

DIN Consumer Council

(DIN-Verbraucherrat)

DIN

Study

Study on the topic of „Consumer Security-Related Knowledge and Behaviour in the Digital Environment”

Imprint

Published by:

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

Authors:

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, December 2022

02 December 2022

Study on the topic of “Consumer Security-Related Knowledge and Behaviour in the Digital Environment”

Study

submitted to:

DIN e. V.
DIN-Verbraucherrat
Dr. Alexander Goschew
Am DIN-Platz
Burggrafenstraße 6
10787 Berlin

by:

ConPolicy GmbH
Institute for Consumer Policy
Crellestr. 37
10827 Berlin
www.conpolicy.de

Author(s):

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

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 implement this personal responsibility in 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 security 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 Cybersecurity 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 concretise 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.**

Contents

Summary	Fehler! Textmarke nicht definiert.
Abstract	1
Contents	2
Index of Figures	5
Index of Tables	6
1. Introduction	7
1.1. Background	7
1.2. Objective and questions	8
1.2.1. The term "IT security"	8
1.2.2. Key issues	8
1.3. Method and structure of the report	9
2. Fundamentals of IT Security in the Law and Standardisation	10
2.1. Statutory bases of IT security	10
2.1.1. BSI Act	10
2.1.2. IT security bases under EU law	12
2.2. Bases of IT security in standardisation	14
2.2.1. Norms and standards: terminology and effect	14
2.2.2. Standardisation on the German, European and international levels	15
2.2.3. Norms and standardisation projects relevant to the security of IoT products	16
2.3. Summary of the bases of IT security in the law and standardisation	17
3. The Current State of Research: Consumers' Knowledge, Behaviour and Attitudes Regarding the Security of IoT Devices	18
3.1. Consumer knowledge and behaviour	19
3.1.1. Use of passwords	19
3.1.2. Two-factor authentication	20
3.1.3. Relevant decision-making factors when purchasing IoT devices	20
3.1.4. Awareness of data security	21
3.2. Discrepancy between knowledge and behaviour: privacy paradox	21
3.3. Attitudes and political demands	22
3.4. Summary of the state of research and conclusions for the survey	23

4. Results of the Population Survey in the Framework of the Project	24
4.1. Overview and procedure	24
4.1.1. Spot check and information about the data set	25
4.1.2. Structure of the results sections	25
4.2. Part 1: Purchasing networked devices and IT security labels	25
4.2.1. Method	26
4.2.2. Results	29
4.2.3. Correlations with socio-demographic attributes	33
4.2.4. Conclusion: Labels that contain information about the security of IoT devices have the desired effect	33
4.3. Part 2: Commissioning IoT devices	34
4.3.1. Method	34
4.3.2. Results	35
4.3.3. Correlations with socio-demographic attributes	38
4.3.4. Conclusion: Most users commission their own devices and additional changes to security settings are frequently carried out before the initial use	39
4.4. Part 3: Use of and updating IoT devices	39
4.4.1. Method	39
4.4.2. Results	40
4.4.3. Correlations with socio-demographic attributes	43
4.4.4. Conclusion: The update behaviour when using digital devices is positive overall. The majority of devices regularly receive security updates.	44
4.5. Part 4: Responsibility for security and expectations placed on lawmakers	44
4.5.1. Method	44
4.5.2. Results	44
4.5.3. Correlations with socio-demographic attributes	46
4.5.4. Conclusion: Users are willing to play a role in ensuring their IT security and also consider themselves responsible. Lawmakers can, however, improve the conditions with respect to requirements and transparency.	46
4.6. Part 5: IT security labels in general and BSI security labels	47
4.6.1. Method	47
4.6.2. Results	48
4.6.3. Correlations with socio-demographic attributes	51
4.6.4. Conclusion: Consumers demand more transparency through seals. The BSI label, however, can be expanded.	51
4.7. Summary of the survey results	52
5. Conclusions and Recommendations for Action	53
5.1. Comparison of the empirical findings with the status quo in the law and standardisation	53
5.2. Recommendations for action for consumer policy	54

5.2.1. Draft law from the EU Commission for a law concerning cyber resilience (Cyber Resilience Act)	54
5.2.2. Cybersecurity certificate according to the EU Cybersecurity Act	56
5.3. Recommendations for action for standardisation	57
5.4. Summary of recommendations for action	61

Index of Figures

Figure 1: Product vignette - multi-tier label with the highest security level (3*).	26
Figure 2: Extended label with information about the update guarantee.	28
Figure 3: Rating of the IT security label: simple design - constant price.	30
Figure 4: Rating of the IT security label: simple design - increasing price.	31
Figure 5: Rating of the IT security label: extended design - constant price.	32
Figure 6: Rating of the IT security label: extended design - increasing price.	33
Figure 7: Responsibility for commissioning.	36
Figure 8: Security adjustments before the Initial use.	37
Figure 9: Reasons users do not set up IoT devices themselves.	38
Figure 10: Execution of and responsibility for updates.	40
Figure 11: Updates handled by another person.	41
Figure 12: Reasons for having another person handle the updates.	42
Figure 13: Reasons for not carrying out updates.	43
Figure 14: Responsibility for the security of IoT devices.	45
Figure 15: IT security label from the BSI.	47
Figure 16: Objective understanding of the BSI's IT security label.	49
Figure 17: Subjective assessment of the BSI's IT security label.	50

Index of Tables

Table 1: Published norms and standardisation projects in progress with an impact on the security of IoT products. Source: DIN Consumer Council; own presentation (ConPolicy)	16
Table 2: Regulation concepts for IT security labels. Source of the visual design of the IT security label: BSI, ISO/IEC; own presentation (ConPolicy).	17
Table 3: Measures to protect against risks on the Internet. Source: BSI (2021), Digitalbarometer 2021, 2021 n = 2025, 2020 n = 2000, multiple choices possible.	22
Table 4: Overview of the products and security label in the survey.	27

1. Introduction

1.1. Background

Digital technologies and applications are taking on a greater role in consumers' everyday consumption. The effects of this expansion are ambivalent: On the one hand, consumers profit from new products, services, applications and increases in comfort. On the other hand, they find themselves facing new challenges and risks, in particular, with respect to the IT security of their devices and the protection of their privacy. Society is intensively discussing matters pertaining to privacy and data protection, but IT security matters are being discussed much less to date. Consumers' knowledge, behaviour and attitudes regarding IT security are therefore the topic of this study.

To protect consumers against security risks and enable them to ensure their own IT security, a mixture of instruments has formed on three levels: *Statutory regulations* define minimum standards and guide rails; sub-statutory *norms and standards* illustrate for the manufacturers and providers how they can comply with the statutory regulations; and *consumer education and consumer information activities* promote informed consumer behaviour.

However, these instruments currently leave large gaps in ensuring IT security. According to the current data collected by the non-profit association Deutschland sicher im Netz e. V. [Germany, Secure Online], the security situation of consumers has deteriorated. A growing number and intensity of threats faces a stagnation regarding the topics of knowledge of and behaviour regarding security. The consequence is that the security index is currently at its lowest measured values.¹

The Internet of Things (IoT) growth market is particularly relevant here. While only 2.3 percent of the consumers surveyed in 2015 used networked home technology, that number increased to 11.0 percent in 2022. 15.4 percent of consumers currently use networked entertainment electronics. This entails a significant, inherent sense of uncertainty: According to the same survey, 31.1 percent of the surveyed consumers consider networked home technology to be dangerous or very dangerous; 25.4 percent have this same concern regarding networked entertainment electronics.²

The effective protection of consumers therefore remains a problem that must be solved in practice. On the three described levels of measures in the IT security sector, it is important to consider the measures from the consumers' side. That is the only way for the measures to protect consumers against IT security risks and enable them to deal with digital products and applications in an informed and competent manner.

¹ Deutschland sicher im Netz e.V. (Hrsg.) (2022), DsiN Sicherheitsindex 2022: Digitale Sicherheitslage von Verbraucher:innen in Deutschland [DsiN Security Index: Digital security situation of consumers in Germany]. Queried from <https://www.sicher-im-netz.de/dsin-sicherheitsindex-2022> (2022-07-11).

² Deutschland sicher im Netz e.V. (Hrsg.) (2022), loc. cit. (Fn. 1).

1.2. Objective and questions

With this in mind, the objective of this study, conducted on behalf of the DIN Verbraucherrat [Consumer Council] (DIN-VR), is to collect data on **consumer knowledge of and behaviour towards IT security and requirements and wishes regarding the further development of the boundary conditions and support measures.**

It focuses on security aspects of devices on the **Internet of Things (IoT)**. The “Internet of Things” refers to **everyday items that are not conventionally seen as computers but that are equipped with network connectivity and computing capacity by way of which they are integrated into the Internet.**³ While some IoT applications, like smart door locking systems or smart heater controllers are currently only used in households with a high affinity to technology, others are widely distributed, like the router as an access point of the home network to the Internet, the smart phone as an Internet-capable progression of the telephone or the smart TV as an Internet-capable television (cf. survey results in Section 4.3, p. 34 et seq.).

1.2.1. The term “IT security”

The term, “**IT security**” or, “cybersecurity”, a synonym thereof, is defined in this paper as per the definition stated in the BSI Gesetz [Act on the Federal Office for Information Security, BSI Act], namely, as the **prevention of data manipulation and unauthorised disclosure of information** (cf. Sec. 2 (2) p. 2 of the BSI Act⁴).

In this respect, **IT security** is considered a fundamentally different matter than **data protection** and **functional security**. There are areas of overlap between the three areas, however, to the extent that data protection also serves to protect personal data against uncontrolled data outflows and to the extent functional security is negatively impacted by data manipulation.

1.2.2. Key issues

This study focuses on the following key issues:

1. **Inventory:** What are the current empirical “blind” spots with respect to consumer *knowledge of* and *behaviour* regarding IT security with respect to IoT devices and what *expectations and requirements* do consumers have with respect to boundary conditions and potential supportive measures?
2. **Consumer survey:** What statements can be derived based on a representative consumer survey about consumers’ knowledge, behaviour and attitudes regarding the security of IoT devices to the extent there are no findings on this to date? Specifically:
 - What is the current state of *consumer knowledge* with respect to security of IoT devices?

³ definition based on Rose, K., Eldridge, S., Chapin, L. (2015), The Internet of Things: An Overview, p. 16 et seq. Queried from <https://www.internetociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf> (2023-12-01)

⁴ Act on the Federal Office for Information Security (BSI Act) dated 14 August 2009 (Federal Gazette I p. 2821), most recently amended by Article 12 of the Act dated 23 June 2021 (Federal Gazette I p. 1982).

- How do consumers *behave* today with respect to IT security of IoT devices?
 - What *requirements and expectations* do consumers have today with respect to the boundary conditions and potential supportive measures with respect to the IT security of IoT devices?
3. **Conclusions and recommendations for action:** What conclusions can be drawn from the results for consumer policy? How can *usable security*⁵ (in terms of usable security that does not limit the usability) be realised? What recommendations for action can specifically be derived for the DIN consumer council’s work in standardisation?

1.3. Method and structure of the report

In order to properly explore the various issues, **three different methods** were combined in the project:

Literature research was conducted to obtain an inventory, in order to provide an overview of the major regulations (cf. Chapter 2) and the relevant standards as well as of the state of research on the consumer knowledge and behaviour (cf. Chapter 3). In this manner, the gap in research to be closed by the survey was put into concrete terms.

In order to generate our own empirical findings regarding consumers’ knowledge, behaviour and expectations regarding the security of IoT products, a **representative online survey** was conducted (cf. Chapter 4). The questionnaires used for this were first subjected to two pretests; one pertaining to the technical accuracy which involved experts, and the other pertaining to comprehensibility, which involved consumers. Details regarding the method used for the consumer survey are presented in conjunction with the individual data collection steps.

After the survey, a **gap analysis** was performed that compared the expectations of the consumers with the determined status quo. **Recommendations for action in consumer policy and standardisation** are derived from this (cf. Chapter 5).

⁵ Brockhaus, A. (2021), Sicherheit darf kein Hindernis sein – Was ist „Usable Security & Privacy“? [Security Mustn’t Be an Obstacle - What is “Usable Security & Privacy“?] Most recently queried on 2022-08-02 from <https://www.is-its.org/it-security-blog/sicherheit-darf-kein-hindernis-sein-was-ist-usable-security-und-privacy>

2. Fundamentals of IT Security in the Law and Standardisation

IT security refers to the security or protection of information technology infrastructure against risks and harm of any kind, whether external threats, for instance, viruses and cyber attacks or internal risks, in particular, caused by human error when working with the technology.⁶

Ensuring IT security in this context is the purpose of the regulation which, on the one hand, is implemented by legislation and, on the other, by norms and standards which put the technical requirements of IT security into more concrete terms. An overview of both will be provided in the following.

2.1. Statutory bases of IT security

2.1.1. BSI Act

In Germany, the **Act on the Federal Office for Information Security (BSI Act)**⁷ amended by the IT-Sicherheitsgesetz 2.0 [IT Security Act 2.0]⁸, is the central normative basis of IT security law⁹.

Operator obligations

The obligations of operators of information technology infrastructures vary based on whether they operate **critical infrastructures (KRITIS)** with a particularly high potential for damage in the event of IT security malfunctions, for instance, in the areas of energy, traffic, health, water, food supply or finances, or whether they are **digital services** less prone to risk.

KRITIS operators are obligated to register the critical infrastructures they operate with the Federal Office for Information Security (BSI) and specify a point of contact. They are obligated to ensure the availability, integrity, authenticity and confidentiality of the IT systems used, however, the law does not stipulate any specific protective measures to be implemented and instead, leaves the specific security measures to the discretion of the companies. The protective measures must meet the state-of-the-art which creates an incentive to development branch-specific security standards which can then be recognised by the BSI as secure system architectures. In the event of malfunctions, KRITIS operators must report them to the BSI. Breaches of duties regularly result in civil liability claims.

⁶ Bussche, A. v. d., Schelinski, T. (2021), Rechtsgrundlagen der IT-Sicherheit, in: Leupold, A., Wiebe, A., Glossner, S. (publisher), IT-Recht [Legal Bases of IT Security in IT Law], 4th Ed., 2021, p. 736 et seq. (Rec. no. 2).

⁷ Act on the Federal Office for Information Security (BSI Act) dated 14 August 2009 (Federal Gazette I p. 2821), most recently amended by Article 12 of the Act dated 23 June 2021 (Federal Gazette I p. 1982).

⁸ Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme [Second Act on the Increase of the Security of Information Technology Systems] (IT Security Act 2.0) from 2021-05-18 (Federal Gazette I p. 1122).

⁹ IT security-related obligations also arise from general statutory regulations like corporate and commercial law since the corporate due diligence obligations stipulated therein also have an impact on IT security, cf. Bussche, A. v. d., Schelinski, T. loc. cit. (cf. Fn. 6), Rec. no. 12.

Digital services in terms of the BSI Act include **online marketplaces, online search engines and cloud computing services**. The providers of these digital services are obligated to defend against risks to the security of the network and information services they use to provide their digital services in the EU. Like the protective measures for operators of critical infrastructures, the protective measures here are also not further specified, but must meet the state-of-the-art. Here too, there are obligations to report to the BSI and potential liability consequences, however, they are not as severe as those for KRITIS operators.

Duties of the BSI

According to the BSI Act, the **Federal Office for Information Security (BSI)** is the **central office for information security on the national level**. To this end, the BSI assumes a number of duties in the area of IT security, for instance, investigating security risks and developing information technology procedures for security in information technology.

The BSI also assumes duties in the field of consumer protection and informing consumers about IT security matters. The BSI's objectives in digital consumer protection are:

- creating the technical bases and boundary conditions for providers and manufacturers to design secure and trustworthy products and services
- informing, advising and warning consumers so they can safely use digital products and services
- supporting consumers in increasing their resilience so they can manage IT security incidents.

A **voluntary IT security label** is also being developed in this context (Section 9c of the BSI Act). This IT security label consists of a static and a dynamic component. The static component displays the manufacturer's or service provider's assurance that the product meets IT security requirements recognised by the BSI for a specified period of time (manufacturer declaration) and forwards consumers to the dynamic component on the BSI's website (security information) via a link and QR code. The label places focus on the dynamic component which consists of a customised product information page that explains the IT security label to consumers and provides information like the term and manufacturer obligations. A special element found there is current security information about the product via which the BSI can provide information about, e.g. necessary updates or current vulnerabilities. In addition, information, prepared for consumers, about the requirements of the underlying standard is also provided.

The use of the security label is only permitted after obtaining approval from the BSI. However, when issuing its approval, the BSI does not check whether the promised security properties have actually been technically implemented in the framework of the manufacturer's declaration, and instead only checks whether the information provided by the manufacturer is plausible and adequately supported by documentation. The plausibility check includes, among other things, a review as to whether the BSI is aware of vulnerabilities in the product at the time the application is submitted. Moreover, in the framework of the application, manufacturers must illustrate how they proceeded with their internal review and explain how they came to the conclusion that their product meets the requirements. If the manufacturer deviates from optional requirements of the security standard, they must provide a comprehensive substantiation as to why. The manufacturer's information will be reviewed by the BSI and checked for contradictions with respect to the underlying security requirements.

