Internet of Things in österreichischen Privathaushalten

Nutzung, Sicherheit und Kriminalität

Wien, 16.09.2021

Durchgeführt im Auftrag von: Dr. Armin Kaltenegger

Internet of Things in österreichischen Privathaushalten

Nutzung, Sicherheit und Kriminalität

Co-Autor*innen
Mag.[a] Dagmar Lehner
Dr.[in] Claudia Riccabona-Zecha
Cyber-Competence-Center des Bundeskriminalamtes

Fachliche Verantwortung
Dr. Georg Plattner

Inhaltsverzeichnis

1. Einführung: IoT aus der Sicht des Cybercrime-Competence-Center des Bundeskriminalamtes

Bei all den Vorteilen, die der Einsatz von IoT für uns alle bringt, darf aber nicht außer Acht gelassen werden, dass die immer weiter fortschreitende Verbreitung von IoT und der zusätzlichen Vernetzungsmöglichkeiten durch 5G auch die Kriminalpolizei vor neue Herausforderungen stellen.

Dabei geht es nicht nur um die Bekämpfung von Cybercrime im engeren Sinne, sondern praktisch um alle Deliktsfelder. War früher noch ein „Dietrich“ das bevorzugte Werkzeug eines Einbrechers so ist es heute der Computer (Laptop, Tablet, Smartphone, …), mit dem das Sicherheitssystem überlistet wird, die Türe zu öffnen. Aber das ist nur eines der unzähligen Beispiele.

Die dabei auf Seiten von IoT ausnutzbaren Schwachstellen sind mannigfaltig. Als hervorstechendste sind unsichere Passwörter (die oft nicht einmal von Benutzer geändert werden können bzw. im Internet veröffentlicht sind, …), fehlende Sicherheitsupdates und Fehler in der Konfiguration zu nennen. Das wirkt sich umso mehr aus, als diese Geräte deutlich länger als herkömmliche Computer im Einsatz sind und für Angriffe zur Verfügung stehen.

Aufgrund der (wirtschaftlichen) Vorgaben wie geringer Stromverbrauch, kleine Abmessungen und attraktiver Preis ist es auch nicht einfach Sicherheit zu implementieren. Hier könnten entsprechende Standards, Vorgaben und Prüfzeichen, wie z.B. bei Elektrogeräten üblich, den Konsumenten bei der Auswahl helfen.

Die kriminelle Nutzung von IoT und Vernetzung über 5G als Werkzeug oder Einfallstor könnten auch viele nützliche Hinweise auf die angewandten Methoden („Handschrift“) und damit auf die Täterschaft selbst liefern. Allerdings werden in vielen Fällen keine oder lediglich unzureichende (technische) Protokolle aufgezeichnet. Außerdem ist es meist nicht einfach möglich, vorhandene Protokolle auszulesen und auszuwerten.

Neben Maßnahmen, die auf Vermeidung von erfolgreichen kriminellen Handlungen abzielen, wie Bewusstseinsbildung bei den Konsumenten und Vorgaben oder gar Zwängen auf Seiten der Hersteller (Standards, Prüfzeichen, …) sind natürlich auch Aspekte der Aufklärung von Straftaten von Bedeutung. Dazu gehören vorallem systematische Erkenntnisse über forensische Möglichkeiten verschiedenste IoT-Geräte auszuwerten. Im Vorfeld der forensischen Untersuchung stellt auch die Lokalisierung von IoT Geräten (geringe Abmessungen, keine Kabel notwendig wegen Akkubetrieb und Vernetzung über 5G, leicht zu verbergen, …) eine Herausforderung dar. Auch hier können entsprechende wissenschaftliche Erkenntnisse und daraus abgeleitete Tools die Kriminalitätsbekämpfung deutlich unterstützen.

Im Zusammenhang mit 5G stellt sich immer wieder die Frage nach der Nachvollziehbarkeit und Zuordenbarkeit der Kommunikation – hauptsächlich bei Netzwerken auf IPv4 Basis (Stichwort CGN). Im Hinblick auf den bevorstehenden Umstieg auf IPv6 können identifizierte und wissenschaftlich belegbare Vorteile für die Strafverfolgung als Argumentationsgrundlage für diesen Umstieg dienen. Im Bewusstsein, dass es kein Licht ohne Schatten gibt, gilt es aber auch auszuloten, welche forensischen und ermittlungstechnischen Nachteile IPv6 mit sich bringt.

Abschließend soll betont werden, dass – bei all den sicherheitstechnischen Herausforderungen – IoT und 5G geeignet sind, nicht nur Wirtschaft, Medizin, … zu unterstützen, sondern auch das Leben der Menschen zu vereinfachen und bequemer zu machen. Wie bei Vielem kommt es auch hier darauf an, wie die Umsetzung erfolgt.

2. Einleitung

Kriminalität und ihre Prävention bedeuten immer auch eine Art Katz-und-Maus-Spiel zwischen jenen, die illegale Handlungen setzen wollen und den staatlichen Strafverfolgungsbehörden. Speziell technologische Entwicklungen führen hier oftmals zu Situationen, in welchen die Prävention der Kriminalität einen Schritt voraus sein könnte oder müsste, de facto jedoch hinterherhinkt. Denn oft ist eine Sicherheitslücke oder eine Produktschwäche so lange unbekannt, bis sie ausgenutzt wird.

Im Besonderen ist jede technologische Entwicklung, die in der breiten Bevölkerungsmasse Anwendung findet, von diesem Risiko betroffen. Denn je mehr Menschen eine Technologie nutzen, um so größer ist auch die Gefahr, dass einige unbedarft und sorglos damit umgehen und es somit Verbrecher*innen besonders leicht machen. Dies ist bereits nachvollziehbar an den nach wie vor sehr stark steigenden Zahlen zu Cyberkriminalität im Allgemeinen. Seit der Einführung des Privat-PCs ist es nicht nur die Innovationsfähigkeit der Kriminellen, sondern auch die Sorglosigkeit der Nutzer*innen, die diese Verbrechensart zu der am stärksten steigenden weltweit macht.

Seit einigen Jahren ist nun die nächste Entwicklungsstufe der Digitalisierung in der breiten Masse der Bevölkerung angekommen: Das „Internet of Things“ (Internet der Dinge, kurz IoT) tritt auch in Österreich seinen Siegeszug an. Die Vorteile dieser smarten Geräte und ihre Vernetzung untereinander und mit dem*der einzelnen User*in sind mannigfaltig: das Haus wird automatisch gereinigt, die Fensterläden werden selbständig bei Sonneneinstrahlung geschlossen, der Kühlschrank bestellt in Eigenregie Milch und Joghurt. Doch auch die Sicherheit zu Hause kann erhöht werden, durch smarte Schließsysteme oder Überwachungskameras.

Was ist neu am Internet of Things? Nun, zunächst die Tatsache, dass IoT keine menschliche Intervention mehr braucht, um zu funktionieren. Sensoren sammeln, kommunizieren, analysieren und handeln basierend auf Informationen, ohne dass der Mensch selbst aktiv werden muss. Doch diese Verknüpfung untereinander ist auch das größte Risiko der neuen Technologie: ein*e Cyberkriminelle muss sich nicht mehr an der Sicherheitstüre abmühen, um in ein Haus einzudringen – stattdessen wird in das durch Sorglosigkeit nur mangelhaft gesicherte Schließsystem eingedrungen und die Tür springt von selbst auf. Die Daten des Saugroboters können Rückschlüsse darauf geben, wann ein*e Besitzer*in nicht zu Hause ist, eine nützliche Information für Einbrecher*innen. Und ein schlecht gesicherter smarter Kühlschrank kann das Einfallstor in den eigentlich gut gesicherten Stand-PC mit sämtlichen sensiblen persönlichen Daten darstellen.

Das KFV will mit der hier vorliegenden Studie einen Beitrag zur Prävention von Cyberkriminalität über IoT-Geräte schaffen. Ausgehend vom Status Quo der Nutzung von IoT in österreichischen Privathaushalten über eine repräsentative Bevölkerungsbefragung wird die Sicherheit der österreichischen Nutzer*innen kritisch analysiert, um anschließend aufzuzeigen, worauf zu achten ist, um diese Innovationen möglichst sicher nutzen zu können. Darüber hinaus wird auch dargelegt, wie die Rechtsprechung die User*innen von IoT-Geräten besser schützen kann.

3. Das „Internet of Things“ als nächste Stufe der privaten Digitalisierung: Chancen und Risiken

3.1. Internet of Things: Definition

Der Begriff „Internet of Things“, zu Deutsch „das Internet der Dinge“ (IoT) lässt sich nur schwer klar definieren. Zum einen gibt es die alltagsgebräuchliche Definition von IoT, die fast schon alles umfasst, was mit einem Netzwerk kommuniziert. Zum anderen existiert auch die sehr enge, technische Definition von IoT, und diese umfasst „kleine, langlebige Devices mit geringem Stromverbrauch die in unserer Umgebung integriert sind“, so DI Mag. Georg Petzl, der Chief Security Officer beim Mobilfunkbetreiber Magenta (Petzl, 2021). Dr. Jaro Krieger-Lamina, Forscher am Wiener „Institut für Technikfolgenabschätzung“ der Österreichischen Akademie der Wissenschaften definiert IoT hingegen etwas breiter: „Es geht nicht nur um Geräte oder ‚Dinge‘, sondern auch um Wearables, also zum Beispiel smarte Kleidung, die miteinander vernetzt werden. Ich würde davon Geräte ausnehmen, deren primärer Zweck die Vernetzung ist, wie zum Beispiel Computer. Es geht also um Geräte, die vernetzt werden müssen, um ihre ganze Funktionalität nutzen zu können“ (Krieger-Lamina, 2021).

Eine einleuchtende und umfassende Definition von Funktion und Zweck des „Internet of Things“ bietet der Halbleiterhersteller Infineon in seinem Dossier zum Thema an:

> *Das Internet der Dinge (Internet of Things, IoT) verbindet physische Objekte mit der virtuellen Welt. Intelligente Geräte und Maschinen sind dabei miteinander und mit dem Internet vernetzt. Sie erfassen relevante Informationen über ihre unmittelbare Umgebung, analysieren diese und verknüpfen sie. Auf dieser Basis erledigen die Geräte bestimmte Aufgaben. Beispielsweise misst ein Sensor die Außentemperatur, woraufhin das smarte Gerät, in das er eingebaut ist, die Heizung aufdreht. Das alles passiert automatisch, ganz ohne aktives Eingreifen des Anwenders* (Infineon, 2019).

3.2. Geschichte

Die Geschichte von IoT begann „offiziell“ im Jahr 1999, als während einer IT-Konferenz ein Toaster mit dem Internet verbunden und ein- und ausgeschalten werden konnte. Den Begriff „Internet of Things“ prägte 1999 der britische Forscher Kevin Ashton. Der Forscher am Massachusetts Institute of Technology (MIT) beschrieb damit passive RFID-Tags. RFID ist eine Technologie, die es einem Lesegerät erlaubt, Daten kontaktlos von einem Funketikett (Tag) zu lesen und zu speichern. Wenig später, im Jahr 2000, stellte der Elektronikkonzern LG die Idee eines internetfähigen Kühlschranks vor: Er sollt den*die Besitzer*in benachrichtigen, wenn die Vorräte an Käse, Butter oder Eiern ausgegangen sind (ebda.).

Seitdem hat die Vernetzung ihren Siegeszug angetreten: Schon 2008 waren mehr Geräte mit dem Internet verbunden, als es Menschen auf der Erde gab, wie der Netzwerkspezialist Cisco ermittelte (Evans, 2011). Gemeint sind damit nicht nur Smartphones und Computer, sondern alle möglichen Gegenstände. In Zukunft werden immer mehr Geräte smart sein: **Rund 75 Milliarden Geräte werden weltweit 2025 mit dem Internet verbunden sein** (IoT Business News, 2020).

3.3. Verwendung und Potential

Dabei kommt IoT in ganz unterschiedlichen Bereichen zum Einsatz, so zum Beispiel in der so genannten Industrie 4.0, also der vierten industriellen Revolution: nach der Erfindung von Dampfmaschine, elektrischer Energie und anschließend der Einführung der Computerisierung in der Produktion folgt nun die Vernetzung von Maschinen, Waren und Anlagen. So soll die gesamte Wertschöpfungskette digitalisiert und damit auch effizienter werden. So ist es in Betrieben der Industrie 4.0 möglich, dass Produkte mit Geräten in weitgehend automatisierten Prozessen kommunizieren und den nächsten Schritt der Produktion selbständig anstoßen können. Außerdem können Maschinen selbst erkennen, wann sie Wartungen benötigen, und Fertigungsroboter können selbständig mit der Lagerlogistik kommunizieren. In der vernetzten Infrastruktur können Prozesse simplifiziert werden und daher auch Waren schneller produziert werden.

