KFV
Kuratorium für Verkehrssicherheit

KFV - Sicher Leben #15

Smart Living in Österreich

Chancen, Risiken, Meinungen & Trends

KFV (Kuratorium für Verkehrssicherheit)

KFV - Sicher Leben #15

Smart Living in Österreich

Chancen, Risiken, Meinungen & Trends

KFV – Sicher Leben. Band #15. Smart Living in Österreich. Wien, 2018

Medieninhaber und Herausgeber
KFV (Kuratorium für Verkehrssicherheit)

Autorinnen
Mag. Monika Pilgerstorfer
Dr. Yvonne Prinzellner

Alle personenbezogenen Bezeichnungen gelten gleichermaßen für Personen weiblichen und männlichen Geschlechts.

KFV
Kuratorium für Verkehrssicherheit

INHALTSVERZEICHNIS

ZUSAMMENFASSUNG

Das KFV beschäftigt sich mit Sicherheitsarbeit in allen Lebensbereichen, ein neues Schlagwort in Sachen Haus & Wohnen ist „Smart Home“. Die innovative Vernetzung aller elektronischen Haushaltsgeräte bringt viele Chancen mit sich, birgt aber auch so manche Risiken. Ein KFV-Expertenteam hat diese Chancen und Risiken analysiert und Empfehlungen für den richtigen Umgang mit den Smart Devices daraus abgeleitet.

Methoden

Um den Status quo sowie mögliche Trends im Bereich Smart Home in der österreichischen Bevölkerung zu erheben, führte *Consent Markt- und Sozialforschung* im Auftrag des KFV eine **telefonische Repräsentativbefragung** von 1.000 Österreichern ab 18 Jahren durch. Dabei wurden die aktuelle Nutzung, geplante Anschaffungen, die persönliche Einstellung zu Smart Home, Beweggründe für die Nutzung oder auch Ablehnung, Gefahrenbewusstsein und eventuell bereits erlebte Schadensfälle erhoben.

Darüber hinaus wurden in zehn qualitativen **Interviews mit IT-Sicherheits- und Technikexperten** aus dem Bereich *Internet of Things* (IoT), durchgeführt von *Consent Markt- und Sozialforschung* im Auftrag des KFV, die Chancen und Risiken von Smart Living näher beleuchtet.

Ergebnisse

In der Befragung stellte sich heraus, dass die Österreicher dem Thema Smart Home zwar hinsichtlich der immer häufiger kolportierten Hackerangriffe eher skeptisch gegenüberstehen, Vorfälle dieser Art in ihrem persönlichen Umfeld jedoch noch nicht in größerem Ausmaß vorgekommen sind.

Trotz ihrer Skepsis verwenden die Österreicher schon jetzt regelmäßig Smart Devices – oft sogar ohne sich dessen bewusst zu sein. Vor allem jüngere Anwender nehmen diese technologische Entwicklung mit Begeisterung auf.

Empfehlungen

- Auf Qualität setzen!
- Beim Datenschutz genauer hinsehen!
- Hackerangriffe erschweren!

Bewusst und gezielt eingesetzt, können Smart Devices eine Entlastung im Alltag darstellen, vor allem durch Zeit- und Energieersparnis. Auf der Website **Sicherheit-mit-Zukunft.at** können Interessierte herausfinden, welcher Nutzertyp sie sind und was sie beachten sollten, um auch zukünftig sicher smart zu leben.

ABSTRACT

KFV's activities cover safety in all areas of life. A new catchphrase nowadays when it comes to house and living is the concept of the "smart home". The innovative networking of all electronic domestic appliances affords plenty of new opportunities but also comes with a number of risks. A team of experts at KFV has analysed the opportunities and risks and developed a set of recommendations for the correct use of so-called smart devices.

Method

To determine the status quo and possible trends regarding smart homes in Austria, KFV commissioned the market research agency *Consent Markt- und Sozialforschung* to carry out a **representative telephone survey** of 1,000 members of the Austrian population over the age of 18. The survey covered their actual use, planned purchase(s) and reasons for the use or rejection of smart devices as well as their personal attitude to smart homes, awareness of the risks and any possible negative experiences they might have already had.

Consent Markt- und Sozialforschung was also commissioned by KFV to carry out ten qualitative **interviews with IT security and technical experts** from the *Internet of Things* (IoT) sector to find out more about the opportunities and risks of smart living.

Findings

The survey revealed that Austrians remain sceptical about the concept of smart homes, due primarily to the frequent reports of hacker attacks. However, the majority have not as yet had any first-hand experience of such incidents.

Despite their scepticism, Austrians already make regular use of smart devices – often without even knowing they are doing so. Younger users embrace these technologies with particular enthusiasm.

Recommendations

- Choose good quality devices!
- Read the data protection information carefully!
- Make hacker attacks more difficult!

When used carefully and for their intended purposes, smart devices can make everyday life easier – especially when it comes to saving time and energy. The website **Sicherheit-mit-Zukunft.at** offers readers the possibility to determine what type of user they are and what they should consider in order to live a safe smart life in future.

KURZFASSUNG

Unsere Gesellschaft erfährt derzeit einen umfassenden Wandel. Die Fokussierung der Work-Life-Balance mit der damit einhergehenden Aufwertung der Freizeit hat auch zu einem Wandel in der Technologieentwicklung geführt. Miteinander vernetzte Geräte sollen unseren Alltag im Haushalt erleichtern. Sie schalten z.B. das Licht aus, wenn wir den Raum verlassen, oder die Heizung ein, sobald es zu kalt wird. Ziel des Smart Home ist es, Komfort und Sicherheit zu verbessern und sogar Energie- und Heizkosten zu sparen. Bezeichnet wird dieses System als „Internet der Dinge", eine digitale Vernetzung von Geräten, die Daten empfangen und aussenden und so über WLAN, Bluetooth- oder RFID[1]-Netzwerke kommunizieren.

Für die Steuerung dieser Prozesse werden Smartphones oder Tablets eingesetzt. Apps dienen als Fernbedienung. Geräte, Apps und Funkprotokolle verknüpfen die Funktionen unterschiedlicher Geräte miteinander.

Ziel

Das KFV beschäftigt sich mit Prävention und Sicherheit in allen Lebensbereichen. Die Digitalisierung macht auch vor dem privaten Heim keinen Halt. Die Vernetzung aller elektronischen Geräte im Haus bringt viele Chancen, birgt aber auch Risiken. Das KFV hat die vorliegende Studie durchgeführt, um herauszufinden,

- wie viele Österreicher bereits „smart" leben,
- wie sicher oder unsicher sich die Österreicher mit smarten Geräten fühlen,
- welche Chancen und ebenso
- welche Risiken Smart Living mit sich bringt.

Um die Chancen eines Smart Home nutzen zu können und dabei das Risiko minimal zu halten, wurden Empfehlungen für einen sicheren Umgang mit Smart Devices abgeleitet.

Methode

Um den derzeitigen Stand der Dinge sowie mögliche Trends im Bereich Smart Home in der österreichischen Bevölkerung zu erheben, führte *Consent Markt- und Sozialforschung* im Auftrag des KFV eine **telefonische Repräsentativbefragung** von 1.000 Österreichern ab 18 Jahren durch. Dabei wurden deren aktuelle Nutzung von Smart Devices, geplante Anschaffungen, die persönliche Einstellung zu Smart Home, Beweggründe für die Nutzung oder auch Ablehnung, das Gefahrenbewusstsein und eventuell bereits erlebte Schadensfälle erhoben.

In zehn qualitativen **Interviews mit IT-Sicherheits- und Technikexperten** aus dem Bereich IoT, durchgeführt von *Consent Markt- und Sozialforschung* im Auftrag des KFV, wurden die Chancen und Risiken von Smart Living erarbeitet. Aus den Ergebnissen der Recherchen und Erhebungen leitete das KFV **Empfehlungen** für die Nutzer der jeweiligen Devices ab.

1 Radio-Frequency Identification: Über einen sehr kleinen Transponder, der einen Code enthält, können Daten gesendet und empfangen werden.

Ergebnisse

Insgesamt ist der Markt in diesem Sektor sehr dynamisch. Eine genaue Definition des Begriffes liegt aufgrund der Vielfalt an verfügbaren smarten Devices, Systemen und Stand-alone-Lösungen noch nicht vor. So haben auch die Endnutzenden unterschiedliche Ansichten darüber, was ein Smart Home oder ein Smart Device ist oder sein kann.

In der Repräsentativbefragung geben 47,8% der Interviewten an, nicht zu wissen, wofür der Begriff „Smart Home" steht. Dennoch **nutzen bereits 45% der Befragten smarte Geräte daheim**. Am häufigsten wird smarte Technologie im Unterhaltungs- und IT-Bereich verwendet. Im **Entertainment-Bereich** werden vor allem Smart-TVs genutzt – rund jeder Dritte nutzt diese. Jeder fünfte Befragte nutzt bereits eine smarte Spielkonsole.

Im Bereich **Licht/Elektrik/Raumklima** werden am häufigsten Bewegungsmelder (13%) und Thermostate (11%) genutzt. Zwei Drittel lehnen smarte Steckdosen ab. Genutzt werden diese von 7% der Befragten. Mehr als ⅓ der Österreicher kann sich die Nutzung von **smarten Rauchmeldern** vorstellen. **Alarmanlagen und Bewegungsmelder** haben ebenso großes Potenzial. Zum Teil werden sie schon genutzt (7% und 12%), mehr als ein Drittel plant eine Anschaffung dieser Art.

Bei Geräten im Bereich **Gesundheit und Medizin** führen sogenannte Fitness-Wearables die Nutzer-Liste mit 7% an. **Smarte Notrufsysteme** sind bisher kaum im Einsatz, 4 von 10 Österreichern planen jedoch deren Kauf. Die Nutzung **smarter Haushaltsgeräte** ist mit 3-5% sehr gering und wird von ¾ der Befragten abgelehnt.

Sowohl Experten als auch Konsumenten sehen eine wesentliche **Chance des Smart Home** in einer **effizienten Alltagsgestaltung**. Experten betonen ebenso ein **gesteigertes Sicherheitsempfinden** als Chance.

Gegen eine Nutzung von Smart Devices sprechen nach Ansicht der Österreicher Argumente wie Abhängigkeit von der Technik und Komplexität der Geräte.

Experten sehen Gefahren in mangelnder Qualität vor allem von Billigprodukten, Unsicherheiten im Datenschutz sowie der Möglichkeit von Hackerangriffen bei unzureichend geschützten Produkten.

Empfehlungen

- **Schutz durch Qualität vor Quantität**
  Beim Kauf von smarten Geräten sollte man sich von Fachpersonal mit IT-Expertise beraten lassen und auf Nachhaltigkeit und Support achten.
- **Datenschutz**
  Eingesetzte Geräte sollten ausreichend technische Möglichkeiten zur Absicherung bieten. Wichtig ist, die Konfiguration aktiv zu betreiben und Einstellungen datenschutzfreundlich zu gestalten.
- **Schutz vor Hackerangriffen**
  Ein überlegtes Passwortmanagement ist Voraussetzung für ausreichenden Schutz. Werden nicht genutzte Geräte ausgeschaltet, erhöht dies zusätzlich den Schutz vor möglichen Angriffen.

EXECUTIVE SUMMARY

Society is currently undergoing a radical change. The focus on work-life balance and associated rise in the value of leisure and free time has also brought about a change in technology development. Networked devices should serve to make life easier. We switch the light of, for example, when we leave a room or turn the heating on as soon as it gets cold. The goal of the so-called smart home is to improve our comfort and security and even save us money on heating and power. This system is referred to as the "Internet of Things" (IoT), a digital linkage of devices which receive and transmit data and thus communicate via WLAN, Bluetooth or RFID[2] networks.

These processes are controlled using smartphones or tablets. Apps are used as remote controls. Devices, apps and communication protocols link the functions of different devices with one another.

Goal

KFV's activities cover safety and prevention in all areas of life. Digitalisation doesn't stop even when it comes to our homes. Linking all electronic appliances in the home affords plenty of new opportunities but also comes with some risks. KFV carried out the study described in this report in order to find out

- how many Austrians already live "smart lives";
- how safe or unsafe Austrians feel with smart devices;
- what chances, and
- what risks come with "smart living".

Based on the findings, recommendations for the safe use of smart devices were developed that will allow people to benefit from the opportunities afforded by smart homes yet at the same time keep the risks to a minimum.

Method

To determine the status quo and possible trends regarding smart homes in Austria, KFV commissioned the market research agency *Consent Markt- und Sozialforschung* to carry out a **representative telephone survey** of 1,000 members of the Austrian population over the age of 18. The survey covered their actual use, planned purchase(s) and reasons for the use or rejection of smart devices as well as their personal attitude to smart homes, awareness of the risks and any possible negative experiences they might have already had.

Consent Markt- und Sozialforschung was also commissioned by KFV to carry out ten qualitative **interviews with IT security and technical experts** from the IoT sector to identify the opportunities and risks of smart living. KFV then used the results of the survey and interviews as well as its own research to develop a set of **recommendations** for users of the different devices.

Findings

The market in this sector is very dynamic. Given the huge variety of smart devices, systems and standalone solutions available on the market, no precise definition of the term really exists. Accordingly, end-users have different ideas on what a smart home or smart device actually is or could be.

2 Radio-Frequency Identification: A method for tracking goods by means of tags which transmit a radio signal.

In the representative survey of the Austrian population, 47.8% of those interviewed admitted that they did not know what the term "smart home" meant. Nonetheless, **45% of them already use smart devices in the home**. Smart technologies are used most frequently in the entertainment and IT sectors. In the **entertainment sector**, smart TVs are the most common such devices – one in three of the interviewees already uses a smart TV. One in five of the interviewees also already uses a smart game console.

In the **lighting/electricity/room temperature** sectors, the most frequently used devices are motion detectors (13%) and thermostats (11%). Two thirds of the interviewees reject smart power sockets, while 7% of them already use such sockets. More than one third of Austrians could imagine using smart **smoke detectors**. **Alarm systems and motion detectors** likewise have strong potential. These are already being used in some cases (7% and 12% respectively), while more than one third of the people interviewed are planning to purchase such devices.

The most common devices in the **health and medical** sectors are so-called fitness wearables, which are used by 7% of the people interviewed. While **smart emergency systems** have so far rarely been adopted, four out of ten Austrians do plan to purchase such a device. The use of **smart household appliances** remains very low (3-5%) and is rejected by three quarters of the interviewees.