After issuing the IT security label, the BSI market surveillance department will audit the product by way of random spot checks without cause and, with cause,

should vulnerabilities become known. In the framework of the surveillance, applications documents, technical documents and manufacturer documents may be referenced and technical reviews may be ordered. Both the conformity with the manufacturer’s declaration and compliance with the manufacturer’s obligations associated with the IT security label may also be reviewed.

With the introduction of a dynamic component and the downstream monitoring by the BSI market surveillance department, the BSI is setting its IT security label apart from other labels for IoT products.

2.1.2. IT security bases under EU law

The background of German IT security legislation under EU law includes various directives enacted by the European Union¹⁰, in particular, the **General Data Protection Regulation**¹¹, the **NIS Directive**¹², the **Radio Equipment Directive**¹³ and the **Cybersecurity Act**¹⁴. Moreover, the EU Commission is planning further measures to improve IT security, in particular, the **Cyber Resilience Act**¹⁵. The BSI Act implements many of the specifications set forth under EU law; at the same time, the bases of IT security under EU law maintain their own relevance in some respects, as explained in the following.

General Data Protection Regulation

The **General Data Protection Regulation (GDPR)** contains obligations to ensure data security with respect to the protection of the confidentiality of personal data (Art. 32 of the GDPR). These obligations are substantively similar to the regulations described above according to the BSI Act and obligate data processors to implement suitable technical and organisational measures to ensure a level of protection commensurate to the risk. The data security obligations pursuant to the GDPR exceed the BSI Act in that they now only apply to the providers of digital services specified in the BSI Act, but also to all processors of personal data, including the providers of IoT products that process personal data. Under the protective measures in the field of data security, the GDPR specifies, among other things, the **ability to ensure the confidentiality, integrity, availability and resilience of the systems and services in conjunction with long-term processing**. Since the GDPR is directly applicable law in Germany, its

¹⁰ In addition to the laws outlined here, there are other specifications regarding IT security, also on the EU level, for instance, Directive 2001/95/EC concerning general product safety or Directive 2019/771 concerning the sale of goods; the latter stipulates that updates for IoT devices must be made available for as long as consumers can reasonably expect them to be.

¹¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal (EU) L 119 from 2016-05-04 (General Data Protection Regulation)

¹² Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal (EU) L 194 dated 2016-07-19 (NIS Directive)

¹³ Directive (EU) 2014/53 of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, Official Journal (EU) L 153 from 2014-05-22 (Radio Equipment Directive)

¹⁴ Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

¹⁵ EU Commission (2022), Request for a statement on an assessment of the consequences of the Cyber Resilience Act. Most recently queried on 2022-08-03 from https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Gesetz-uber-Cyberresilienz-neue-Cybersicherheitsvorschriften-fur-digitale-Produkte-und-Nebendienstleistungen_de

specifications must be applied directly, even without passing an implementation act under national law.

Radio Equipment Directive

The objective of the Radio Equipment Directive is to ensure the marketability of radio equipment on the domestic market. Radio equipment in terms of the directive includes all electrical or electronic products that, by design, emit or receive radio waves for the purpose of radio communication and/or radio location as well as IoT devices that are connected to the Internet via WLAN. The marketability of this radio equipment is subject to the proviso that they meet fundamental security requirements. These include, to start, the protection of the health and safety of humans, pets and livestock, as well as electromagnetic compatibility. Radio equipment must also guarantee that they **do not cause any harmful impacts to the network or its operation**, that they are equipped with preventive security measures that **ensure that personal data and the privacy of users are protected**, and that they support specific **functions to prevent fraud**.

A **delegated regulation from the EU Commission**¹⁶ bindingly defines a broad scope of applicability of these obligations. In this manner, it activates the corresponding obligations of the Radio Equipment Directive in the area of **cybersecurity**. As a result, all radio equipment that is able to process personal data, traffic data or location data is equipped with security devices that ensure that personal data and the privacy of the user and participant are protected. The corresponding obligations apply starting from 2024-08-01.

Cybersecurity Act

The **Cybersecurity Act** governs, on the one hand, the responsibilities of the **European Union Agency for Cybersecurity (ENISA)** and the **national IT security agencies** and, on the other, sets forth other specifications for a **European cybersecurity certification**¹⁷.

The Cybersecurity Act does not, however, directly establish the European cybersecurity certification, but instead, only creates the legal basis for it. As soon as a cybersecurity certification is approved and accepted on this basis, it will render **national schemes for cybersecurity certification invalid** (Art. 57).

Three different security assessment levels are slated to be implemented in the European cybersecurity certification (low, medium, high, Art. 52). The **requirements of the BSI's IT security label exceed the “low” level, however, they are below the “medium” level** with respect to the security level.

A **self-assessment of the conformity** is only permitted for the “low” assurance level (Art. 53). To obtain certification with the “medium” and “high” assurance levels, compliance with the requirements for awarding the cybersecurity certification must be reviewed by an independent **conformity assessment body**.

¹⁶ Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3 (3), points (d), (e) and (f), of that Directive, Official Journal (EU) L 7 from 2022-01-12

¹⁷ cf. Section 0, p. 63 below.

2.2. Bases of IT security in standardisation

The statutory bases of IT security outlined above usually only define assessments, but not technical measures or procedures. In this respect, the laws are designed to be **supplemented by technical standards and sets of rules**.

Thus, norms are regularly referenced when statutory requirements stipulate **compliance with the state-of-the-art**, for instance, when the BSI Act stipulates that operators of information technology infrastructures or providers of IT services apply the current state-of-the-art to their security measures.

The relevance of norms in conjunction with the **label for IoT products** is even more relevant: The provisions of the BSI Act concerning the security label, like the EU regulations concerning cybersecurity certification, will not become practically effective until the **security measures to be complied with are specifically defined by way of sets of technical rules** and these sets of rules have been officially recognised for the purposes of labelling.

Accordingly, there are **numerous norms and ongoing standardisation projects in the field of IT security**. A brief overview of the most important sets of norms and standardisation projects is provided in the following.

2.2.1. Norms and standards: terminology and effect

Norms and standards are documents that define requirements for products, services or procedures. Their objective is to provide clarity regarding their properties and thus support rationalisation and quality assurance.

In Germany, the standardisation process is organised by the **Deutsches Institut für Normung e.V. (DIN)** [German Institute for Standardisation]. DIN is a registered association and is financed by private industry.

By **involving all interested parties**, irrespective of their financial capacity, DIN ensures fair procedural guidelines. These are defined and publicly available for review in the standards from the DIN 820 “Standardisation Work” series.

The **various types of norms and standards** can be differentiated based on the degree of consensus, i.e., based on the breadth of participation of interested parties. The higher the degree of consensus, the higher the recognition of a standardisation document by society. However, as the degree of consensus increases, so does the amount of time required to develop the standardisation document.

In detail, DIN publishes the following **types of documents**:

1. Norms:

Norms are developed based on consensus. This means that experts agree on a jointly developed version of the contents, taking the state-of-the-art into account, that attempts to take all of the interests of the parties involved into account and eliminate counterarguments.

DIN norms are reviewed every five years with respect to their up-to-datedness. If a norm no longer meets the state-of-the-art, its content is revised or the norm is withdrawn.

2. Standards

- **Technical Specifications (TS)**: A TS is the result of a standardisation process that is not published as a standard by DIN due to certain reservations regarding the content, due to a preparatory procedure that deviates from that of a standard or with respect to the European boundary conditions.

- **Technical Report (TR):** A TR is a progress report that contains findings, data, etc. from standardisation projects that serve to inform about the state of standardisation, including at other international and regional standardisation organisations, and can be referenced as a basis during subsequent standardisation work.
- **DIN SPEC:** A DIN SPEC can be created and published within a few months. Not all parties have to be involved and they do not necessarily have to be created by consensus. DIN SPECS created according to the PAS (publicly available specification) procedure are provided free of charge as a download on the Beuth-Verlag’s website.

The one thing all of these normative documents have in common is that their **application is voluntary**. They only have to be complied with if they have been contractually agreed or are referenced by lawmakers. They cannot **amend, replace or void applicable regulations**. A norm can therefore not clarify any legal matters in the sense that it makes a binding decision regarding the permissibility of a legally disputed corporate practice. This decision falls to lawmakers and jurisprudence.

However, norms and standards can **define undefined legal terms on the sub-statutory level**. Norms define the state-of-the-art in more concrete terms and update it in a flexible manner. Since norms are clear (recognised) rules, references to norms in contracts offer legal certainty. In legal disputes, judges regularly consider DIN norms to be “**prima facie evidence**”. This is a rebuttable legal presumption that results in a **reversal of the burden of proof**.

If a norm or standard is used, the corresponding requirements must also be complied with as a whole. In return, a public statement can be made about the fact that the **respective product complies with a specific norm or a specific standard**. A corresponding **confirmation from a third party in the form of a certification** in return for a fee is also possible.

2.2.2. Standardisation on the German, European and international levels

Standardisation work is carried out **on the German, European and international levels**. Because IT security and the security of IoT products can only be sensibly ensured with cross-border cooperation, the European and international levels are particularly important here.

The **European standardisation organisations** are the **European Committee for Standardization (CEN)**, the **European Committee for Electrotechnical Standardization (CENELEC)** and the **European Institute for Telecommunications Standards (ETSI)**.¹⁸

On the international level, the **International Organisation Standardization (ISO)** and the **International Electrotechnical Commission (IEC)** are active in the areas relevant here.¹⁹

The **German Institute for Standardisation (DIN)** is involved in negotiations pertaining to standards on the European and international levels as a **national mirror committee**. European norms must be applied, without change, as national norms once they are ratified. International norms can also be adopted into the national set of norms after they are published by national standardisation

¹⁸ DIN (2022), DIN in Europa [DIN in Europe]. Queried from <https://www.din.de/de/din-und-seine-partner/din-in-der-welt/din-in-europa> (2022-07-13)

¹⁹ DIN (2022), Internationale Normung [International Standardisation]. Queried from <https://www.din.de/de/din-und-seine-partner/din-in-der-welt/internationale-normung> (2022-07-13)

organisations. However, in contrast to the European norms, there is no obligation to do this.

2.2.3. Norms and standardisation projects relevant to the security of IoT products

The following table provides an overview of the most relevant norms and standardisation projects pertaining to the security of IoT products (cf. p. 16).

Of particular significance in this context is the **European standard ETSI EN 303 645**. It defines **fundamental requirements for the cybersecurity of IoT products for end consumers**. The topics covered include, in particular, password protection and authentication, the disclosure of vulnerabilities, security updates, the secure storage of essential security data, communication security, protection against attacks and a variety of requirements for the easy installation and maintenance of the devices. The associated conformity assessment is based on the ETSI TS 103 701 standard.

The **ISO 27404 standardisation project** is also relevant in the context examined here.²⁰ The objective of this standardisation project is to define a **framework for cybersecurity labels for end consumer IoT devices**. Four assurance levels are assumed here. The first two assurance levels, according to the current state of consultations, are still less exacting than the requirements of the EU Cybersecurity Act; the third and fourth levels, like the EU Cybersecurity Act, require external certification.

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

Table 1: Published norms and standardisation projects in progress with an impact on the security of IoT products. Source: DIN Consumer Council; own presentation (ConPolicy)

²⁰ ISO/IEC, Document dated 2022-05-31, Document No. 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. Summary of the bases of IT security in the law and standardisation

The legal analysis demonstrated the **vast range of selective legal bases in the field of IT security on the German and European levels**. However, there is still a lack of a **consistent requirement for ensuring a high level of security in consumer IT products**.

The requirements of these regulations are **generally formulated** and do not provide any specific technical measures. In this respect, **exacting and practically relevant norms and standards are indispensable** in order to effectively ensure IT security.

With respect to specific matters, **there are various, competing regulatory approaches**. The resulting level of consumer protection in the field of IT security therefore depends on **which regulation concept asserts itself**. As an example of this, the following provides a comparison of the **requirements for an IT security label according to the German BSI Act, according to the EU Cybersecurity Act and the ISO 27404 draft norm** (cf. Table 2).



Basis	BSI Act (supplemented by norms and industry standards)	EU Cybersecurity Act	ISO 27404 draft norm ²¹
Security requirements	Defined by norms or industry-specific IT security standards that are recognised by the BSI.	Basic, minimum requirements for IT security Further requirements depending on the level of protection	No general requirements Protection level defined differently based on the security level
Security level	No differentiation between different security levels	Three security levels	Four security levels
External certification	Plausibility check	Partial: Level 1 no, levels 2, 3 yes.	Partial: Levels 1, 2 no, Levels 3, 4 yes.
Visual design		no specifications (yet)	

Table 2: Regulation concepts for IT security labels. Source of the visual design of the IT security label: BSI²², ISO/IEC²³, own presentation (ConPolicy).

²¹ Presentation according to the draft status of the norm pursuant to ISO/IEC, loc. cit. (cf. Fn. 20) – the presentation may change throughout the further course of consultations regarding the norm.

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

²³ ISO/IEC, loc.cit. (cf. Fn. 20)

3. The Current State of Research: Consumers’ Knowledge, Behaviour and Attitudes Regarding the Security of IoT Devices

There is already comprehensive research on consumers’ knowledge, behaviour and attitudes regarding IT security. Many of the existing surveys pertain explicitly to the security of IoT devices, others to IT security in general. Relevant findings on the security of IoT devices in particular are also gleaned from the latter, general surveys.

The state of research on consumers’ knowledge, behaviour and attitudes regarding the security of IoT devices and IT security in general will be presented in the following as determined based on literature research conducted in the framework of this project.

3.1. Consumer knowledge and behaviour

3.1.1. Use of passwords

Findings on consumer knowledge of IT security are available, in particular on the topic of the **use of passwords**.

Numerous investigations confirm that the vast majority of consumers possess **elementary knowledge of the security requirements** for passwords. 92 percent of consumers worldwide know that it is risky to use the same or similar passwords.²⁴ When it comes to specific security requirements, however, consumer knowledge appears to reach its limits.²⁵ The surveyed consumers tended not to believe that they themselves can effectively protect themselves against hackers using passwords. They also tended not to know when a password starts to be secure.²⁶

Nonetheless, the use of secure passwords is increasing among the population. According to the Digitalbarometer 2021 [Digital Barometer 2021] from the Federal Office for Information Security (BSI), 60% of the German population (14 to 69 years of age) use secure passwords. In comparison to the previous year, this indicates an increase; in 2020, only 48% of the surveyed persons used secure passwords.²⁷

Consumers continue to use **many different accounts** which tends to increase the number of passwords. 78% use up to 20 accounts.²⁸ As a result, many simple or similar passwords are easier to remember. Remembering a difficult password that would meet the security recommendation requires far more cognitive capacity which most do not want to expend. Nonetheless, 63% of the respondents use different passwords for different services according to Initiative D21 (2021).²⁹

Password managers can make the assignment of secure passwords and the practical use thereof easier. 39 percent of the consumers are familiar with password managers, 27 percent of the consumers also use them.³⁰ The discrepancy between the knowledge and practical use might be explained by the fact that the majority of consumers have **reservations regarding password managers**. 78 percent of the consumers in Germany were concerned that a hacker could access all passwords at once³¹.

²⁴ LastPass (Hrsg.) (2021), Psychology of Passwords. Last queried on 2022-07-12:

<https://www.lastpass.com/-/media/9fe0bf5dc473413b8ab4df3bd8688295.pdf>

²⁵ Federal Office for Information Security (BSI) (2020), Die Lage der IT-Sicherheit in Deutschland 2020 [The IT Security Situation in Germany in 2020]. Bonn. Last queried on 2022-07-12:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2

²⁶ BSI (2020), loc. cit. (Fn. 25)

²⁷ Federal Office for Information Security (BSI) (2021), Digitalbarometer 2021: Bürgerbefragung zur Cyber-Sicherheit [Digital Barometer: Population Survey on Cybersecurity]. Bonn. Last queried on 2022-07-12: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2021.pdf?__blob=publicationFile&v=2

²⁸ BSI (2020), loc. cit. (Fn. 25)

²⁹ Initiative D21 (2021). Digital Policy: Digital Skills Gap. https://initiated21.de/app/uploads/2021/08/digital-skills-gap_so-unterschiedlich-digital-kompetent-ist-die-deutsche-bevölkerung.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), loc. cit. (Fn. 25)

³¹ BSI (2020), loc. cit. (Fn. 25)

What is interesting is that 45% of the respondents in a global study had **not changed their password** in the past year, even after a security incident.³²

3.1.2. Two-factor authentication

What was revealing, also with regards to other IT security matters, is the relationship between knowledge and behaviour when it comes to the topic of **two-factor authentication**. The **term** itself, according to a representative survey conducted on behalf of Verbraucherzentrale Bundesverband [Federation of German Consumer Organisations](vzbv)³³, is familiar to **only 43 percent of the respondents** without further clarification. However, **75 percent are familiar with the principle of two-factor authentication**. This indicates that the practical experience with security procedures, for instance when executing banking transactions, also contributes towards practical knowledge based on experience with security technology.

