein Gesetz zur Cyberwiderstandsfähigkeit (Cyber Resilience Act)

Die EU-Kommission plant, den EU-Rechtsrahmen für IT-Sicherheit durch ein **Gesetz zur Cyberwiderstandsfähigkeit (Cyber Resilience Act)** zu ergänzen. Der entsprechende Vorschlag wurde am 15.09.2022 vorgelegt.[74] Er setzt in seiner Problemanalyse wie auch in seinen Lösungsvorschlägen an den hier festgehaltenen Punkten an.

Die EU-Kommission stellt in ihrer **Begründung für den Vorschlag des Cyber Resilience Act** fest, dass es mit Blick auf die IT-Sicherheit derzeit zwei Probleme gebe, nämlich

- ein **niedriges Niveau der Cybersicherheit**, das sich in weit verbreiteten Schwachstellen und der unzureichenden und uneinheitlichen Bereitstellung von Sicherheitsupdates zu deren Behebung widerspiegelt, und
- **unzureichendes Verständnis** und **unzureichender Zugang zu Informationen seitens der Nutzer:innen**, was sie daran hindert, Produkte mit angemessenen Cybersicherheitseigenschaften auszuwählen oder sie auf sichere Weise zu nutzen.[75]

Die von der EU-Kommission formulierten **Ziele des Cyber Resilience Act** entsprechen den eben formulierten Schlussfolgerungen zu den politischen Herausforderungen im Bereich der IoT-Sicherheit:

- Die Kommission nennt zwei Zielsetzungen, um generell ein **hohes Niveau an IT-Sicherheit** zu erreichen:
    - Gewährleistung von Maßnahmen der Hersteller für die Sicherheit von Produkten mit digitalen Elementen bereits in der Entwurfs- und Entwicklungsphase und während des gesamten Lebenszyklus;
    - Gewährleistung eines kohärenten Rahmens für die Cybersicherheit, der die Einhaltung der Vorschriften für Hardware- und Softwarehersteller erleichtert
- Sie benennt das Ziel der **Usable Security**: Unternehmen und Verbraucher:innen sollen in die Lage versetzt werden, Produkte mit digitalen Elementen sicher zu nutzen.
- Sie betont das Ziel, die **Transparenz der Sicherheitseigenschaften von Produkten mit digitalen Elementen** zu verbessern.

[74] EU-Kommission (2022), Proposal for a Regulation on cybersecurity requirements for products with digital elements - Cyber resilience Act - COM(2022) 454 final. Abgerufen von https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[75] EU-Kommission, COM(2022) 454 final (vgl. Fn. 74), S. 1.

Die umfassenden Vorgaben des Cyber Resilience Act können hier nicht im Einzelnen dargestellt werden. Verdeutlicht werden kann aber die grundsätzliche Herangehensweise mit Blick auf die beschriebenen Zielsetzungen:

- **Ein hohes Niveau an IT-Sicherheit** soll gewährleistet werden, indem IT-Sicherheit generell für alle Produkte mit digitalen Elementen verpflichtend werden soll (Art. 5 des Vorschlags). Durch Konformitätsbewertungen (Art. 18 ff.) und Marktüberwachungsbehörden (Art. 41 ff.) sollen die Einhaltung der entsprechenden Vorgaben kontrolliert und durchgesetzt werden. Das ist ein großer Schritt gegenüber der heutigen Rechtslage, wonach Anforderungen an die IT-Sicherheit bisher nur im Bereich der Kritischen Infrastrukturen und einiger digitaler Dienste konkret definiert und durch Aufsichtspflichten hinterlegt sind.
- **Usable Security** soll verwirklicht werden, indem Nutzer:innen einfache, verständliche Informationen und Gebrauchsanleitungen zur Sicherheit digitaler Produkte zur Verfügung gestellt werden (Art. 10 Nr. 10 i. V. m. Annex II).
- **Zur Transparenz über Sicherheitsaspekte von IT-Produkten beim Kauf** verweist der Cyber Resilience Act in erster Linie auf das Cybersicherheitszertifikat nach dem EU-Rechtsakt für Cybersicherheit (vgl. nachfolgenden Abschnitt 05.2.2). Dieses wird zusätzlich dadurch aufgewertet, dass für risikoreiche IT-Produkte das Cybersicherheitszertifikat verpflichtend gemacht werden kann (Art. 6 Nr. 5). Außerdem wird das Cybersicherheitszertifikat mit der Konformitätsbewertung verbunden: Soweit für die Erteilung des Cybersicherheitszertifikats die Einhaltung bestimmter Sicherheitsanforderungen Voraussetzung ist, wird vermutet, dass Produkte, die das Cybersicherheitszertifikat tragen, diese Sicherheitsanforderungen tatsächlich einhalten (Art. 18 Nr. 3).