Die wichtigsten Veränderungen, die die Digitalisierung bringen wird, ist vor allem eine weitere Vernetzung von Unternehmensprozessen, sowohl für die üblichen Geschäftsbereiche (IT – Information Technology), sowie aber auch für die Produktionsanlagen und -technologien (OT-Operational Technology). Je vernetzter diese Bereiche werden, umso mehr verändern und verstärken sich auch die Schutzziele dieser Bereiche (Verein Industrie 4.0, 2019).

Die unter dem Schlagwort IoT zusammengefassten Umwälzungen der Rolle, die digitale, smarte Technologie in unserer Gesellschaft spielen wird, ist eines der relevantesten Themen für Unternehmen, um zukunftsfit zu werden. Eine deutsche Studie zum Thema (Vogt, 2019) zeigt, dass IoT ein sich ständig weiter entwickelnder Prozess ist, den Unternehmen durchaus aktiv durchleben, aber oftmals auch von den Anforderungen überfordert sind.

IoT führt jedoch auch zu einer Revolution in Privathaushalten. Themen wie Smart Home oder E-Health sind bereits in vielen europäischen Haushalten angekommen. Egal ob der Staubsaugerroboter, die automatische Heizung, die Sonnenlichtsensoren, die die Jalousien automatisch senken lassen, oder die smarten Fitnesstracker: IoT ist im Alltag der Menschen allgegenwärtig.

Für Jaro Krieger-Lamina ist jedoch die momentane Nutzung von IoT erst der Beginn, und das Potential von IoT vor allem für gesellschaftlichen Mehrwert noch lange nicht ausgereizt: „Ich glaube, dass das große Potential darin steckt, dass man sehr viele Sensordaten erheben kann und sich damit etwas anderes erspart“. Hier ist vor allem gemeint, dass der Staat oder andere öffentliche Dienstleister bereits vorhandene Sensordaten von IoT-Geräten nutzen, um zum Beispiel den Straßenzustand zu erheben, ohne diese Straße selbst überprüfen zu müssen. „Man kann auf etwas zurückgreifen, das ohnedies vorhanden ist, und in diesem Fall auch unproblematisch zu verwenden ist, weil es vollkommen reicht, dass die Daten anonym zur Verfügung gestellt werden, weil ich sie aggregieren kann und dann auf eine sehr breite Datenbasis zurückgreifen kann“ (Krieger-Lamina, 2021).

3.4. Risiken von IoT

Diese Revolutionen im Privaten und in der Wirtschaft führen jedoch natürlich auch zu neuen Risiken. Speziell technologische Entwicklungen führen nämlich oftmals zu Situationen, in welchen die Prävention der Kriminalität einen Schritt hinterherhinkt. Denn oft ist eine Sicherheitslücke oder eine Produktschwäche so lange unbekannt, bis sie ausgenutzt wird. Dies gilt genauso für das Thema Internet of Things.

Das bedeutet, dass Innovationen wie IoT, die sich schnell weiterentwickeln, immer eine besondere Herausforderung für Strafverfolgungsbehörden darstellen. Sie müssen hier oftmals zunächst vor allem reagieren – denn selbst wenn die Schwachpunkte ungefähr bekannt sind, ist die Art und Weise, in der eine kriminelle Handlung letztendlich gesetzt wird, oft nicht direkt vorhersehbar. Und die Innovationskraft nicht nur auf Seiten des Gesetzes, sondern auch auf Seiten der Kriminellen, führt zu einem ständigen Wettrennen um das nächste Schlupfloch.

Für IoT ist das Hauptrisiko schlicht die rasant und unaufhaltsam steigende Anzahl an mit dem Internet verbundenen Geräten. Jedes Gerät ist ein potentielles Sicherheitsrisiko, und je kleiner und „unwichtiger“ das Gerät, umso wahrscheinlicher ist es, dass dieses nicht ausreichend vor Fremdzugriff geschützt wurde. Hinzu kommt, dass die Geräte oft klein sind und eine lange Batterieleistung aufweisen sollen, wenn sie nicht selbst im Stromnetz hängen. Georg Petzl gibt hier zu bedenken, dass hier der Wille der Hersteller*innen, die Sicherheit der Soft- und Firmware einigermaßen sicherzustellen, niedrig ist, vor allem wenn gleichzeitig der Preis der Geräte niedrig ist (Petzl, 2021).

Die IT-Sicherheitsforscher*innen Stephen Hilt, Vladimir Kropotov, Fernando Mercês, Mayra Rosario und David Sancho (2019) analysierten in einem Bericht für Trend Micro Research die Chats in fünf Untergrundforen zum Thema IoT und Cyberkriminalität. Die Untersuchungen ergaben, dass momentan der Fokus der kriminellen Aktivitäten darauf liegt, den Zugang zu vernetzten Geräten zu verkaufen – hierbei vor allem zu Routern, Webcams und Druckern. Der Zugang zu diesen Geräten wird meist mit so genannten Brute Force Attacken bewerkstelligt. Dies bedeutet, dass direkt versucht wird, ein Passwort oder Benutzer*innennamen zu knacken, und zwar nach dem Trial-and-Error Prinzip. Das bedeutet, es wird so lange ein Passwort eingegeben, bis es passt. Hierfür werden mittlerweile meistens Tools wie Wörterbücher verwendet, um die Arbeit zu automatisieren und massiv zu beschleunigen.

In dem Bericht von Trend Micro wird klar, dass IoT-Geräte momentan vor allem für Botnetzwerke genutzt werden – entweder zum Cryptomining[1] oder für DDoS-Attacken[2] beispielsweise. Mit der weiteren Verbreitung von schlecht gesicherten IoT-Geräten wird daher auch die Armee der Bots

[1] „Als Cryptomining ist das „Abschürfen“ von Einheiten einer Cryptowährung wie Bitcoin zu verstehen. Da solche rein digitalen Währungen nicht von Staaten oder Banken verwaltet und ausgegeben werden, benötigen sie sogenannte Cryptominer, die sämtliche Transaktionen aufzeichnen, verifizieren und verbuchen. Nur so kann sichergestellt werden, dass mit einer Geldeinheit zeitgleich immer nur eine Transaktion ausgeführt wird“ (IT-Service Network, 2021). Hierfür werden die komplexen Daten von den Geräten der Miner*innen mittels Blockchain verarbeitet. Auf Grund der hohen Rechenleistung, die benötigt wird, um Cryptomining zu ermöglichen, dauert es lange und kostet sehr viel Strom. Cryptomining selbst ist komplett legal, wird jedoch illegal, wenn hierfür auf Fremdgeräte zugegriffen wird.

[2] DDoS steht für Distributed Denial of Service. Es ist das Ergebnis einer gezielten Attacke, die in der Regel mit Schadsoftware durchgeführt wird. Im „Erfolgsfall“ führt eine solche Attacke zu einem Ausfall eines oder mehrerer Dienste bzw. Systeme. Ursache für die Nicht-Verfügbarkeit oder den Total-Ausfall dieser Dienste und Systeme ist häufig eine Überlastung der Infrastruktur. Botnetzwerke sorgen dafür, dass in kurzer Zeit eine enorm hohe Zahl an Anfragen an einen Server oder eine Netzwerk-Infrastruktur gestellt wird. Hierfür werden viele – manchmal hunderttausende – Geräte mit einem Computerwurm infiziert, der dann die Anfragen ausführt.

für Cyberkriminelle extrem wachsen. Hier wird es vor allem um Geräte gehen, die entweder direkt ans Stromnetz angebunden sind und auf Android oder Linux basieren, wie Smart TVs, Router, Kühlschränke oder Drucker. Denn sowohl Mining als auch DDoS-Attacken kosten sehr viel Strom und würden bei Geräten mit Akku sehr schnell auffliegen.

Doch auch für sehr viel direktere und für die Einzelperson schädlichere Missetaten können IoT-Geräte genutzt werden. Sind die Zugangsdaten erstmal geknackt, können im schlimmsten Fall Geräte ferngesteuert und manipuliert werden. So kann dann der Einbrecher die Haustür per Mausklick öffnen, während seine Komplizin über die Sicherheitskameras im Haus darauf achtet, dass niemand den Täter bei der Arbeit stört.

Ein weiteres Risiko besteht in der Vernetzung selbst, wie Jaro Krieger-Lamina ausführt: „Normalerweise habe ich, wenn ich ein Smart Home habe, auch einen Computer, und diese zwei sind miteinander vernetzt. Das heißt, möglicherweise habe ich einen abgesicherten Computer, aber wenn man dann über mein Smart-Home-Netzwerk reinkommt, dann kommt man vielleicht auch auf meinen Computer“ (Krieger-Lamina, 2021).

Darüber hinaus kann laut den Expert*innen davon ausgegangen werden, dass in Zukunft das Geschäft der Cyberkriminellen mit dem Zugang zu und der Ausnutzung von IoT-Geräten weiter ansteigen wird. Sei es für die bereits jetzt häufigsten Formen, wie oben beschrieben, oder für ganz neue Formen von Kriminalität, die die Kreativität von Kriminellen erfordert. Die Forscher*innen gehen davon aus, dass sich die Geschäftsmodelle der Kriminellen weiterentwickeln und komplexer werden.

4. Methoden

Um das Themenfeld von mehreren Seiten zu beleuchten, hat das KFV zwei Methoden gewählt:

Zum einen wurden im Frühjahr 2021 zwei Experteninterviews durchgeführt. Hierfür wurde zum einen ein Experte für Technikfolgenabschätzung, zum anderen der Sicherheitschef des Mobilfunkanbieters Magenta befragt. Die Experten stellten hier ihre Sicht auf den Themenkomplex dar und erlaubten tiefgehende Einblicke in IoT, dessen Gefahren und Potentiale.

Tabelle 1: Befragte Experten

Experte	Funktion	Datum des Interviews
Jaro Krieger-Lamina, Msc	Wissenschaftlicher Mitarbeiter am Institut für Technikfolgenabschätzung (ITA) der österreichischen Akademie der Wissenschaften	8.4.2021
DI Mag. Georg Petzl	Chief Security Officer Magenta	22.3.2021

Darüber hinaus wurde in Kooperation mit dem Marktforschungsinstitut Kantar eine repräsentative quantitative Bevölkerungsbefragung durchgeführt. Ziel war es herauszufinden, wie der Wissensstand der Österreicher*innen zum Internet der Dinge ist, wie weit verbreitet IoT-Geräte bereits sind, und wie gut die Österreicher*innen ihre Geräte schützen. Darüber hinaus wurde auch untersucht, ob und falls ja auf welche Art und Weise Österreicher*innen bereits Opfer von Cyberkriminalität über ihre IoT-Devices wurden.

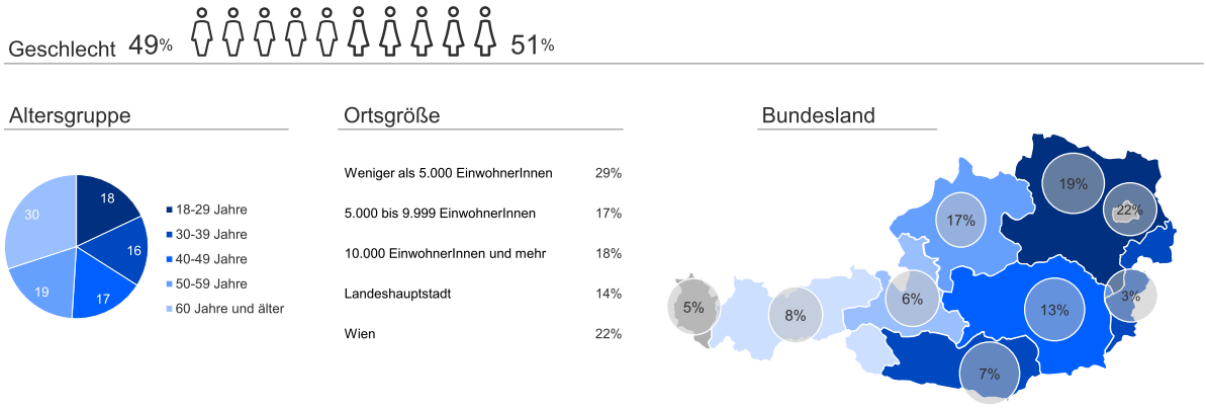


Abbildung 1: Sample der quantitativen Erhebung

5. IoT in Österreichs Privathaushalten: eine Analyse

In der Bevölkerungsbefragung wurde zunächst gefragt, ob die befragte Person prinzipiell weiß, was das „Internet der Dinge“ ist. Bevor eine Definition vorgelegt wurde, gab ein Drittel der Befragten an zu wissen, was das „Internet der Dinge“ ist. Überdurchschnittlich hoch war der subjektive Kenntnisstand bei Männern, jüngeren Personen bis 39 Jahre sowie im städtischen Bereich.