Both experts and consumers alike think that **smart homes help people to be more efficient in their everyday lives**. Experts also emphasise the **increased sense of security** as a positive opportunity.

Arguments against the use of smart devices from an Austrian perspective include dependence on technology and the complexity of the devices themselves.

Experts also consider the lack of quality encountered above all in low-price articles, uncertainty concerning data protection and the possibility of hacker attacks on inadequately protected devices to be a risk.

Recommendations

- **Protection through quality over quantity**
  When purchasing smart devices, users should seek the advice of qualified experts with IT expertise and make sure they buy sustainable devices that come with support.
- **Data protection**
  The devices used should offer adequate technical security options. Care should be taken to actively configure the device and make sure the settings comply with data protection requirements.
- **Protection against hacker attacks**
  Good password management is a prerequisite for adequate protection. Switching devices off when not in use increases protection against possible attacks.

1

1 EINLEITUNG

1.1 Hintergrund & Zielsetzung

Smarte Geräte bieten viele Chancen, unseren Alltag komfortabler zu gestalten, uns sicherer fühlen zu lassen und das Gefühl zu vermitteln, jederzeit über alles informiert zu sein. Doch Tatsache ist: Jeder Nutzer, der sich überall in seine Systeme einwählen bzw. bequem zu Hause vom Sofa aus seine Geräte, Lichter etc. bedienen möchte, öffnet ein Fenster für unerwartete externe Zugriffe. Das sind die Risiken des Komforts eines smarten Lebens. Diese Risiken sind bei achtsamem Umgang sehr gering, aber dennoch vorhanden.

In der vorliegenden Studie des KFV wurde untersucht, wie „smart" Österreicher leben. In diesem Bericht werden Chancen und auch Risiken des *Smart Living* dargestellt und Empfehlungen für den sicheren Umgang mit einem Smart Home gegeben.

1.2 Das Internet der Dinge

Das „Internet der Dinge" bezeichnet die digitale Vernetzung von Geräten, die Daten empfangen und aussenden und so über WLAN-, Bluetooth- oder RFID-Netzwerke kommunizieren. Im Haushalt sollen miteinander vernetzte Geräte unseren Alltag erleichtern, indem sie z.B. das Licht ausschalten, wenn wir den Raum verlassen oder die Heizung einschalten, sobald es zu kalt wird. Ziel eines Smart Home ist es, Komfort und Sicherheit zu verbessern sowie Energie- und Heizkosten zu sparen.

Abbildung 1 zeigt die verschiedenen Gebrauchsfelder, in denen vernetzte Geräte bereits Anwendung finden sowie dafür eingesetzte Geräte.

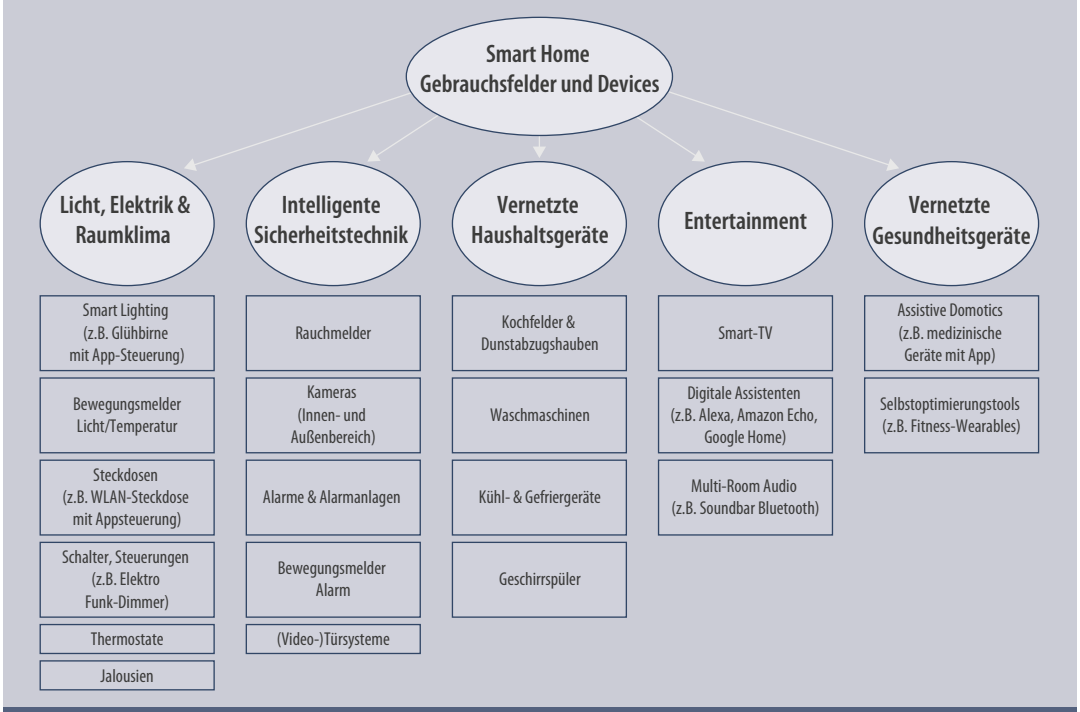

Abbildung 1: *Gebrauchsfelder und Devices im Smart Home*

Zur Steuerung der Systeme werden meist Smartphones oder Tablets eingesetzt. Dabei werden Apps verwendet, die als Fernbedienung für die Geräte funktionieren. Darüber hinaus existieren Geräte, Apps und Funkprotokolle, mit denen man die Funktionen verschiedener Geräte miteinander verknüpfen und durch Wenn-Dann-Szenarien automatisieren kann.

1.2.1 Smart-Home-Lösungen

Ein Smart Home kann einerseits aus diversen einzelnen Smart Devices bestehen, die nicht zwingend untereinander vernetzt sind (Stand-Alone-Lösung). Andererseits kann ein Smart Home als ein über eine zentrale Steuereinheit vernetzter Haushalt (Integriertes Smart Home) verstanden werden.

1.2.1.1 Integriertes Smart Home

Unter integrierten Smart Homes werden Haushalte verstanden, die über eine zentrale, mit dem Internet verbundene Steuereinheit verfügen. Dabei können beliebig viele Geräte und Sensoren miteinander vernetzt werden.

Zur Steuerung des Systems wird eine Basisstation benötigt. Diese Basisstation, auch Hub oder Gateway genannt, kommuniziert mit anderen Geräten über unterschiedliche Funk-Protokolle, wie etwa WLAN, Bluetooth, ZigBee, Z-Wave und andere proprietäre Protokolle (z.B. Beschränkungen durch Patente oder Lizenzen). Diese Systeme sind in der Regel geschlossen, um die Nutzung von Geräten anderer Hersteller einzuschränken. Hersteller können aber auch kooperieren, um die Steuerung von Geräten über nicht herstellereigene Basisstationen zu ermöglichen. Der Trend bewegt sich aber allgemein in Richtung Offenheit solcher Systeme, sodass die Kommunikation mit anderen Devices und eine Standardisierung der Kommunikationsprotokolle ermöglicht wird.[3]

1.2.1.2 Stand-Alone-Lösungen

Bei Stand-Alone-Lösungen erfolgt die Steuerung direkt von einem Smart Device aus, das einen isolierten Funktionszweck erfüllt.

1.2.1.3 Smart Speaker

Diese Systeme haben eine Internetverbindung und können mit anderen kompatiblen Geräten verbunden werden. Smart Speakers können somit als Steuerungsmodule für viele Smart-Home-Produkte verwendet werden. Die bekanntesten Systeme am Markt werden von Amazon, Google und Apple angeboten, es gibt aber auch andere Anbieter. Allgemein haben alle Systeme dieser Art die folgenden Grundfunktionen:[4,5]

- **Möglichkeit zur Steuerung von Lampen, Lichtschaltern, Thermostaten und anderen kompatiblen Geräten**
- **Beantwortung von Fragen; Darbietung von Hörbüchern; Lieferung von Nachrichten, Verkehrs- und Wetterinformationen sowie Sportergebnissen; Abspielung von Musik über Streaming Services etc.**

3 https://www.homeandsmart.de/was-ist-ein-smart-home
4 http://www.techradar.com/news/amazon-echo-vs-homepod-vs-google-home-the-battle-of-the-smart-speakers
5 https://www.amazon.de/Amazon-Zertifiziert-general%C3%BCberholt-Vorherige-Generation/dp/B01GAGVGH8?psc=1&SubscriptionId=AKIAIPHVZTVH6LZ5BFZA&tag=techracom00-21&linkCode=xm2&camp=2025&creative=165953&creativeASIN=B01GAGVGH8&smid=A3JWKAKR8XB7XF&ascsubtag=trd-1112504992-21

1.2.2 Marktentwicklung von Smart Devices

Die meisten Unternehmen bieten in Österreich Produkte für Privat- und Kommerzkunden an. Der aktuelle Trend lässt erwarten, dass die Anzahl der Anbieter smarter Produkte in den nächsten Jahren zunehmen wird.[6]

Allein von September bis Oktober 2015 stiegen die Suchanfragen zum Thema Smart Devices bei Google um 32,9% von 22.200 auf 33.100 und bleiben seitdem auf diesem Niveau.[7] Die häufigsten Suchbegriffe dieser Recherchen sind: „Smart Home Geräte“ (1.600 Suchanfragen), „Smart Home Systeme“ (1.600), „Smart Home Test“ (1.300) und „Smart Home Anbieter“ (320). [8]

Schätzungen zufolge wird der Umsatz am österreichischen Smart-Home-Markt im Jahr 2018 etwa 225 Mio. € betragen. Dabei beträgt der durchschnittliche Erlös pro bestehendem Smart Home derzeit 113,02 €. Laut Prognose wird im Jahr 2022 ein Marktvolumen von 487 Mio. € erreicht. Dies entspricht einem jährlichen Umsatzwachstum von 21,2% (CAGR 2018-2022).[9]

Starter-Sets[10] hatten mit 23.766 Käufen einen Anteil von 19,3% an allen von Mydealz im Zeitraum November 2011 bis März 2016 vermittelten 123.139 Transaktionen.[11]

18,8% der 59,7 Millionen vermittelten Online-Käufe entfielen 2015 auf Elektronikprodukte, 12,8% auf Thermostate, mit denen sich per Funk die Temperatur in einzelnen Räumen tageszeitabhängig und automatisch regeln lässt. Bewegungssensoren und Überwachungskameras haben einen Anteil von 2,2%. Nur 1,9% der Käufe entfallen auf „intelligente Steckdosen“, die die Stromzufuhr für angeschlossene Geräte automatisch regeln.[12]

1.2.3 Delikte und Störfälle im Bereich Smart Home

In der österreichischen Kriminalstatistik scheinen Straftaten im Zusammenhang mit Smart Home oder dem Internet der Dinge nicht gesondert auf. Straftaten wie Datendiebstahl, externe Steuerung von Geräten u. ä. sind in der Kategorie „Cybercrime“ angeführt. Hierunter fallen jedoch auch weitere Delikte wie Infizierung des Computers (Viren, Trojaner etc.), digitale Erpressung, Einsatz von Schadsoftware, Identitätsdiebstahl etc., weshalb eine konkrete Abgrenzung nicht möglich ist.

Generell ist im Bereich Cyberkriminalität ein starker Anstieg zu beobachten. So wurden im Jahr 2014 8.966 Cybercrime-Delikte zur Anzeige gebracht, 2015 um 11,6% mehr (10.010), 2016 stieg die Anzahl erneut um knapp 31% auf 13.103 Anzeigen.[13]

Störfälle von Smart Devices größeren und kleineren Ausmaßes kamen international immer wieder vor und werden medial auch stark bespielt. So feierte etwa „Alexa“ allein zu Hause eine Party: [14]

Der smarte Amazon-Lautsprecher sorgte in Hamburg unaufgefordert mitten in der Nacht für Partystimmung – sehr zum Missfallen der Anrainer. Alexa hatte sich, laut Aussage des Wohnungsbesitzers, selbstständig eingeschaltet und laute Musik aufgedreht, während ihr Eigentümer in der Stadt unterwegs war. Daraufhin wurde von den Nachbarn die Polizei gerufen, die schließlich

6 https://www.it-business.de/der-durchbruch-von-smart-home-steht-noch-bevor-a-525906/
7 Analyse von Mydealz.de und Google-Suchanfragen durch die Social-Commerce-Gruppe Pepper. Indikatoren sind die Angebote, die geteilt und diskutiert werden, sowie die Zahl der Nutzer, die dem Link zum jeweiligen Online-Shop folgen.
8 https://www.it-business.de/der-durchbruch-von-smart-home-steht-noch-bevor-a-525906/
9 https://de.statista.com/outlook/279/128/smart-home/oesterreich
10 Sie bestehen beispielsweise beim Hersteller Archos aus einem Tablet sowie jeweils zwei Mini-Cams, Wetter- und Bewegungssensoren, also der Basis-Ausstattung eines smarten Zuhauses.
11 https://www.it-business.de/der-durchbruch-von-smart-home-steht-noch-bevor-a-525906/
12 https://www.it-business.de/der-durchbruch-von-smart-home-steht-noch-bevor-a-525906/
13 http://bundeskriminalamt.at/501/start.aspx
14 https://www.derstandard.de/story/2000067317360/alexa-spielte-selbststaendig-laute-musik-polizeieinsatz-in-hamburg

die Wohnungstür aufbrach und Alexa abschaltete. Lange Zeit war nicht klar, wer die Kosten für diesen Störfall übernehmen würde. Alexa fiel mittlerweile bereits durch mehrere Störfälle negativ auf.

Besonders betreffend die Sicherheit und den Schutz von Kindern kommt es beim Einsatz beliebter smarter Entertainment-Devices ab und an zu Zwischenfällen. Diese Vorfälle, aber auch die Art der Berichterstattung können auf das subjektive Sicherheitsempfinden der Konsumenten erhebliche Auswirkungen haben.