Diese Herangehensweise mit Blick auf die Verwirklichung der Zielsetzungen des Cyber Resilience Act entspricht den aus der Befragung abgeleiteten Handlungsempfehlungen für die Verbraucherpolitik. Wichtig ist, dass die Inhalte des Cyber Resilience Act auch im Einzelnen den beschriebenen Zielsetzungen entsprechen und dass im Verlauf des Rechtsetzungsverfahrens noch bestehende Verbraucherschutzdefizite[76] behoben und weitere Abschwächungen verhindert werden.

Ergebnis 23: Zielsetzung und Maßnahmen des Cyber Resilience Act sind nachdrücklich zu unterstützen. Im Verlauf des Rechtsetzungsverfahrens sollten noch bestehende Verbraucherschutzdefizite behoben und weitere Abschwächungen verhindert werden.

[76] So beschränkt der Vorschlag für den Cyber Resilience Act die Verpflichtung des Herstellers, Sicherheitslücken zu schließen, auf maximal 5 Jahre(vgl. Art. 10 Abs. 6 des Vorschlags). Aus Verbrauchersicht sollte diese Verpflichtung für die gesamte voraussichtliche Lebensdauer eines Produkts gelten, da das Produkt ansonsten zum Sicherheitsrisiko wird, obwohl es physisch noch funktionsfähig ist. Mit Blick auf die Kriterien für die Einstufung von IT-Produkten in Risikokategorien nach Art. 6 des Vorschlags sollten ferner Verbraucherprodukte wie smarte Türschließungsanlagen („security functions“, Art. 6 Abs. 2 (a) (iv)) oder Wearables („processing personal data“, Art. 6 Abs. 2 (c)) als risikogeneigte Produkte eingestuft werden.

5.2.2. Cybersicherheitszertifikat nach dem EU-Rechtsakt für Cybersicherheit

Das Cybersicherheitszertifikat nach dem EU-Rechtsakt für Cybersicherheit wurde bereits im Zusammenhang mit den rechtlichen Grundlagen der IT-Sicherheit beschrieben (vgl. oben Abschnitt 2.1.2, S. 16).

Im Unterschied zum IT-Sicherheitskennzeichen des BSI sieht das **EU-Cybersicherheitszertifikat drei Sicherheitsstufen** vor. Während ein binäres Label wie das BSI-Sicherheitslabel von Verbraucher:innen als absolute Sicherheitsgarantie verstanden werden kann, macht diese Abstufung deutlich, dass **Sicherheit stets relativ** ist. Insofern ist der Ansatz des EU-Cybersicherheitszertifikats vor dem Hintergrund der im Rahmen dieses Vorhabens gewonnenen empirischen Erkenntnisse vorzugswürdig.