Moreover, in the same survey, **50 percent of the respondents** declared that they would accept only being able to log into a service **with “two-factor authentication”**.

For the use of networked devices/smart home technologies (**IoT devices**), 5% of German Internet users (16 years of age or older) use **two-factor authentication as a security measure**.³⁴

3.1.3. Relevant decision-making factors when purchasing IoT devices

A survey of IoT consumers showed that they **consider data protection and security to be among the most important factors to take into account when purchasing IoT devices**.³⁵

Nonetheless, most of the respondents stated that they had, **in fact, not considered data protection and IT security aspects into account** when purchasing an IoT device.³⁶

An examination of the consumer preferences confirms that, when it comes to smart home devices, consumers tend to **ignore the potential risks** and focus more on the potential benefits that will result from the use.³⁷

³² LastPass (Hrsg.) (2021), loc. cit. (Fn. 24)

³³ Verbraucherzentrale Bundesverband (vzbv) (2021), Zwei-Faktor-Authentisierung [Two-Factor Authentication]. Last queried on 2022-07-12: https://www.vzbv.de/sites/default/files/2022-03/21-08-31_2FA-Chartbericht_freigegeben_0.pdf

³⁴ vzbv (2021), loc. cit. (Fn. 33)

³⁵ Emami-Naeini, P., Dixon, H., Agarwal, Y. and 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, p. 1–12. <https://doi.org/10.1145/3290605.3300764>

³⁶ Emami-Naeini, P., et. al. (2019), loc. cit. (Fn. 35)

³⁷ Wang, X., McGill, T. J. and Klobas, J. E. (2020), *I Want It Anyway: Consumer Perceptions of Smart Home Devices*. Journal of Computer Information Systems. 60:5. p. 437-447.

doi: [10.1080/08874417.2018.1528486](https://doi.org/10.1080/08874417.2018.1528486)

3.1.4. Awareness of data security

At 83%, a majority of the consumers are aware that **services and applications pass on personal data**.³⁸ Moreover, in turn, **only every second consumer is interested in information about security on the Internet**. 22 percent of the consumers even stated that they never inform themselves.³⁹ However, with regards to the topic of **cyber criminality**, a marked desire for more information was determined: According to a representative survey, two-thirds of the respondents would like more information about protection against data theft.⁴⁰

3.2. Discrepancy between knowledge and behaviour: privacy paradox

In summary, it can be said that the knowledge of consumers regarding IT security matters is highly fragmented. The actions of consumers, however, remains far behind this elementary knowledge. The discrepancy between knowledge and action is confirmed by many studies to be a **privacy paradox**. Thus, approximately 67 percent of the consumers in one study were familiar with the security recommendations regarding protection against criminality on the Internet, but only 37 percent implemented them at least partially and only 12 percent implemented them fully.⁴¹

The following **reasons**, among others, can be cited: Consumers **are not familiar with basic IT security standards**. They are also **too optimistic** with respect to the risks of the Internet and cannot imagine being affected. The implementation of IT security measures **takes time users would rather use for their actual tasks or interests**.⁴²

As a positive development, it should be noted that, according to Digitalbarometer 2021, at least **60 percent of the respondents use secure passwords, 62 percent use an up-to-date virus programme, 53 percent an up-to-date firewall, 40 percent use two-factor authentication and 32 percent allow automatic installation of updates**. In comparison to the previous year (Digitalbarometer 2020), protective measures were implemented at a higher rate. There was an average increase of 6.5% per measure.⁴³ (cf. Table 3).

³⁸ Initiative D21 (2021), *Digitalpolitik [Digital Policy]: Digital Skills Gap*. Most recently queried on 2022-07-12: https://initiated21.de/app/uploads/2021/08/digital-skills-gap_so-unterschiedlich-digital-kompetent-ist-die-deutsche-bevölkerung.pdf

³⁹ BSI and ProPK (2021), loc. cit. (Fn. 27)

⁴⁰ Bundeskanzleramt [German Chancellery] & Federal Office for Information Security (2020), Schutz von Online-Konten [Protection of Online Accounts]. <https://www.bundesregierung.de/resource/blob/975272/1732446/4c4377ce98f697a94011955fdc9a1f62/de-passwort-download-zwischenbericht-data.pdf?download=1>

⁴¹ BSI and ProPK (2021), loc. cit. (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 and ProPK (2021), loc. cit. (Fn. 39)

How do you protect yourself against risks on the Internet?	2020	2021
Up-to-date virus programme	57%	62%
Secure passwords	48%	60%
Up-to-date firewall	47%	53%
Secure https connection when transmitting personal data	31%	41%
Two-factor authentication	33%	40%
Automatic update installation	25%	32%
Regular creation of backup copies	20%	28%
Encrypted email communication	18%	23%
Non-use of social media	10%	13%
Non-use of online banking	10%	9%

Table 3: Measures to protect against risks on the Internet. Source: BSI (2021), Digitalbarometer 2021⁴⁴, 2021 n = 2025, 2020 n = 2000, multiple choices possible.

3.3. Attitudes and political demands

When consumers are asked about their demands and wishes, **differences appear based on the degree of digital affinity: Population groups with an affinity for digital media** (especially younger generations between 26 and 55 years of age) would like **more competence in terms of expanding their knowledge and qualifications**. Older generations (older than 56 years of age) who have **little personal, practical experience** with digital media would **primarily like protection by policy-makers** in addition to competence.⁴⁵

In general, consumers are in favour of the idea of having **security and data protection assessments carried out by trustworthy and independent organisations on security labels**.⁴⁶ IoT consumers perceive labels as being accessible and useful when making purchasing decisions.⁴⁷

In the current purchasing environment, however, it is **difficult to impossible for IoT consumers to find information about data protection and security before making a purchase**.⁴⁸ Data protection and security features on an IoT label can impact the perception of risk and willingness to purchase.⁴⁹ 43% of the German Internet population would also like comprehensible information about all of

⁴⁴ BSI (2021), loc. cit. (cf. Fn. 27).

⁴⁵ Initiative D21 (2021), Digitalpolitik: Diese Themen dürfen aus Sicht der BürgerInnen in den Koalitionsverhandlungen nicht fehlen [These Topics Must Not Be Left Out of the Coalition Negotiations According to the Population]. Berlin. Last queried on 2022-07-12: https://initiated21.de/app/uploads/2021/10/d21_kurzexpertise_digitalpolitik.pdf

⁴⁶ Emami-Naeini, P., Agarwal, Y., Cranor, L. F. and Hibshi, H. 2020. *Ask the Experts: What Should Be on an IoT Privacy and Security Label?*. IEEE Symposium on Security and Privacy (SP) 2020. p. 447-464. doi: 10.1109/SP40000.2020.00043. Last queried on 2022-07-12: <https://ieeexplore.ieee.org/abstract/document/9152770>

⁴⁷ Emami-Naeini, P., et. al. (2019), loc. cit. (Fn. 35)

⁴⁸ Emami-Naeini, P., et. al. (2019), loc. cit. (Fn. 35)

⁴⁹ Emami-Naeini, P., Dheenadhayalan, J., Agarwal, Y. and 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. p. 519-536, doi: 10.1109/SP40001.2021.00112.

the important topics related to the private use of IT.⁵⁰ Information about protection against data theft, practical tips on using online nodes and additional security information should be provided by official bodies.⁵¹

3.4. Summary of the state of research and conclusions for the survey

According to the presented research findings, there are **differences between security awareness and security behaviour**. There are also approaches for explaining these differences, but **uncertainties remain regarding the motivation behind consumer behaviour**.

Thus, the following **questions for the empirical survey** can be defined in the framework of this project, which have not been adequately answered by the current literature:

- What role do security aspects play in the motivation of consumers when purchasing IT products?
- What role do security aspects play when putting IT products into service and while using them, for instance, updates?
- How do consumers assess their own responsibility for IT security and what expectations do they have with regard to policy?
- How do consumers specifically assess the IT security label from the Federal Office for Information Security (BSI) recently established in Germany?

⁵⁰ German Chancellery & BSI (2020), loc. cit. (Fn. 40)

⁵¹ German Chancellery & BSI (2020), loc. cit. (Fn. 40)

4. Results of the Population Survey in the Framework of the Project

The consumer survey was aimed at **eliminating blind spots in consumer knowledge and behaviour and expectations pertaining to IoT security aspects** as these have not been or have only been inadequately covered by the literature or other studies.

4.1. Overview and procedure

The survey was structured into five different parts which covered the **entire customer journey of a digital IoT product** or an application and examined all IT security-related aspects:

1. In the first part of the survey, an analysis was carried out to determine which **attributes play a role in the selection of a digital product**. The main focus was on security-related aspects like the inspection body, the objective security level and the update period. Moreover, the role costs or the price of the product play was also illuminated.
2. In the second part, an examination of how customers behave when putting digital products and applications **into service** was conducted. The focus was on the security settings before the initial use of IoT devices.
3. Then, the **usage phase** of the device and how **security updates** are handled were examined in the third part of the survey.
4. In the fourth part, the consumers’ general willingness to assume **responsibility** for their own IT security and the **expectations** placed on lawmakers were illuminated.
5. The fifth and last part dealt with **IT security labels in general** and in the specific case, the static component of the IT security label from the Federal Office for Information Security. The dynamic component, which is the focus of the label, was not looked at.

In addition to these aspects, the questionnaire also covered matters pertaining to socio-demographic attributes. These will not be evaluated separately in the following, but instead taken into account in the respective main segments, if they play a systematic role in the response behaviour.

4.1.1. Spot check and information about the data set

The **entire random sampling** comprises **N=995 participants** who completed the questionnaire in September 2022. The participants were recruited via an actively managed online panel and selected for the study to be representative of online users (quotas set for age, gender and place of residence).⁵²

The average age of the respondents was 48.7 years; the youngest person was 16 and the eldest was 83 years of age. 49% of the respondents were male, 51% female and <1% non-binary. 22% of the respondents had completed a low level of education, 29% a moderate level and 51% a higher level of education. On average, the respondents required just under 19 minutes to complete the questionnaire (average = 17 minutes).

4.1.2. Structure of the results sections

Since the individual parts of the consumer survey deal with **different steps** of the **customer journey**, they will be reported separately from each other, i.e., in separate sections. In each part of the survey, first the **objective** and the relevant **research questions** will be presented. The specific **method**, i.e., the vehicles chosen to optimally answer the research questions follow that. Then, the **results** are presented alongside the research questions. Superordinate results are presented in yellow results boxes. Additional data and facts and figures are presented below that.⁵³

In the statistical evaluation of the data set, the primary variables were also examined with respect to the **correlations with socio-demographic attributes**. These include the participants' age in years, gender and digital affinity. The latter, in turn, includes three individual batteries of questions that were each compiled to a total: (1) the number of IoT devices the participants own, (2) their familiarity with various digital terms, like fake news, biometrics or block chain, and (3) their use of various protective measures for their own data security, like separate WLAN networks, updates or offline mode.⁵⁴

An **overall summary** of the results and a **conclusion** can be found in the final section of the individual chapters.

4.2. Part 1: Purchasing networked devices and IT security labels

The objective of the first part of the survey was to examine the **users' behaviour when purchasing IoT devices** and to review which factors play a role when selecting a networked product.

The specific research questions were:

- Do IT security labels play a role in the purchase of smart products? Do users interpret the information on such labels correctly and purchase the most secure product with the help of the label?

⁵² In total, N=1,000 persons completed the survey. For quality assurance reasons, however, 5 persons were excluded because they either demonstrated abnormally fast response times or did not fully complete the questionnaire.

⁵³ It should be noted that for the purpose of better readability, numeric results like fractions are presented as whole numbers. As a result of rounding to whole numbers, the sum of the response options may not always add up to 100%.

⁵⁴ The entire questionnaire is available as a separate document.

- Does it make a difference whether the products are externally tested or the security is certified by the manufacturer?
- Does the price of the products play a role in the likelihood of purchase?
- Does it make a difference whether additional information about the products' update guarantee is available?

4.2.1. Method

In order to systematically examine the research questions, an **experimental design in the style of a vignette**⁵⁵ was developed in which participants were asked to indicate how **likely they were to purchase** a product with different designs.

Product: The product on offer was a conventional commercial router shown with a brand-neutral image and a fictitious, neutral product name. In addition, the price and information about IT security were shown in each product vignette. Figure 1 shows a sample product vignette.



Figure 1: Product vignette - multi-tier label with the highest security level (3*).

Ranking of five different products: In each decision-making situation, the participants were asked to imagine themselves in a realistic purchasing situation and to state which product they would be most likely to purchase (rank 1), which product would be the second-most likely purchase (rank 2), which would be the third-most likely purchase (rank 3), etc. They were shown five different products that differ with respect to their IT security and, in part, with respect to price. There were also five ranks, from the first to the fifth, that respondents awarded based on their own discretion, influenced by the product characteristics.

Products with varying security levels: Table 4 provides an overview of the five products and information about their features. They each had different security levels that were based on and, with respect to design, derived from the requirements of the IT security label from the BSI, the considerations concerning the EU Cybersecurity Act and the ISO 27404 draft norm.

⁵⁵ A vignette is a product description consisting of systematically varying characteristics. It therefore compiles the characteristics that are relevant to the decision-making situation at a glance and presents them to the respondents.





Product and designation	Description	Figure in the product vignette
Product 1: No label	<ul style="list-style-type: none"> Control group Product does not meet any IT security requirements and therefore does not have a label Objectively the least secure product 	
Product 2: Binary label	<ul style="list-style-type: none"> Product meets the minimum IT security requirements IT security is indicated by a simple label The requirements are certified by the manufacturer The security level is identical to the following label Visual design is based on the static component of the BSI's IT security label 	
Product 3: Multi-tier label (1*)	<ul style="list-style-type: none"> Product meets the minimum IT security requirements IT security is indicated by a multi-tier label The product meets the requirements of the first of three security levels The requirements are certified by the manufacturer The security level is identical to that of the previous label Visual design is based on the EU Cybersecurity Act and the ISO 27404 draft norm 	
Product 4: Multi-tier label (2*)	<ul style="list-style-type: none"> The product meets the medium IT security requirements IT security is indicated by a multi-tier label The product meets the requirements of two of the three security levels The requirements are reviewed by an independent body Visual design is based on the EU Cybersecurity Act and the ISO 27404 draft norm 	
Product 5: Multi-tier label (3*)	<ul style="list-style-type: none"> The product meets the maximum IT security requirements IT security is indicated by a multi-tier label The product meets the requirements three of the three security levels The requirements are reviewed by an independent body Objectively the most secure product Visual design is based on the EU Cybersecurity Act and the ISO 27404 draft norm 	

Table 4: Overview of the products and security label in the survey.

Static label: Only the static aspects were taken into account in all labels, i.e., the label, with the visual design as it is seen by the consumers.

The hybrid concept on which the BSI's IT security label is based was not taken into account in the framework of this study. By combining an Internet page for the specific product via a QR code or link, this relatively new concept offers information, specially prepared for consumers, about the label itself, the underlying security requirements, the update status, current vulnerabilities and the validity of the specific label.

This concept offers an abundance of additional information that cannot be provided on a purely static label due to its up-to-datedness and scope. At the same time, the consumers must take action themselves (e.g. by scanning the QR code) to gain access to the information.

The investigational design, which is limited to the static component of the IT security label, is therefore based on a situation in which these additional information offers cannot be used in practice. Comparable, other case constellations, for instance those applicable in chemical labelling, result in the expectation that this is a frequent situation in practice.

Further studies should, however, be conducted to examine the extent to which the additional information offers are, in fact, accepted by the consumers in practice and how the additional information impacts consumer behaviour.

Four experimental conditions: In total, the design allows for the testing of four experimental conditions that differ with respect to the integrated security label and the price of the products. The first experimental group (“simple constant”) received the already presented, simple design of the security label. In the product vignette, only the product name, the image, information about the security level itself and the issuing body (manufacturer or independent body) were shown. Furthermore, the price of all five products was constant at 99 euros.

The second experimental condition (“simple increasing”) was designed to examine the role of the price or the impact of the product costs on the likelihood of purchase. The price therefore increased with each security level. The product without a label remained at 99 euros. The product with the binary label and the product with the multi-tier label and one star met the minimum IT security requirement level and was identical in both cases. Therefore, the two products each cost 109 euros. The product that met the medium security level and therefore bore the multi-tier label with two stars cost 119 euros accordingly. The objectively most secure product, certified by the multi-tier label with three stars, cost 129 euros.