In Deutschland wurde etwa der Verkauf smarter Kinderuhren verboten, die eine Abhörfunktion besitzen. Diese können mit einer SIM-Karte ausgerüstet werden und ermöglichen somit den Eltern das Bespitzeln ihres Nachwuchses (und somit z.B. auch der Lehrer in der Schule). Bereits durch den Besitz dieser Uhren macht man sich in Deutschland strafbar. [15,16]

1.3 Methoden

1.3.1 Experteninterviews

In zehn qualitativen Interviews[17] mit IT-Sicherheits- und Technikexperten aus dem Bereich IoT (durchgeführt im Zeitraum Dezember 2017 bis Jänner 2018 von Consent Markt- und Sozialforschung im Auftrag des KFV) wurden Chancen und Risiken von Smart Homes unter die Lupe genommen.

1.3.2 Bevölkerungsbefragung

Um ein Bild über den derzeitigen Stand sowie mögliche Trends im Bereich Smart-Home-Nutzung innerhalb der österreichischen Bevölkerung zu erheben, führte Consent Markt- und Sozialforschung im Auftrag des KFV eine telefonische Repräsentativbefragung[18] mit 1.000 Österreichern ab 18 Jahren durch (November bis Dezember 2017). Dabei wurden die aktuelle Nutzung, geplante Anschaffungen, die persönliche Einstellung zum Thema Smart Home, Beweggründe für die Nutzung oder auch Ablehnung, das Gefahrenbewusstsein und mögliche bereits erlebte Schadensfälle erhoben.

15 http://help.orf.at/stories/2878852/
16 http://www.sueddeutsche.de/digital/it-sicherheit-bundesnetzagentur-verbietet-spionierende-kinderuhren-1.3754397
17 Interviewleitfaden im Anhang
18 Fragebogen im Anhang

2

2 SMART LIVING IN ÖSTERREICHS HAUSHALTEN

Am Beginn der Repräsentativbefragung (vgl. Kapitel 1.3.2) wurde allgemein das Verständnis von Smart Home erfragt. Dabei gab rund die Hälfte der Befragten an, die Bedeutung des Begriffs „Smart Home" zu kennen. Neben „Vernetzung" und „zentraler und intelligenter Steuerung" denken die Befragten bei diesem Begriff auch an „Erleichterung im Haushalt", „Komfort" und „Effizienz".

Nachdem alle Befragten über die folgende Definition von Smart Home informiert wurden, wurde die Befragung fortgeführt.

Von einem Smart Home spricht man, wenn im Haus verwendete Geräte wie z.B. Heizkörper, Fernseher, Kühlschrank sowie Leuchten oder Lichtschalter untereinander vernetzt sind und Daten speichern. Smart-Home-Geräte können über das Internet und über erweiterbare Apps z.B. mit Hilfe eines Smartphones gesteuert werden. D.h., auch Smartphone und Smart-TV gehören zum Bereich Smart Home.

2.1 Die smarte Ausstattung

45% der Österreicher nutzen smarte Geräte. Insbesondere bei jüngeren Befragten (18 bis 25 Jahre) sind smarte Produkte bereits wesentlicher Bestandteil des Haushalts, rund drei Viertel nutzen sie bereits, weitere 14% können sich die Nutzung zumindest vorstellen (Abbildung 2).

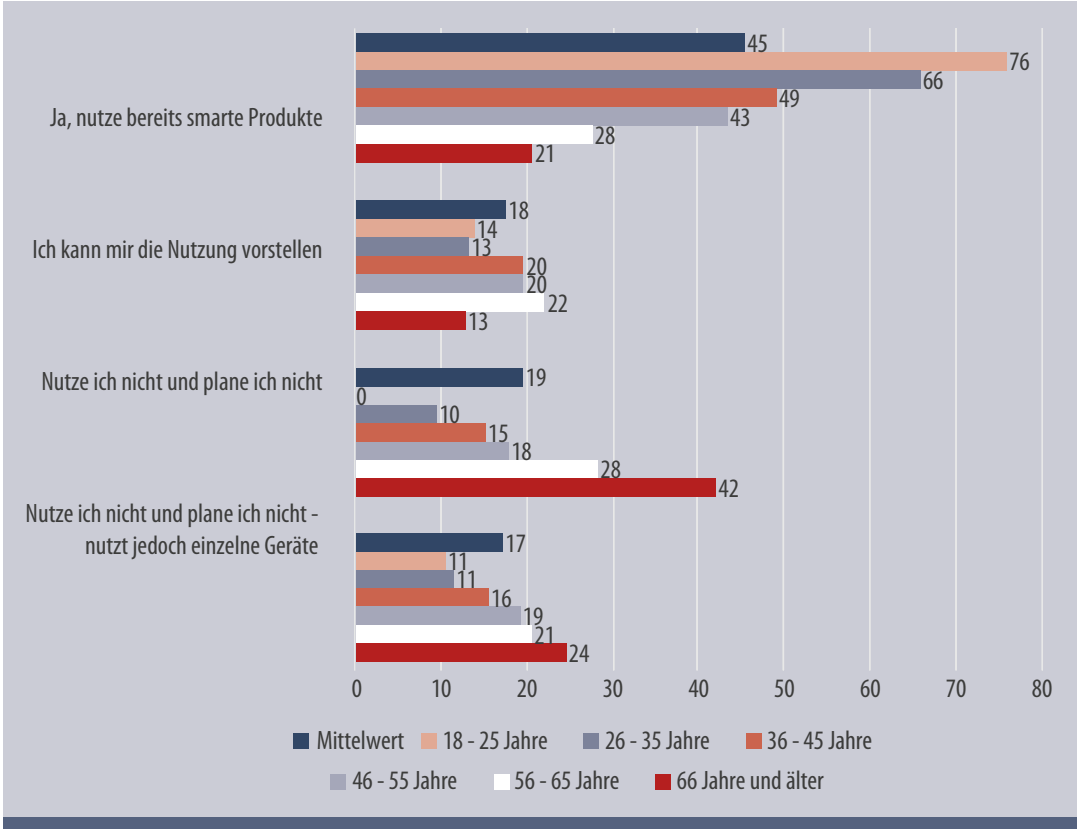

Abbildung 2: *Nutzung smarter Geräte, N=1.000, Angaben in %*

In Haushalten ohne Kinder wird Smart Home eher genutzt (59%) als in Haushalten mit Kindern (40%).

Tendenziell werden smarte Geräte mit zunehmendem Alter der Befragten vermehrt abgelehnt. Hier ist jedoch anzumerken, dass mit zunehmendem Alter auch das Bewusstsein dafür abnimmt, wie „smart" man tatsächlich bereits lebt. Betrachtet man die Daten nämlich genauer, stellt sich heraus, dass auch von vermeintlichen „Nicht-Nutzern" einzelne smarte Geräte genutzt werden. Insgesamt geben 66% der Österreicher über 65 Jahren an, Smart-Home-Geräte weder zu nutzen noch sich deren Nutzung vorstellen zu können. Die Ergebnisse der quantitativen Befragung zeigen jedoch, dass von 24% der Befragten bereits einzelne smarte Geräte genutzt werden. Im Mittel trifft diese unbewusste Nutzung auf 17% zu (Abbildung 2).

Am häufigsten ist die Verwendung smarter Technologien im Unterhaltungs- und IT-Bereich zu verzeichnen (Abbildung 3).

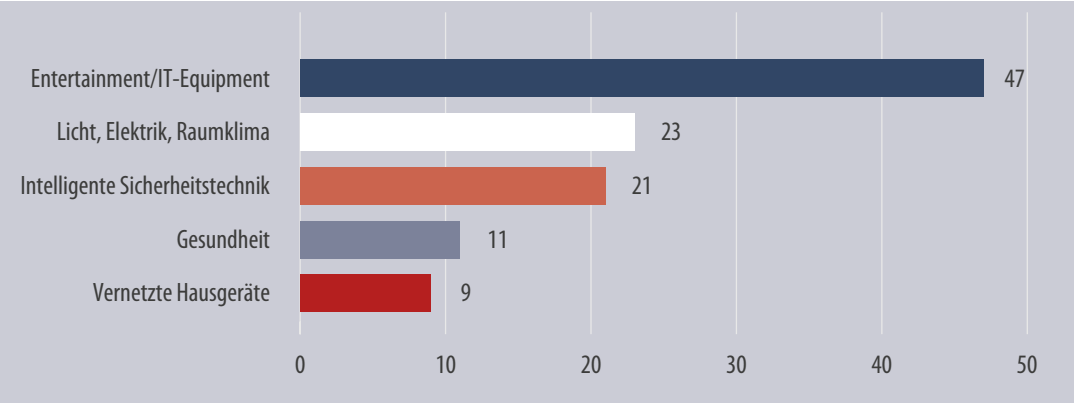

Abbildung 3: *Nutzung smarter Geräte nach Produktkategorien, N=1.000, Angaben in %*

Nahezu ein Drittel der Befragten (31%) gibt an, ein Smart-TV zu besitzen. Jeder 5. Befragte verwendet eine internetfähige Spielkonsole. Auf Platz 3 befinden sich smarte Bewegungsmelder, deren Nutzung bei immerhin 13% liegt, sowie digitale Assistenten wie z.B. Alexa von Amazon oder Google Home.

In Sachen Planung orientieren sich die Österreicher sowohl in Richtung Komfort und Sicherheit als auch in Richtung Gesundheit (Abbildung 4). So stehen etwa Notrufsysteme für medizinische Notfälle und smarte Thermostate mit 41% ganz oben auf der Liste der geplanten Anschaffungen.

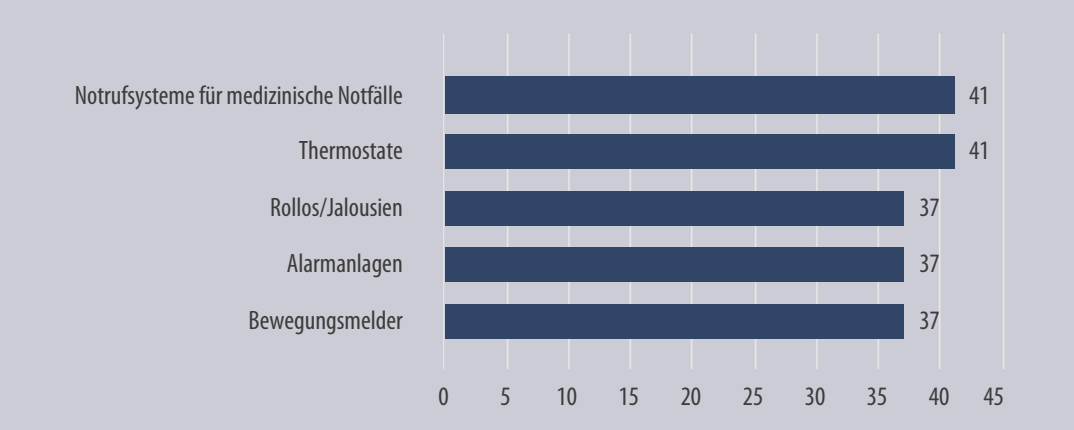

Abbildung 4: *Geplante Anschaffung smarter Geräte, N=1.000, Angaben in %*

2.1.1 Nutzung smarter Geräte nach Einsatzbereichen

Am häufigsten werden smarte Technologien im **Unterhaltungs- und IT-Bereich** verwendet. Neben klassischer Hardware wie Tablets (36%) sind insbesondere Smart-TVs mit 31% verbreitet, weitere 21% der Befragten planen deren Anschaffung. Digitale Assistenten wie zum Beispiel Google Home, Alexa oder Echo werden bisweilen lediglich von 13% genutzt (Abbildung 5).

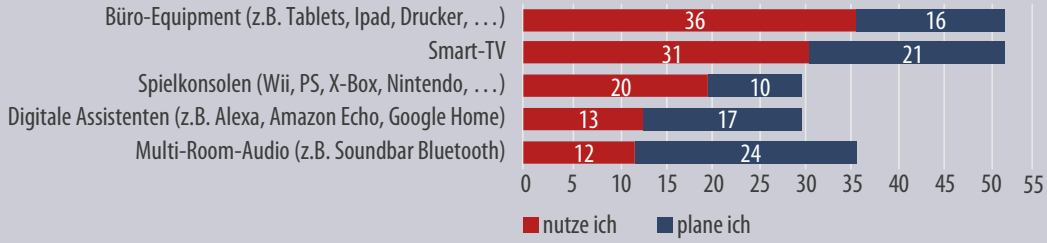

Abbildung 5: *Nutzung smarter Geräte im Bereich Entertainment und IT, N=1.000, Angaben in %*

Im Bereich **Licht/Elektrik/Raumklima** werden am ehesten smarte Bewegungsmelder (13%) und Thermostate (11%) genutzt. Smarte Steckdosen sind in zwei Dritteln der Haushalte kein Thema (Abbildung 6).

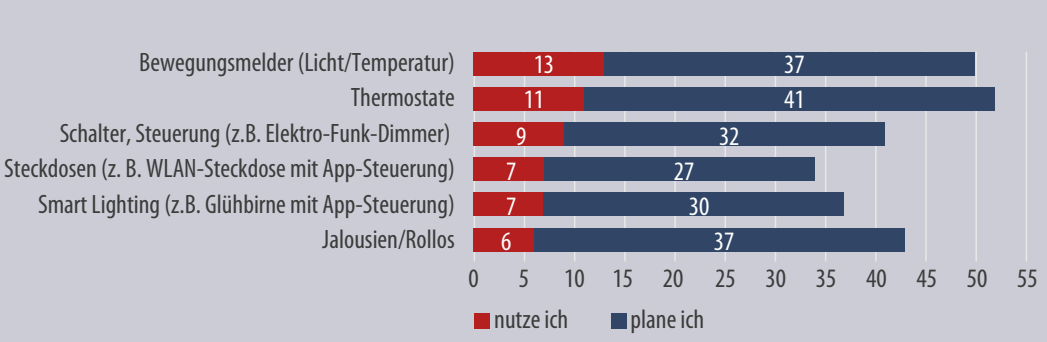

Abbildung 6: *Nutzung smarter Geräte im Bereich Licht/Elektrik/Raumklima, N=1.000, Angaben in %*

Bezüglich intelligenter **Sicherheitstechnik** kann sich mehr als ein Drittel der Befragten die Nutzung smarter Rauchmelder vorstellen. Smarte Kameras zur Haustier-Überwachung werden hingegen abgelehnt (Abbildung 7).