Der Rechtsrahmen für die Einführung des EU-Cybersicherheitszertifikats besteht seit Verabschiedung des Cyber Security Act zum Zeitpunkt der Erstellung dieser Studie seit deutlich mehr als drei Jahren. Die Vorschläge des Cyber Resilience Act gehen ebenfalls von der Schaffung des EU-Cybersicherheitszertifikats aus. Der Bedarf nach einem einfachen, verständlichen Sicherheitszertifikat für IT-Produkte wird durch die vorliegende Studie nochmals untermauert. **Es ist daher an der Zeit, dass die Europäische Kommission die Initiative ergreift, um das europäische Cybersicherheitszertifikat praktisch einzuführen.**

Wenn das EU-Cybersicherheitszertifikat auf der Grundlage des Cyber Security Act eingeführt wird, wird sich die Frage stellen, welche Folgen sich hieraus für das nationale IT-Sicherheitskennzeichen des BSI ergeben. Soweit IKT-Produkte, -Dienste und-Prozesse vom EU-Cybersicherheitszertifikat und gleichzeitig von einem nationalen IT-Sicherheitszertifikat erfasst werden, wird das **nationale IT-Sicherheitszertifikat unwirksam** (Art. 57 des Cyber Security Act). Dadurch wird ein Nebeneinander zweier unterschiedlicher IT-Sicherheitskennzeichen vermieden.

Ergebnis 24: Die EU-Kommission sollte die Initiative ergreifen, um das EU-Cybersicherheitszertifikat praktisch einzuführen.

Bei der **graphischen Ausgestaltung** des EU-Cybersicherheitszertifikats sollte der **Bezugsrahmen des Zertifikats für die unterschiedlichen Bewertungsstufen verdeutlicht** werden. Das heißt, wenn etwa ein IT-Produkt einen Stern für die niedrigste Sicherheitsstufe erhält, dann muss deutlich sein, dass die Bewertungsskala bis zu drei Sterne umfasst (vgl. hierzu die Ausgestaltung im Testdesign, Tabelle 4, S. 31). Verbesserungsfähig ist insofern die graphische Ausgestaltung des Sicherheitskennzeichens nach dem derzeit vorliegenden Entwurf für die **ISO 27404**[77]. Hier werden die unterschiedlichen Niveaus der Cybersicherheit mit vier Sternen gekennzeichnet, allerdings ohne die Gesamtskala des Bewertungssystems deutlich zu machen.

[77] vgl. die Darstellung in Tabelle 2, S. 19.

Da Verbraucher:innen in der Umfrage ihr **hohes Interesse an Transparenz zu IT-Sicherheitsaspekten** deutlich gemacht haben, ist ferner zu erwägen, ob die Cybersicherheitszertifizierung in Ausweitung der entsprechenden Vorgabe aus Art. 6 Nr. 5 des Vorschlags für den Cyber Resilience Act nicht nur für besonders riskante IT-Produkte, sondern **generell für verbrauchernahe IT-Produkte verpflichtend** sein sollte.

Ergebnis 25: Die graphische Ausgestaltung des EU-Cybersicherheitszertifikats sollte den Bezugsrahmen der Zertifizierung mit drei Sicherheitsstufen verdeutlichen. Es sollte geprüft werden, inwieweit das Cybersicherheitszertifikat verpflichtend sein soll.

5.3. Handlungsempfehlungen für die Normung

Der Vorschlag der EU-Kommission für den Cyber Resilience Act misst der **Normung bei der Konformitätsbewertung einen großen Stellenwert** zu: Soweit Standards zu Sicherheitsanforderungen gemäß dem Cyber Resilience Act im Amtsblatt der EU veröffentlicht sind, wird vermutet, dass Produkte, die diese Standards einhalten, auch die Sicherheitsanforderungen nach dem Cyber Resilience Act einhalten (Art. 18 Nr. 1 des Vorschlags für den Cyber Resilience Act). In abgeschwächter Form gilt diese Vermutung auch für andere Standards (Art. 18 Nr. 2).

Soweit Normen zur Konkretisierung der EU-Gesetzgebung dienen, werden Standardisierungsorganisationen im Rahmen **eines Standardisation Request der EU-Kommission** tätig.[78] Die Normen, die aufgrund solcher Standardisation Requests im Rahmen des Cyber Resilience Act entwickelt werden, sind durch die Vermutungswirkung **in ihrer Wirkung der Gesetzgebung angenähert**. Insofern ist eine **starke Vertretung der Verbraucherinteressen** bei diesen Normungsvorhaben für ein hohes Niveau des Verbraucherschutzes in der IT-Sicherheit noch wichtiger als sonst. .