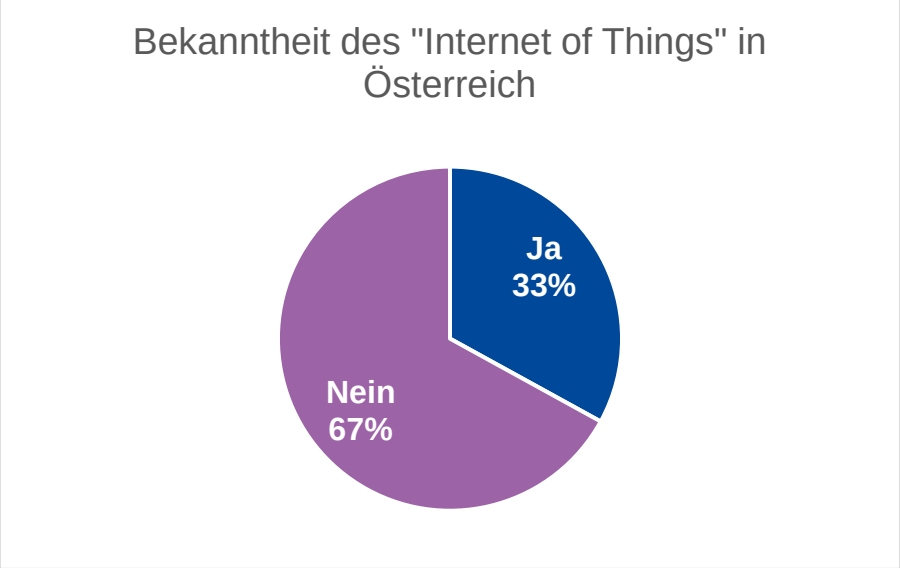


Abbildung 2: „Wissen Sie, was das „Internet of Things“, das „Internet der Dinge“ ist?“

Nach der Erklärung *„Als „Internet der Dinge“ wird die Vernetzung verschiedener Geräte im Internet bezeichnet. Diese Geräte sind smart, kommunizieren also miteinander und können selbständig Aufgaben für den*die Nutzer*in erledigen.“* **geben 36% des Samples an, derartige Geräte (Smartphones wurden dezidiert als nicht gemeinte Geräte erwähnt) zu nutzen, 56% verneinen dies und 8% enthalten sich der Antwort (siehe Abbildung 3).** Im Vergleich zu einer im Jahr 2017 durchgeführten Bevölkerungsbefragung des KFV ging diese Zahl zwar um 9 Prozent zurück (2017: 45%). Dies hat jedoch mit Sicherheit damit zu tun, dass in der 2017-Befragung das Smartphone als Teil des Internet of Things betrachtet wurde (Prinzellner & Pilgerstorfer, 2018, S. 15) .

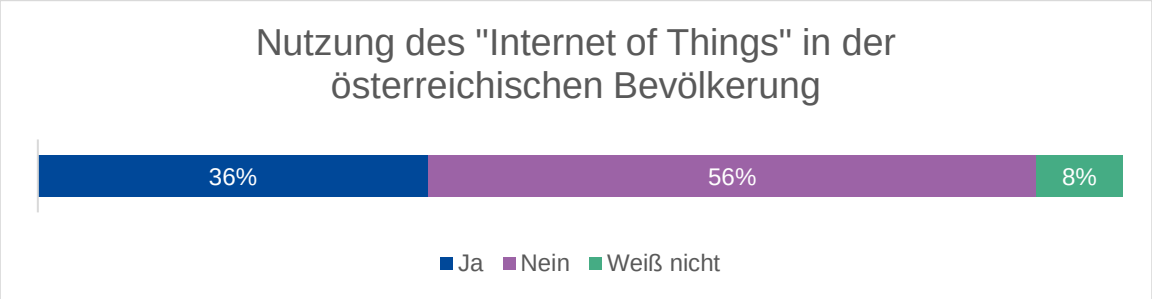


Abbildung 3: „Haben Sie selbst „smarte Internet of Things-Geräte“ zu Hause bzw. in privater Verwendung?“

Die Differenzen zwischen den Subgruppen (Geschlecht, Alter, Ortsgröße) sinken gegenüber der spontanen Abfrage merklich ab, wenngleich die Nutzung von IoT-Geräten bei Personen ab 50 Jahren und vor allem ab 60 Jahren markant abnimmt. Etwas mehr als die Hälfte jener Personen, die ungestützt angegeben haben, das „Internet der Dinge“ zu kennen, nutzen laut eigenen Angaben diese Technik auch.

Gründe für die Anschaffung gibt es viele, es überwiegt jedoch die Erleichterung des Alltags. Dies geben zwei Drittel der Befragten an (siehe Abbildung 4). Dies schätzt auch Georg Petzl von Magenta so ein. Angesprochen darauf, welche Art von Geräten im IoT-Bereich in Zukunft große Rollen spielen werden: „Alles, was in Richtung Automatisierung geht, also was den Menschen einfach Arbeit im Alltag abnimmt“. Er geht davon aus, dass speziell dieser Bereich weiterwachsen wird, da hier ein Markt-Nachholbedarf besteht – die Technologie gibt es schon lange und ist schon sehr viel weiter als das, was bisher auf dem Markt zu kaufen und auch für den*die Endnutzer*in praktisch ist.

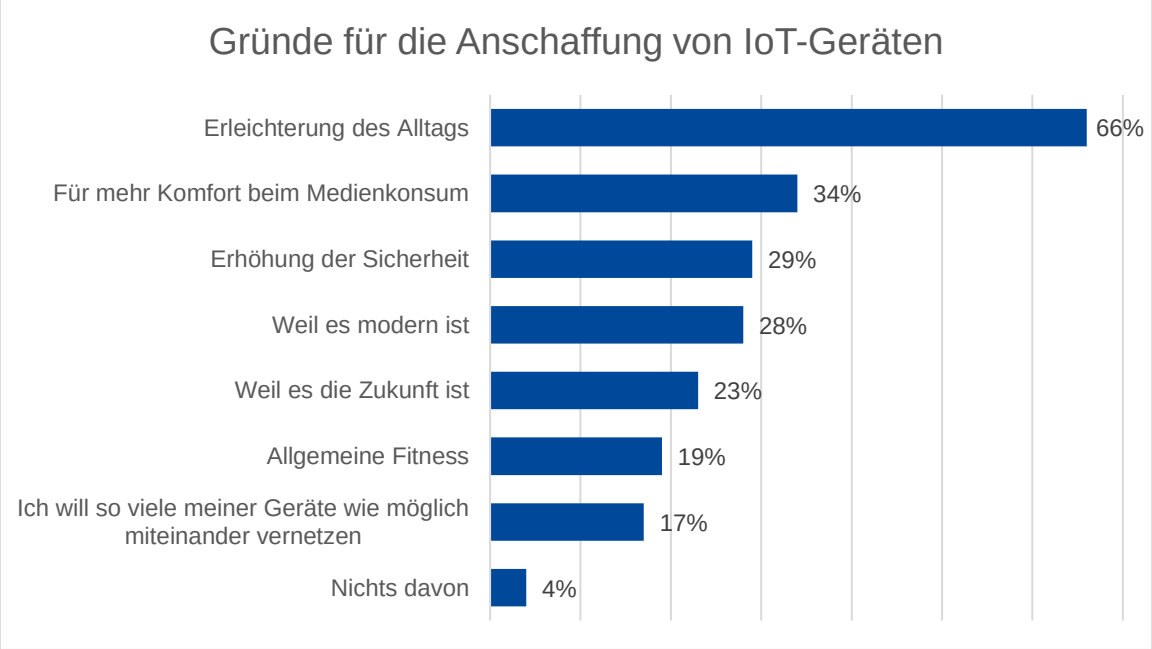


Abbildung 4: Gründe für die Anschaffung von IoT-Geräten

Wenig überraschend gestaltet sich die Verteilung der konkreten Nutzung von IoT-Geräten. **Die bei weitem gängigsten IoT-Geräte kann man dem Bereich smartes IT-Equipment zuordnen (92%, siehe Abbildung 5).** Hier ist das bei weitem am meisten genutzte Gerät der smarte Fernseher (70% der Nutzer*innen von smartem IT-Equipment besitzen ein solches Gerät). Weitere gern genutzte Geräte sind der digitale Assistent (Alexa, Google Dot), sowie Spielkonsolen.

Der zweite oft genannte Nutzungsbereich betrifft Haushaltshilfen (68% der Nutzer*innen von IoT-Geräten nutzen Devices dieser Kategorie). Hier dominiert der Staubsaugroboter, gefolgt von smarter Belichtung und smarter Kaffeemaschine.

Fast die Hälfte der Nutzer*innen besitzen Geräte aus dem Bereich Smarte Sicherheitssysteme. Das dominierende Device hier ist die smarte Überwachungskamera, andere Sicherheitsgeräte wie Türschlösser oder Babyphone werden nur wenig genutzt.

Smarte Geräte für den Garten sowie die Überwachung der eigenen Gesundheit sind noch sehr selten in österreichischen Haushalten zu finden: Nur jeweils etwa ein Drittel der User*innen hat solche Geräte zu Hause. Dabei sind smarte Selbstoptimierungstools (Smart Watches oder Fidbits usw.) noch am ehesten etabliert, in österreichischen Gärten ist hingegen der smarte Rasenmäher noch am ehesten zu finden.

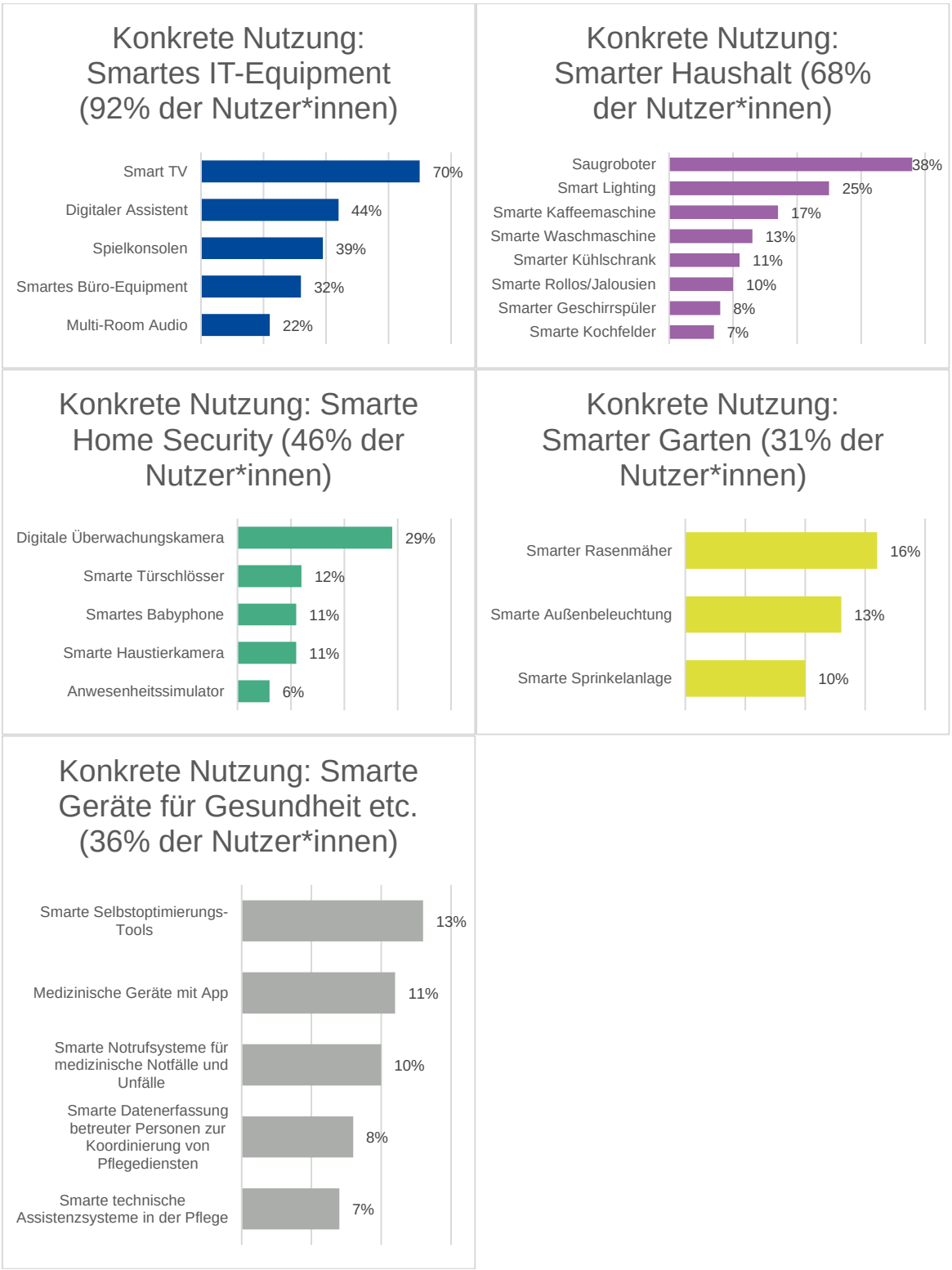


Abbildung 5: Konkrete Nutzung von IoT-Geräten in Österreich

Nach wie vor denkt knapp die Hälfte der Österreicher*innen nicht daran, sich (weitere) IoT-Geräte anzuschaffen (siehe Abbildung 6). Hier ist ganz klar zu erkennen, dass jene Menschen, die bereits IoT-Geräte in ihrem Alltag integriert haben, bei weitem motivierter sind, sich weitere Geräte anzuschaffen. Die Hürde, sich ein erstes smartes Gerät anzuschaffen scheint nach wie vor hoch zu sein. Darüber hinaus ist auch hier, wie bei fast allen Digitalisierungs-Themen, eine große Alters-Kluft zu erkennen: je jünger die Befragten, umso höher ist die Bereitschaft, sich (weitere) IoT-Geräte anzuschaffen. Ältere Personen sind hingegen weit zurückhaltender.