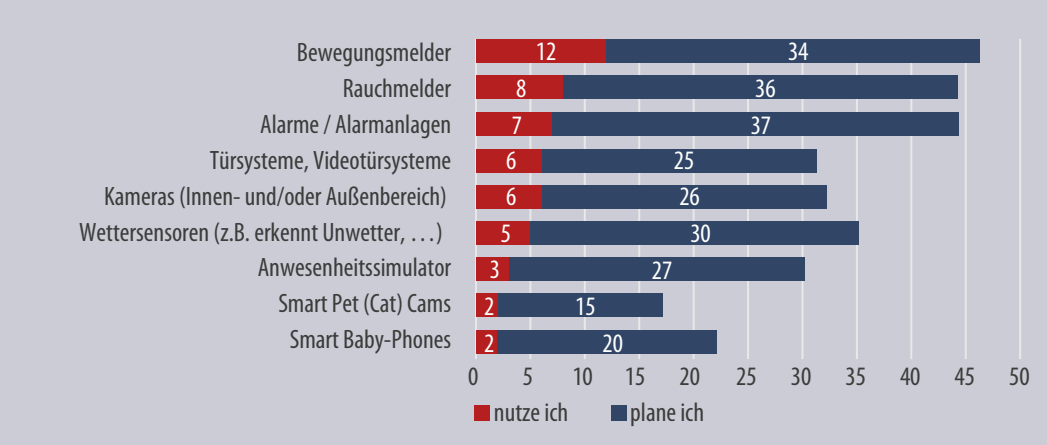

Abbildung 7: *Nutzung smarter Geräte im Bereich Sicherheit, N=1.000, Angaben in %*

Recht wenig verbreitet sind bisher smarte Geräte im Bereich **Gesundheit und Unfallvermeidung**. Am ehesten werden mit 7% sogenannte Wearables verwendet – darunter fallen zum Beispiel Fitness-Armbänder oder -Uhren, die Schrittzahl, Herzfrequenz und teilweise auch Schlafaktivität überwachen. 4 von 10 Befragten planen die Anschaffung smarter Notrufsysteme (Abbildung 8).

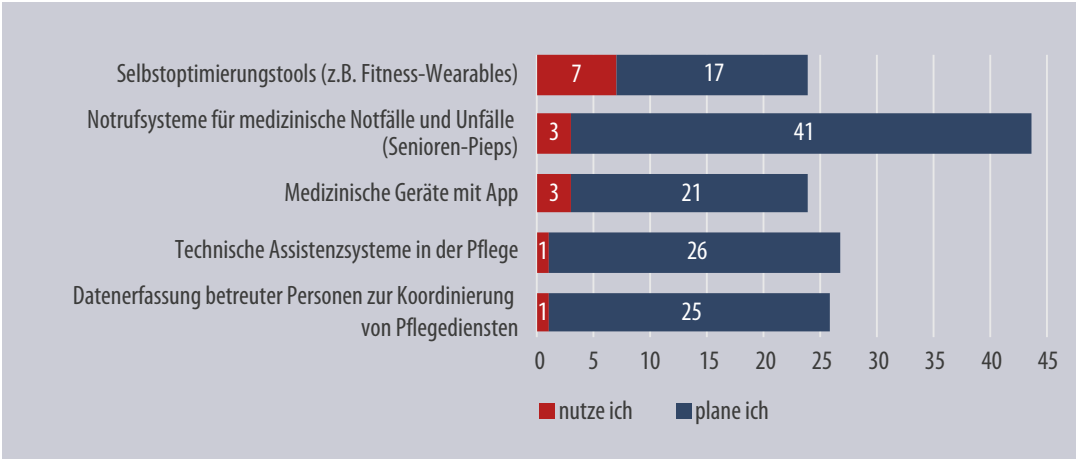

Abbildung 8: *Nutzung smarter Geräte im Bereich Gesundheit und Unfallvermeidung, N=1.000, Angaben in %*

Insgesamt ist die Nutzung **smarter Haushaltsgeräte** mit jeweils 3-5% sehr gering, auch eine Anschaffung planen mit jeweils 17-23% vergleichsweise wenige der Befragten (Abbildung 9).

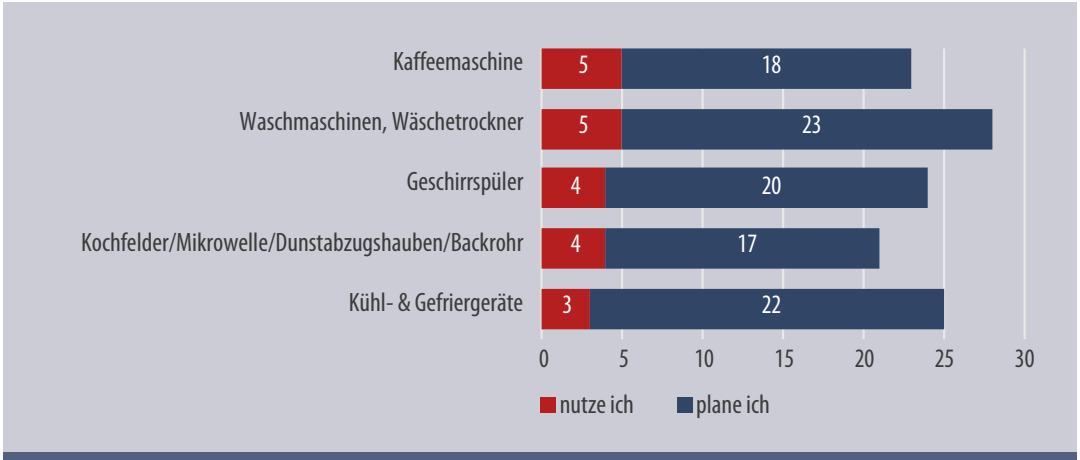

Abbildung 9: *Nutzung smarter Haushaltsgeräte, N=1.000, Angaben in %*

2.2 Die Einstellung der Österreicher zum Thema Smart Home

Generell stufen die Österreicher Smart Homes tendenziell als nützlich ein. So stimmt eine überwiegende Mehrheit der Befragten (68%) zu, dass die automatische Anpassung der Heizung und ähnliche Maßnahmen nützlich sind, 56% meinen, dass dadurch Energie gespart wird. Mehr als die Hälfte der befragten Personen gehen (eher) davon aus, dass in Zukunft alle Geräte im Haushalt Internetverbindung haben werden, und 70% halten Bewohner von Smart Homes für sehr zukunftsorientiert. 80% fühlen sich zu Hause ausreichend vor Hackerangriffen geschützt (Abbildung 10).

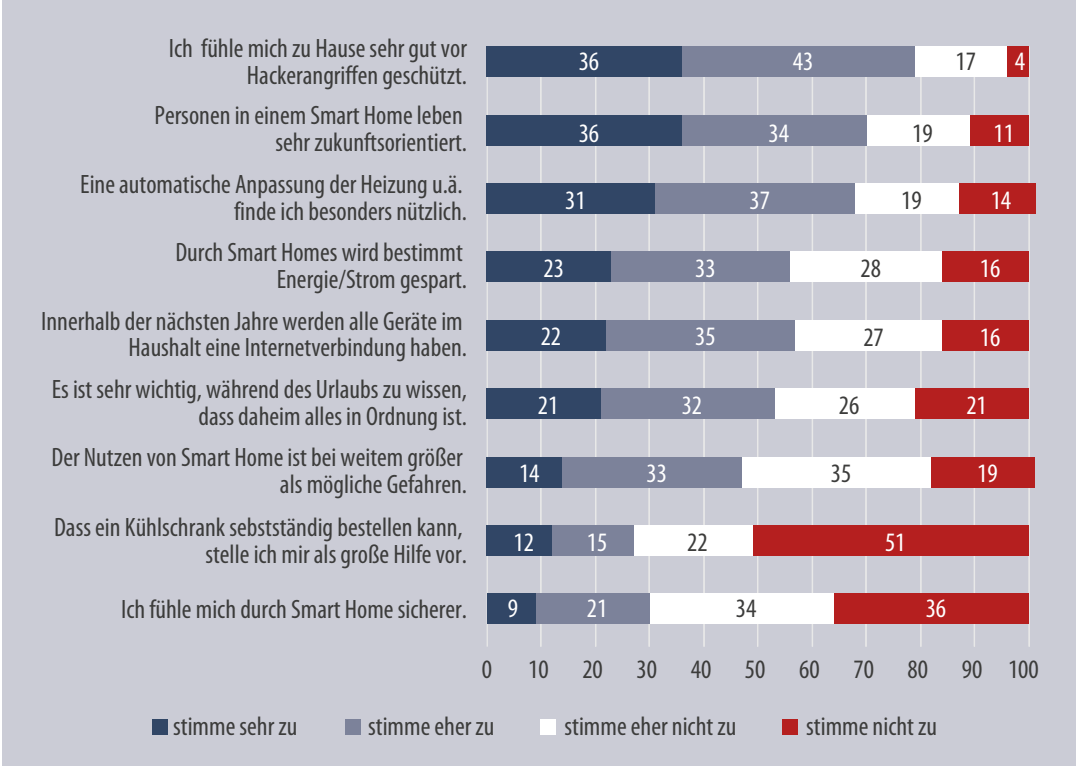

Abbildung 10: *Zustimmung zu Aussagen bezüglich Smart Home N=1.000, Angaben in % (Werte ungleich 100% ergeben sich durch Rundungen)*

Ältere Personen (> 60 Jahre) stehen dem Thema Smart Home insgesamt skeptischer gegenüber als jüngere (bis 25-jährige). Nur etwa jeder 4. im Alter von über 60 Jahren hält Personen mit einem Smart Home für zukunftsorientiert, und rund jeder 5. empfindet die automatische Anpassung der Heizung als sehr nützlich. Ebenso nur annähernd jeweils jeder 5. Senior – und damit unterdurchschnittlich wenige ältere Befragte – stellt sich einen selbstständig Lebensmittel bestellenden Kühlschrank als eher nützlich vor und fühlt sich durch ein Smart Home sicherer. Für 63% der älteren Befragten überwiegen zudem die möglichen Gefahren den Nutzen.

Auch wenn dies so konkret insgesamt nur etwa die Hälfte der Befragten angibt, meinen 72%, mit einem Smart Home öffne man Tür und Tor für Datenangriffe. 67% halten Smart-Home-Technologien zumindest derzeit noch für sehr fehleranfällig, und 59% halten es generell für leichtsinnig, Geräte mit dem Internet zu verbinden.

64% fühlen sich durch vernetzte Technologien (eher) überwacht. 55% befürchten, die Kontrolle über die Geräte zu verlieren, und knapp die Hälfte (47%) befürchtet sogar, dass Geräte sich verselbstständigen könnten (Abbildung 11).

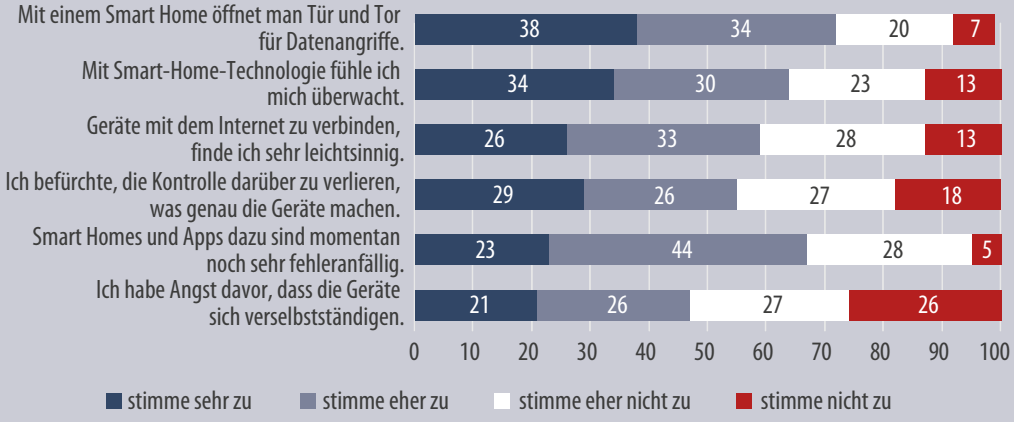

Abbildung 11: *Zustimmung zu Aussagen bezüglich Smart Home N=1.000, Angaben in % (Werte ungleich 100% ergeben sich durch Rundungen)*

Jüngere Befragte stehen dem Thema Smart Home aufgeschlossener und sorgenfreier gegenüber. Ältere Befragte fühlen sich durch smarte Technologien noch stärker überwacht, befürchten auch eher, die Kontrolle über smarte Geräte zu verlieren (jeweils 71%) und haben mehr Sorge, dass die Geräte sich verselbstständigen (64%). Zudem hält es jeder 3. Ältere für sehr leichtsinnig, Geräte mit dem Internet zu verbinden.

Tendenziell stehen Männer dem Smart Home etwas positiver gegenüber als Frauen. Sie halten smarte Technologien eher für nützlich und hilfreich und haben insgesamt eher weniger Sorge als Frauen, überwacht zu werden oder die Kontrolle über die Geräte zu verlieren.

2.2.1 Einstellung zu einzelnen Einsatzgebieten

Großen Nutzen von Smart Homes sehen die Befragten insbesondere in den Bereichen Einbruchsschutz und Warnsysteme bei Naturkatastrophen (je 36%) sowie in puncto Pflege und Sicherheit von Senioren (32%). Aber auch in anderen Einsatzgebieten sehen die Befragten zumindest einen gewissen Nutzen. Gar keinen Nutzen sieht hingegen mehr als jeder 5. in smarten Haushaltshelfern (Abbildung 12).