Ergebnis 26: Ein hohes Niveau an Verbraucherschutz in den Normen für IT-Sicherheit wird mit dem Cyber Resilience Act noch wichtiger, da Normen im Rahmen von Standardisation Requests der EU-Kommission entwickelt werden sollen, um die gesetzlichen Anforderungen zu konkretisieren.

[78] Vgl. EU-Kommission (ohne Datum), Standardisation requests. Abgerufen von https://single-market-economy.ec.europa.eu/single-market/european-standards/standardisation-requests_en (6.01.2023).

Für die Berücksichtigung von Verbraucheraspekten in der Normung von IT-Sicherheit hat das folgende **Konsequenzen**:

Die Grundlage für ein hohes Niveau an IT-Sicherheit ist Security by Design, d. h. dass Hersteller bereits bei der Konzeption von IT-Produkten IT-Sicherheit konsequent nach dem neuesten Stand der Technik umsetzen und IT-Produkte auch während deren gesamter Lebensdauer sicher halten. Dies müssen die **Normen zu den technischen Anforderungen an IT-Sicherheit** gewährleisten. Der Cyber Resilience Act wie auch die einschlägigen Normungsvorhaben behandeln hierzu eine **breite Palette von Themen** (z. B. Reset-Optionen, Maßnahmen zum Schutz vor nicht autorisiertem Zugang, Maßnahmen zum Schutz der Vertraulichkeit gespeicherter oder übermittelter Daten, Maßnahmen zum Schutz vor Datenmanipulation, Maßnahmen zum Schutz gegen Angriffe, Maßnahmen bei festgestellten Sicherheitslücken[79]).

Im Rahmen dieses Vorhabens kann nicht im Einzelnen ermittelt werden, welche Festlegungen in diesen unterschiedlichen Handlungsfeldern aus Verbrauchersicht konkret getroffen werden sollten. Richtungweisend für die Normung ist aber der Befund aus der empirischen Erhebung im Rahmen dieses Vorhabens: **Mit 63 Prozent sprach sich eine klare Mehrheit der Befragten für stärkere gesetzliche und normative Anforderungen an die IT-Sicherheit aus.**[80]

Soweit in Normen konkrete Anforderungen definiert werden, die der IT-Sicherheit dienen, **sollten diese Anforderungen daher nicht optional in Form von „should“ oder „may“ formuliert werden, sondern verbindlich im Wortlaut von „shall“**. Denn nur durch die Formulierung „shall“ ist sichergestellt, dass Unternehmen die entsprechenden Anforderungen tatsächlich einhalten müssen, wenn sie sich auf die Norm berufen wollen. Das gilt zum einen für die **Erarbeitung von neuen Normen**, aber auch für die turnusmäßige, alle fünf Jahre fällige **Überprüfung von bestehenden Normen** wie der Norm ETSI EN 303 645.

Derzeit sind Sicherheitsstandards im geltenden Normenwerk im Bereich der IT-Sicherheit häufig noch nicht als Verpflichtungen formuliert. Beispielsweise heißt es in der Norm ETSI EN 303 645 beim Umgang mit Sicherheitslücken: „Disclosed vulnerabilities should be acted on in a timely manner“. Es widerspricht der Norm also nicht, wenn auf Sicherheitslücken nicht zeitnah reagiert wird. Auch das Monitoring von Sicherheitslücken ist nur als „Soll“-Vorschrift formuliert: „Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period.“[81]

[79] Vgl. hierzu etwa Annex I aus dem Vorschlag für den Cyber Resilience Rechtsakt.
[80] Vgl. oben S. 50.
[81] Norm ETSI EN 303 645, Provision 5.2-1.

Festzuhalten ist ferner, dass **eine durchgängige Vertretung der Verbraucherinteressen bei der Normung von IT-Sicherheitsfragen in Zukunft noch wichtiger als bisher sein wird.**

Ergebnis 27: Um Security by Design zu gewährleisten, sollten hohe IT-Sicherheitsanforderungen in Normen nicht optional in Form von „should“ oder „may“, sondern verbindlich im Wortlaut von „shall formuliert werden. Verbraucherinteressen sollten bei technischen Normungsvorhaben im Bereich der IT-Sicherheit durchgängig vertreten werden.