The third experimental condition (“extended constant”) was designed to examine whether additional information about the update guarantee played a role in the likelihood of purchase. To this end, the product labels were expanded to include information about the update guarantee commensurate with their security level. As shown in Figure 2, there is a note on the label on the two products with minimum IT security, that updates would be available for another two years. On the product with the medium security level, updates were available for another five years and on the offer with the maximum security level, ten years. All of the products in the third experimental group had a constant price of 99 euros.



Figure 2: Extended label with information about the update guarantee.

The fourth experimental conditions (“extended increasing”) was added to also examine the extended label with respect to increasing costs or prices. Therefore, the extended labels with information about the availability of security updates were shown (cf. Figure 2) and the prices increased incrementally from 99 euros (least secure product) to 129 euros (most secure product) in the same manner as in the second experimental condition.

Random assignment of the products and order: In each decision-making situation, all five, different products were simultaneously displayed to the participants on the screen. The order of the five products was fully randomised, i.e., which product was on top and which was below that was selected randomly.

Each participant made their purchase decision twice (assessment of the likelihood of purchase). Which experimental condition was presented first and which thereafter was selected randomly. This resulted in four potential constellations:

1. Constellation: first “simple constant”, then “simple increasing”
2. Constellation: first “simple increasing”, then “simple constant”
3. Constellation: first “extended constant”, then “extended increasing”
4. Constellation: first “extended increasing”, then “extended constant”

This design was chosen to avoid both potential impacts of the order of display and to maximise the number of observations per experimental condition. As part of the assessment while preparing the final data set, an analysis was performed to identify any potential impact caused by the order and the statistical analyses showed that there were no systematic differences in the presentation of the order. Thus, the observations from the individual experimental conditions can be viewed together, irrespective of whether they were presented on the first or second decision-making level.

Observations per experimental condition: Unless otherwise noted, the results are based on the following observation numbers per experimental condition:

- Simple constant N=498
- Simple increasing N=498
- Extended constant N=497
- Extended increasing N=497

4.2.2. Results

Results 1: Users appear to interpret the different security levels represented by the labels correctly. Products with an (objectively) higher security standard are purchased more frequently than those with a lower standard.

Figure 3 shows the rating of the products as shares of the ranking in the “simple constant” experimental condition. If one looks at the median ranks of the various labels, a clear picture arises. The multi-tier label with the three stars, meaning the highest security level with external testing, is in first place, followed by the multi-tier label with two stars and external testing. The users ranked the binary label on which the manufacturer certifies the security in third place. The product with objectively identical features with the multi-tier label and one star and which is also certified by the manufacturer took fourth place.

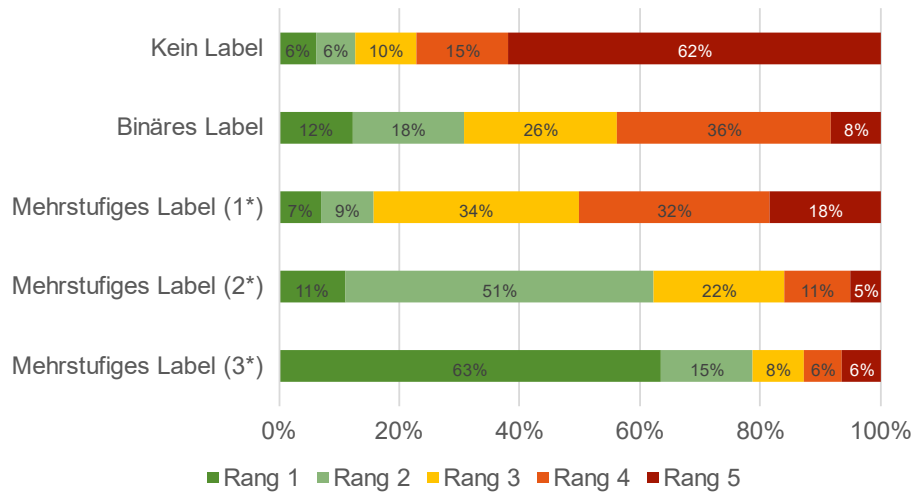


Figure 3: Rating of the IT security label: simple design - constant price.⁵⁶

The result therefore indicates that consumers are able to select the most secure product in a purchase situation with the help of the information on the security labels.

Results 2: Products without labels are purchased less frequently than products with a label.

The product without a label landed in fifth and last place. It is assessed, on average, as being inferior to the other products that bear a security label or those whose IT security is at least partly certified. Almost two-thirds of the consumers put the product in last place and thus express the lowest intention to purchase by comparison.

Results 3: Products with externally reviewed security are purchased more frequently than those whose security is certified by the manufacturer.

The security labels also differ with respect to the inspection body that certifies the security level. On the one hand, there is the group of products whose security is certified by the manufacturer and have also noted this on the label. These include the binary label and the multi-tier label with a rating of one star with respect to the security level. On the other hand, there is the group of products whose security is certified by an independent body. These include the multi-tier label with a security rating of two to three stars. If the two groups are compared, it can be determined that products that undergo independent testing are purchased more frequently than those certified only by the manufacturer. They are ranked higher by the users in the average rating.

What is also interesting is that ratings of the two products whose security is only tested by the manufacturer also differ. Thus, the likelihood of purchasing the product with the binary label is, on average, higher than the likelihood of purchasing the product with the multi-tier label with one star for the security level.

⁵⁶ The average rating as a rank between 1 (best rank and highest likelihood of purchase) and 5 (lowest rank and thus the lowest likelihood of purchase) of the individual products and labels was: No label 4.2, binary label 3.1, multi-tier label (1*) 3.5, multi-tier label (2*) 2.5, and multi-tier label (3*) 1.8.

The fictitious products, however, are designed identically with respect to the testing and the security level and merely differ with respect to their appearance and product name.

Results 4: The price plays no systematic role in the users’ purchasing preferences.

Figure 4 shows the rating of the likelihood of purchasing (ranking order) the products with a simple label and an increasing price. As already outlined in the section on the method, the product without a security label (least secure product) was assigned the lowest price and the product with the highest security level (3 stars, most secure product) was assigned the highest price. The price then increased with each higher security level.

In the median ranks of the various products and labels, the order remained the same, with one exception. In the experimental group with the increasing price, the binary label and the multi-tier label with one star share third place. Nonetheless, the binary label is rated significantly higher here, too.

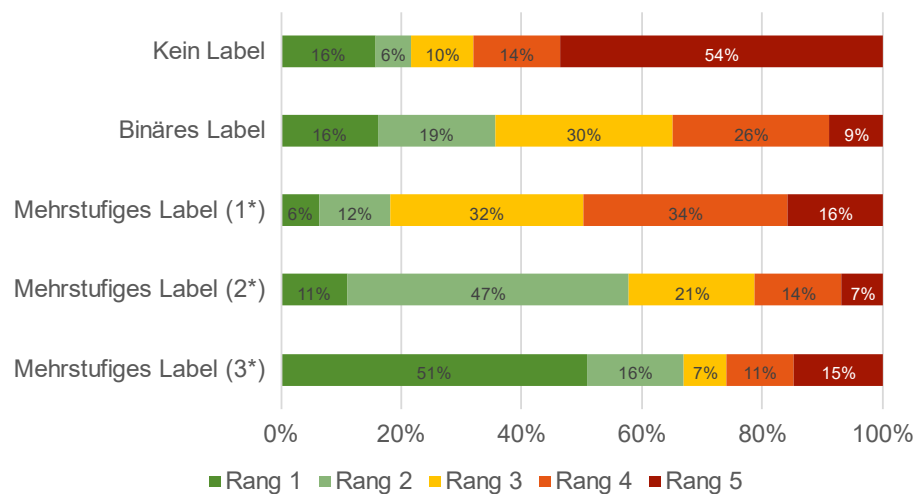


Figure 4: Rating of the IT security label: simple design - increasing price.⁵⁷

What is interesting is that the rank of the objectively more secure products does not change, although their price increased. This cannot be taken to mean that consumers, in reality, would definitely pay more for security, but the analysis does indicate these welcome tendencies.

This result is also confirmed when one compares the average values of the individual products with the constant price and the increasing price. Isolated tests indicate significant differences, but the effect sizes are, at most, small. Consequently, the idea that the price systematically impacts the rating/ranking order cannot be supported.⁵⁸

⁵⁷ The average rating as a rank between 1 (best rank and highest likelihood of purchase) and 5 (lowest rank and thus the lowest likelihood of purchase) of the individual products and labels was: No label 3.8, binary label 2.9, multi-tier label (1*) 3.4, multi-tier label (2*) 2.6, and multi-tier label (3*) 2.2.

⁵⁸ The following were compared during the tests (t tests): multi-tier label with three stars for EUR 99 and multi-tier label with three stars for EUR 129, multi-tier label with two stars for EUR 99 and multi-tier label with two stars for EUR 119, etc.

Results 5: The users' preferences are stable if an extended label with information about the availability of security updates is presented.

Figure 5 shows the rating of the likelihood of purchasing the products furnished with an extended label. In addition to the information about the security level and the inspection body, information about the availability of security updates was displayed. The more secure the product itself was, the longer the security updates were available.

In this case, too, the evaluations show that the rating of the likelihood of the users making a purchase remains unchanged. The more secure a product is, the higher the likelihood of purchase (average and median rank). The binary label and the multi-tier label with one star continue to share third place (median), whereby the average rating for the binary label is better. The least secure product without a label remains in last place.

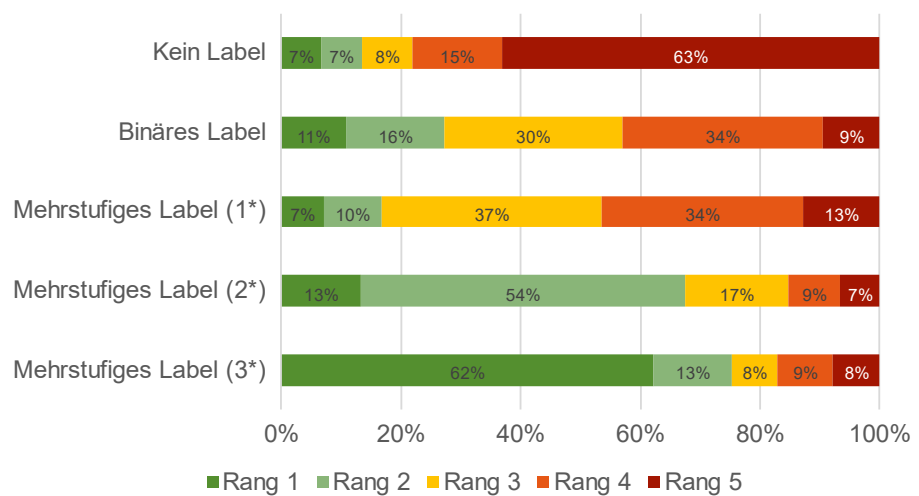


Figure 5: Rating of the IT security label: extended design - constant price.⁵⁹

Results 6: The price also does not appear to have a systematic impact on the users' purchasing preferences with the extended label, either.

Figure 6 shows the results of the rating of the likelihood of purchase (rank) for the extended label with an increasing price. As before, the least secure product is the least expensive and the prices increase incrementally up to the most secure product.

Here, too, the ratings and order of the products remains as is. The average likelihood of purchasing the most secure product with the multi-tier label and three stars is highest. The multi-tier label with two stars follows, then the binary label and the multi-tier label with one star. In last place, and thus the product with the lowest likelihood of being purchased, is the product without a label.

⁵⁹ The average rating as a rank between 1 (best rank and highest likelihood of purchase) and 5 (lowest rank and thus the lowest likelihood of purchase) of the individual products and labels was: No label 4.2, binary label 3.1, multi-tier label (1*) 3.4, multi-tier label (2*) 2.4, and multi-tier label (3*) 1.9.

In comparison to the experimental condition with the constant price, the differences in rating are not systematic.⁶⁰ That means that even in this case, the price of the products does not impact the likelihood of the user making a purchase.

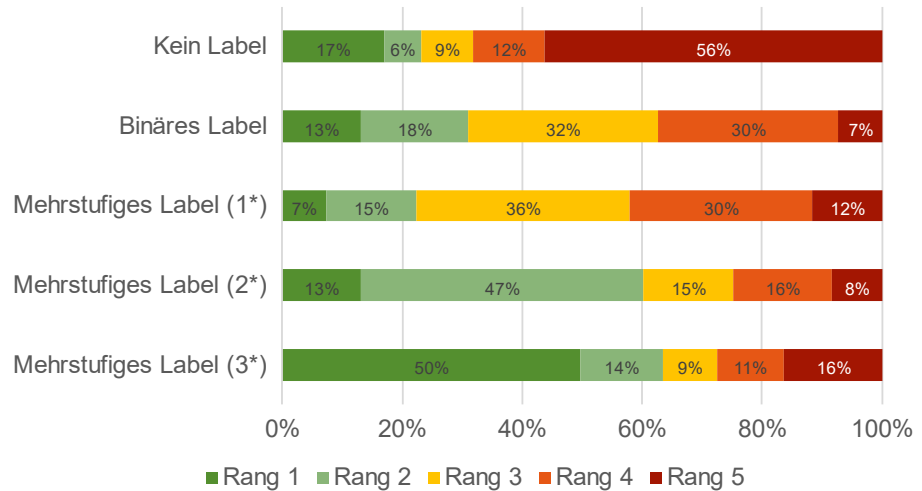


Figure 6: Rating of the IT security label: extended design - increasing price.⁶¹

4.2.3. Correlations with socio-demographic attributes

In addition to the superordinate evaluation of the data, the results were also reviewed with respect to potential correlations with socio-demographic attributes of the respondents.⁶² It was found that there is a positive correlation between familiarity with various technological terms as an indicator of digital affinity and the rating of the most secure product. That means, **the more familiar the consumers are with digitalisation, the more likely they were to purchase the most secure product.** A similar correlation can also be identified for the number of smart devices used. The more IoT devices the respondents own, the more likely they were to purchase the most secure product.

4.2.4. Conclusion: Labels that contain information about the security of IoT devices have the desired effect

The results of the survey show that **labels or security labels** that inform users about the security of digital devices, appear to have the **desired effect**: If the price remains constant, consumers prefer products that meet the requirements of a higher security standard in comparison to non-secure products. Products whose security has not been tested and therefore do not bear a security label, are also rated lowest. In addition, products whose security is certified by an in-

⁶⁰ Isolated, significant differences can be identified in the analysis, however, they are not systematic. The effective sizes of the isolated, significant differences remain very small.

⁶¹ The average rating as a rank between 1 (best rank and highest likelihood of purchase) and 5 (lowest rank and thus the lowest likelihood of purchase) of the individual products and labels was: No label 3.8, binary label 3.0, multi-tier label (1*) 3.2, multi-tier label (2*) 2.6, and multi-tier label (3*) 2.3.

⁶² Only statistically significant results (min. $p < 5\%$) are presented. In group comparisons, the results are based on Chi² tests and logistical regression analyses were used for metric variables.

dependent body are preferred over those whose security is certified by the manufacturer. A positive aspect worth highlighting is that **user preferences are stable** when the **price of security is higher**.⁶³

In addition, the survey was able to demonstrate that the consumers' **purchasing preferences** are also **stable** if **extended information about the availability of updates** are **added** to the label. Ergo, they do no harm, but they also do not have an improved impact on the consumers' decision to purchase. Moreover, secure products are preferred over non-secure products irrespective of the price of the products.

Overall, when implementing labels, it is important to convey a **simple and intuitive message about security**, e.g., “yes or no” or on a scale (in stars). This makes it easier for consumers to select products that are secure. The amount of information should also be considered as should the fact that consumers with a lesser degree of digital affinity should receive support. Moreover, it is also not necessary to pack the label full of superordinate information.

4.3. Part 2: Commissioning IoT devices

In the second part of the survey, the respondents were asked to provide information about their **behaviour before the initial use or commissioning** of a digital device.

The specific research questions were:

- Who sets up the devices before their initial use? Do users do this themselves or do they hand off the commissioning to a third party like persons in their personal environment or external service providers?
- Do users change specific security settings before use? If yes, which?
- What reasons are there for handing off the commissioning to a third party?
- Does the type of digital device play a role in the users' behaviour?

4.3.1. Method

Several **closed questions** were derived from the previously formulated research questions and presented to the participants. To examine any potential **differences with respect to product types**, the participants were divided into three groups, each with a random probability of one third. The first group answered the questions pertaining to the commissioning of a **router**, the second group a **smartphone** and the third group, a **smart TV**.

The respondents were also filtered based on their **personal and specific experience** with commissioning such a device. Thus, at the start of the set of questions, a filter was in place based on whether the respondents had purchased or

⁶³ Here, however, it must be noted that the results of the survey are based only on hypothetical decisions, i.e., the decision to purchase was not actually executed in practice. As a result of the survey design, however, the purchase situation was very realistically simulated. This method has proven itself in research and meets scientific standards.

leased a digital device within the past five years and could therefore report on the follow-up questions pertaining to their behaviour in real life.⁶⁴

The results reported in the following include N=205 observations regarding the commissioning of a router, N=260 observations regarding the commissioning of a smartphone and N=159 observations regarding the commissioning of a smart TV.