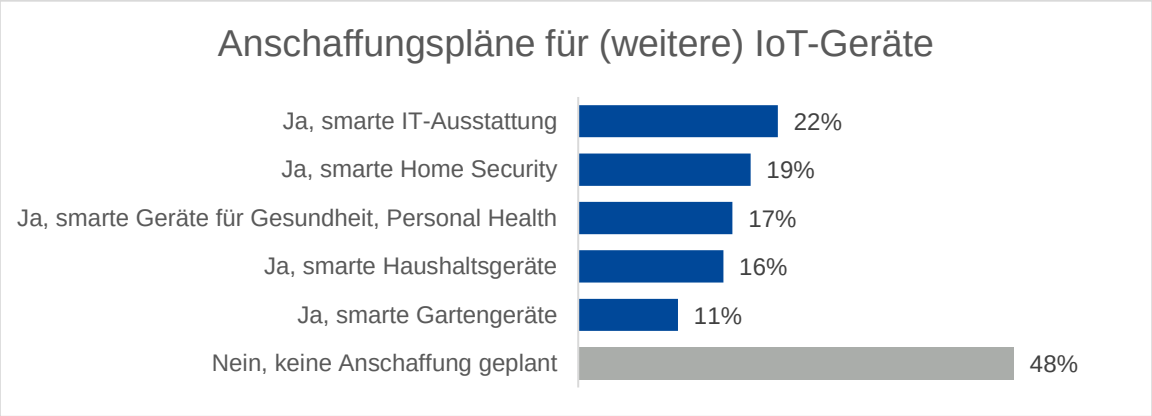


Abbildung 6: Anschaffungspläne (weiterer) IoT-Geräte

Gefragt nach der Einschätzung des Nutzens von IoT-Geräten zeigt sich ein gemischtes Bild: **Zwar sehen die meisten Befragten für fast alle Bereiche einen entweder „sehr großen“ oder „großen“ Nutzen (siehe Abbildung 7)**. Den größten Nutzen sehen die Befragten bei der Kindersicherheit sowie dem Einbruchsschutz. Die geringsten Werte erzielen IoT-Geräte mit dem Ziel der Unfallvermeidung (20% schreiben IoT-Geräten hier einen „geringen“ oder „gar keinen“ Nutzen zu). Darüber hinaus sind sich die Befragten auch unsicher, ob IoT-Geräte im Bereich Gesundheit und Fitness nützlich sein sollen. In dieser Kategorie sind 37% der Meinung, dass die Geräte nur „teils, teils“ helfen, weitere 17% gehen davon aus dass es „weniger“ oder „gar keinen“ Nutzen hat.

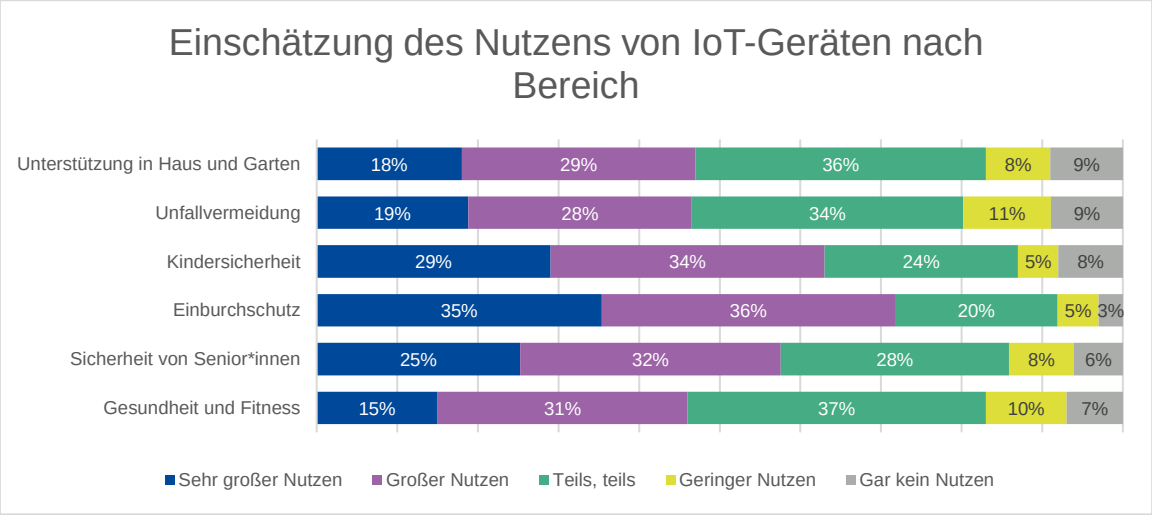
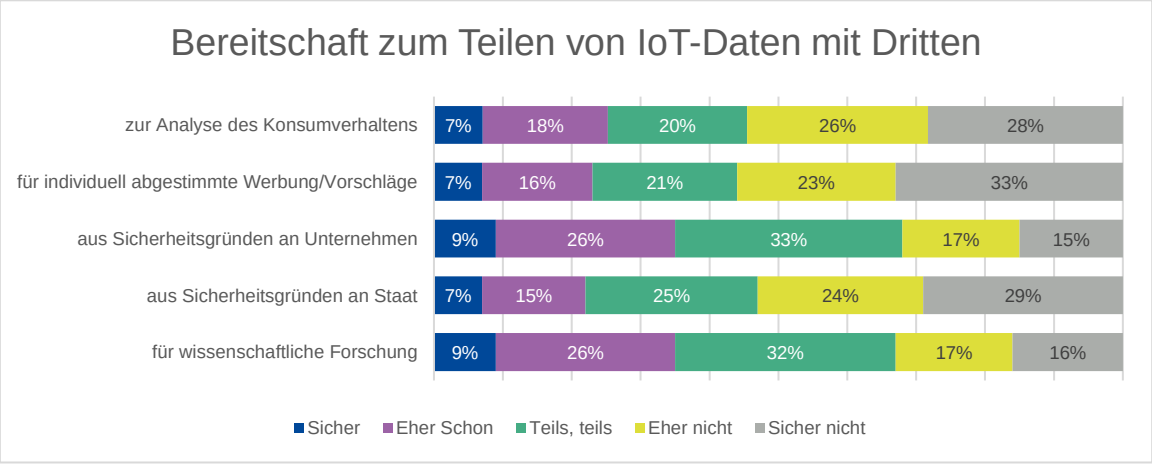


Abbildung 7: Einschätzung des Nutzens von IoT-Geräten nach Bereich

Bei der Frage, wem man seine*ihre durch die IoT-Geräte gesammelten Daten zur Verfügung stellen würde, ergeben sich interessante Präferenzen der Befragten: **35% der Befragten geben jeweils an, ihre Daten „sicher“ oder „eher schon“ mit Unternehmen aus Sicherheitsgründen oder zum Zweck der wissenschaftlichen Forschung teilen zu wollen**. Diese Bereitschaft zeigt auch eine prinzipiell gute Basis für das vom Experten Krieger-Lamina genannte wichtigste Potential von IoT-Geräten, nämlich die Sensordatenanalyse im großen Stil für die Wissenschaft.

Weit weniger gewillt sind die Befragten bei der Datenweitergabe an Wirtschaftsunternehmen zur Analyse des Konsumverhaltens oder zur Individualisierung von Werbung. Hier sprechen sich jeweils mehr als die Hälfte dagegen aus („eher nicht“ oder „sicher nicht“).

Auch dem Staat stehen die Befragten eher kritisch gegenüber, wenn es um das Teilen von Daten geht – im Gegensatz zur Frage, von wem man sich mehr Unterstützung bei der Sicherheit der Geräte wünscht, siehe Kapitel 6). Auch hier sprechen sich mehr als die Hälfte dagegen aus.



Die bei weitem gängigsten IoT-Geräte kann man dem Bereich smartes IT-Equipment zuordnen (92% der Nutzer*innen)

Die Befragten sehen bei IoT für fast alle (Lebens-)Bereiche einen entweder „sehr großen“ oder „großen“ Nutzen. Den größten sehen sie bei Kindersicherheit sowie Einbruchsschutz

35% der Befragten geben jeweils an, ihre Daten „sicher“ oder „eher schon“ mit Unternehmen aus Sicherheitsgründen oder zum Zweck der wissenschaftlichen Forschung teilen zu wollen. Die Bereitschaft zum Teilen von Daten mit Unternehmen oder dem Staat ist dagegen weit geringer.

6. Sicherheit und Risiko

6.1. Sicherheit in Österreichs Haushalten

Wie ist es um die Sicherheit der IoT-Geräte in Österreichs Privathaushalten bestellt, und welche Grundsätze sollten laut den Experten beachtet werden?

Die zwei augenscheinlichsten Risikobereiche sind, wie bei den meisten technologischen Geräten, die Passwortsicherheit und die herstellerseitige Update-Policy. Hier besteht laut Georg Petzl auch bereits das erste Grundproblem durch die schiere Masse an kostengünstigen IoT-Geräten: wenn diese nämlich massenhaft für wenig Geld in Umlauf gebracht werden, sei es mit der Lust des Herstellers an einer vernünftigen Update-Policy meist nicht weit her (Petzl, 2021). Dies wäre natürlich auch ein beidseitiges Problem, so Petzl. Denn solange die Kund*innen nicht bereit wären, für Qualität auch entsprechend zu bezahlen und solange diese Lücke rechtlich nicht geschlossen wird, so lange würden Hersteller*innen auch keine Notwendigkeit sehen, ihre Geräte regelmäßig und langfristig upzudaten.

Im Bereich der Passwortsicherheit sieht Petzl das Problem etwas komplexer. Hier sei vor allem das Problem, dass das von Hersteller*innen gewählte Passwort oft auch mit der Firmware verknüpft ist und dies zu Problemen in der Programmierung führen könne. Generell sieht er Passwörter als eher kleinen Hebel in der Erhöhung der Sicherheit von IoT-Geräten, da hier andere Themen wie geschützte Netzwerke wichtiger wären. **Die österreichischen Nutzer*innen von IoT-Geräten können in mehr als der Hälfte der Fälle bei allen Devices ein Passwort vergeben bzw. konnten das Herstellerpasswort ändern. Weitere 28% können dies zumindest bei manchen Geräten**, aber eine bedenklich hohe Zahl von zwölf Prozent weiß es schlicht nicht (siehe Abbildung 8).

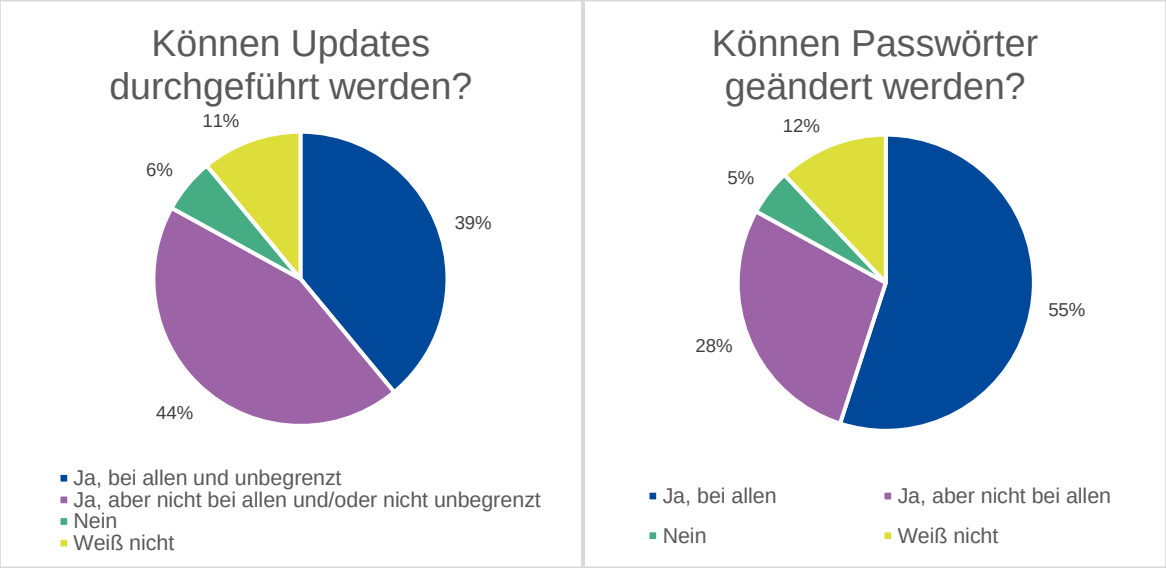


Abbildung 8: Updates und Passwörter bei IoT-Geräten

Die Situation sieht auch in Bezug auf Updates auf den ersten Blick besser aus als befürchtet. Immerhin 39% der befragten Nutzer*innen geben an, dass auf all ihren Geräten die Möglichkeit besteht, unbegrenzt Sicherheitsupdates zu erhalten. 44% geben an, dass dies entweder nur bei manchen, oder nicht zeitlich unbegrenzt der Fall ist. Auch hier stechen die elf Prozent Unwissenden negativ ins Auge.