Ein wichtiger Hinweis für die Normung im Bereich der IT-Sicherheit ist darüber hinaus die Feststellung, dass Verbraucher:innen zwar mit 52 Prozent der Verantwortung zunächst sich selbst als verantwortlich für die Sicherheit von IoT-Geräten sehen, dass sie aber **mit 30 Prozent der Verantwortung auch Herstellern und Anbietern der Geräte eine wichtige Rolle beimessen.**[82] Hieraus kann sich ein **Normungsauftrag** ergeben, die **Verantwortung der Wirtschaft für die Sicherheit von IoT-Geräten oder allgemeiner von digitalen Geräten und Diensten** konkret zu definieren. Grundlegende Prinzipien für ein verantwortungsvolles Handeln der Wirtschaft mit Blick auf die Unternehmensverantwortung im Zeitalter der digitalen Transformation hat etwa die Corporate Digital Responsibility Initiative entwickelt.[83] Diese Prinzipien könnten den Ausgangspunkt für eine Norm zu Corporate Digital Reponsibility bilden.

Sofern eine Norm zur Verantwortung der Wirtschaft für die Auswirkungen von digitalen Produkten und Dienstleistungen auf Verbraucher:innen grundsätzlich für sinnvoll gehalten wird, stellt sich weiter die Frage, wie umfassend dieses Normungsvorhaben von der **Bandbreite der erfassten IT-Anwendungen** sein soll (nur IoT oder umfassender für alle IT-Geräte und -Dienste), und wie umfangreich die damit **angestrebten Zielsetzungen** sein soll (nur IT-Sicherheit oder allgemein Wahrung von Verbraucherinteressen).

Ergebnis 28: Es sollte geprüft werden, ob ein Normungsvorhaben für die Verantwortung der Wirtschaft für die Wahrung von Verbraucherinteressen bei digitalen Produkten und Dienstleistungen initiiert werden soll. Wenn der Bedarf für ein solches Normungsvorhaben gesehen wird, sind die der Norm unterfallenden Geräte und Dienstleistungen sowie die Zielsetzung des Normungsvorhabens weiter zu konkretisieren.

Der DIN Verbraucherrat als Interessenvertretung der Verbraucher:innen in der Normung sollte sich darüber hinaus besonders dafür einsetzen, dass IT-Sicherheit für Verbraucher:innen verständlich und handhabbar ist und dass die Idee der **Usable Security auf diese Weise praktisch umgesetzt** wird. Es ist zu begrüßen, dass der

[82] Vgl. oben S. 50 Abbildung 14.
[83] Corporate Digital Responsibility Initiative (CDR-Initiative), https://cdr-initiative.de; vgl. dort insbesondere den CDR-Kodex, https://cdr-initiative.de/kodex

Vorschlag des Cyber Resilience Rechtsakts dieses Thema durch ausführliche Festlegungen zu Informationspflichten und Gebrauchsanleitungen angeht (Vgl. Annex II des Vorschlags für den Cyber Resilience Rechtsakt und s. o. Abschnitt 5.2.1).

Gerade im Bereich der **Usable Security** kann Normung verschiedene konkrete Beiträge leisten:

- **Gebrauchsanleitungen und Sicherheitshinweise sollten für Verbraucher:innen einfach verständlich sein.**

  Allgemeine Hinweise hierzu können etwa der Norm DIN EN 82079-1 für die Erstellung von Gebrauchsanleitungen entnommen werden (Auflistung und Erklärung unvermeidbarer Fachbegriffe, Akronyme und Abkürzungen, Glossar, gleichbleibende Terminologie). Konkret sollten Gebrauchsanleitungen bei IT-Produkten, die in Deutschland vertrieben werden, in deutscher Sprache sowie in gängigen Sprachen von Einwohner:innen mit Migrationshintergrund verfasst sein (türkisch, polnisch, russisch, ggf. weitere[84]). Unverzichtbar für die Verständlichkeit ist auch die Konsistenz der verwendeten Begriffe – sowohl innerhalb eines Dokuments wie einer Gebrauchsanleitung als auch im Sinne eines gemeinsamen Begriffsverständnisses unterschiedlicher Hersteller von IT-Produkten.