4.3.2. Results

Results 7: The majority of the users set up their networked devices themselves before initial use, followed by a set-up carried out by persons in their personal environment. External parties were rarely engaged.

Figure 7 shows the responsibility for commissioning per product. The fact that the majority of users commission the device themselves before initial use applies to all three products. The share is somewhat lower for routers at 62% than for smartphones (75%) and smart TVs (72%). Conversely, routers appear to be more frequently set up by providers or sellers (12%). The shares are somewhat lower for smartphones (3%) and smart TVs (5%). Across all products, family members or friends handle the set-up in a good fifth of the cases. The total share for the router is 22%, for smartphones 21% and for smart TVs, 22%. In very rare cases, external service providers are engaged to carry out the set-up. These comprise 3% for routers, 1% for smart TVs, and <1% for smartphones.

⁶⁴ The period of five years was selected to ensure that the respondents would be able to remember the specific commissioning process. Furthermore, the period had to be long enough for the new purchase or replacement of an existing device to be realistic. To avoid too few respondents being able to report on their personal and specific experience, a hypothetical scenario was formulated parallel to the real scenario. Since the number of observations in the three product categories is adequate, only the actual behaviour will be reported in the following.

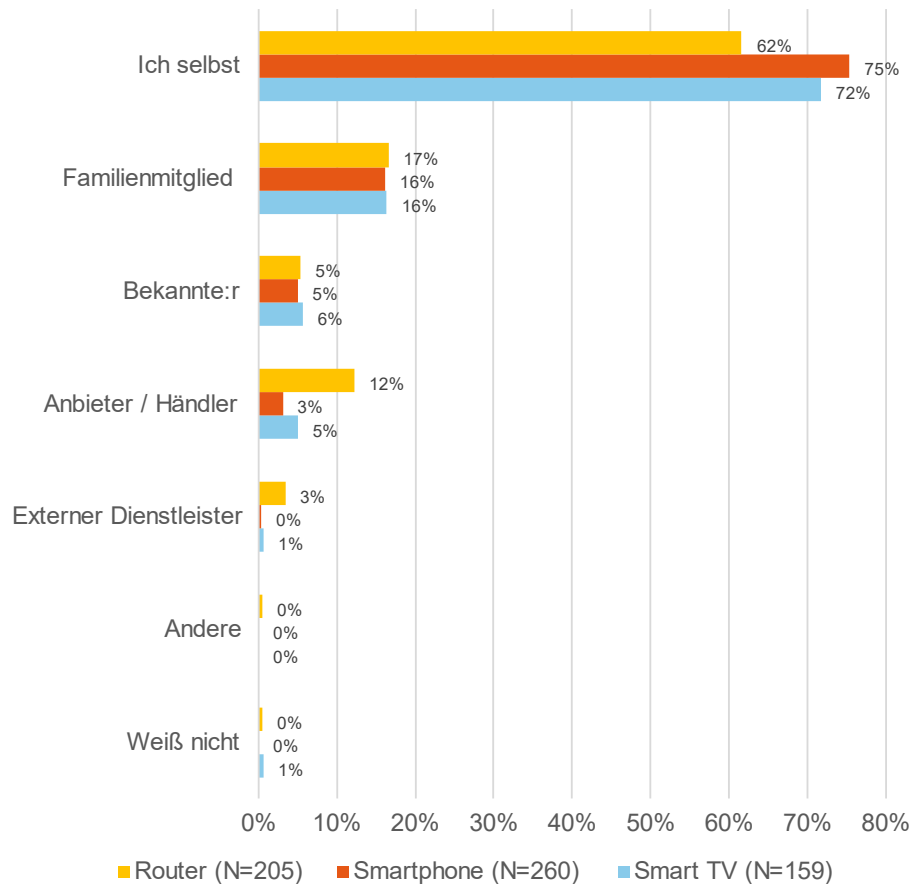


Figure 7: Responsibility for commissioning.

Results 8: The majority of users who set up their own devices also adjust security settings before initial use. The frequency differs from product to product.

Figure 8 shows the share of users who adjust security settings themselves before initial use, by product category. Across all three products, the majority state that they make such security changes, but the shares vary based on the product category. The share of security changes among smartphone users is 84%, followed by 73% for smart TVs and 62% for routers.

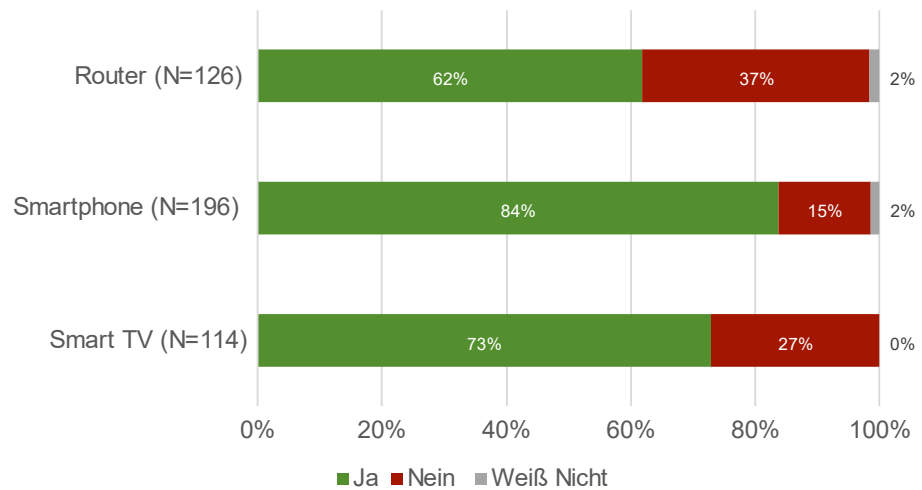


Figure 8: Security adjustments before the Initial use.

In addition, the respondents who stated that they make personal security changes before initial use were asked to specify these changes in an open text field. 34% of these respondents from the router group indicated that they changed their router's password, another 30% specified additional security precautions, e.g. changing the encryption procedure or individual settings pertaining to access to devices in household that are used by children. 49% provided unclear or non-specific information. With regard to smartphones, 27% of the users stated that they had installed additional antivirus protection on their device, 20% mentioned a separate PIN code for the device, 13% use a biometric security procedure to unlock the devices and 12% made other changes like two-factor authentication or update settings. 40% provided unclear or non-specific information. Among smart TV users, 13% stated that they had set up a password or PIN lock for their device. 33% specified further aspects like child locks on the device or the setting that other mobile devices in the household are not permitted to pair with the smart TV. 54% of the respondents provided unclear or non-specific information.

Results 9: In particular, incomprehensibility and a high degree of complexity hinder users in setting up devices on their own. Concerns about making errors during set-up are also among the most frequent obstacles.

As illustrated in Figure 9, 30% of the users hand off the set-up of their smart devices to third parties like persons in their immediate environment or the provider/service provider. Figure 9 shows the reasons the respondents gave for not setting up their digital devices themselves. Across all products, 31% of the users indicate that they do not understand what they have to do during a set-up process. 28% state that the set-up is too complicated for them, whereby this reason is stated more frequently for smartphones and smart TVs at 33% and 34% respectively than for routers at 22%. Another 26% state that they are afraid of changing the settings of the device during the set-up process in such a way that the devices will stop functioning. This share is even as high as 39% for smartphones, while routers, by comparison, are at only 21% and smart TVs 18%. At least 22% of the users across all three products state that the set-up annoys them so much they hand it off to a third person. Further reasons played a subordinate role and can be found in the figure.

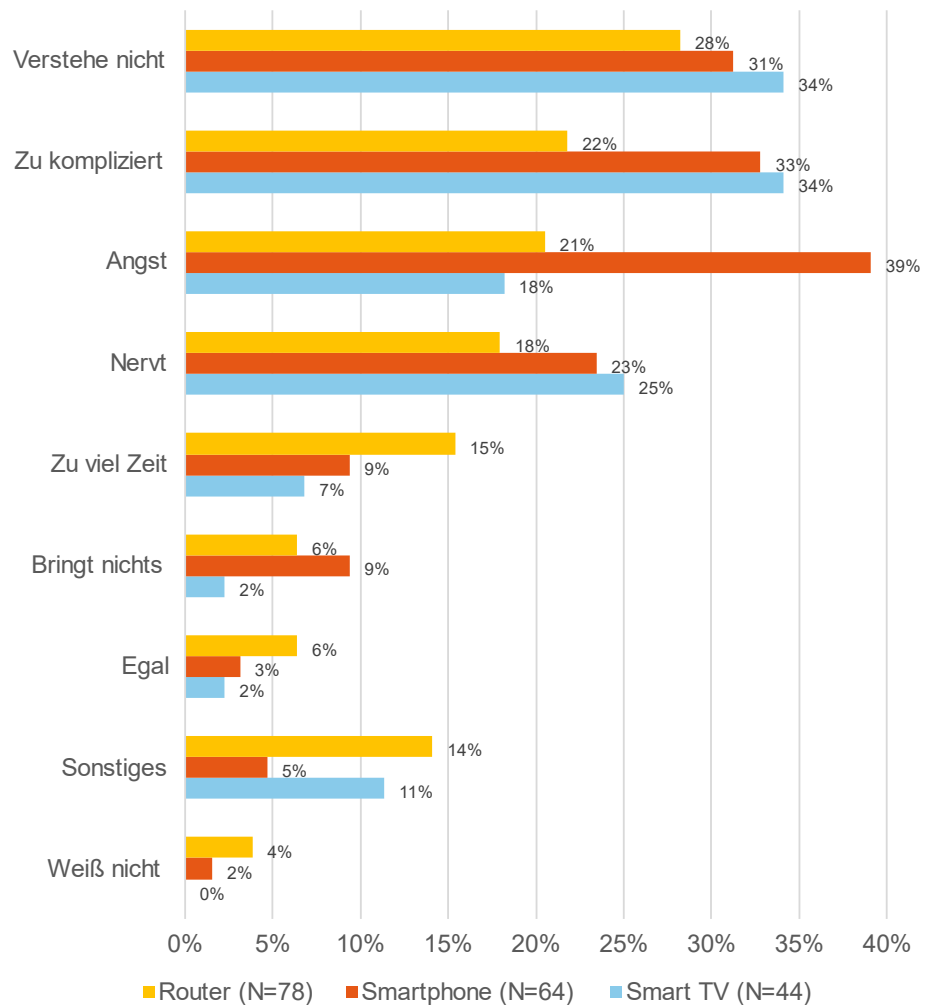


Figure 9: Reasons users do not set up IoT devices themselves.

4.3.3. Correlations with socio-demographic attributes

A further analysis pertaining to correlations with the collected socio-demographic variables also provide interesting findings.⁶⁵ According to these, **male users set up their devices more frequently** than female users (79% versus 60%). Moreover, the age in years has a negative correlation with the probability of a person setting up their own digital device, i.e., **the older the person, the less likely they are to set up a device themselves**. With respect to the **digital affinity**, which is reflected in the number of smart devices in the home, familiarity with the various technologies and technical terms and the use of specific security measures, a **positive correlation with the probability that a user will set up their own device** was identified. That means, (1) the more devices a user owns, (2) the better the users’ state of knowledge is with respect to the various technologies and (3) the more frequently users take precautions for data security, the more probable it is that they will set up their own digital device.

⁶⁵ Only statistically significant results (min. p<5%) are presented. In group comparisons, the results are based on Chi² tests and logistical regression analyses were used for metric variables.

4.3.4. Conclusion: Most users commission their own devices and additional changes to security settings are frequently carried out before the initial use

The survey showed that the **majority of users handle the set-up of their IoT devices themselves and make additional changes to security settings**. This pertains, in particular, to digital products like smartphones which are a constant companion for many users and, in many cases, are characterised by user-friendly user interfaces (operating systems like Android or iOS). Routers, too, are generally set up by the users themselves.

While the set-up is rarely carried out by service providers or the manufacturer, users do, in some cases, hand off the set-up to **persons in their personal environment**. This applies, in particular, to **older consumers** and to consumers who have a **lower degree of digital affinity**. The reasons for handing off the set-up to family, friends or acquaintances include, in particular, that the set-up is **incomprehensible and highly complex**. In some cases, consumers are also concerned that they might make mistakes during the set-up process.

4.4. Part 3: Use of and updating IoT devices

In the third part of the survey, the participants were asked to provide information about their **security-related behaviour while using the products**. This included, in particular, **security updates** intended to ensure the security of the device while it is in use.

The specific research questions were:

- Are digital devices regularly updated by users? Who assumes responsibility for updates?
- Do users who update their IoT devices themselves find this task to be simple or difficult?
- What reasons are there for having third parties perform updates? What reasons are cited for not performing updates at all?
- Does the type of digital device play a role in the users' behaviour?

4.4.1. Method

In response to the formulated research questions, **closed questions** were also developed and presented to the participants. As in the second part of the survey, the participants were assigned to **three different product groups**, namely, routers, smartphones and smart TVs, in order to be able to examine any differences in the products. Therefore, in the third part, respondents remained in the product groups to which they were randomly assigned in the second part.

Moreover, the respondents were asked about their **personal and specific experiences** with the use of the digital devices. The filter question was whether the participants own the digital product.

The results reported in the following include N=305 observations regarding the commissioning of a router, N=313 observations regarding the commissioning of a smartphone and N=242 observations regarding the commissioning of a smart TV.

4.4.2. Results

Results 10: Digital devices are regularly updated by users. This is either carried out completely independently or automatically by the device.

Figure 10 shows the update behaviour of users in practice. Irrespective of the product, 90% of the respondents stated that their devices are updated regularly. With respect to smartphones, the majority of users, 55%, perform the update themselves; with respect to smart TVs, 42% and routers, just under a third at 30%. Automatic device updates are carried out for routers in 45% of the cases; for smart TVs, the share is at 36% and for smartphones, 33%. Very rarely, i.e., in just under 10% of the cases across all products, is the update carried out by another person.

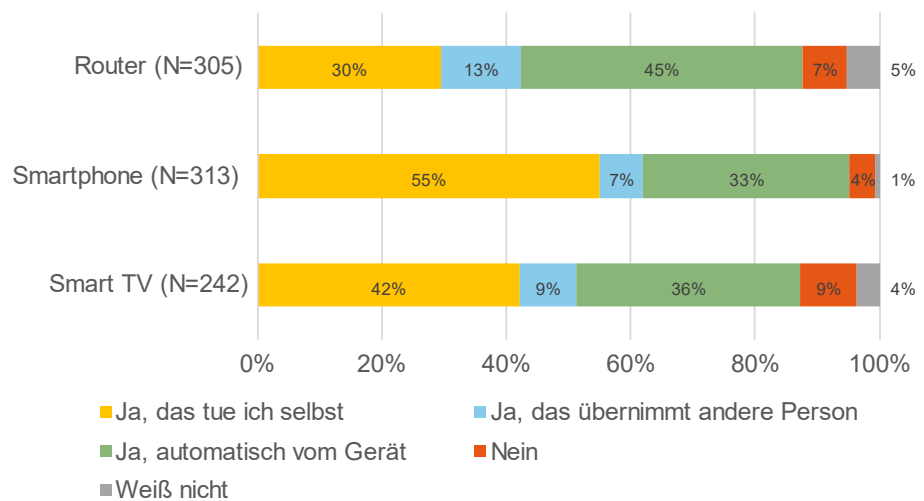


Figure 10: Execution of and responsibility for updates.

Results 11: On average, users find the implementation of updates to be fairly easy.

Users who stated that they carry out updates on their device themselves were asked to evaluate the implementation. This was done on a scale from 1 to 5, 1 being “very difficult” and 5 being “very easy”. The average for all products was 4 (“rather easy”).⁶⁶

Results 12: Updates carried out by third parties are most frequently delegated to personal contacts and less often to external parties.

As already specified, only 10% of the updates are carried out by third parties. Figure 11 shows which shares are allocated to various groups of people and that there are differences in the product groups. 95% of the updates of smart TVs carried out by third parties are carried out by persons in the personal environment (family, friends), routers are at 82% and smartphones, 68%. Conversely, the share of smart TV updates carried out by external persons (providers or external service providers) is 5%, for routers, it is 15% and for smartphones, 32%.

⁶⁶ The average value for routers was 3.63, for smart TVs, 3.9 and for smartphones, 4.0.

It is, however, important to note here that the results are based on very few observations and therefore, individual opinions are weighted more heavily. However, the results correspond with the numbers pertaining to commissioning, so it can be assumed that, in particular, third parties from the personal environment handle the security settings during the usage phase and not external persons.