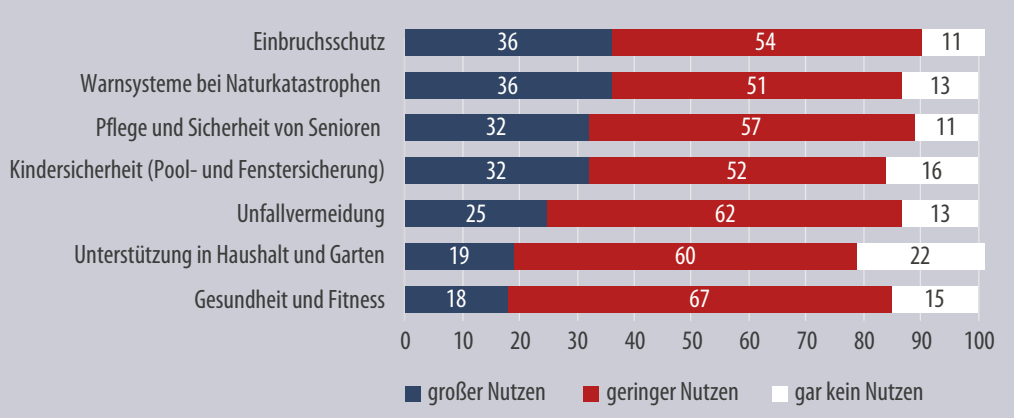

Abbildung 12: *Nutzen von Smart Home in einzelnen Einsatzgebieten, N=1.000, Angaben in % (Werte ungleich 100% ergeben sich durch Rundungen)*

Die Skepsis der älteren Österreicher spiegelt sich auch bezüglich des Nutzens smarter Technik in einzelnen Einsatzbereichen wider. So sehen im smart geregelten Einbruchsschutz nur 29% der befragten Senioren einen großen Nutzen und lediglich 27% in Warnsystemen bei Naturkatastrophen. Auch hinsichtlich der Pflege und Sicherheit von Senioren liegt der eingeschätzte Nutzen smarter Systeme mit 26%, in Sachen Kindersicherheit mit 22%, Unfallvermeidung mit 19%, bei smarter Hilfe in Haushalt und Garten mit 9% und bei smarter Assistenz im Bereich Gesundheit und Fitness mit 13% jeweils unter dem Durchschnitt.

Den größten Nutzen von Smart Homes sehen Personen im Alter von 18 bis 25 Jahren, insbesondere Geräte im Bereich des Einbruchsschutzes hält nahezu die Hälfte in diesem Alter für sehr nützlich. Smarte Technologien für Gesundheit und Fitness halten in dieser Altersgruppe immerhin 23% für sehr nützlich.

Abbildung 13 zeigt, wie groß der jeweilige Nutzen smarter Haushaltstechnologien durchschnittlich in den verschiedenen Altersgruppen eingeschätzt wird.

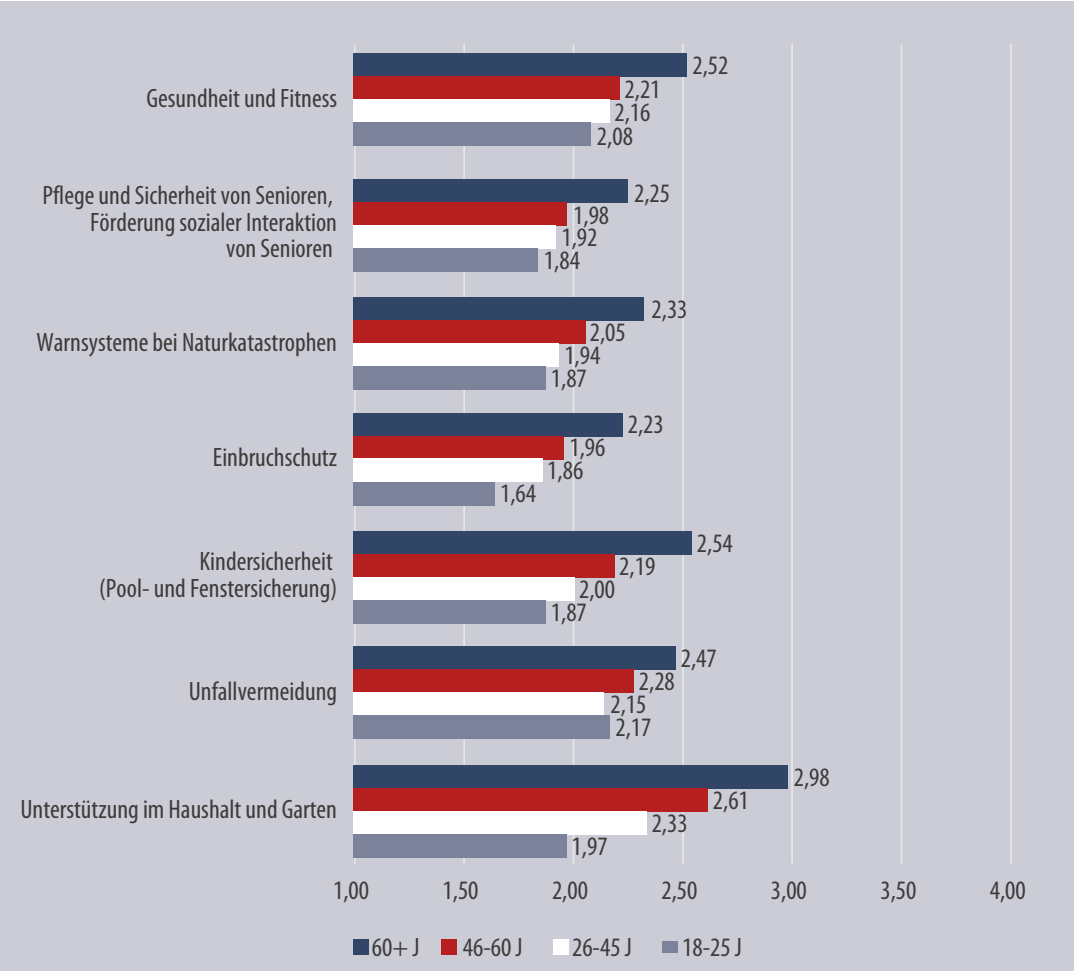

Abbildung 13: *Eingeschätzter Nutzen von Smart Home in einzelnen Einsatzgebieten nach Alter, N=1.000, Angaben in Mittelwerten, Skala 1 – sehr groß bis 4 – gar kein Nutzen*

Zwischen Frauen und Männern sind jedoch hinsichtlich des eingeschätzten Nutzens smarter Produkte für konkrete Einsatzbereiche keine Unterschiede festzustellen.

Smarte Geräte zur Überwachung von Haustieren oder gar Kindern sowie smarte Küchenhelfer werden mehrheitlich abgelehnt. Auch bei medizinischen Geräten misstrauen drei Viertel der Befragten smarten Technologien (Abbildung 14).

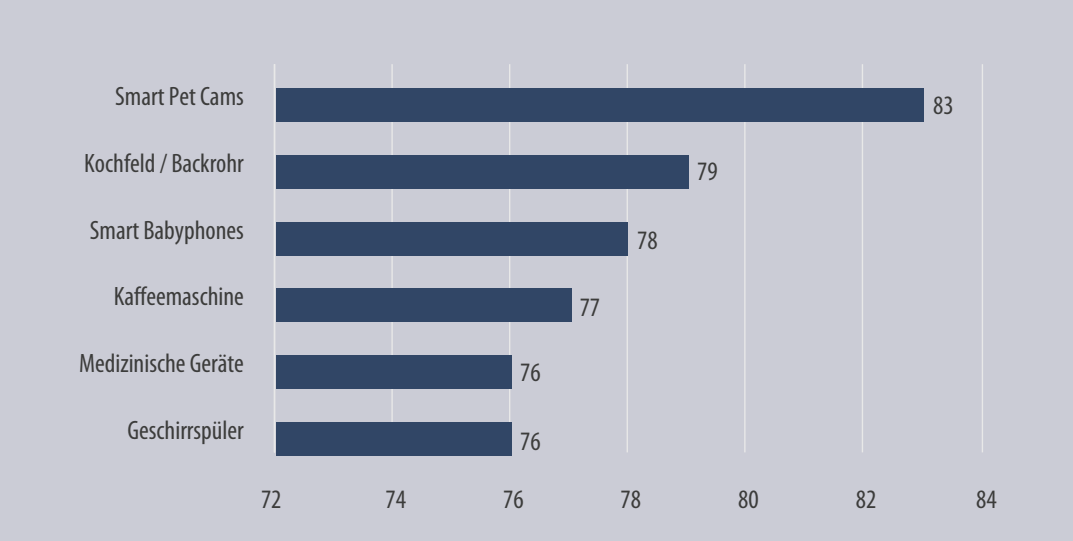

Abbildung 14: *Ablehnung einzelner smarter Produkte, N=1.000, Angaben in %*

2.3 Erlebte Schadensfälle

Jeder zehnte Nutzer vernetzter Geräte hat bereits mindestens einen Schadensfall erlebt. Die wenigsten dieser Fälle betreffen jedoch die Sicherheit. Am häufigsten werden Verbindungsfehler (19 Fälle) und Programmfehler (16 Fälle) berichtet. Immerhin neun Nutzende haben bereits Daten verloren, 8 Nutzende sind bereits Opfer von Hackerangriffen oder Datendiebstahl geworden.

Art der Schadensfälle		
Fehlfunktionen	**Sicherheit**	**Komfort**
• Programmfehler, fehlerhafte Programmierung (16) • Systemabsturz (7) • Fehlerhafte App, App funktioniert nicht, Neuinstallation nötig (5) • Datenzugriff nicht möglich (2)	• Hackerangriff, Datendiebstahl/-weitergabe (8) • Verselbstständigung der Geräte (5)	• Verbindung zu Endgeräten schlägt fehl, Verbindungsherstellung zu Endgeräten dauert zu lange (19) • Datenverlust (9) • Endgerät liefert falsche Werte, dadurch keine adäquate Umsetzung/Speicherung (2) • Spracherkennung funktioniert nicht (2) • Lichtsensor funktioniert nicht richtig, daher Fehlbestellung (1)

Tabelle 1: *Erlebte Schadensfälle, 65 berichtete Schadensfälle, N=626 Nutzende*

3

3 DIE 3 NUTZERTYPEN

Aus den Ergebnissen der Repräsentativbefragung wurden mittels Faktorenanalyse **Nutzertypen** abgeleitet. Im Wesentlichen können 3 Typen unterschieden werden – vom Skeptiker über den Praktiker bis hin zum Technikfreak.

3.1 Der Skeptiker

Der Skeptiker hält sich beim Kauf von Smart Devices eher zurück. Er findet es leichtsinnig, bloß aufgrund eines Trends vernetzte Geräte zu kaufen. Diese könnten ihn eventuell ausspionieren oder unerlaubt Daten von ihm sammeln. Momentan traut er dem Stand der Technik noch zu wenig und kauft daher keine smarten Produkte.

3.2 Der Praktiker

Der Praktiker genießt vor allem den Komfort smarter Geräte. Alexa und Co. sind ein selbstverständlicher Bestandteil seines Zuhauses. Smarte Alarmanlagen geben ihm ein sicheres Gefühl. Angst vor Eingriffen in seine Privatsphäre durch die modernen Geräte hat er nicht. Er weiß genau, welche smarten Devices ihm den Alltag erleichtern.

3.3 Der Technikfreak

Dem Technikfreak gefallen grundsätzlich technische Neuheiten. Meistens fackelt er nicht lange und legt sich diese schnell zu. Alexa war bereits Teil seiner Wohnzimmerausstattung, bevor die erste Werbung dafür im Fernsehen geschalten wurde. Er lässt sich von smarten Geräten auch gerne Tätigkeiten wie Kaffeekochen oder die Essensbestellung abnehmen. Es ist ja auch zu praktisch …

4

4
DIE EXPERTENSICHT[19]

Anhand der 10 durchgeführten Experteninterviews konnten Chancen und Risiken ermittelt und daraus Forderungen abgeleitet werden.

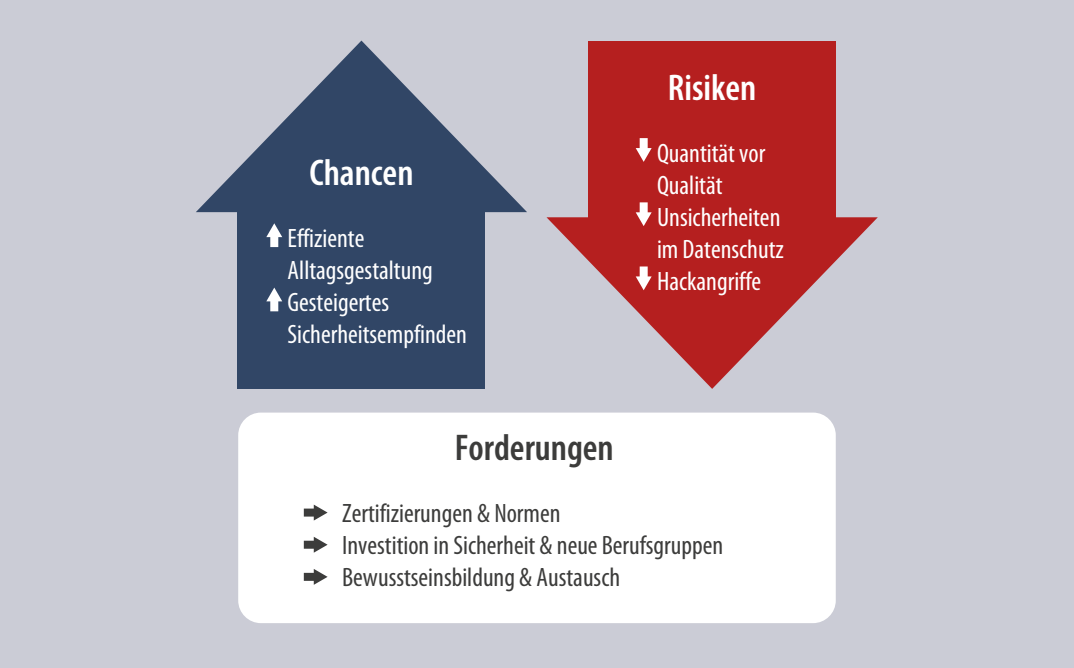

Abbildung 15: *Chancen, Risiken und Forderungen der österreichischen Experten in den Bereichen Smart Home, IT-Security und Sicherheit*

4.1 Vorteile von Smart Devices

4.1.1 Effiziente Alltagsgestaltung[20]

Bereits einzelne smarte Geräte im Wohnbereich bieten das Potenzial, den **Alltag des einzelnen Nutzenden effizienter** zu gestalten. Gleichzeitig können sie aber auch den **Komfort erhöhen**. Systeme dieser Art können in Zeiten des Klimawandels und Umweltschutzes dazu beitragen, **Energie zu sparen** und grundsätzlich energieeffizientere Haushalte zu führen, was sowohl dem einzelnen Nutzenden als auch der Gesamtgesellschaft zugutekommt.
Der Einsatz von Smart Homes kann für die Konsumenten auch eine enorme **Zeitersparnis** bedeuten (z.B. Arbeiten, die aufgrund des Einsatzes von Technik parallel verrichtet werden können).