  Die Forderung nach **verständlichen Gebrauchsanleitungen** betrifft insbesondere die derzeit in Erarbeitung befindliche Norm **ISO 27403 (Cybersecurity – IoT and privacy – Guidelines for IoT-domotics**); die Forderung nach **konsistenter Begriffsverwendung** betrifft **alle einschlägigen Normen und Standards**.

- **Default-Einstellungen sollten genutzt werden, um ein hohes Sicherheitsniveau voreinzustellen.**

  Besonders dort, wo den Sicherheitsbedürfnissen von Verbraucher:innen kein anderes Interesse entgegensteht, sollte das höchstmögliche Sicherheitsniveau voreingestellt sein und dann aktiv werden, wenn Verbraucher:innen von sich aus keine manuelle Einstellungen vornehmen. Sicherheitsupdates sollten etwa automatisch installiert werden, sofern Verbraucher:innen das nicht anders einstellen. Andere Updates, die erweiterte Funktionen zum Gegenstand und ggf. auch erweiterte Datenerhebungen zur Folge haben, sollten dagegen nur auf eine explizite Anforderung durch Verbraucher:innen installiert werden. Sicherheitsupdates sollten dementsprechend von anderen, funktionserweiternden Updates getrennt gehalten werden und Verbraucher:innen unabhängig von diesen angeboten werden. Verbraucher:innen sollten auch stets die Möglichkeit haben, Sicherheitsupdates auch für die ursprünglich erworbene Version eines IT-Produkts zu erwerben.

[84] Vgl. Bundeszentrale für politische Bildung (2022), Bevölkerung mit Migrationshintergrund. Abgerufen von https://www.bpb.de/kurz-knapp/zahlen-und-fakten/soziale-situation-in-deutschland/61646/bevoelkerung-mit-migrationshintergrund/ (02.12.2022).

Derzeit entsprechen die Normen im Bereich der IT-Sicherheit diesen Anforderungen noch nicht:

Die **Norm ETSI EN 303 645** enthält keine zwingende Anforderung, Sicherheitsupdates auf automatischem Weg zur Verfügung zu stellen.[85] Die Trennung von Sicherheitsupdates und funktionserweiternden Updates wird nur optional erwähnt.[86]

Der **Normentwurf für die Norm ISO 27402 (Cybersecurity – IoT Security and Privacy- Device baseline requirements)** sieht in seiner derzeitigen Fassung nur vor, dass die Software eine Einstellung für automatische Updates vorsehen muss; eine Default-Einstellung für automatische Sicherheitsupdates wird nicht erwähnt.[87]

- Der **Normentwurf für die Norm ISO 27403 (Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics)** verweist zu den Update-Anforderungen auf die allgemeine Norm ISO 27400 (Cybersecurity — IoT security and privacy — Guidelines). Diese wiederum erwähnt Default-Einstellungen und automatische Updates in ihren Anforderungen überhaupt nicht.[88]**Normung sollte Wege zur technischen Umsetzung von Usable Security bereiten.**

  Beispielsweise sind gegenwärtig Passwörter das hauptsächliche Mittel zum Schutz gegen unautorisierten Zugang zu geschützten Daten. Bei besonders sensiblen Daten ist inzwischen die Zwei-Faktor-Authentisierung Standard geworden - mit der Folge, dass es auch für die Berechtigten aufwändig geworden ist, Zugang zu ihren eigenen Bankkonten oder ähnlichen sensiblen Daten zu bekommen.