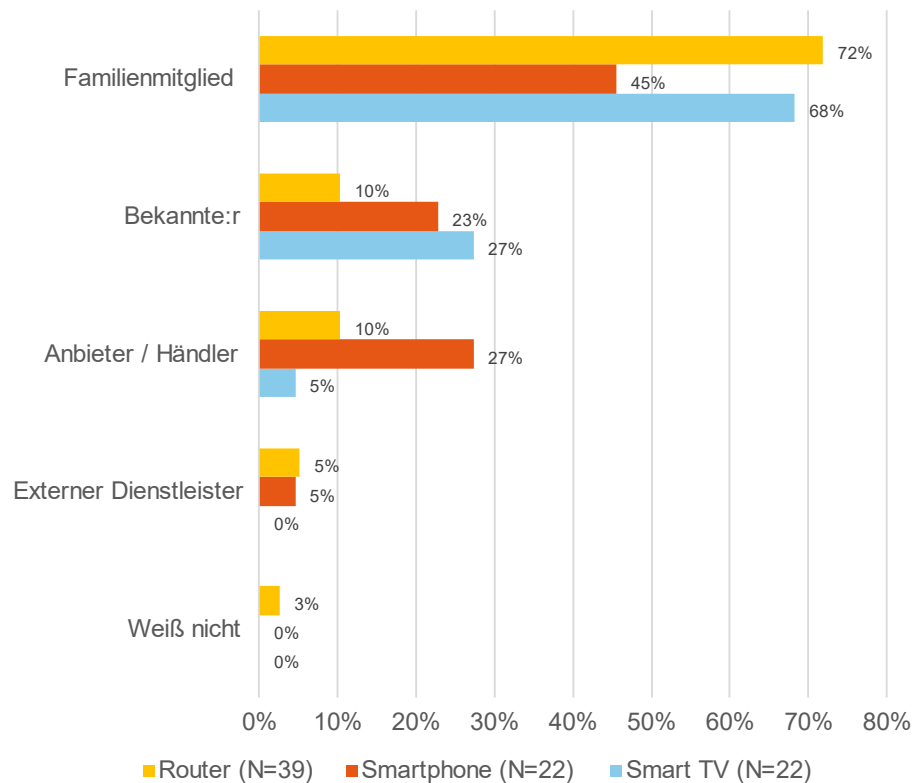


Figure 11: Updates handled by another person.

Results 13: In particular, incomprehensibility, fear and a high degree of complexity are reasons why users have third parties handle updates.

Figure 12 shows the reasons users specify when they have third parties handle updates for them. Here, too, it must be noted that the results are based on a small number of observations, since only very few of the respondents even handed this task off to a third party. Thus, isolated information is weighted more heavily, however, the pattern corresponds to the reasons specified in relation to commissioning.

Across all three products, 33% of the respondents state that they do not understand what to do to execute an update and they therefore hand off the task. 30% also state that they are worried that the updates might change the settings in such a manner that the device no longer functions. Another 22% state that the updates are too complicated for them.

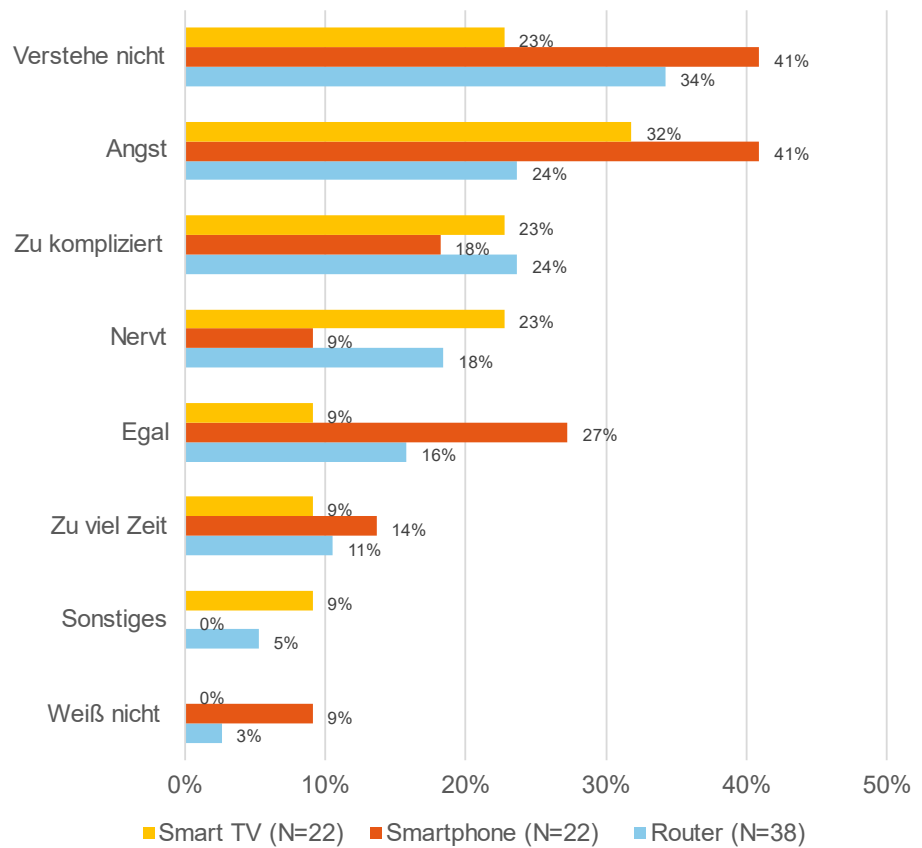


Figure 12: Reasons for having another person handle the updates.

Results 14: Similar reasons are stated as to why users do not carry out any updates at all.

Figure 13 shows the reasons why users do not carry out any updates at all, i.e., neither themselves nor do they have a third party carry them out. First, it must be noted that the share of users who do not carry out any updates at all is very low, at 7% across all products (cf. Results 10).

26% of the users state that fear that the device might not work after an update is the reason. 25% state that they do not understand what to do to implement an update.

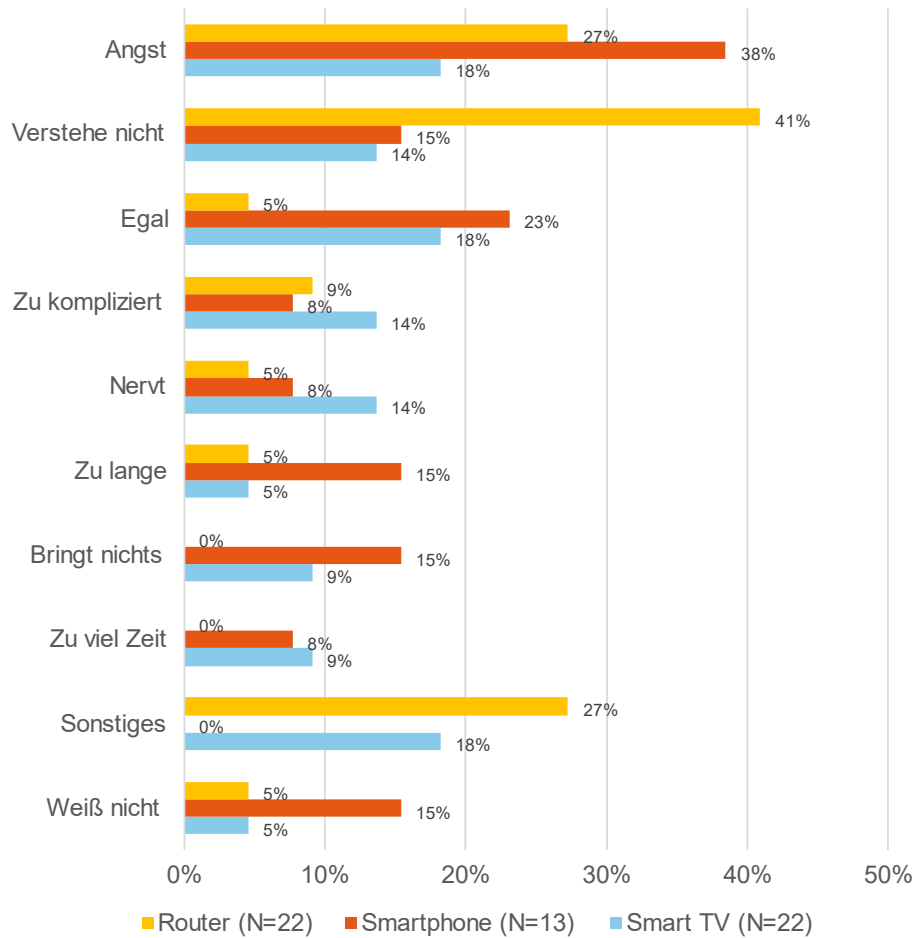


Figure 13: Reasons for not carrying out updates.

4.4.3. Correlations with socio-demographic attributes

Interesting findings were also identified with respect to the additionally collected socio-demographic attributes of the respondents.⁶⁷ These largely correspond to the results regarding commissioning behaviour and draw a clear image that shows that users more or less handle security themselves when using digital devices.

On the one hand, a negative correlation between age and the probability of implementing updates can be identified, i.e., **the older the user, the less likely it was that their devices received security updates**. On the other hand, there is a **positive correlation between digital affinity**, i.e., the number of devices, familiarity with technologies and protective measures taken and the **likelihood that a user will carry out security updates**. Specifically, this means that, (1) the more devices a user owns at home, (2) the more familiar they are with digital technologies and, (3) the more protective measures they use in their private digital lives, the more likely it is that they carry out updates on their digital devices, i.e., routers, smartphones and smart TVs.

⁶⁷ Only statistically significant results (min. p<5%) are presented. In group comparisons, the results are based on Chi² tests and logistical regression analyses were used for metric variables.

4.4.4. Conclusion: The update behaviour when using digital devices is positive overall. The majority of devices regularly receive security updates.

Overall, the survey shows that the majority of the **users regularly update IoT devices and install security updates during the usage period**. This is either done independently or is handled automatically by the device.

Only rarely are updates delegated **to a third party**. Frequently these are users who do not carry out the updates themselves, **older consumers and consumers who have less of a digital affinity**. As is the case with the commissioning of IoT devices, **incomprehensibility fear**, of mistakes and **a high degree of complexity** are cited as **reasons**. Another aspect that must be positively highlighted is that only rarely do users explicitly not install updates.

4.5. Part 4: Responsibility for security and expectations placed on lawmakers

The fourth part of the survey deals with the **responsibility for the security of digital devices** and **expectations** the users place **on legislation** and transparency when communicating security aspects of digital products.

The specific research questions were:

- Are users prepared to play a role in ensuring the security of their digital products?
- Who, in the users' opinion, bears responsibility for the security of their digital devices? How much responsibility do they believe they bear, how much do the manufacturers bear and how much do lawmakers bear?
- What expectations do users have with respect to stricter requirements, i.e., laws or norms pertaining to digital devices and the transparency of IT security aspects.

4.5.1. Method

In order to answer the research questions, **closed questions** were developed and answered by the participants. In the fourth part of the survey, **no additional filtering** is applied to the respondents, so N=995 observations are available for all of the questions.

4.5.2. Results

Results 15: Users are generally willing to change their passwords regularly, but not under any conditions.

First, the participants were asked about their general willingness to change all of their passwords regularly, e.g. for accounts like email, social media, online shopping. 44% of the consumers stated that they were willing (to a limited extent) to change their passwords regularly. Another 39% stated that they would only do this if they were forced by the provider or system. Only 13% stated that they were not prepared and 3% did not provide a statement.

The analyses showed an overall high willingness to take personal responsibility and are also reflected in the already reported actual behaviour of the users. Accordingly, 90% of the users stated that they or another person they engage carry out updates or updates are installed automatically (cf. Figure 10).

Results 16: Users believe they are responsible for the security of their devices.

With respect to the security of digital devices and services, there are different responsible parties. On the one hand, the users are responsible for the security of the device themselves, for instance, avoiding non-secure behaviours. On the other hand, the manufacturer or provider of the device is responsible, for instance, for preventing vulnerabilities that external attackers can use. There is also an external responsibility borne by lawmakers, based on regulation that ensures that, for instance, specific security requirements for products are complied with or non-secure products are excluded from the market. In order to answer the question as to what share of the responsibility these groups bear in the users' opinion, the respondents were asked to divide the overall responsibility (in 100%) across the three groups. They therefore stated which share of the responsibility they bore for the security of their digital devices and what share should be allocated to the providers and lawmakers.

Figure 14 shows the average shares of responsibility for the security of the devices and services used. At 52%, on average, users believe they themselves bear more than half the of the overall responsibility. 30% of the responsibility is allocated to the providers or manufacturers of the devices and services and 18% on lawmakers.

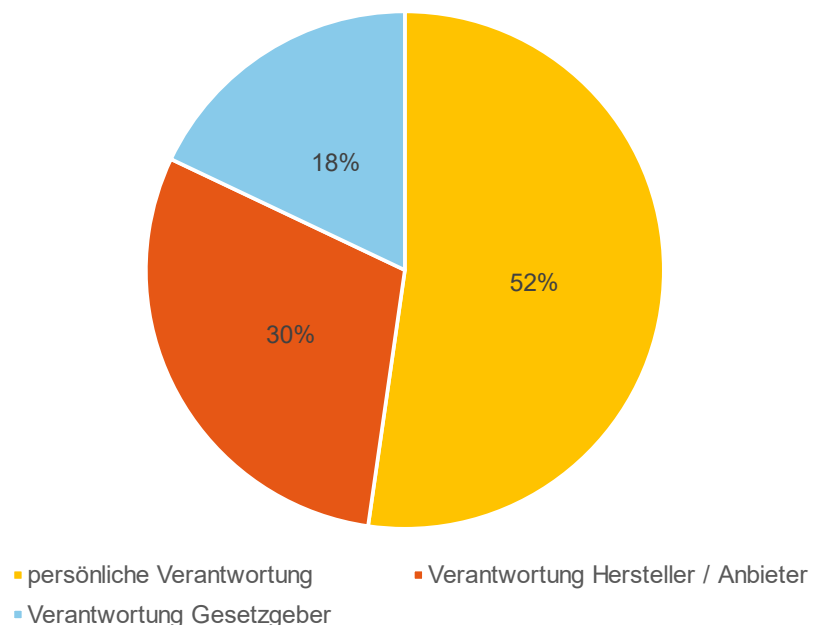


Figure 14: Responsibility for the security of IoT devices.

Results 17: In principle, users would like stricter requirements, i.e., laws or norms pertaining to digital devices and more transparency regarding the IT security aspects of products.

Moreover, the respondents were asked about their expectations regarding the approval of products and the transparency of IT security aspects. The first question pertained to the desire for stricter requirements with respect to the security of digital products, e.g., by way of norms or laws. 63% of the consumers said yes to the desire for stricter requirements for IT security of products, 28% said no and 9% weren't certain.

The second question pertained to the desire for more transparency regarding IT security aspects of products or applications. Here, too, the majority (74%) of the users stated that they desire more transparency. 19% of them did not share this desire and 7% did not respond.

4.5.3. Correlations with socio-demographic attributes

Interesting findings can also be identified with respect to the correlation between the assumption of responsibility and the expectations and the socio-demographic attributes of the consumers.⁶⁸

Thus, there is a **positive correlation between the principle willingness** to regularly change the passwords of the services used and the users' **digital affinity**, i.e., the number of devices used in the home, familiarity with various technological terms and implemented protective measures. Specifically, this means that: (1) The more digital devices a person uses, (2) the more familiar a person is with technological terms and, (3), the more security measures a person implements when using their digital devices, the higher the willingness to regularly change passwords.

With respect to the shares of responsibility allocated to the various groups, there are no systematic differences among the socio-demographic attributes.

Interestingly, there is a **positive correlation between the desire for stricter regulation and familiarity with digital technologies and personal security behaviour**. That means that people who are more familiar with digital technological terms and persons with more pronounced protection behaviours frequently demand stricter requirements, i.e., laws and norms, for devices. A **similar correlation** can also be identified between the digital affinity of the consumers and their **desire for more transparency** regarding IT security aspects. Here, too, the following applies specifically: (1) the more digital devices a person uses, (2) the more familiar they are with digital technologies, and (3) the more protective measures they implement, the more likely it is that they desire more transparency regarding IT security aspects of products or applications. This is similar with respect to the age of the consumers. The older they are, the more transparency they desire.

4.5.4. Conclusion: Users are willing to play a role in ensuring their IT security and also consider themselves responsible. Lawmakers can, however, improve the conditions with respect to requirements and transparency.

The survey shows that **consumers not only demand** security for their IoT devices, **they are also willing to play a role in ensuring their security**. So, they do not pass on the primary responsibility to the manufacturer or lawmakers

⁶⁸ Only statistically significant results (min. $p < 5\%$) are presented. In group comparisons, the results are based on Chi² tests and logistical regression analyses were used for metric variables.

alone. Moreover, they are, in principle, willing to change their passwords. This corresponds to the personal responsibility the users assume when commissioning and using their devices (cf. Parts 2 and 3).

Irrespective thereof, **lawmakers** can provide consumers **additional support**. Thus, consumers generally want **stricter requirements**, i.e., laws or norms for digital devices and **more transparency** regarding IT security aspects of products.