Es bedarf hierzu aber nicht immer kompletter Smart-Home-Lösungen, auch der **Einsatz einzelner Smart Devices** kann im Haushalt einen positiven Effekt auf die Konsumenten haben. Vor allem bezogen auf den Bereich **Gesundheit** und den Einsatz personenbezogener **Wearables** (z.B. Fitness-Tracker, Blutdruckmesser), die einen **positiven Effekt auf die Motivation** zu einem gesünderen Lebensstil des Einzelnen haben können.

19 In zehn leitfadengestützten Interviews wurden Experten im Bereich der IT-Sicherheit und Technik hinsichtlich der Chancen und Risiken von Smart Devices sowie ihrer Forderungen an unterschiedliche Stakeholder für Endverbraucher befragt.
20 Experteninterviews

Smart Devices bieten im Gesundheitsbereich grundsätzlich vielversprechende Optionen für **ältere, gebrechliche und/oder körperlich und geistig beeinträchtigte Menschen**. So können beispielsweise in der Nacht durch bessere Umgebungsausleuchtung bei Bodenkontakt durch den Einsatz von Bodenleuchten mit Sensorik Unfälle (z.B. Stürze) älterer Personen verringert werden. **„Assisted Living"** gewinnt durch die laufenden Innovationen im Bereich des Smart Homes an Aufwind und kann zu einer ernsthaften Verbesserung der Lebensqualität und längeren Unabhängigkeit von gesundheitlichen Risikogruppen beitragen.

4.1.2 Gesteigertes Sicherheitsempfinden[21]

Vernetzte Geräte, ob als Einzel- oder Komplettlösungen für den Heimgebrauch, bieten mehr oder weniger umfangreich, und vor allem mit der Möglichkeit der individuellen Abstimmung, die **Chance, die Wohnung oder das Eigenheim sicherer zu gestalten**. So kann man hier auf vernetzte Kamera- und Sensorsysteme zurückgreifen, die mit der installierten Alarmanlage kommunizieren. Solche, sinnvoll eingesetzten, Sicherheitsinstallationen können durchaus das **subjektive Sicherheitsempfinden der Nutzenden steigern** und tragen zusätzlich zur **Abschreckung von Einbrechern** bei.

4.2 Mögliche Gefahrenquellen[22]

4.2.1 Quantität statt Qualität

Aktuell ist der Markt der Smart Devices und Smart-Home-Lösungen sehr dynamisch. Dies liegt vor allem an der großen **Anzahl von Start-ups mit innovativen neuen Systemen**, aber auch an der **kostengünstigen Importware aus dem Ausland**.

Will man ein gut funktionierendes, sicheres Gerät haben, sollte man sich als Konsument dessen bewusst sein, dass die Herstellerfirmen **viele Dienstleistungen** zu erbringen haben. Der Hersteller muss das Produkt und die dazugehörige Software herstellen, Sicherheitsupdates müssen her- und zur Verfügung gestellt und für die Datenspeicherung muss eine Cloud-Infrastruktur geschaffen werden. Entscheidet man sich für ein **Billigprodukt**, so muss dieses nicht unbedingt immer die schlechtere Wahl sein, man kann allerdings davon ausgehen, in den oben genannten Punkten teilweise **(erhebliche) Abstriche** in Kauf nehmen zu müssen.

Software benötigt Updates, insbesondere **Sicherheitsupdates**, um den optimalen Schutz und die Funktionstüchtigkeit gewährleisten zu können. Beim automatischen Griff auf ein billig produziertes smartes Gerät läuft man allerdings Gefahr, **keinen Zugriff auf Sicherheitsupdates** zu erhalten. Besonders bei der Herstellung dieses Produktsegments besteht eine hohe Fluktuation an Firmengründungen und Konkursen. Erschwerend kommt hinzu, dass viele dieser Produkte aufgrund der kostengünstigeren **Produktion im Ausland** *hergestellt* werden und dabei teilweise keinerlei (Qualitäts-) Kontrollen erfolgen. Auch hinsichtlich der Haftung bei Störfällen und Fehlfunktionen sollte man sich die Vorteile eines Qualitätsproduktes vor Augen führen.

Auch die **Kompatibilität der smarten Devices untereinander** ist ein wichtiger Faktor. Smart-Home-Lösungen stellen immer stark individualisierte Nutzungsoptionen dar. Jeder Haushalt stellt eigene Anforderungen an ein (zukünftiges) „smartes Zuhause". Dementsprechend unterschiedlich sind die käuflich zu erwerbenden Produkte. Diese sind aber nicht unbedingt so konzipiert, dass sie untereinander kompatibel sind. Das kann dazu führen, dass die Produkte ihren Einsatzzweck im Smart Home nicht erfüllen können, da sie **mit den anderen Geräten nicht „kommunizieren" können**.

21 Experteninterviews
22 Experteninterviews

Es ist daher von Vorteil, auf die **Qualität der Herstellung oder der Marke** eines Produktes zu achten. Besonders im Bereich der technischen Neuerungen und der smarten Geräte werden oftmals bewusst **Produkte in der Testphase auf den Markt** gebracht. Will man damit eventuell einhergehende technische Störfälle vermeiden, muss man sich mit dem Gerät und der Anschaffung bereits im Vorfeld vertraut machen.

4.2.2 Unsicherheiten im Datenschutz

Grundsätzlich herrscht eine gewisse Unsicherheit der Konsumenten in Bezug auf den **Datenschutz** bei der Nutzung von Smart Devices. Smart Devices zeichnen sich unter anderem durch ihre Vernetzungsoptionen aus. Sind diese aktiviert (z.B. hat das Gerät Zugang zum Internet), besteht **potenziell auch die Möglichkeit der Übertragung von Daten**. Dies erfüllt bei den meisten Smart Devices eine wichtige Aufgabe für die Funktionstüchtigkeit, kann allerdings auch einen negativen Mehrwert für die Endverbraucher implizieren.

Die oftmals für den Konsumenten **unbewusste Datenaufzeichnung** ist ein Risiko. Dies lässt sich am Beispiel von sprachgesteuerten Geräten (z.B. sprachgesteuerte Fernbedienungen) verdeutlichen: Das Gerät ist so konzipiert, gewisse Befehle zu registrieren und dann darauf zu reagieren. Bedeutet das, dass alle Gespräche in unmittelbarer Umgebung aufgezeichnet werden? Was geschieht mit den Daten? Werden diese weitergeleitet? Antworten darauf kann (in den meisten Fällen) nur der Hersteller selbst liefern. Dieser ist zumeist nicht unmittelbar greifbar. Beispiele aus der Praxis gibt es zur Genüge. Erst im Jahr 2017 hat die interaktive Spielzeugpuppe „Cayla“ mit Spionagefällen in deutschen Kinderzimmern Schlagzeilen gemacht und musste daraufhin aus dem käuflichen Sortiment im Spielwarenhandel entfernt werden.

Man sollte als Endnutzer vor dem Kauf eines Produktes immer die **wirtschaftlichen Interessen der Hersteller mitbedenken**, da besonders mit den ausgelesenen, teilweise sehr sensiblen Daten von Smart Devices viel Geld verdient werden kann (z.B. Fitness-Wearables und deren gesundheitsbezogene Daten der Nutzenden, die an interessierte Institutionen weiterverkauft werden könnten).

4.2.3 Hackerangriffe

Obwohl es bislang in **Österreich noch keine nennenswerten Vorfälle** bezüglich Hackerangriffen auf Smart Devices gegeben hat, bestätigen die Experten die Sorge der Konsumenten[23], Opfer von Hackerangriffen zu werden.

Internationale Beispiele zeigen, dass Hackerangriffe auf internetfähige Endgeräte (wozu auch Smart Devices zählen) bedrohliche **Blackouts in ganzen Landregionen** hervorrufen können. Diese können für die Bevölkerung gehörige kurz- bis mittelfristige Nachteile mit sich bringen (z.B. Lahmlegung der Infrastruktur, Wasserknappheit, Lebensmittelknappheit etc.).

Es gilt die Faustregel:
Je mehr Smart Devices man besitzt, desto größer ist die Angriffsfläche für potenzielle bösartige Hacks.

Was an dieser Stelle jedoch betont werden muss, ist die Tatsache, dass den größten aller Angriffspunkte immer noch der Anwender selbst darstellt. Gemeint ist hier vor allem der Umgang der Konsumenten mit den Geräten.

23 Siehe Repräsentativbefragung, Consent

Einer der größten Knackpunkte ist der **fehlende und falsche Umgang mit Passwörtern**. So werden oftmals gar keine eingerichtet und/oder es wird bei den gekauften Produkten nicht auf die Sicherheitsvoreinstellungen geachtet. Nicht zu vergessen ist, dass jegliche Geräte mit WLAN-Zugang legal online aufzuspüren sind, wobei auch deren **Standard-Passwörter relativ schnell im Internet aufzufinden sind**. So erlangt man problemlos den Zugriff auf ungeschützte Geräte und kann mühelos z.B. den Zugriff auf die Fernsehkamera im Schlafzimmer übernehmen. In Anbetracht dessen, dass internationale Online-Ransomware-Attacken im Steigen begriffen sind, stellt sich das unreflektierte Agieren der Konsumenten als eine potenziell bedenkliche Situation dar. Es gibt aber auch Fälle, in denen **bereits bei der Herstellung des jeweiligen Produktes auf den Einsatz eines Passworts vergessen** wurde. Auch hier gilt es sich vorab zu informieren.

Viele **Hersteller** machen nicht gezielt auf eine notwendige **Passwortänderung** ihrer Geräte **aufmerksam**, was dazu führt, dass diese vulnerabel bleiben. Grundsätzlich ist es jedem vernetzten, noch so harmlos wirkenden Smart-Gerät (z.B. Waschmaschine) möglich, einen Hackerangriff zu hosten. Die Endnutzer sollten sich daher auch immer dessen bewusst sein, dass **Alltagsgeräte als IoT-Devices vollwertige mit dem Internet verbundene Computersysteme** mit den gleichen Fehleranfälligkeiten wie ein Heim-PC sind.

Ein besonderes Risiko stellt die **Überschneidung unterschiedlicher Frequenzen von IoT-Devices** dar, die dem Endnutzer oftmals **nicht bewusst** sind. Diese können die eingesetzten Geräte außer Gefecht setzen. Vor allem bei **IoT-Sicherheitslösungen** kann das schwerwiegende Folgen haben, wenn beispielsweise die Waschmaschine die Alarmanlage aufgrund von Frequenzüberlappungen außer Gefecht setzt. Neben der unfreiwilligen Aushebelung von Smart Devices gibt es auch die Möglichkeit, diese **bewusst** mittels „**Jammer**“ (also Störgerät) zu beeinträchtigen. Jammer können zwar in Österreich nicht käuflich erworben werden, was Kriminelle natürlich nicht davon abhält, sich dieser anderswo erlangten Devices zu bedienen, um Sicherheitsvorkehrungen lahmzulegen.

5

5 CHANCEN UND RISIKEN IM ÜBERBLICK

Insgesamt sehen die Befragten den Nutzen von Smart Devices in Sachen Einbruchsschutz und **Pflege/Sicherheit von Senioren** am deutlichsten. Jeder zweite Österreicher erkennt einen Nutzen in **smarten Geräten für Gesundheit und Fitness**. Vor allem **jüngere Österreicher** (bis 25 Jahre) sind von den smarten Technologien überzeugt. Die Chancen von Smart Home liegen den Österreichern zufolge in der effizienten Alltagsgestaltung und damit einhergehendem Komfort. Auch das Sicherheitsempfinden steigt im Smart Home (Abbildung 16).

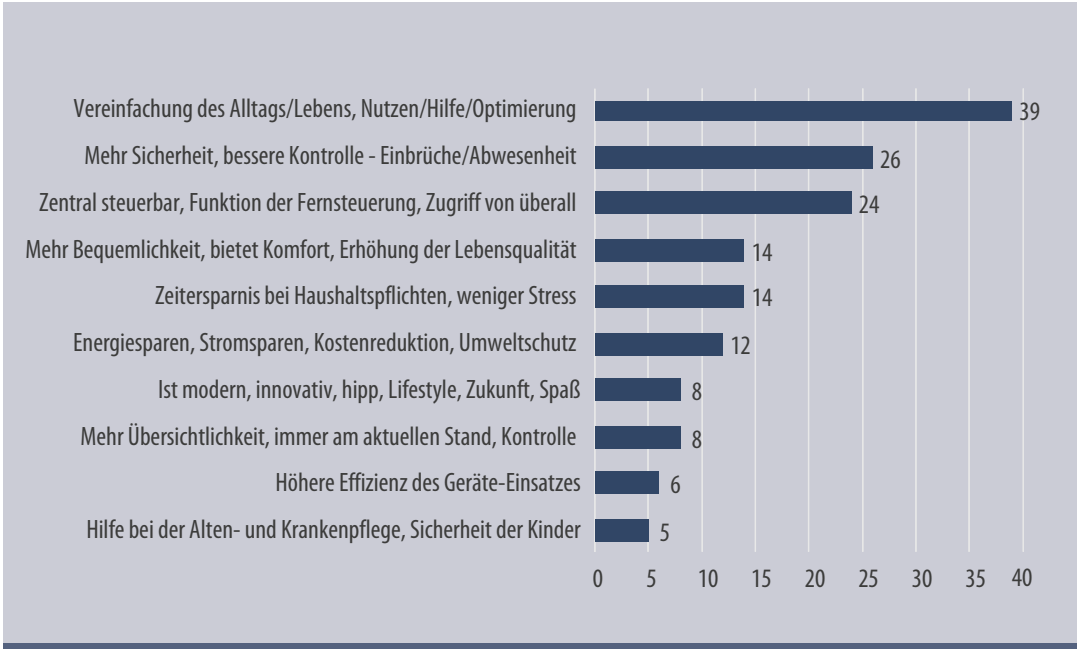

Abbildung 16: *Vorteile und Nutzungs-Gründe smarter Geräte, N=626 Nutzende, Angaben in %*

Zusammenfassend lässt sich sagen, dass den vielen Vorteilen im Bereich Smart Home auch einige Nachteile gegenüberstehen. So können etwa Alarmanlagen und Haushaltsgeräte, wenn sie online gesteuert werden, theoretisch auch fremdgesteuert werden. Wenn die Heizung protokolliert, wann jemand zu Hause ist, können möglicherweise Einbrecher von dieser Information profitieren. Dem kann jedoch entgegengehalten werden, dass es in Österreich bisher **noch keine nennenswerten Vorfälle bzgl. Hackerangriffen** auf Smart Devices gab.