Ein Blick auf die Maßnahmen, die getroffen werden, um die eigenen IoT-Geräte vor fremdem Zugriff zu schützen ist ebenso aufschlussreich: **So geben immerhin fast zwei Drittel an, auf allen Geräten sichere Passwörter zu verwenden. Weniger gut ist die Update-Disziplin der Nutzer*innen: nicht einmal die Hälfte der befragten Österreicher*innen führt diese regelmäßig durch.** Dieses mangelnde Bewusstsein spiegelt sich auch in anderen Studien des KFV zu anderen Cybersicherheitsthemen wider. Updates sind immer noch für eine zu große Zahl der Österreicher*innen kein zentraler Punkt in ihrer Cybersicherheitsplanung. Ein weiteres Drittel verwendet schlicht die Einstellungen des*der Hersteller*in oder Händler*in.

Nur 22 Prozent der Befragten geben an, ein separates Netzwerk zu verwenden, in dem ihre IoT-Geräte miteinander kommunizieren, eine Maßnahme, die von beiden interviewten Experten als wichtiger Schritt zu mehr Sicherheit gesehen wird. Alle weiteren Maßnahmen, die vor allem von Cyber-Expert*innen genannt werden, werden nur von einer kleinen Minderheit der Nutzer*innen angewendet.

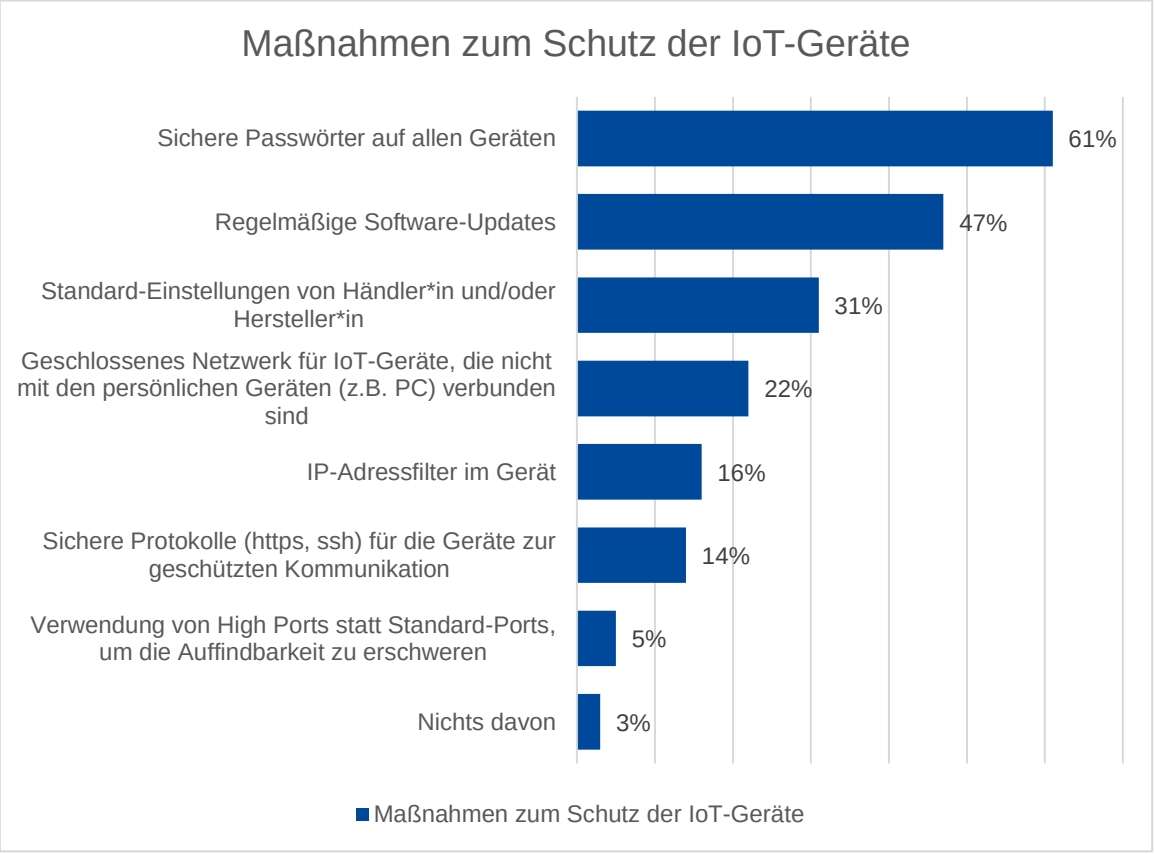


Abbildung 9: Ergriffene Maßnahmen zum Schutz von IoT-Geräten

Bei den Maßnahmen, die den Nutzer*innen von Hersteller*in oder Verkäufer*in genannt wurden ist ebenfalls deutliches Verbesserungspotential zu erkennen: **So hat fast jede*r fünfte Hersteller*in oder Verkäufer*in keinerlei Sicherheitsmaßnahmen genannt** (siehe Abbildung 10). Auch bei Updates und Passwörtern waren Hersteller*innen/Händler*innen zurückhaltend: lediglich knapp über die Hälfte empfahlen regelmäßige Softwareupdates, weniger als die Hälfte schlugen die Änderung des Ursprungspassworts vor.

Hier sieht man auch eine der großen Gefahren der Digitalisierung: Wenn nicht in der gesamten Produktions- und Verkaufskette auf Cybersicherheit Wert gelegt wird und dementsprechend auch Personal geschult wird, wird der*die Endnutzer*in mit einem Gerät ausgestattet, von dem er*sie nicht weiß, wie es adäquat zu schützen ist. Damit macht man es Kriminellen noch einfacher, diese Geräte für ihre illegalen Tätigkeiten zu nutzen. Ein wichtiger Aspekt hierbei ist die Schulung des Personals sowohl im Verkauf als auch in der Installation dieser Geräte, damit diese den Käufer*innen ein gutes Basisinformationspaket für ihren Schutz mitgeben können (siehe hierzu auch Kapitel 8).

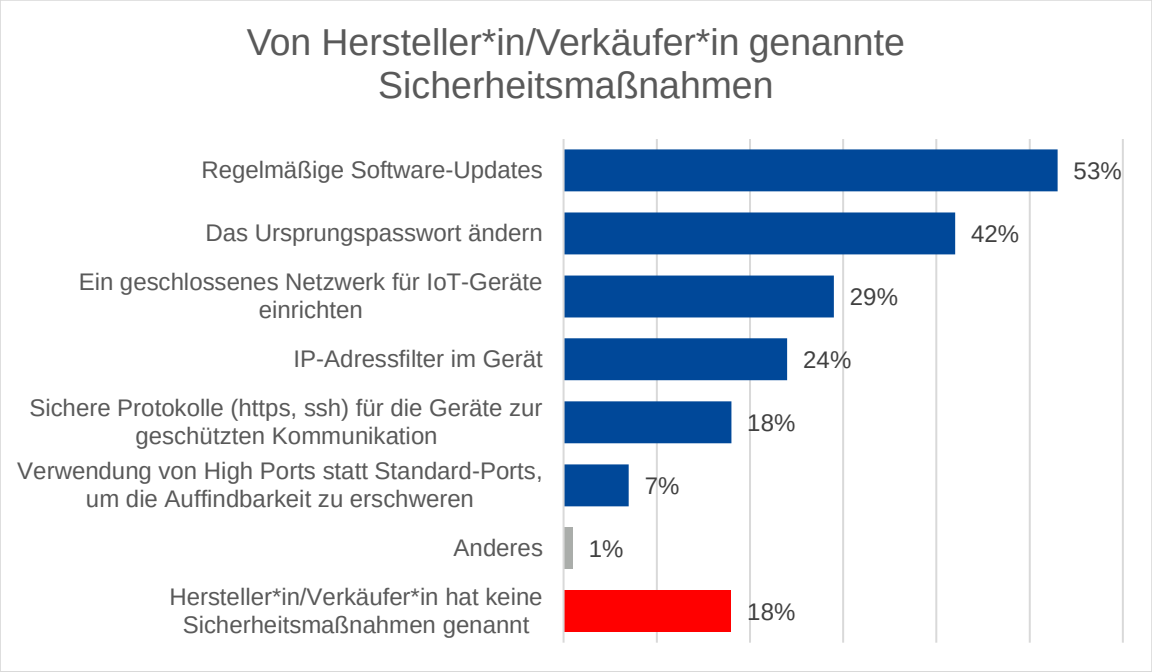


Abbildung 10: Von Hersteller*in oder Verkäufer*in genannte Sicherheitsmaßnahmen

Umso verwunderlicher ist die Antwort der Österreicher*innen auf die Frage, ob sie mit den erhaltenen Informationen zufrieden waren: über zwei Drittel gaben an, dass dies der Fall war (siehe Abbildung 11). Hier herrscht also augenscheinlich eine große Diskrepanz zwischen dem, was aus Cybersicherheitsperspektive notwendig wäre und dem, was die Nutzer*innen sich von den entsprechenden Expert*innen erwarten.

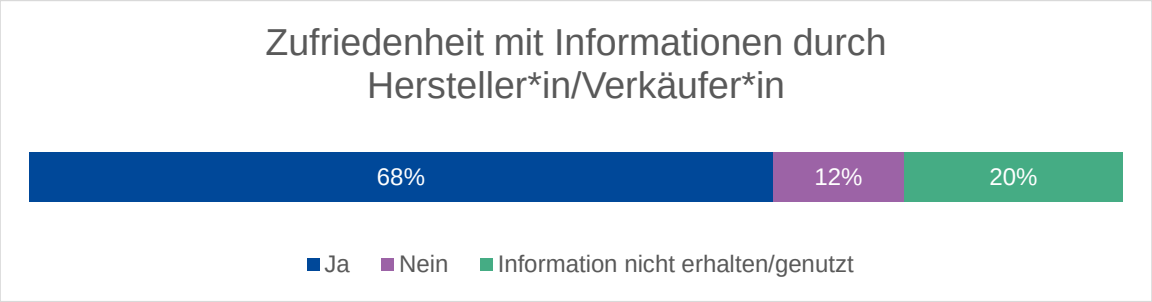


Abbildung 11: Zufriedenheit mit Information durch Hersteller*in/Händler*in

Der Wunsch nach mehr Unterstützung ist trotzdem hörbar. Jeweils etwa die Hälfte der Befragten wünscht sich mehr Unterstützung durch den Staat oder Hersteller*innen/Verkäufer*innen. **Interessant hierbei ist die Tatsache, dass diese Zahl bei jenen, die bereits einen illegalen Zugriffsversuch erlebt haben, sprunghaft auf jeweils circa zwei Drittel ansteigt**. Man sieht hier eindeutig, dass der Wunsch nach Unterstützung zunimmt, wenn man mit den Risiken der Digitalisierung konfrontiert ist, während zuvor eine gewisse laissez-faire Attitüde vorzuherrschen scheint.

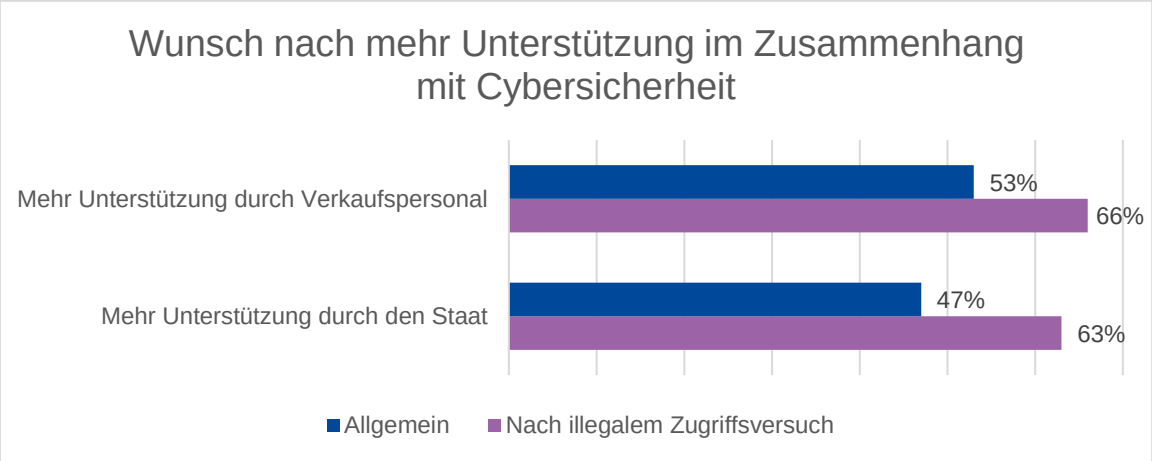


Abbildung 12: Wunsch nach mehr Unterstützung in Zusammenhang mit Cybersicherheit

6.2. Illegale Zugriffsversuche und verursachter Schaden

17 Prozent der Nutzer*innen von IoT-Geräten gaben an, bereits einen illegalen Zugriffsversuch erlebt zu haben (n=62). Dies ist zwar auf den ersten Blick keine große Zahl, jedoch muss man hier auch mitbedenken, dass dies nur diejenigen sind die einen solchen Zugriffsversuch auch bemerkt haben.