A positive aspect worth highlighting is that not only persons who might require more assistance from lawmakers due to their low degree of digital affinity, also demand it. In contrast, persons with a high degree of digital affinity, and those who already protect themselves to a large extent, demand stricter requirements for devices and more transparency.

4.6. Part 5: IT security labels in general and BSI security labels

The fifth and final part of the survey deals in more detail with the **transparency of security aspects**, namely in the form of so-called IT security labels that can assist consumers when purchasing products. A **specific security label, the so-called IT security label from the Federal Office for Information Security** (hereinafter referred to as the: BSI label) was examined.

The specific research questions were:

- To what extent do consumers find a security label helpful?
- What is the objective comprehensibility of the BSI label? How does it rank in the consumers’ subjective assessment?

4.6.1. Method

To answer the research questions, **closed questions** were formulated for this part, too and posed to the survey participants. The participants were **not filtered** into different groups. Unless otherwise noted, the statistics are therefore based on the overall sample of N=995.

For the questions that pertain specifically to the BSI label, the static components of the **original IT security label from the BSI were always displayed at the same time as the question texts** (cf. Figure 15). The participant were therefore able to consider the information provided on the static component in their responses. Using the original illustration of the static component of the label ensured that participants who were not at all familiar with the BSI label were given a realistic impression.



Figure 15: IT security label from the BSI.

4.6.2. Results

Results 18: In principle, users find an IT security seal or label useful when making a purchase.

First, the respondents were asked to state whether an IT security seal or label that provided information about a device and is printed on the product packaging or is displayed when making a purchase from an online shop, would be helpful. The majority, 75%, said yes; 18% said it would not be helpful and 7% did not respond.

Results 19: The objective understanding of the BSI security label can, in general, be expanded.

In the next step, the participants were shown the BSI label and asked a question about the objective comprehensibility. The results are shown in Figure 16. The question was asked in a quiz format and respondents were supposed to choose which statements or properties correctly apply to the BSI label. Six different statements were presented as answers, two of which were correct and four of which were incorrect.

In total, 7% of the respondents answered the questions completely correctly.^{69,70} A positive aspect worth highlighting is that 59% of the respondents correctly derived from the label that the manufacturer guarantees the security of the device. However, 44% of the respondents incorrectly interpreted the label as an indication that the BSI checks that the requirements have been met before issuing the label. 43% correctly recognised that, with the help of the label, current information about the product could be called up (cf. QR code on the label as well as the hyperlink).

Moreover, almost a third of the respondents incorrectly estimated the security of the device, i.e., they estimated it as higher than it actually was. 30% stated that the label indicated that the product was more secure than other products on the market and 29% interpreted the label as proof that the product meets the highest security standards.

⁶⁹ That means, they correctly selected the two aspects and none of the incorrect aspects.

⁷⁰ 90% answered the question incorrectly and 2% answered “I don’t know”.

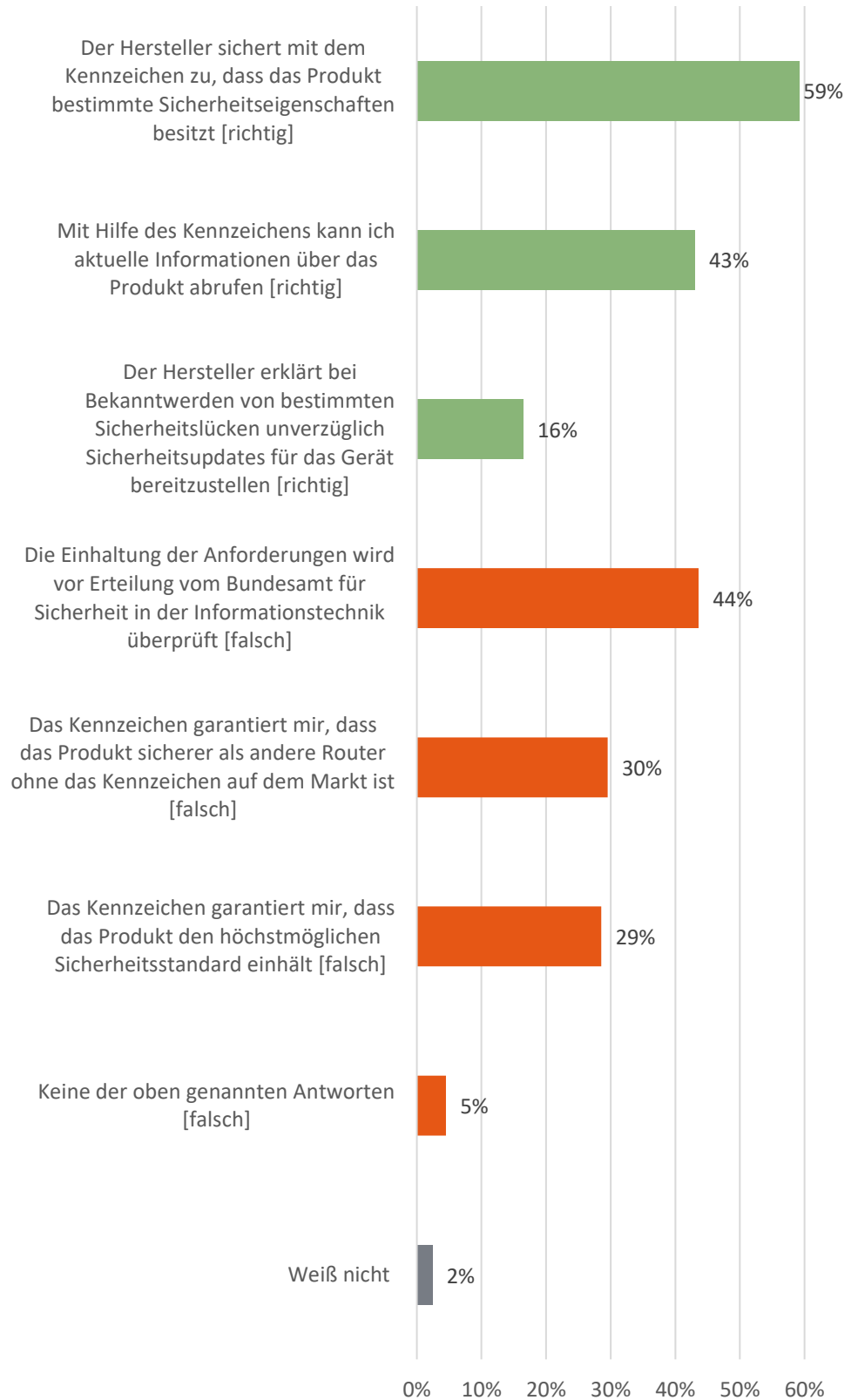


Figure 16: Objective understanding of the BSI's IT security label.

Results 20: Overall, the BSI label is rated positively by the consumers.

Figure 17 shows the results of the two questions pertaining to the subjective assessment of the BSI label. On the one hand, the respondents were asked to assess the (subjective) comprehensibility. 16% stated that the BSI label was "fully and completely comprehensible" and another 44% stated that it was "rather comprehensible". 23% selected "neither", 12% found the label to be "rather incomprehensible" and 3% found it "fully and completely incomprehensible".⁷¹

The second question pertained to the trustworthiness of the BSI label. Here, too, the label was rated very positively. 18% of the respondents stated that the BSI label, in their opinion, was "fully and completely trustworthy", 45% rated it as "rather trustworthy", 26% as "neither", and 7% as "rather untrustworthy". Only 2% stated that the label was "fully and completely untrustworthy".⁷²

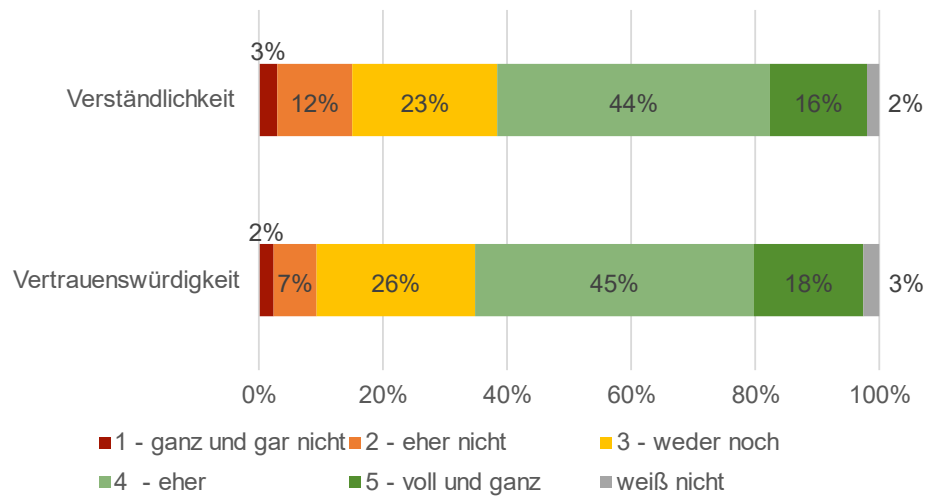


Figure 17: Subjective assessment of the BSI's IT security label.

Results 21: The extent to which the dynamic component of the BSI's IT security label (current, additional information that can be called up via a link) and how this additional information impacts the consumers should be examined in a follow-up study.

As already stated under 4.2.1., the BSI's IT security label conveys its information primarily via the dynamic components to which the participants did not have access in the framework of the survey. In the framework a follow-up study, the BSI's IT security label should be examined including the dynamic component.

⁷¹ 2% no response/don't know.

⁷² 3% no response/don't know.

4.6.3. Correlations with socio-demographic attributes

With respect to the assessment of security labels, several correlations with the socio-demographic attributes of the respondents can be observed.⁷³ Age and **digital affinity correlate with the assessment of the assistance provided by the IT security label**. The older the consumer, the more helpful they rated a seal. In addition, it can be observed that, (1) the more digital devices a person uses, (2) the more familiar they are with digital technological terms, and (3) the more protective measures they are familiar with and utilise, the higher they rated the helpfulness of an IT security label.

Interestingly, with respect to the objective understanding, only isolated correlations with socio-demographic attributes were observed. Only **age and familiarity with digital technological terms** correlate with the **correct interpretation of the BSI label**. The older the respondent and the more familiar they are with various technological terms, the more likely it is that they will answer the question regarding objective knowledge correctly.

A difference can also be identified between the genders when it comes to subjective comprehensibility. On average, **men** rated the BSI label as **more comprehensible than women did**, though, with respect to the objective comprehensibility, there is no difference. With respect to **digital affinity, positive correlations** can be identified in both the **subjective comprehensibility** and the **assessment of the trustworthiness** of the BSI label. Specifically, this means: (1) the more devices the consumers use, (2) the more familiar they are with various digital technologies and, (3) the more protective measures they take, the higher they rate the comprehensibility and trustworthiness of the BSI label.

4.6.4. Conclusion: Consumers demand more transparency through seals. The BSI label, however, can be expanded.

As part 4 of the survey showed, consumers generally want more transparency regarding the security of their IoT devices. Such a design might be, e.g., a label provided to consumers when purchasing products. The **majority of consumers find** such a **label helpful** and, in the first part of the survey on the purchase of digital products, it was shown that the security label does, in fact, have the desired effect. Secure products are purchased more frequently than non-secure products with the help of the label.

One potential design of the label might be the **IT security label from the Federal Office for Information Security**. The survey shows that consumers **rate the label positively overall**, i.e., as rather comprehensible and rather trustworthy. However, what is problematic here is that the subjective comprehensibility deviates from the objective comprehensibility. The **majority** of the consumers **do not correctly understand the contents of the BSI label**. A majority of the respondents assigned attributes to the BSI label that it does not possess. As long as products are secure in general, this isn't a problem. If, however, vulnerabilities arise that render the use of the labelled products non-secure, the BSI label may also cause the consumers to be lulled into a false sense of security if they do not follow the detailed instructions accessible via the QR code and via the link to the BSI website.

Another aspect that the survey identified is that, persons with a high degree of digital affinity in particular rated the BIS label as subjectively comprehensible. In principle, this is hardly surprising, but it also indicates that the contents of the

⁷³ Only statistically significant results (min. $p < 5\%$) are presented. In group comparisons, the results are based on Chi² tests and logistical regression analyses were used for metric variables.

label can be expanded with respect to comprehensibility, particularly for people who require support in the digital world.

4.7. Summary of the survey results

The goal of the consumer survey was to **eliminate blind spots in consumer knowledge and behaviour and expectations pertaining to IoT security aspects** as these have not been or have only been inadequately covered by the literature or other studies. To this end, a total of N=995 online participants, who are representative of the German population, were surveyed.

The results of the survey show that **labels for IT security generally help consumers when purchasing IoT products**. What is important is the design of the labels, therefore, it is crucial to design them in a simple and comprehensible manner. A potential implementation of a security label examined as part of the survey is the IT security label from the Federal Office for Information Security. It is rated positively with respect to the subjective comprehensibility and trustworthiness, however, the static elements examined here can be expanded with respect to the objective comprehensibility. Consumers assign the BSI label properties it does not actually possess. This is not a problem, in principle, for products that are generally secure. If, however, vulnerabilities arise that are problematic with respect to the use of the product, security labels can, in the worst case, lead to people being lulled into a false sense of security if they do not access the information offered by the BSI label via the dynamic component in the form of a product information page via the link or QR code printed on the label. However, in summary, the survey shows that labels for IT security help consumers and the introduction is generally welcome. Here, lawmakers can have a supportive impact and optimise the design of the label and the underlying requirements.

Another focus of the survey was on the consumers' behaviour and use of their own IoT devices. Overall, a positive aspect worth highlighting is that **users are prepared to assume a high degree of personal responsibility for the security of their IoT devices** and already do. They often set up their devices independently and handle the installation of security updates. What would be interesting, in light of this, would be an examination of consumers' willingness to utilise an information offer such as that provided, e.g. via the dynamic component of the BSI's IT security label. The behaviour depends, however, on the type product and the consumers' digital affinity. Some consumers hand off the set-up and updating of their devices to a third party in their personal environment, citing incomprehensibility and a high degree of complexity as the reasons. Some also worry that they will set the device incorrectly and it will stop functioning. For this reason, it is crucial, particularly with respect to user-friendliness and the design of the products during commissioning and updates, that the needs of consumers with a lower degree of digital affinity also be taken into account.

Moreover, the high degree of personal responsibility does not release the manufacturer or lawmakers from their shared responsibility for the security of IoT devices. The surveyed consumers make **clear demands of policy-makers** here and desire **stricter rules**, e.g., concerning the approval of products or with respect to bans on non-secure products. They also want **more transparency** regarding the security of digital devices.

5. Conclusions and Recommendations for Action

Based on the literature analysis and the new findings gleaned from the empirical collection of data in the framework of the study, an attempt will be made to find a conclusive answer to the question of which conclusions must be drawn with respect to consumer policy-related awareness of the topic of IT security and the further role of standardisation in this context.

To this end, the findings obtained throughout the project about the awareness and behaviour of consumers regarding IT security matters will first be compared to the status quo in the law and standardisation (Section 5.1). Based on this comparison, conclusions for consumer policy in general (Section 5.2) and standardisation in particular (Section 5.3) will be drawn.

5.1. Comparison of the empirical findings with the status quo in the law and standardisation

The **consumer survey** made the following core points clear:

- Consumers want **stricter requirements, i.e., laws or norms, for digital devices**.
- Consumers are willing to assume a **high degree of personal responsibility for the security of their IT products**. However, some find it difficult to implement this personal responsibility in practice because they perceive **the devices as incomprehensible and the settings as too complicated**.
- Consumers place great value on creating **transparency regarding IT security when purchasing IoT devices**.

A comparison of the **statutory and normative framework** with respect to these requirements leads to the following results:

- The **statutory provisions pertaining to IT security still have gaps and are very generalised**; there are currently no specific statutory requirements for most IT security issues that are relevant to consumers. **Standardisation** provides more specific requirements, but these are **not implemented consistently in practice**.
- Currently, consumers find it difficult to assume personal responsibility for the security of IT products because the concept of “**usable security**”, i.e., the easy, if possible, intuitive handling of security aspects by consumers, is **currently only implemented to a limited extent in practice**.
- With the **BSI’s IT security label**, a novel, hybrid label was created that provides consumers an instrument for creating transparency regarding IT security when making purchasing decisions. The BSI label also meets a need of the consumers and, accordingly, is **seen in a positive light** overall. However, the BSI security label can, at times, awaken **inaccurate expectations that are too far-reaching** with respect to the security of the labelled products if the consumers only rely on the static element and not the information offered by the BSI label via the dynamic component in the form of a product information page which can be accessed via the printed link and QR code. Therefore, **other multi-tier concepts for security labels like the security certificate** slated to be implemented by the **EU Cybersecurity Act** should be considered as alternatives.

5.2. Recommendations for action for consumer policy

Based on the comparison of the survey results with the status quo in the law and standardisation, the following conclusions can be drawn:

- **A high level of IT security for consumer IT products** must be consistently, seamlessly and specifically defined and implemented by way of laws and standardisation.
- **Usable security** in terms of easy, intuitive use of security features by consumers should be consistently realised by way of legislation and standardisation.
- Above a standard defined by law, the **level of IT security for consumers should be made transparent to consumers when purchasing IoT products**.