Das größte Sicherheitsrisiko ist in diesem Fall immer noch der Nutzende selbst. Denn die Nutzer bestimmen, welche Sicherheitsvorkehrungen getroffen werden, welche Smart Devices nötig und brauchbar für den eigenen Alltag sind und wer diese installiert und regelmäßig überprüft. Diese selbstverständlichen, aber oftmals nicht zu Ende gedachten Abläufe können die Sicherheit eines Smart Homes verbessern oder aber – bei Nichtbeachtung – auch erheblich einschränken. Verantwortlich hierfür ist immer noch der Eigentümer. Tabelle 2 gibt einen Überblick über Chancen und Risiken des Smart Home.

Chancen	Risiken
• **Effiziente Gestaltung des Alltags** - Der Alltag wird vereinfacht und optimiert (39% der Nutzenden stimmen zu) • **Abschreckung von Einbrechern, Erhöhung des subjektiven Sicherheitsempfindens** - Nutzer fühlen sich besser vor Einbrüchen geschützt und haben mehr Kontrolle über ihr Eigentum bei Abwesenheit (26% der Nutzenden stimmen zu) • **Erhöhung des Komforts** • **Energie sparen** • **Positiver Effekt auf Motivation und Gesundheit (z.B. Wearables)**	• **Technikabhängigkeit als abschreckender Faktor** - Einschränkung der spontanen Entscheidungen im Alltag aufgrund der Technik • **Unsicherheiten im Datenschutz** - Möglichkeit der Übertragung von Daten - Unbewusste Datenaufzeichnung mittels Smart Devices • **Gefahr von Hackerangriffen** - Je mehr Smart Devices, desto größer ist die Angriffsfläche für potenzielle bösartige Hacks. - Fehlende Passwörter und falscher Umgang damit (z.B. Standard-Passwörter) • **Quantität statt Qualität** - Wirtschaftliche Interessen der Hersteller - Kauf von Billigprodukten

Tabelle 2: *Gegenüberstellung von Chancen und Risiken, Ergebnisse aus Experteninterviews & Bevölkerungsbefragung*

6

6 EMPFEHLUNGEN

Auf Basis der vorangegangenen quantitativen und qualitativen Erhebungen konnten für den Bereich Smart Home in Österreich Empfehlungen für Nutzende abgeleitet werden, die in drei Themenfeldern die Qualität der Smart Devices, den Datenschutz und die Vorbeugung von Hackerangriffen ansprechen.

6.1 Schutz durch Qualität vor Quantität

> Wenn man an einer kompletten Smart-Home-Lösung und nicht nur an einzelnen smarten Devices interessiert ist, lohnt es sich, die **Kompatibilität neuer und bestehender Geräte** im Auge zu behalten.
> Beim beratenden oder beauftragten **Fachpersonal** darauf achten, dass hier eine **IT-Sicherheitsexpertise** besteht.
> Auf **Nachhaltigkeit und Support** achten, anstatt Billigprodukte zu kaufen.

6.2 Datenschutz

> Bei der Installation möglicher Software (z.B. Apps) die **Nutzungsvereinbarungen lesen**, um sich der eventuellen Aufzeichnung und/oder Verwertung der eigenen Daten seitens der Herstellerfirma bewusst zu werden.
> Bei einem geplanten Einsatz von Smart Devices sich bereits vorab erkundigen und online recherchieren, **welche technischen Möglichkeiten und Softwarelösungen die jeweiligen Geräte bieten**.
> Konfiguration aktiv betreiben und Settings datenschutzfreundlich einstellen.

6.3 Hackerangriffe

> Mit einem **überlegten Passwortmanagement** kann man Störfälle und Angriffe von außen am effektivsten und einfachsten verhindern.
> Es gilt auch verstärkt die **Gebrauchsanleitungen** zu berücksichtigen, auf die Abänderung von **Standardpasswörtern** zu achten, **Standardkonfigurationen** zu bedenken und **Sicherheitsinformationen in Bedienungsanleitungen** zu sichten. Wichtig ist zudem, bei den Smart Devices zu beachten, ob sie mit **codierten Passwörtern** versehen sind, die sich nach jedem Update automatisch zurücksetzen und stets aufs Neue vom Konsumenten geändert werden müssen.
> Als Schutzvorkehrung gegen Hackerangriffe empfiehlt es sich, **nur jene Geräte in Betrieb** zu nehmen, die einen **tatsächlichen Mehrwert** und/oder eine konkrete Qualitätssteigerung für das eigene Leben und den eigenen Alltag bedeuten.
> Zudem sollten (v.a. sprachgesteuerte) **Smart Devices ausgeschaltet** werden, wenn das Haus für längere Zeit verlassen wird oder die Geräte **über einen längeren Zeitraum nicht verwendet** werden.

7

7 GRUNDSÄTZE FÜR DIE ZUKUNFT

Zukünftig sollte sowohl in der Entwicklung als auch in der Anschaffung von Smart Devices ein **starker Fokus auf die Qualität der Produkte** gelegt werden, um Sicherheitsstandards zu gewährleisten und aufrecht zu erhalten. Dies gilt vor allem für Sicherheitssysteme (z.B. Brandschutz).

Die **Anwender sind hiermit besonders in die Pflicht genommen**, da sie sich aktiv mit den Möglichkeiten smarter Geräte auseinandersetzen sollten. Aber auch **Prüfungsinstanzen** (z.B. TÜV, WKO, AK) sollten eine präsentere Rolle einnehmen und verstärkt Aufklärungsarbeit betreiben (z.B. Geräte prüfen, Empfehlungen formulieren).

Die Schwerpunkte der Sicherheitsarbeit in Sachen Smart Living lassen sich im Detail auf folgende gesellschaftliche Ebenen clustern: **Politik, Wirtschaft & Medien**.

Politik

- **Einheitliche Standards**
  Regulierung des derzeit noch herrschenden Wildwuchses,
  Unsicherheiten der Konsumenten hinsichtlich der Funktionalitäten & Haftungen abfangen
- **Zertifizierungen**
  Orientierungsleistung für Konsumenten und Herstellerfirmen
- **Einführung von Normen für smarte Produktgruppen**
  Schaffung von im gesamteuropäischen Bereich gültigen Normen
- **Produkthaftungen klären**
  z.B. bei Konkurs der Firma, Stör- und Schadensfällen etc.,
  Unsicherheit gegenüber Technikinnovationen mindern

Wirtschaft

- **Investition in die Sicherheit von IoT-Devices**
  Seitens der Hersteller z.B. durch regelmäßige Sicherheitsupdates smarter Geräte
- **Etablierung neuer Berufsgruppen & spezialisierten Fachpersonals**
  Intensivierte Schaffung von Ausbildungsmöglichkeiten mit Fokus auf spezifischem Know-how für Fachpersonal (z.B. IT-Sicherheit)

Medien

- **Aufklärungsauftrag in Form von verstärkter Berichterstattung zu den neuesten Entwicklungen im Bereich Smart Home**
  Information über Sicherheitsmaßnahmen, die die Konsumenten selbst ergreifen können, um sich optimaler vor Störfällen und Angriffen von Smart Devices zu schützen
- **Austausch der Konsumenten über die Effektivität, Funktionalität und Zufriedenheit im Internet**
  Durch Forenkommunikation und/oder per Produktrezensionen Endnutzer dazu bringen, sich bewusst mit den neuen Technologien und deren Herausforderungen auseinanderzusetzen

8

8 ANHANG

ANHANG – LEITFADEN EXPERTENINTERVIEWS

1. Einleitung

- Ich möchte mich heute bei diesem Gespräch auf das Thema Smart Home konzentrieren. Können Sie mir bitte einmal sagen, inwiefern Sie beruflich mit Smart Home zu tun haben?

2. Aktueller Fokus

- Wo sehen Sie aktuell den Schwerpunkt im Bereich Smart Home. Was sind da die wichtigsten Einsatzbereiche?
- Und bezogen auf Ihren Beruf: worauf konzentrieren Sie sich gerade im Bereich „Smart Home".
- Warum ist gerade dieser Bereich so spannend, interessant, …

3. Chancen und Risiken

- Überwiegen Ihrer Meinung nach die Chancen oder eher Gefahren von Smart Home?
- Wo sehen Sie aktuell Chancen?
- Wo mögliche Defizite oder Gefahren? Was ist eventuell noch nicht ausgereift?
- Welche Erfahrungen haben Sie mit Schadensfällen? (Mögl. lustige Anekdoten?)
- Was kann da verbessert werden bzw. wo wird bereits daran gearbeitet?
- Sind da Unterschiede bei verschiedenen Verwendergruppen?

4. Standards

- Wo sollte man ansetzen um die genannten Defizite zu reduzieren?
- Was halten Sie von verbindlichen Sicherheitsstandards? Welche könnten das sein? Wer sollte haftbar sein für welche Gefahren/Schäden?
- Wie können Konsumenten sonst noch geschützt werden?

5. Marktausblick

- Was denken Sie, wohin wird sich „Smart Home" im nächsten Jahr entwickeln? In den nächsten 5 Jahren / nächsten 10 Jahren?
- Was kommt da auf uns zu?

6. Persönliche Wünsche

- Angenommen, Sie wären Leiter eines der großen multinationalen Konzerne und könnten alleine entscheiden, wie es mit dem Thema Smart Home in den nächsten Jahren weitergehen soll. Worauf würden Sie den Fokus legen?
- Was wäre für Sie persönlich am wichtigsten?
- Und was wäre wohl am wichtigsten für die Konsumenten?
- In wie fern sollte der Staat oder Staaten eine Rolle spielen oder sonstige Organisationen?

7. Gemeinsame Zusammenfassung

- Ich möchte zum Schluss die wesentlichen Punkte zusammenfassen, bitte unterbrechen Sie mich und korrigieren oder ergänzen Sie mich, damit es für Sie passt.
- Danke und Verabschiedung

ANHANG – FRAGEBOGEN

061 Fragebogen CATI KFV: Smart Home

Guten Tag, mein Name ist … von Consent Markt- & Sozialforschung.
Wir führen eine Erhebung zum Thema „Smart Home“ im Namen des Kuratoriums für Verkehrs-sicherheit durch.
Darf ich Ihnen dazu ein paar Fragen stellen? Die Befragung wird ca. … Minuten dauern.

F1. Wissen Sie, was der Ausdruck „Smart Home“ bedeutet?

-1 Ja
-2 Nein

Falls F1. = Ja
F1.1. Bitte erklären Sie den Ausdruck "Smart Home", was bedeutet dieser Begriff?

INT: Offene Antwort, ausführlich beantworten!

_____

Falls F1. = Nein
Von einem Smart Home spricht man, wenn im Haus verwendete Leuchten, Schalter und Geräte, wie Heizkörper, Fernseher, Kühlschrank untereinander vernetzt sind und Daten speichern.
Smart Home Geräte können über das Internet und über erweiterbare Apps zB. mit Hilfe eines Smartphone gesteuert werden. D.h. auch Smartphone oder auch Smart-TV gehören zu Smart Home.

ALLE, PROG: Aussagen rotieren
F2. Wie sehr stimmen Sie den folgenden Aussagen zu? Bitte antworten Sie anhand einer Skala von 1-„stimme sehr zu“ bis 4-„stimme überhaupt nicht zu“. Dazwischen können Sie abstufen:

	1	2	3	4
a. Mit einem Smart Home öffnet man Tür und Tor für Datenangriffe.				
b. Ich fühle mich durch ein Smart Home sicherer.				
c. Innerhalb der nächsten Jahre werden nahezu alle Geräte im Haushalt „smart“ sein und z.B. eine Internetverbindung haben.				
d. Ich habe Angst davor, dass die Geräte sich verselbständigen.				
e. Ich befürchte, die Kontrolle darüber zu verlieren, was genau die Geräte machen.				
f. Dass ein Kühlschrank selbständig bestellen kann, stelle ich mir als große Hilfe im Haushalt vor.				
g. Eine automatische Anpassung der Heizung, Kühlung und Belüftung - ohne, dass ich dazu eingreifen muss - finde ich besonders nützlich.				
h. Der Nutzen von Smart Home ist bei weitem größer als die möglichen Gefahren.				
i. Durch Smart Homes wird bestimmt Energie/Strom gespart.				

j. Smart Homes und die dazugehörigen Apps sind momentan noch sehr fehleranfällig.				
k. Während des Urlaubes ist es sehr wichtig, versichert zu sein, dass daheim alles in Ordnung ist mit Hilfe von Smart Home Technologie.				
l. Wenn mein Zuhause mit Smart Home Technologie ausgestattet ist, fühle ich mich überwacht.				
m. Ich finde, dass Leute, die etliche Geräte in ihrem Zuhause mit dem Internet verbinden, sehr leichtsinnig sind.				
n. Personen, die sich für ein Rund-um-Smartes-Zuhause entscheiden, leben sehr zukunftsorientiert.				

ALLE

F3. Nutzen Sie oder können Sie sich die Nutzung dieser SMART Produkte- und Technologien vorstellen?

-1 Ja, ich nutze Smart Produkte
-2 Ja, ich kann mir die Nutzung Smart Produkte vorstellen
-3 Nein, nutze ich nicht und kann mir diese auch nicht vorstellen

ALLE

F4. Im Folgenden beziehe ich mich ausschließlich auf Geräte und/oder Technologien, die SMART - miteinander vernetzte bzw. fernsteuerbare Geräte – betreffen. Bitte sagen Sie mir, welche dieser SMARTEN Geräte Sie bereits nutzen oder planen anzuschaffen oder sich gar nicht vorstellen können zu nützen. Bleiben wir zuerst bei dem Bereich *Licht/Elektrik/Raumklima*…

	Nutze ich bereits	Plane ich anzuschaffen	Lehne ich ab
a. Smart Lightning (z.B. Glühbirne mit App-Steuerung)			
b. Bewegungsmelder (Licht/Temperatur)			
c. Steckdosen (z.B. WLAN-Steckdose mit App-Steuerung)			
d. Schalter, Steuerung (z.B. Elektro-Funk-Dimmer)			
e. Thermostate			
f. Jalousien/Rollos			

F4.1. Gibt es andere SMARTE Geräte aus dem Bereich Licht/Elektrik/Raumklima, die Sie nutzen oder planen anzuschaffen?