Von denjenigen, die einen illegalen Zugriffs(-versuch) erlebt haben, erlitten 55 Prozent glücklicherweise keinen Schaden. Jedoch führte der illegale Zugriff bei immerhin einem Viertel der Betroffenen zu finanziellem Schaden (n=14), und fünf Prozent hatten gestohlene Daten zu beklagen (siehe Abbildung 13).

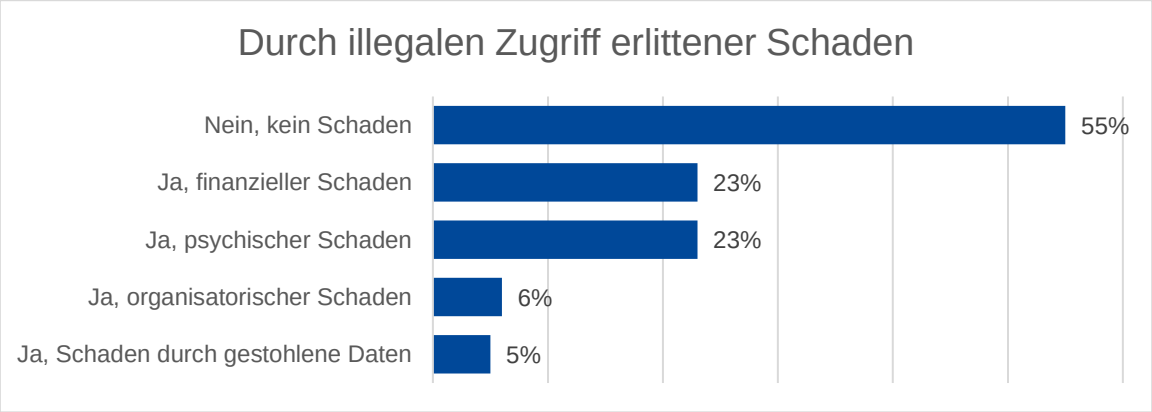


Abbildung 13: Durch illegalen Zugriff erlittener Schaden

Die 14 Personen, die einen finanziellen Schaden erlitten haben, hatten sehr unterschiedliche Schadenssummen zu beklagen: Jeweils vier Personen erlitten einen Schaden von 500-999 bzw. von 1.000-10.000 Euro. Jeweils drei Personen hatten Schäden von weniger als 100 oder bis zu 500 Euro angegeben (siehe Abbildung 14).

Lediglich ein Drittel der von einem illegalen Zugriffsversuch betroffenen Personen hat diesen bei der Polizei angezeigt. Diese enorm niedrige Zahl ist aber auch in Zusammenhang mit anderen Cyberkriminalitätsdelikten zu beobachten. Hier zeigt sich eine Tendenz, die das KFV bereits seit Jahren mit Sorge beobachtet: (Versuchte) Delikte im digitalen Raum werden von den Opfern fahrlässiger gehandhabt als Delikte im „analogen“ Raum. Gründe dafür sind zum einen, dass die Sinnhaftigkeit einer Anzeige allgemein angezweifelt wird, da man nicht davon ausgeht, dass die Täter*innen gefasst werden. Zum anderen liegt es auch daran, dass die Menschen einen nicht erfolgreichen Zugriffsversuch, oder einen erfolgreichen ohne Schaden, nicht als anzeigungswürdig ansehen. Doch fast jede*r würde es zum Beispiel zur Anzeige bringen, wenn an der eigenen Wohnungstüre eindeutige Einbruchsspuren sichtbar sind, auch wenn das Schloss gehalten hat. Diese Fahrlässigkeit in der Anzeigemoral führt auch dazu, dass die Polizei große Schwierigkeiten hat, Kriminalitätstrends festzustellen und entsprechend zu reagieren.

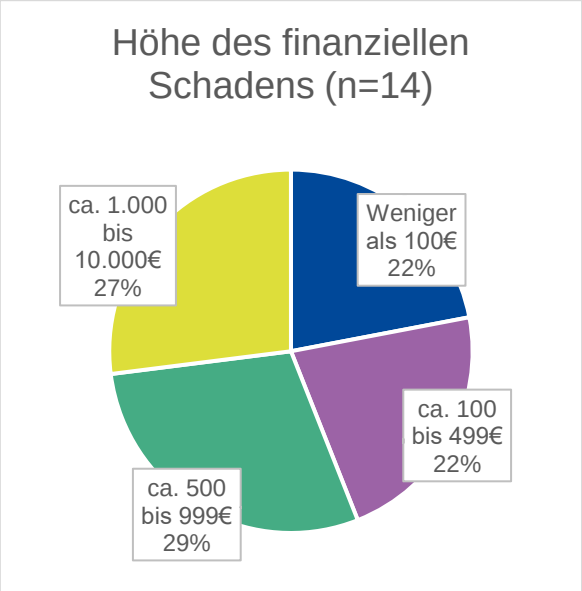


Abbildung 14: Höhe des finanziellen Schadens durch unerlaubten Zugriff auf IoT-Geräte

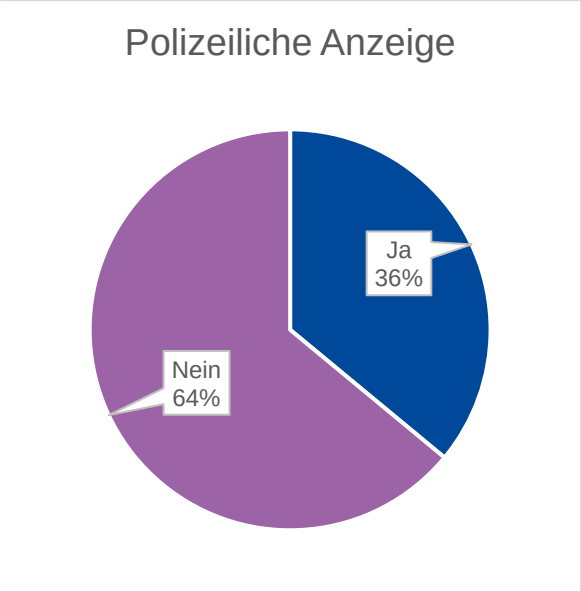


Abbildung 15: Wurde nach unerlaubtem Zugriff auf IoT-Geräte polizeiliche Anzeige erstattet?

Insgesamt ist zu sagen, dass die Zahl derer, die bereits einen unerlaubten Zugriffsversuch erlebt haben, geschweige denn Schaden genommen haben, verschwindend gering ist. Dies wird sich jedoch mit der weiteren Verbreitung von IoT-Geräten in Österreich radikal verändern. Cyberkriminelle suchen für ihre Zwecke immer den Weg des geringsten Widerstandes, es sei denn, sie wollen eine spezifische Person oder Institution mit einem spezifischen Zweck attackieren. **Wenn mit der wachsenden Zahl von IoT-Geräten nicht auch das Sicherheitsbewusstsein der Nutzer*innen massiv anwächst, dann wird es für Cyberkriminelle sehr viele kaum geschützte Wege in die Wohnungen, Häuser, Eigentum und private Daten der Österreicher*innen geben.**

Fast zwei Drittel der österreichischen IoT-Nutzer*innnen geben an, auf allen Geräten sichere Passwörter zu verwenden. Weniger gut ist die Update-Disziplin der Nutzer*innen: nicht einmal die Hälfte der befragten Österreicher*innen führt diese regelmäßig durch.

Jede*r fünfte Verkäufer*in hat beim Verkaufsgespräch keine Sicherheitsmaßnahmen genannt. Jeweils etwa die Hälfte der Befragten wünscht sich mehr Unterstützung durch den Staat oder Hersteller*innen/Verkäufer*innen.

17 Prozent der Nutzer*innen von IoT-Geräten gaben an, bereits einen illegalen Zugriffsversuch erlebt zu haben. 55 Prozent der Betroffenen erlitten keinen Schaden. Bei immerhin einem Viertel der Betroffenen kam es zu finanziellem Schaden (n=14), und fünf Prozent hatten gestohlene Daten zu beklagen

7. Rechtliche (Heraus-)Forderungen

7.1. Haftungsfragen: Überblick

Im Internet der Dinge (d.h. bei „vernetzten Waren“, „Smart Homes“)[3] sorgen häufig mehrere Anbieter*innen ineinandergreifend für Hardware, Software, Software-Wartung und digitale Infrastruktur oder die Verarbeitung und Nutzung der Daten.

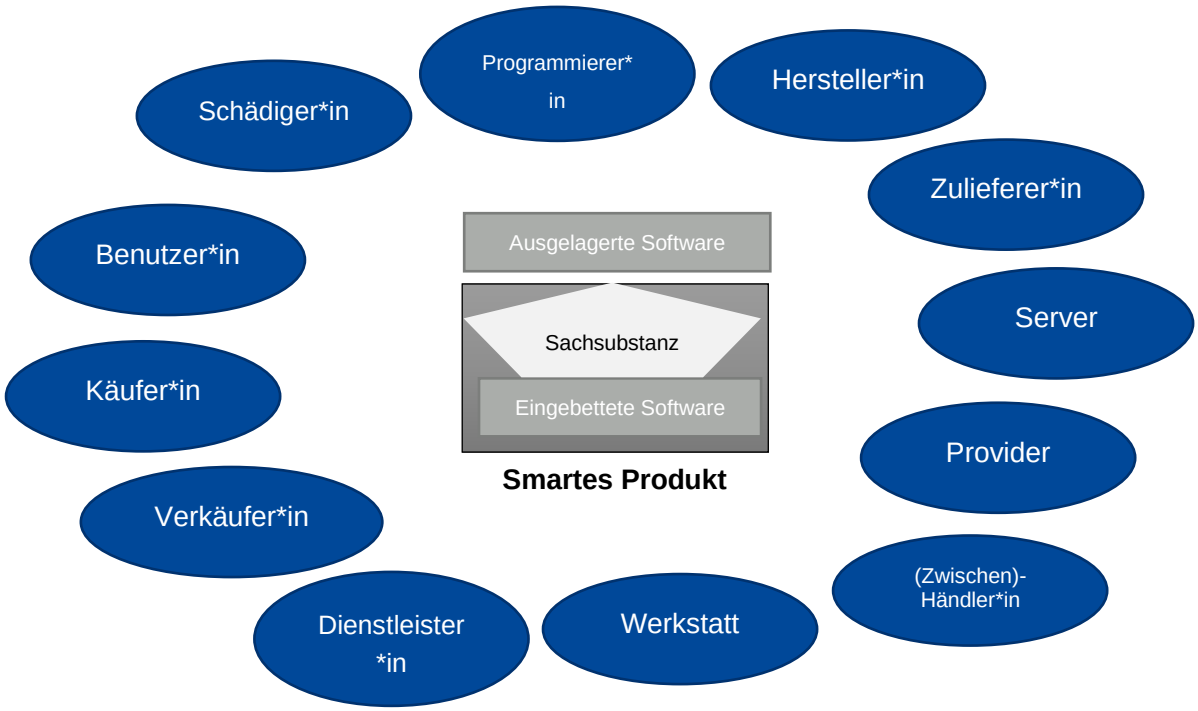


Abbildung 16: Geflecht (beispielhaft) der Akteur*innen rund um ein IoT-Produkt

Der Erwerber*innen eines IoT-Produkts schließt somit häufig neben dem Kaufvertrag über die Hardware zahlreiche weitere Verträge bzw. Nutzungsvereinbarungen mit verschiedenen Anbieter*innen digitaler Inhalte ab. Dieses System stellt die bisherigen Regeln über die **vertragliche und außervertragliche Haftung** vor neue Herausforderungen. Ein klarer Sicherheits- und Haftungsrahmen ist jedoch wichtig, um sowohl Verbraucher*innenschutz als auch Rechtssicherheit für Unternehmen zu gewährleisten.