  Angesichts dessen sollte nach Mitteln und Wegen gesucht werden, den Aufwand für die Mitwirkung von Verbraucher:innen bei den erforderlichen Sicherheitsmaßnahmen zu minimieren. Hierfür gibt es unterschiedliche Möglichkeiten: Biometrische Erkennungsmerkmale wie Iris-, Gesichts- oder Fingerabdruckerkennung machen den Passwortschutz verzichtbar, schaffen aber weitere Risiken mit Blick auf die Erhebung sensibler persönlicher Daten. Passwortmanager können den Aufwand bei der Speicherung und Eingabe von Passwörtern minimieren, stoßen bisher bei Verbraucher:innen aber auf Skepsis. Möglicherweise wären Zertifizierungen oder nicht kommerzielle Angebote hier nützlich, um das Vertrauen der Verbraucher:innen zu stärken.

  Im Rahmen dieses Vorhabens kann nicht ermittelt werden, welche Option aus Verbrauchersicht die beste zum Schutz gegen unautorisierten Zugang zu geschützten Daten ist. Wichtig ist aber, dass die Verbrauchervertretung in der

[85] ETSI, Norm ETSI EN 303 645, Provision 5.3.-4.
[86] “It is often advisable not to bundle security updates with more complex software updates, such as feature updates.“, vgl. ETSI, Norm ETSI EN 303 645, Provision 5.3.-4.
[87] ISO, Normentwurf ISO 27402, Abschnitt 5.2.8 Software and firmware updates.
[88] ISO, Norm 27400, Abschnitt 7.1.2.17 Provision of software and firmware updates.

Normung auch innovative technische Optionen zur Lösung von Sicherheitsfragen berücksichtigt und diesen durch die Normung Wege eröffnet.

Ergebnis 29: Um Usable Security praktisch zu verwirklichen, sollte die Normung aus Verbrauchersicht für folgendes eintreten:

- Gebrauchsanleitungen und Sicherheitshinweise sollten für Verbraucher:innen einfach verständlich sein.
- Default-Einstellungen sollten genutzt werden, um ein hohes Sicherheitsniveau voreinzustellen.
- Normung sollte Wege zur technischen Umsetzung von Usable Security eröffnen.

5.4. Zusammenfassung der Handlungsempfehlungen

Der Abgleich der Befragungsergebnisse mit der Analyse von Recht und Normung im Bereich der IT-Sicherheit hat folgende **zentrale Zielsetzungen für die Verbraucherpolitik mit Blick auf die IT-Sicherheit** ergeben:

- **Ein durchgängig hohes Niveau an IT-Sicherheit für verbrauchernahe IT-Produkte,**
- **Usable Security sowie**
- **Transparenz über IT-Sicherheitsaspekte beim Kauf.**

Konkret lassen insbesondere der Vorschlag der EU-Kommission für einen Cyber-Resilience-Act sowie das Cybersecurity-Zertifikat nach dem EU-Rechtsakt zur Cybersicherheit Perspektiven zur Verwirklichung dieser Zielsetzungen erkennen:

- **Der Vorschlag der EU-Kommission für einen Cyber Resilience-Act** verspricht, erstmalig ein durchgängig hohes Sicherheitsniveau bei verbrauchernahen IT-Produkten zu schaffen und **ist insofern sehr zu begrüßen**.
- Das durch den Cyber Security-Act der EU vorgegebene **Cybersecurity-Zertifikat** ermöglicht mit einer abgestufte Bewertung von IT-Sicherheit ein **hohes Maß an Transparenz und sollte daher alsbald eingeführt werden**.

Für die Normung ergeben sich folgende Handlungsempfehlungen:

- Ein **hohes Verbraucherschutzniveau in IT-Sicherheitsnormen wird mit dem Cyber Resilience Act noch wichtiger,** da Normen das Gesetz konkretisieren.
- Um **Security by Design** zu gewährleisten, müssen **Verbraucherinteressen bei IT-technischen Normungsvorhaben durchgängig vertreten werden.**
- **Normung sollte Usable Security befördern**, indem die **Verständlichkeit von Gebrauchsanweisungen und Sicherheitshinweisen** gewährleistet wird, indem ein hohes **Sicherheitsniveau voreingestellt** wird und indem **technische Sicherheitslösungen** entwickelt werden.