-1 Ja
-2 Nein

Falls F4.1 = JA

F4.2. Welche SMARTEN Geräte sind das?

ALLE

F5. Im Folgenden beziehe ich mich wieder ausschließlich auf Geräte und/oder Technologien, die SMART (miteinander vernetzte bzw. fernsteuerbare Geräte) betreffen.
Bitte sagen Sie mir, welche dieser SMARTEN Geräte Sie bereits nutzen oder planen anzuschaffen oder sich gar nicht vorstellen können zu nützen.
Aus dem Bereich intelligente Sicherheitstechnik …

	Nutze ich bereits	Plane ich anzuschaffen	Lehne ich ab
a. Rauchmelder			
b. Kameras (Innen- und oder Außenbereich)			
c. Alarme / Alarmanlagen			
d. Bewegungsmelder			
e. Türsysteme, Videotürsysteme			
f. Anwesenheitssimulator			
g. Smart Baby-Phones			
h. Smart Pet (Cat) Cams			
i. Wettersensoren (z.B. erkennt Unwetter,…)			

F5.1. Gibt es andere SMARTE Geräte aus dem Bereich intelligente Sicherheitstechnik, die Sie nutzen oder planen anzuschaffen?

-1 Ja
-2 Nein

Falls F5.1 = JA
F5.2. Welche SMARTEN Geräte sind das?

_____

ALLE

F6. Im Folgenden beziehe ich mich wieder ausschließlich auf Geräte und/oder Technologien, die SMART (miteinander vernetzte bzw. fernsteuerbare Geräte) betreffen.
Bitte sagen Sie mir, welche dieser SMARTEN Geräte Sie bereits nutzen oder planen anzuschaffen oder sich gar nicht vorstellen können zu nützen.
Aus dem Bereich vernetzte Haushaltsgeräte …

	Nutze ich bereits	Plane ich anzuschaffen	Lehne ich ab
a. Kochfelder/Mikrowelle/Dunstabzugshauben			
b. Waschmaschinen			
c. Kühl- & Gefriergeräte			
d. Geschirrspüler			
e. Kaffeemaschine			

F6.1. Gibt es andere SMARTE Geräte aus dem Bereich vernetzte Haushaltsgeräte, die Sie nutzen oder planen anzuschaffen?

-1 Ja
-2 Nein

Falls F6.1 = JA
F6.2. Welche SMARTEN Geräte sind das?

_____

ALLE
F7. Im Folgenden beziehe ich mich wieder ausschließlich auf Geräte und/oder Technologien, die SMART (miteinander vernetzte bzw. fernsteuerbare Geräte) betreffen.
Bitte sagen Sie mir, welche dieser SMARTEN Geräte Sie bereits nutzen oder planen anzuschaffen oder sich gar nicht vorstellen können zu nützen.
Aus dem Bereich *Entertainment / IT-Equipment* …

	Nutze ich bereits	Plane ich anzuschaffen	Lehne ich ab
a. Smart-TV			
b. Digitale Assistenten (z.B. Alexa, Amazon Echo, Google Home)			
c. Multi-Room Audio (z.B. Soundbar Bluetooth)			
d. Spielkonsolen			
e. Büro-Equipment (z.B. Tablets, Drucker, ...)			

F7.1. Gibt es andere SMARTE Geräte aus dem Bereich vernetzte Haushaltsgeräte, die Sie nutzen oder planen anzuschaffen?

-1 Ja
-2 Nein

Falls F7.1 = JA
F7.2. Welche SMARTEN Geräte sind das?

_____

ALLE
F8. Im Folgenden beziehe ich mich wieder ausschließlich auf Geräte und/oder Technologien, die SMART (miteinander vernetzte bzw. fernsteuerbare Geräte) betreffen.
Bitte sagen Sie mir, welche dieser SMARTEN Geräte Sie bereits nutzen oder planen anzuschaffen oder sich gar nicht vorstellen können zu nützen.
Aus dem Bereich *Gesundheit, Unfallvermeidung, Hilfe in medizinischem Notfall* …

	Nutze ich bereits	Plane ich anzuschaffen	Lehne ich ab
a. Medizinische Geräte mit App			
b. Selbstoptimierungstools (z.B. Fitness-Wearables)			
c. Notrufsysteme für medizinische Notfälle und Unfälle (Senioren-Pieps)			
d. Datenerfassung betreuter Personen zur Koordinierung vom Pflegediensten			
e. Technische Assistenzsysteme in der Pflege			

F8.1. Gibt es andere SMARTE Geräte aus dem Bereich vernetzte Haushaltsgeräte, die Sie nutzen oder planen anzuschaffen?

-1 Ja
-2 Nein

Falls F8.1 = JA
F8.2. Welche SMARTEN Geräte sind das?

_____

ALLE
F9. Für wie groß halten Sie den Nutzen eines Smart Home in der Zukunft für folgende Einsatzgebiete. Bitte antworten Sie anhand einer Skala von 1-„sehr großer Nutzen“ bis 4-„gar kein Nutzen“. Dazwischen können Sie abstufen:

	1	2	3	4
a. Unterstützung im Haushalt und Garten				
b. Unfallvermeidung				
c. Kindersicherheit (Pool- und Fenstersicherung)				
d. Einbruchschutz				
e. Warnsysteme bei Naturkatastrophen				
f. Pflege und Sicherheit von Senioren, Förderung sozialer Interaktion von Senioren				
g. Gesundheit und Fitness				

FALLS F3 = Nutzt bzw. Plant zu nutzen
F10. Sie haben u.a. gesagt, dass Sie Smart Home Geräte nutzen bzw. anschaffen möchten. Was genau sind da Ihrer Meinung nach die besonderen Vorteile bzw. die Gründe der Nutzung?

INT: Offene Antwort, ausführlich beantworten!

_____

FALLS F3 = Lehnt Smart Home ab

F11. Sie haben u.a. gesagt, dass Sie Smart Home Geräte generell nicht nützen wollen. Was sind die Nachteile bzw. warum wollen Sie sie nicht nutzen?

INT: Offene Antwort, ausführlich beantworten!

ALLE

F12. Denken Sie bitte an sämtliche Geräte, Einrichtungen, Technologien, die Sie zuhause haben, die „smart" sind. Haben Sie bei der Nutzung irgendeine Störung, ein Fehlverhalten oder sogar einen Schadensfall erlebt?

INT: gemeint sind nicht technische Gebrechen im engeren Sinn, sondern Datenverluste, Fehlverhalten, Programmfehler, Hacker-Angriffe u.ä.

-1 Ja

-2 Nein

FALLS F12 = JA

F13. Was genau ist da passiert?

INT: Offene Antwort, ausführlich beantworten!

ALLE

F14. Leben in Ihrem Haushalt auch Kinder oder Jugendliche im Alter bis 18 Jahren?

-1 Ja

-2 Nein

FALLS F14 = JA

F15. Wie viele Kinder (im Alter bis 18 Jahre) wohnen bei Ihnen im Haushalt?

FALLS F14 = JA

F16. Wie alt sind die Kinder?

FALLS F14 = JA

F17. Welche Geräte bezogen auf Smart Home / Smart Living nutzt das Kind / die Kinder/ Jugendliche, die wir noch nicht besprochen haben? Bitte denken Sie auch an Tablets, Play-Station, Wii und Spielzeuge mit Spracherkennung?

FALLS F14 = JA

F18. Welche Vorteile sehen Sie in der Nutzung?

FALLS F14 = JA
F19. Welche Gefahren bzw. Nachteile könnten diese bergen?

_____

ALLE
F20. Wie sicher fühlen Sie sich in Ihrem Zuhause gegenüber „Hacker-Angriffen“? Bitte antworten Sie anhand einer Skala von 1-„stimme sehr zu“ bis 4-„stimme überhaupt nicht zu“. Dazwischen können Sie abstufen:

	1	2	3	4
a. Ich fühle mich sehr sicher.				

ALLE
F21. Wie viele Smartphones nutzen Sie im Haushalt (ggfs. Ihres mit eingeschlossen)?

ALLE
F22. Wie viele Tablets nutzen Sie im Haushalt (ggfs. Ihres mit eingeschlossen)?

ALLE
F23. Wie ist Ihre aktuelle Wohnsituation? Bitte berücksichtigen Sie auch eventuelle Zweitwohnsitze.

-1 Ich wohne ausschließlich in einer Wohnung.
-2 Ich wohne ausschließlich in einem Haus.
-3 Ich wohne überwiegend in einem Haus, aber auch in einer Wohnung.
-4 Ich wohne überwiegend in einer Wohnung, aber auch in einem Haus.
-5 Sonstiges.

Nun zum Abschluss einige soziodemografische Angaben:

D1. Geschlecht des Befragten:

-1 Männlich
-2 Weiblich

D2. Alter des Befragten:

INT: in Jahre, nur Zahl als Antwort zulässig!

_____

D3. Anzahl der Personen im Haushalt (Befragten eingeschlossen):

INT: nur Zahl als Antwort zulässig!

_____

D4. Wie hoch ist das Haushalts-Netto-Einkomme (d.h. die Summe aller Netto-Einkünfte aller Haushaltsmitglieder)?

-1 1.000 € und weniger
-2 1.001 - 1.500 €
-3 1.501 - 2.000 €
-4 2.001 - 2.500 €
-5 2.500 - 3.000 €
-6 3.500 - 4.000 €
-7 Über 4.000 €

D5. Höchste abgeschlossene Ausbildung des Befragten:

-1 Pflichtschule
-2 Lehre/Berufsschule
-3 AHS/BHS ohne Matura
-4 AHS/BHS mit Matura
-5 Hochschulabschluss (FH/Uni)

D6. Bitte notieren Sie die aktuelle berufliche Situation des Befragten:

-1 Selbständiger, Freiberufler
-2 Angestellter, Arbeiter
-3 Beamter
-4 Schüler, Student
-5 Karenz, Zivildienst, Bundesheer
-6 Arbeitslos
-7 In Pension

D7. Arbeitsausmaß der Beschäftigung:

-1 Vollzeit
-2 Teilzeit
-3 Geringfügige Beschäftigung

D8. Bundesland:

-1 Wien
-2 NÖ
-3 Burgenland
-4 OÖ
-5 Steiermark
-6 Kärnten
-7 Salzburg
-8 Tirol
-9 Vorarlberg

D9. Einwohnergröße des Wohnorts des Befragten:

-1 Bis 5.000 Einwohner
-2 Bis 10.000 Einwohner
-3 Bis 20.000 Einwohner
-4 Bis 50.000 Einwohner
-5 über 50.000 Einwohner

D10. Nationalität des Befragten:

-1 Österreich -2 Anderes Land

Falls D10 = Anderes Land
D11. Welche Nationalität gehört der Befragte an?

_____

Vielen Dank für die Beantwortung Ihrer Fragen. Auf Wiedersehen.

9

9 ABBILDUNGSVERZEICHNIS

10

10 TABELLENVERZEICHNIS

11

11 LITERATURVERZEICHNIS

https://www.it-business.de/der-durchbruch-von-smart-home-steht-noch-bevor-a-525906/

https://www.homeandsmart.de/was-ist-ein-smart-home

http://www.techradar.com/news/amazon-echo-vs-homepod-vs-google-home-the-battle-of-the-smart-speakers

https://www.amazon.de/Amazon-Zertifiziert-general%C3%BCberholt-Vorherige-Generation/dp/B01GAGVGH8?psc=1&SubscriptionId=AKIAIPHVZTVH6LZ5BFZA&tag=techracom00-21&linkCode=xm2&camp=2025&creative=165953&creativeASIN=B01GAGVGH8&smid=A3JWKAKR8XB7XF&ascsubtag=trd

https://www.it-business.de/der-durchbruch-von-smart-home-steht-noch-bevor-a-525906/

https://www.it-business.de/der-durchbruch-von-smart-home-steht-noch-bevor-a-525906/ https://de.statista.com/outlook/279/128/smart-home/oesterreich

https://www.it-business.de/der-durchbruch-von-smart-home-steht-noch-bevor-a-525906/

http://bundeskriminalamt.at/501/start.aspx

https://www.derstandard.de/story/2000067317360/alexa-spielte-selbststaendig-laute-musik-polizeieinsatz-in-hamburg

http://help.orf.at/stories/2878852/

http://www.sueddeutsche.de/digital/it-sicherheit-bundesnetzagentur-verbietet-spionierende-kinderuhren-1.3754397

12

12 IMPRESSUM

Medieninhaber, Herausgeber und Verleger:
KFV (Kuratorium für Verkehrssicherheit)
Schleiergasse 18
1100 Wien
Tel: +43 (0)5 77 0 77-1919
Fax: +43 (0)5 77 0 77-1187
kfv@kfv.at
www.kfv.at

Vereinszweck und Richtung
Der Verein ist eine Einrichtung für alle Vorhaben der Unfallverhütung und eine Koordinierungstelle für Maßnahmen, die der Sicherheit im Verkehr sowie in sonstigen Bereichen des täglichen Lebens dienen. Er gliedert sich in die Bereiche Verkehr und Mobilität, Heim, Freizeit, Sport, Eigentum und Feuer sowie weitere Bereiche der Sicherheitsarbeit.

Geschäftsführung
Dr. Othmar Thann, Dr. Louis Norman-Audenhove

ZVR-Zahl
801 397 500

Grundlegende Richtung
Die Publikationsreihe "KFV – Sicher Leben" dient der Veröffentlichung von Studien aus dem Bereich Eigentumsschutz, die vom KFV oder in dessen Auftrag durchgeführt wurden.

Autorinnen
Mag. Monika Pilgerstorfer
Dr. Yvonne Prinzellner

Fachliche Verantwortung
Dr. Armin Kaltenegger

Redaktion
Sabine Fuger
KFV (Kuratorium für Verkehrssicherheit)
Schleiergasse 18
1100 Wien

Verlagsort
Wien, 2018

Lektorat
Mag. Eveline Wögerbauer
Angela Dickinson, MSc.

Grafik
catharinaballan.com

Fotos
KFV (Kuratorium für Verkehrssicherheit)

ISBN – pdf-Version
978-3-7070-0150-1

Zitiervorschlag
KFV – Sicher Leben. Band #15. Smart Living in Österreich. Wien, 2018

ISBN (PDF) 978-3-7070-0150-1