Results 22: A consistently high level of IT security for consumer IT products, usable security and transparency regarding IT aspects when making purchases are central objectives of consumer policy.

Though the current legal framework does not yet currently cover these objectives, there are **draft laws** that address these objectives. Two central draft laws are illustrated in the following.

5.2.1. Draft law from the EU Commission for a law concerning cyber resilience (Cyber Resilience Act)

The EU Commission is planning to supplement the EU legal framework for IT security with a **law on cyber resilience (Cyber Resilience Act)**. The corresponding draft law was submitted on 2022-09-15.⁷⁴ In both its problem analysis and its recommendations for solutions, it starts with the points outlined here.

In its **grounds for the recommended Cyber Resilience Act**, the EU Commission states that there are currently two problems pertaining to IT security, namely,

- a **low level of cybersecurity** that is reflected in the widespread vulnerabilities and the inadequate and inconsistent provision of security updates to rectify them and
- **inadequate understanding and inadequate access to information on the users' part** which prevents them from selecting products with appropriate cybersecurity properties or using them in a secure manner.⁷⁵

The **objectives of the Cyber Resilience Act** formulated by the EU Commission correspond to the conclusions formulated above regarding the political challenges in the field of IoT security:

- The commission specifies two objectives to achieve a **high level of IT security** in general:

⁷⁴ EU Commission (2022), Proposal for a Regulation on cybersecurity requirements for products with digital elements - Cyber Resilience Act - COM(2022) 454 final. Queried from <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>

⁷⁵ EU Commission, COM(2022) 454 final (cf. Fn. 74), p. 1.

- Guaranteeing measures implemented by the manufacturer for the security of products with digital elements during the conception and design phase and throughout the entire life cycle;
- Guaranteeing a coherent framework for cybersecurity that makes complying with regulations easier for hardware and software manufacturers
- It specifies the objective of **usable security**: Companies and consumers should be put in a position to securely use products with digital elements.
- It highlights the objective of improving **the transparency of security features of products with digital elements**.

The comprehensive specifications of the Cyber Resilience Act cannot be presented in detail here. What can, however, be made clear is the principle approach with the outlined objectives in mind:

- **A high level of IT security** should be ensured by making IT security generally mandatory for all products with digital elements (Art. 5 of the draft law). Compliance with the relevant specifications will be monitored and implemented by way of conformity assessments (Art. 18 et seq.) and market surveillance authorities (Art. 41 et seq.). This is a major step in comparison to the current legal situation, according to which requirements for IT security are only concretely defined and supported by oversight duties in the field of critical infrastructures and several digital services.
- **Usable security** should be realised by providing users simple, comprehensible information and user instructions concerning the security of digital products (Art. 10 No. 10 in conjunction with Annex II).
- **With respect to transparency regarding security features of IT products when making purchases**, the Cyber Resilience Act primarily refers to the cybersecurity certificate according to the EU Cybersecurity Act (cf. the following Section 05.2.2). This is made even more valuable due to the fact that the cybersecurity certificate can be made mandatory for high-risk IT products (Art. 6 No. 5). The cybersecurity certificate will also be connected to the conformity assessment: If compliance with specific security requirements is a prerequisite for the issuance of the cybersecurity certificate, presumably, products that bear the cybersecurity certificate actually meet these security requirements (Art. 18 No. 3).

This approach, with the realisation of the objectives of the Cyber Resilience Act in mind, corresponds to the recommendations for action for consumer policy derived from the survey. What is important is that the contents of the Cyber Resilience Act also correspond, in detail, to the outlined objectives and that data on existing consumer deficits⁷⁶ are collected throughout the course of the legislative process and further attenuation is prevented.

⁷⁶ The draft law for the Cyber Resilience Act limits the obligation of the manufacturer to eliminate vulnerabilities to a maximum of 5 years (cf. Art. 10 (6) of the draft law). From a consumer perspective, this obligation should apply for the entire service life of a product, as the product otherwise becomes a security risk although it is still physically functional. With the criteria for the classification of IT products into risk categories according to Art. 6 of the draft law in mind, consumer products like smart door locking systems (“security functions”, Art. 6 (2)(a) (iv)) or wearables (“processing personal data”), Art. 6 (2)(c)) should also be classified as products that are prone to risk.

Results 23: The objective and measures of the Cyber Resilience Act must be firmly supported. Throughout the course of the legislative process, existing consumer deficits should be rectified and further attenuation prevented.

5.2.2. Cybersecurity certificate according to the EU Cybersecurity Act

The cybersecurity certificate according to the EU Cybersecurity Act has already been outlined in conjunction with the legal bases of IT security (cf. above Section 2.1.2, p. 13).

In contrast to the BSI’s IT security label, the **EU cybersecurity certificate provides for three security levels**. While a binary label like the BSI security label can be interpreted by consumers as an absolute security guarantee, this gradation makes it clear that **security is always relative**. Therefore, the approach of the EU cybersecurity certificate is preferable in light of the empirical findings gained in the framework of this project.

The legal framework for the introduction of the EU cybersecurity certificate has existed since the Cybersecurity Act was passed, which was more than three years ago at the time this study was created. The drafts of the Cyber Resilience Act also assume the EU cybersecurity certificate will be created. The need for a simple, comprehensible security certificate for IT products is once again confirmed by this study. **It is therefore time for the European Commission to take the initiative in order to introduce the European cybersecurity certificate in practice.**

If the EU cybersecurity certificate is introduced on the basis of the Cybersecurity Act, the question will arise as to which consequences result for the national IT security label from the BSI. If ICT products, services and processes are covered by the EU cybersecurity certificate and, at the same time, by a national IT security certificate, the **national IT security certificate will be rendered void** (Art. 57 of the Cybersecurity Act). This will prevent two different IT security labels appearing next to each other.

Results 24: The EU Commission should take the initiative in order to introduce the EU cybersecurity certificate in practice.

With respect to the **graphic design** of the EU cybersecurity certificate, the **certificate’s frame of reference for the different rating levels must be clarified**. That means, if an IT product receives one star for the lowest security level, it must be clear that the rating scale comprises up to three stars (cf. the design in the test design, Table 4, p. 27). The graphic design of the security label according to the current draft of **ISO 27404**⁷⁷ can therefore be improved. Here, the various levels of cybersecurity are indicated with four stars, however, without making the overall scale of the rating system clear.

Since consumers made their **high degree of interest in transparency regarding IT security aspects** clear in the survey, it should be considered whether the cybersecurity certification should be mandatory not only for particularly risky IT products, but **also in general for consumer IT products** by expanding the applicability of Art. 6 No. 5 of the draft of the Cyber Resilience Act.

⁷⁷ cf. the illustration in Table 2, p. 19.

Results 25: The graphic design of the EU cybersecurity certificate should make the reference framework of the certification with three security levels clear. The extent to which the cybersecurity certificate should be mandatory should be examined.

5.3. Recommendations for action for standardisation

The EU Commission’s draft of the Cyber Resilience Act heavily **relies on standardisation with respect to conformity assessment**: If standards pertaining to security requirements set forth by the Cyber Resilience Act are published in the Official Journal of the EU, it is assumed that products that comply with these standards also comply with the security requirements set forth by the Cyber Resilience Act (Art. 18 No. 1 of the draft of the Cyber Resilience Act). This assumption applies, to a lesser extent, to other standards (Art. 18 No. 2).

If standards serve to further clarify EU legislation, standardisation organisations will become active in the framework of **a standardisation request from the EU Commission**.⁷⁸ The standards that will be developed based on such standardisation requests in the framework of the Cyber Resilience Act are **adapted to legislation with respect to their effect** as a result of the effect of the assumption. Therefore, **strong representation of consumer interests** in this standardisation project is even more important than before to achieve a high level of consumer protection in IT security.

Results 26: A high level of consumer protection in the norms for IT security will become even more important with the Cyber Resilience Act because norms are to be developed in the framework of standardisation requests from the EU Commission in order to further specify the statutory requirements.

⁷⁸ Cf. EU Commission (undated), Standardisation requests. Queried from https://single-market-economy.ec.europa.eu/single-market/european-standards/standardisation-requests_en (2023-01-06).

This results in the following **consequences** for the consideration of consumer aspects in the standardisation of IT security:

The basis for a high level of IT security is security by design, i.e., manufacturers consistently implement IT security according to the newest state-of-the-art when designing IT products and keep IT products secure throughout their entire service life. The **norms concerning the technical requirements for IT security** must ensure this. To this end, the Cyber Resilience Act and the relevant standardisation projects deal with a **wide range of topics** (e.g., reset options, measures to protect against unauthorised access, measures to protect the confidentiality of stored or transmitted data, measures to protect against data manipulation, measures to protect against attacks, measures when vulnerabilities are identified⁷⁹).

In the framework of this project, which specifications should be concretely defined in these various areas of action from the consumer perspective cannot be determined in detail. However, what is informative with respect to standardisation, is the finding from the empirical data collected in the framework of this survey: **At 63%, a clear majority of the respondents spoke in favour of stricter statutory and normative requirements for IT security.**⁸⁰

If specific requirements are defined in norms that serve the purpose of IT security, **these requirements should therefore not be formulated using the optional form of “should” or “may”, but with the binding formulation of “shall”**. Only the formulation “shall” ensures that the companies must, in fact, comply with the corresponding requirements if they want to invoke the norm. This applies, on the one hand, to the **development of a new norm**, but also to the cyclical **review of existing norms**, like the ETSI EN 303 645 standard, every five years.

Currently, security standards are frequently not formulated as obligations in the applicable set of norms in the area of IT security. For instance, the ETSI EN 303 645 standard states, with regard to handling vulnerabilities: “Disclosed vulnerabilities should be acted on in a timely manner”. It therefore does not contradict the act if the response to security vulnerabilities is not prompt. The monitoring of security vulnerabilities is also only formulated as a “should” regulation: “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 Cf., for instance, Annex I from the draft of the Cyber Resilience Act.

⁸⁰ Cf. p. 50 above.

⁸¹ Standard ETSI EN 303 645, Provision 5.2-1.

It must also be noted that **consistent representation of consumer interests in the standardisation of IT security issues will be even more important in the future than it has been to date.**

Results 27: To ensure security by design, high IT security requirements in standards should not be formulated using "should" or "may", but with the binding formulation "shall". Consumer interests should be consistently represented in the technical standardisation project in the area of IT security.

Another important note for the standardisation in the area of IT security is that 52 percent of consumers consider themselves initially responsible for the security of IoT devices, but that **30 percent also attribute an important role to manufacturers and provider of the devices.**⁸² This can result in a **standardisation request** to concretely define the **responsibility for the security of IoT devices or, more generally, digital devices and services.** Fundamental principles for the responsible actions of the economy with respect to corporate responsibility in the age of digital transformation have been developed by the Corporate Digital Responsibility Initiative.⁸³ These principles could constitute the starting point of a norm concerning corporate digital responsibility.

If a norm concerning the responsibility of trade and industry for the impacts of digital products and services on consumers is generally considered expedient, the question arises as to how comprehensive this standardisation project should be with respect to the **bandwidth of the included IT applications** (only IoT or more comprehensive for all IT devices and services) and how comprehensive the **associated objectives** should be (only IT security or general preservation of consumer interests).

Results 28: A review should be conducted to determine whether a standardisation project concerning the responsibility of trade and industry for the protection of consumer interests in the context of digital products and services should be initiated. If the need for such a standardisation project is determined, the devices and services that fall within the scope of the norm and the objective of the standardisation project must be specified in further detail.

The DIN Consumer Protection Council as a representative of the interests of the consumers in standardisation should also particularly advocate for IT security being comprehensible to and usable by consumers and that the idea of **usable security is practically implemented in this manner.** The fact that the draft of the Cyber Resilience Act addresses this topic by way of comprehensive definitions of duties to provide information and instructions for use should be welcomed (cf. Annex II of the draft of the Cyber Resilience Act and see Section 5.2.1 above).

Standardisation can make various concrete contributions, particularly in the area of **usable security**:

- **Instructions for use and security notices should be easy to understand for consumers.**

General instructions on this can be found in the DIN EN 82079-1 standard for the creation of instructions for use (list and explanation of unavoidable technical terms, acronyms and abbreviations, glossary, consistent terminology). Concretely, instructions for use for IT products sold in Germany should

⁸² Cf. p. 50 Figure 14 above.

⁸³ Corporate Digital Responsibility Initiative (CDR Initiative), <https://cdr-initiative.de>; cf., in particular, the CDR Codex, <https://cdr-initiative.de/kodex>

be in German and common languages spoken by residents with an immigration background (Turkish, Polish, Russian, others if applicable⁸⁴). Consistency in the terminology used, both within a document like instructions for use and in terms of a shared understanding of terminology from various IT product manufacturers, is also essential for comprehensibility.

The demand for **comprehensive instructions for use** pertains particularly to the norm currently being developed, **ISO 27403 (Cybersecurity – IoT and privacy – Guidelines for IoT-domotics)**; the demand for the **consistent use of terminology** pertains to **all relevant norms and standards**.

- **Default settings should be used to preset a high level of security.**

The highest possible security level should be preset, particularly where consumers' security needs do not stand in conflict with any other interests, and then activated if consumers do not change settings manually. Security updates should, for instance, be installed automatically unless consumers change the setting. In contrast, other updates that contain extended features and which potentially also result in extended data collection should only be installed on explicit request of the consumers. Accordingly, security updates should be kept separate from other, functional expansion updates and offered to consumers independently thereof. Consumers should also always have the option of acquiring security updates for the originally acquired version of an IT product.

Currently, the norms in the area of IT security do not yet meet these requirements:

The **ETSI EN 303 645 standard** does not contain any mandatory requirement to provide security updates automatically.⁸⁵ The separation of security updates and functional updates is only mentioned as an option.⁸⁶

The current **draft of the ISO 27402 standard (Cybersecurity – IoT Security and Privacy- Device baseline requirements)** only stipulates that the software must have a setting for automatic updates; a default setting for automatic security updates is not mentioned.⁸⁷

- **The draft of the ISO 27403 standard (Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics)** refers to the general ISO 27400 standard (Cybersecurity — IoT security and privacy — Guidelines) with respect to the update requirements. This, in turn, does not mention default settings and automatic updates in its requirements at all.⁸⁸ **Standardisation should pave the way for the technical implementation of usable security.**

For instance, currently, passwords are the primary means of protection against unauthorised access to protected data. For particularly sensitive data, two-factor authentication has become the standard, with the consequence that it has become complicated for the authorised persons to gain access to their own bank accounts or similar sensitive data.

⁸⁴ Cf. Bundeszentrale für politische Bildung (2022), Bevölkerung mit Migrationshintergrund [Federal Agency for Civic Education, Residents with an Immigration Background]. Queried from <https://www.bpb.de/kurz-knapp/zahlen-und-fakten/soziale-situation-in-deutschland/61646/bevoelkerung-mit-migrationshintergrund/> (2022-12-02).

⁸⁵ ETSI, Standard 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.", cf. ETSI, Standard ETSI EN 303 645, Provision 5.3.-4.

⁸⁷ ISO, ISO 27402 draft standard, Section 5.2.8 Software and firmware updates.

⁸⁸ ISO, Standard 27400, Section 7.1.2.17 Provision of software and firmware updates.

In light of this, ways and means should be sought to minimise the amount of effort consumers have to invest in the required security measures. There are various options for this: Biometric recognition characteristics like iris, facial or fingerprint recognition do away with password protection, but create additional risks with respect to the collection of sensitive personal data. Password managers can reduce the effort required to store and enter passwords, but consumers remain sceptical of them. Certifications or non-commercial offers may be useful here in order to increase consumer trust.

Which option is the best to protect against unauthorised access to protected data from the consumer perspective cannot be determined in the framework of this project. What is important, however, is that consumer representation consider innovative technical options to solve security matters in standardisation and open up paths for their use by means of standardisation.

Results 29: In order to implement usable security in practice, standardisation should advocate for the following from a consumer perspective:

- Instructions for use and security notices should be easy to understand for consumers.
- Default settings should be used to preset a high level of security.
- Standardisation should open up paths for the technical implementation of usable security.

5.4. Summary of recommendations for action

The comparison of the survey results with the analysis of the law and standardisation in the area of IT security resulted in the following **central objectives for consumer policy with IT security in mind**:

- **A consistently high level of IT security for consumer IT products,**
- **usable security and**
- **transparency regarding IT security aspects when making purchases.**

Particularly the recommendation of the EU Commission for a Cyber Resilience Act and the cybersecurity certificate in accordance with the EU Cybersecurity Act specifically allow for the identification of perspectives for the realisation of these objectives:

- **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 Cybersecurity Act enables a **high degree of transparency with a graduated assessment of IT security and should, therefore, be implemented as soon as possible.**

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 concretise 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**.