Eine pauschale Haftungsregelung gibt es nicht; es ist zwischen folgenden Bereichen zu differenzieren:

- **Gewährleistungsrechtliche Ansprüche,** i.d.R. gegen den*die Verkäufer*in/Dienstleister*in (bei reinem Nichtfunktionieren des Produkts, Fragen der

[3] In der Regel geht es um Konsumgüter mit eingebetteter oder ausgelagerter Software, welche die Produkte unmittelbar (eigene IP-Adresse) oder mittelbar (z.B. Bluetooth) mit dem Internet verbindet und welche über das Netzwerk identifiziert und gesteuert werden können. Dabei werden Daten verarbeitet und ausgetauscht. Ware und digitale Inhalte wirken also funktionell zusammen und ergeben erst in ihrer Kombination ein für den Erwerber funktionsfähiges Produkt.

Mängelhaftung oder Einräumung von Garantien, beispielsweise Nachbesserung oder Ersatz bei Mängeln oder Nichterfüllung zugesicherter Eigenschaften);
- **Deliktische Schadenersatzansprüche** gegen Dritte (z.B. Händler*in, Hersteller*in, Ingenieur*in, Programmierer*in, etwaige Schädiger*in – sofern diese ausgeforscht werden können) gemäß nationalem (österr.) Deliktsrecht.
- **Produktsicherheits- und haftungsrechtliche Ansprüche** gegen den*die Hersteller*in (Schutz insbesondere von Personen und Gütern sowie Haftung beispielsweise bei Personen- oder Sachschäden) durch das Produkthaftungsgesetz (vollharmonisiert durch die EU-Produkthaftungsrichtlinie);

Tabelle 2:Überblick Haftungsfragen IoT

	Gewährleistung	Schadenersatz	Produkthaftung
Umfang	Haftung für die Sache selbst, nicht für Folgeschäden: Sach- und Rechtsmängel, die zum Übergabe- bzw. Lieferzeitpunkt schon vorhanden sind	Haftung für Schaden an der Sache selbst als auch für Folgeschäden	nur für nur Folgeschäden, nie für fehlerhafte Sache selbst. (Als Produkte gelten nur bewegliche, körperliche Sachen sowie Energie; der Fehler muss bereits im Zeitpunkt des Inverkehrbringens des Produkts vorliegen.)
Verschulden	**verschuldensunabhängige** Haftung des*der **Verkäufer*in**	**Verschulden** (mind. leicht fahrlässig)	**verschuldensunabhängige** Haftung des*der **Hersteller*in**
Dauer der Haftung	Frist bei beweglichen Sachen 2 Jahre	Verjährung nach 3 Jahren ab Kenntnis von Schaden sowie Schädiger*in bzw. 30 Jahren	Verjährung 3 Jahre ab Kenntnis von Schaden sowie Schädiger*in bzw. jedenfalls 10 Jahre nach dem Inverkehrbringen

7.2. Gewährleistung

Rechtsquellen, insb.:

EU-Richtlinien, die die Gewährleistung fit für den digitalen Binnenmarkt machen sollen, sind
- **Warenkauf-RL** (WKRL) 2019/771/EU über bestimmte Aspekte des Warenkaufs
- **Digitale Inhalte-RL** (DIRL) 2019/770/EU über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen

Die österreichische Umsetzung (mit erstmals dezidierter Aufnahme von digitalen Leistungen und Waren mit digitalen Inhalten in das Gewährleistungsrecht) ist durch das **Gewährleistungsrichtlinien-Umsetzungsgesetz**[4] vorgesehen.

[4] Vom Nationalrat im Juli 2021 beschlossen, aber derzeit (Stand August 2021) noch nicht im BGBl veröffentlicht

Inhalte der beiden EU-RL:

- Kombination aus einem **sehr weiten Begriff der „Waren mit digitalen Elementen".**
- **Fokussierung auf den Inhalt des Vertrags** zur Entscheidung darüber, wofür der*die Verkäufer*in gewährleistungsrechtlich verantwortlich sein soll (also Ware oder Dienstleistung) und gleichzeitig damit auch zur Abgrenzung der beiden RL.
- Für Kaufverträge nach der WKRL und für Verträge über die einmalige Bereitstellung digitaler Inhalte oder Dienstleistungen nach der DIRL gilt eine **Gewährleistungsfrist von zwei Jahren** ab Übergabe bzw. ab Bereitstellung. Bei der **fortlaufenden Bereitstellung** digitaler Inhalte und Dienstleistungen besteht die Gewährleistungspflicht nach der DIRL **für die gesamte Vertragslaufzeit**. Für digitale Elemente einer Ware nach der WKRL gilt dies nur, wenn die Vertragslaufzeit länger als zwei Jahre ist; bei einer kürzeren Vertragslaufzeit gilt dagegen die zweijährige Gewährleistungsfrist.
- Verkäuferhaftung (Händler*in) – keine Herstellerhaftung.
- Eine weitere entscheidende Neuerung besteht in der **Verlängerung der Dauer der Beweislastumkehr**. Während der*die Verbraucher*in ursprünglich sechs Monate lang nicht beweisen musste, dass die Vertragswidrigkeit schon bei Lieferung der Ware vorhanden war, gilt diese Vermutung nach den beiden neuen RL ein Jahr lang.
- Update/(Aktualisierungs)-Verpflichtung: Die **Dauer der Verpflichtung zu Information und Bereitstellung von Updates** richtet sich bei kontinuierlicher Bereitstellung nach der Vertragslaufzeit und bei einmaliger Bereitstellung danach, was der*die Verbraucher*in vernünftigerweise erwarten kann, wobei Art und Zweck der Waren sowie die Umstände und die Art des Vertrags zu berücksichtigen sind. Keine Haftung des*der Verkäufer*in, wenn der*die Verbraucher*in die Installation von Aktualisierungen binnen eines bestimmten Zeitraums unterlässt und dadurch Vertragswidrigkeiten entstehen.
- Keine Abweichung der Regeln zum Nachteil des Verbrauchers möglich.

Österreich: ABGB (§§ 922 ff), Konsument*innenenschutzgesetz (KSchG), Gewährleistungsrichtlinien-Umsetzungsgesetz (s.o.)

7.3. Produkthaftung

Hersteller*innen von IoT-Produkten haben bis dato die allgemeinen Produkthaftungs- und Produktsicherheitsvorschriften zu beachten.

Rechtsquellen, insb.:

- **Produkthaftungsrichtlinie** 85/374/EWG zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte
- **Produktsicherheitsrichtlinie** 2001/95/EG
- **Cybersecurity Act**, Verordnung (EU) 881/2019: schafft einen EU-Rahmens für die IT-Sicherheitszertifizierung von Produkten, Dienstleistungen und Prozessen
- **Normen und Standards**, z.B. IT-Sicherheitsstandards; europäische Standard ETSI EN 303 6458 für die Sicherheit von IoT-Verbraucherprodukten, Guidelines for Securing the Internet of Things" der Agentur der Europäischen Union für Cybersicherheit (ENISA) v. November 2020[5]

[5] https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things/at_download/fullReport

- Österr. **Produkthaftungsgesetz**
- Österr. **Produktsicherheitsgesetz**

Regelungen:
Die Produkthaftung umfasst Personen- und Sachschäden, die durch Fehler verursacht werden, welche ein in Verkehr gebrachtes Produkt aufweist. Zwischen dem*der Erzeuger*in eines Produktes und der geschädigten Person muss keine vertragliche Bindung bestehen. Auch außenstehende Dritte – und nicht nur der*die Käufer*in des Produktes – können Ansprüche stellen.
Nach dem Produkthaftungsgesetz kann Schadenersatz dann geltend gemacht werden, wenn

- das Produkt fehlerhaft ist,
- ein Schaden entstanden ist und
- nachweislich ein ursächlicher (kausaler) Zusammenhang zwischen Fehler und entstandenem Schaden besteht.

Die **verschuldensunabhängige Haftung** führt dazu, dass ein*e Geschädigte*r allein das Vorliegen eines Produktfehlers, eines Schadens sowie des kausalen Zusammenhangs zwischen Produktfehler und Schaden nachzuweisen hat.

Weiters:
Die Pflichten der Hersteller*innen (vgl. z.B. ETSI EN 303 6458 und Cyber Security Act), sind nach dem Grundsatz der Verhältnismäßigkeit im Einzelfall zu bestimmen, bzw. ergeben sich dadurch Möglichkeiten für den*die Hersteller*in, die Haftung zu reduzieren:

- Beachtung cyberspezifische Sicherheitsanforderungen bei der Konstruktion und Fabrikation sowie Instruktions- und Informationspflichten (Nutzung von Konzepten wie „**Security by Design**“ und „**Security-by-Default**“)
- Einhaltung cyberspezifischer Produktbeobachtungspflichten („Monitoring“, Reporting)
  - Integrierte Produktbeobachtung
  - Bereitstellung von Software-**Updates**
  - Beobachtung von Kombinationsgefahren
- Einrichtung eines Informationssicherheits-Management-Systems
- Warnung vor IT-Sicherheitslücken

Probleme, bspw.:

- Produktanforderungen, etwaige Updateverpflichtungen: Die Produkthaftungs-Richtlinie stammt aus der vor-digitalen Zeit und regelt die Haftung für digitale Anwendungen nicht ausdrücklich. Auch gerichtlich wurden wesentliche Fragen bislang nicht geklärt. Bereits beim **Produktbegriff** stellt sich daher die Frage, ob und welche vernetzten Produkte überhaupt erfasst sind: z.B. Software oder sonstige Online-Komponenten.
- **Zurechnung der Haftung zu einer bestimmten Person**: Das menschliche Fehlverhalten spielt bei der Haftung nach dem österr. Deliktsrecht vom Wortlaut her eine größere Rolle als im Rahmen des europäisch harmonisierten Produkthaftungsrechts. Es bleibt abzuwarten, ob es im Zusammenhang mit IoT Anwendungen Fälle geben wird, bei denen zwar ein Produktfehler ausgemacht werden kann, dieser aber gerade nicht auf die Verletzung einer menschlichen Verkehrssicherungspflicht zurückgeführt werden kann – und zwar nicht mangels Verschuldens, sondern schlicht mangels einer menschlichen Handlung.
- **Nachweis der Kausalität** der Schädigungshandlung für den eingetretenen Schaden wird derzeit als Belastung für die Verbraucher*innen angesehen (Frage der Beweisbarkeit).

7.4. ETSI Standard EN 303 645

Der*die Besitzer*in eines zertifizierten Kühlschrankes kann sich darauf verlassen, dass keine Stromschlag-Gefahr von dem Produkt ausgeht, solange das Gerät bestimmungsgemäß und vorhersehbar verwendet wird. Ist dieser Kühlschrank jedoch „smart“ oder vernetzt, kann dieser gleichzeitig Teil eines riesigen Botnetzes sein, oder seine Software kann seit Jahren nicht mehr auf dem neuesten Stand der IT-Sicherheit sein, ohne dass es die Zertifizierung tangieren würde.

Das Europäisches Institut für Telekommunikationsnormen (ETSI) hat daher einen Standard entwickelt, der dazu beitragen soll, sinnvolle europäische Zertifikate für IoT-Geräte zu entwickelnd. Grundlage für die Vergabe von Sicherheitszertifikaten durch akkreditierte Zertifizierungsstellen bildet der im Juni 2020 verabschiedete Standard “ETSI EN 303 645, Cyber Security for Consumer Internet of Things: Baseline Requirements”[6]. Dieser Standard ist zwar nicht rechtlich bindend, doch er zeigt exemplarisch auf, was nötig wäre, um Europas IoT-Universum sicherer zu gestalten.

Die wichtigsten Anforderungen werden im Folgenden vorgestellt, zusammengefasst vom deutschen IT-Sicherheitsexperten Dr. Lothar Burger (Burger, 2021):

1. Keine universellen Standardpasswörter
Die Anforderungen in dieser Gruppe beschäftigen sich mit der in der Vergangenheit immer wieder beobachteten Problematik, dass Geräte mit der Standardeinstellung des Herstellers und bekannten Passwörtern in Betrieb genommen wurden.

2. Meldeprozesse für Sicherheitslücken und aktives Sicherheitsmonitoring
Es wird vom Gerätehersteller gefordert, dass er einen Prozess implementiert, über den Sicherheitslücken gemeldet werden können, und der zudem sicherstellt, dass Lösungen im angemessenen Zeitrahmen (90 Tage) entwickelt werden. Der Gerätehersteller ist zudem aufgefordert, selbst aktives Sicherheitsmonitoring zu betreiben, indem er z.B. Meldungen über Sicherheitslücken in Software-Komponenten, die in seinem Gerät verwendet werden, verfolgt.

3. Software-Updates
Die Software-Komponenten eines Geräts müssen updatefähig sein. Die Update-Mechanismen müssen zudem sicher sein, um zu verhindern, dass Schadsoftware per Software-Update auf ein Gerät gelangen kann.

4. Sichere Speicherung von kritischen Sicherheitsparametern
Kritische Sicherheitsparameter, wie z.B. Geräteidentitäten oder geheime Schlüssel müssen sicher gegen Ausleseversuche oder Manipulation im Gerät gespeichert werden. Lösungsansätze sind unter dem Oberbegriff “HW based Root of Trust” bekannt und verwenden HW-Elemente wie z.B. Secure Elements, TPM, TEE, etc.

5. Sichere Kommunikation
Geräte müssen verschlüsselt kommunizieren unter Verwendung von kryptographischen Verfahren, die als „Best Practice“ gelten.

6. Minimierung von Angriffsflächen
Ein Gerät muss möglichst wenig Angriffsfläche bieten, z.B. durch physikalisches Entfernen oder logisches Deaktivieren von Schnittstellen, die nur während der Geräteentwicklung benötigt wurden (Debug-Ports, Netzwerkschnittstellen, etc.).

7. Integrität der Software
Ein IoT-Gerät muss sich gegen Schadsoftware schützen, indem es die Integrität seiner Software prüft. Ein bekannter Schutzmechanismus ist z.B. “Secure Boot” im Zusammenspiel mit “Hardware based Root of Trust”.

[6] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

8. Sicherheit von personenbezogenen Daten
Personenbezogene Daten sind besonders schutzbedürftig. Solche Daten dürfen nur verschlüsselt übertragen werden. Die Fähigkeit eines Geräts, solche Daten zu erfassen, z.B. durch eingebaute Kameras oder Mikrofone, muss dokumentiert und für den Benutzer erkennbar sein.

9. Resilienz gegen Ausfälle
IoT-Geräte müssen damit umgehen können, dass Strom oder Netzwerke ausfallen. Zum Beispiel indem sie bei einem Netzwerkausfall ihre lokale Funktion aufrecht erhalten oder nach einem Stromausfall selbstständig in einen fehlerfreien Betriebszustand zurückkehren.

10. Überwachung von Telemetriedaten
Wenn ein Gerät Telemetriedaten erfasst (Sensor-Messwerte, Nutzungsdaten oder sonstige Logdaten), dann sollen solche Daten auch zum Erkennen von Anomalien verwendet werden. Anomalien können aus Cyber-Angriffen oder auch aus fehlgeschlagenen Wartungsaktionen (z.B. fehlerhafte Software-Updates) resultieren.

11. Einfache Löschung von Benutzerdaten
Ein Gerät muss einfach handhabbare Mechanismen zur Verfügung stellen, mit denen Benutzerdaten (Konfigurationsdaten, Passwörter, etc.) gelöscht werden können. Der Bedarf, solche Daten zu löschen, entsteht z.B. beim Beenden eines Mietvorgangs, beim Verkauf oder bei der Entsorgung von Geräten.

12. Einfache Installation und Wartung
Verfahren zur Installation und Wartung von Geräten müssen möglichst einfach gestaltet sein, z.B. in Form von Installationswizzards oder automatischen Prüfverfahren, mit denen die Sicherheit der Gerätekonfiguration überprüft werden kann.

13. Validierung von Eingabedaten
Sämtliche Eingabedaten, die ein Gerät über Benutzerschnittstellen, APIs oder Netzwerkprotokolle erreichen, müssen validiert werden.

14. Datenschutz
Der Gerätehersteller muss seine Kunden darüber informieren, welche personenbezogenen Daten von einem Gerät erfasst, gespeichert oder übertragen werden. Der Kunde muss die Verwendung dieser Daten explizit gestatten (durch Opt-in) und er muss dies auch jederzeit widerrufen können. Für personenbezogene Telemetriedaten gilt das Minimalitätsprinzip.

7.5. Stand der Überlegungen:

Seit einigen Jahren ist eine umfangreiche und langfristige Weiterentwicklung entsprechender Rechtsgrundlagen und Normungsaktivitäten zu beobachten. Derzeit findet ein umfangreicher Diskussions- und Findungsprozess zu IoT-Haftungsfragen sowie der Verknüpfung von Produkt- und IT-Sicherheit in Gesetzgebung und Normung statt. Auch die Rechtsprechung in Zusammenhang mit der Sicherheit von IoT-Produkten dürfte sich in den kommenden Jahren weiterentwickeln.

Die EU-Kommission hat Anfang 2020 mit ihrem Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik[7] im Hinblick auf Sicherheit und Haftung einen Revisionsprozess der Produktsicherheits- und Produkthaftungsvorschriften angestoßen.

7.6. Juristische Forderungen

- **Klarere Definition von Begriffen: z.B. Überarbeitung des Begriffs des „Inverkehrbringens“ – auch um abzuklären, wer für Änderungen an einem Produkt haftbar ist.**
- **Weitere Präzisierung des Anwendungsbereichs des „Produkt“-Begriffs,**
  - **um sicherzustellen, dass für durch fehlerhafte Produkte verursachte Schäden, die auf Software oder andere digitale Merkmale zurückzuführen sind, stets Schadenersatz gewährt wird;**
  - **um abzuklären, wer als Hersteller im Sinne der Produkthaftungsrichtlinie angesehen werden kann.**
- **Überprüfung der Beibehaltung einer verschuldensunabhängigen Haftung oder Einführung einer Gefährdungshaftung. Anpassung der Beweislast (Erleichterung, Umkehr).**
- **Eindeutigere Regelungen bzgl. der Bereitstellung von Security Updates (z.B. Zeitraum, Kostentragung) und Rechtsfolgen bei Unterlassung der Aktualisierung durch den Konsumenten**
- **Verpflichtung zum Abschluss einer verfügbaren Versicherung**

[7] COM(2020) 64 final, report-safety-liability-artificial-intelligence-feb2020_de.pdf (europa.eu).

8. Conclusio

Zusammengefasst lässt sich sagen, dass IoT in Österreich langsam beginnt, den Mainstream zu erobern. Doch nach wie vor sind die meisten Nutzer*innen von IoT-Geräten eher im an sich schon „technikaffinen“ Bevölkerungsteil zu verorten. Daher ist es auch nicht verwunderlich, dass grundsätzlich ein gewisses Maß an Sicherheitsbewusstsein und -maßnahmen in Österreichs IoT-Haushalten herrscht. Doch diese Maßnahmen sind noch stark ausbaubar. Denn mit dem nicht aufzuhaltenden Siegeszug von „smarten“ Geräten und dem Internet of Things wird die heimische Technik zum Angriffsvektor für Kriminelle. Und um dieser Gefahr nicht schutzlos ausgeliefert zu sein, wird es notwendig sein, das Schutzniveau nachhaltig zu steigern.

IoT ist gekommen, um zu bleiben, und die Digitalisierung sämtlicher Gesellschaftsbereiche wird dazu führen, dass auch unser Alltag immer digitaler wird. Umso wichtiger ist es, sich der Risiken bewusst zu werden und diese vor allem auch ernst zu nehmen. IoT wird den Menschen viele Dinge im Alltag und in der Arbeit erleichtern und haben noch großes Potential, das unter anderem durch den neuen Mobilfunkstandard 5G entfaltet werden kann. Doch mit großem Potential zum positiven geht immer auch kriminelles Potential einher. Hier wird es wichtig sein, sich frühzeitig von staatlicher wie von individueller Seite mit den Risiken zu beschäftigen und Gegenstrategien zu entwickeln, damit auch Österreich die positiven Seiten der Digitalisierung genießen kann.

Hier sind für das KFV drei Maßnahmen zentral, um die Österreicher*innen fit für die Zukunft im „Internet der Dinge“ zu machen und sie bestmöglich zu schützen:

1. Schulung des Verkaufspersonals

Doch nicht nur die Nutzer*innen selbst sollten dazu angehalten werden, ihre IoT-Geräte entsprechend vor Fremdzugriffen zu sichern. Die Prävention beginnt bereits im Vorfeld, beim Verkauf und der Beratung. Hier wird in der Befragung auch offensichtlich, dass noch Luft nach oben ist. **Verkaufspersonal und Installateur*innen müssen den Endnutzer*innen mehr Informationen geben, wie sie sich selbst schützen können, wo die Gefahren liegen, und was im Falle eines Sicherheitsvorfalls zu tun ist.**

2. Konsument*innenschutz ausbauen

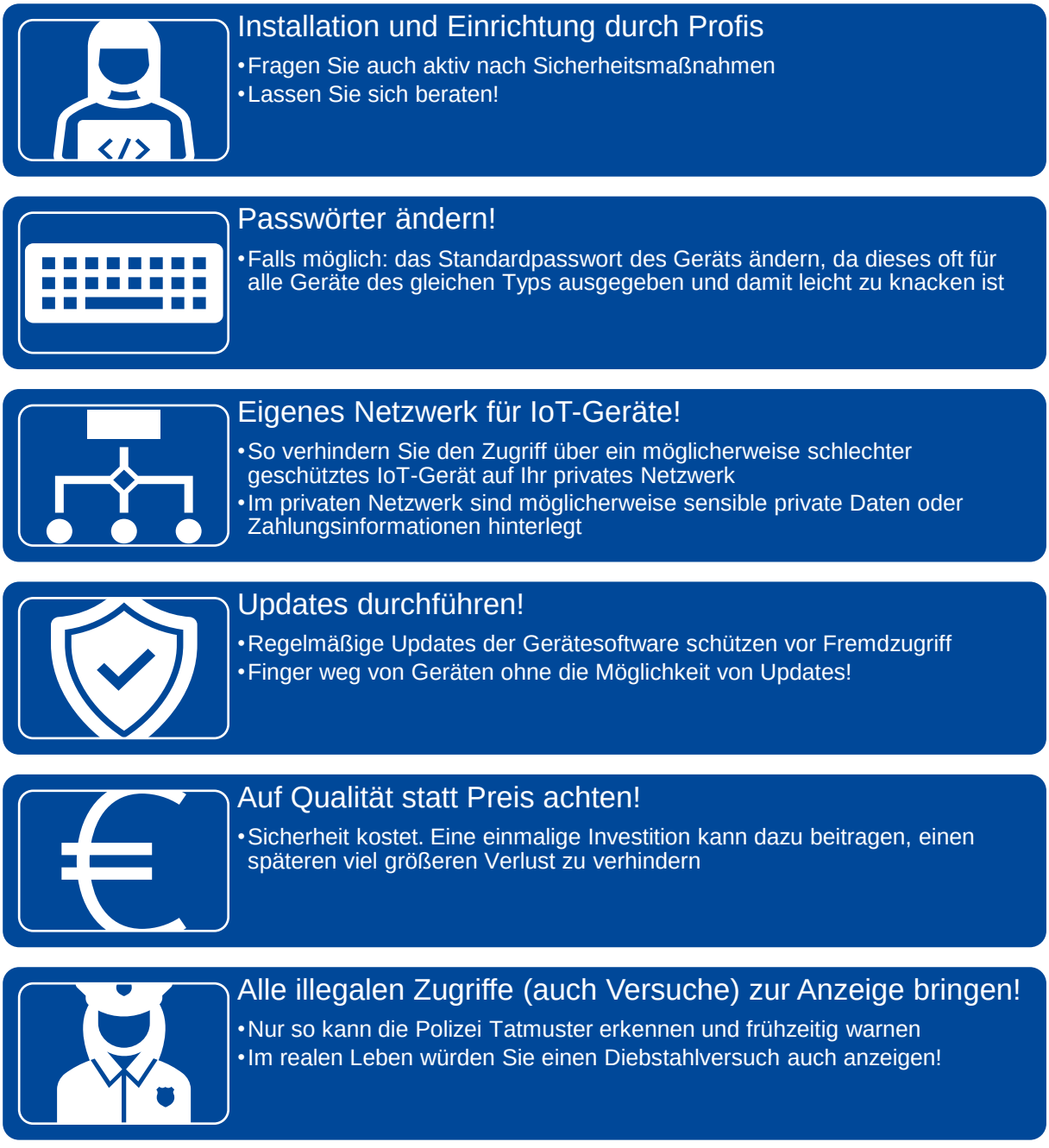
Auch der Konsument*innenschutz kommt zu ähnlichen Forderungen, so wird unter anderem gefordert, Basisinformationsblätter für Konsument*innen gefordert, aus denen hervorgehen soll, welche Daten übermittelt und wozu diese verwendet werden.

3. Zertifizierung für IoT-Geräte entwickeln

Weiters wird es notwendig werden, Sicherheitsnormen für IoT-Geräte zu definieren, um die österreichischen Nutzer*innen bestmöglich zu schützen. **Hier ist es mit Sicherheit am sinnvollsten, entweder auf europäischer oder auf nationaler Ebene Zertifizierungen basierend auf dem ETSI-Standard 303 645 (siehe Kapitel 7.4) zu entwickeln, um verschiedene Sicherheitsstufen zu definieren. Jedenfalls wäre außerdem sinnvoll, einen Mindeststandard zu entwickeln, dessen Sicherheitsvorkehrungen verpflichtend für neue IoT-Geräte sein müssen.**

9. Tipps für Anwender*innen

Die vorliegende Studie zeigt, wie wichtig ein angemessener Schutz der privaten IoT-Infrastruktur ist. Österreichs Haushalte sind auf einem guten Weg, was die Prävention unerlaubter Zugriffe angeht, jedoch kann hier immer noch nachgebessert werden. Vor allem aber wird es wahrscheinlich in Zukunft auch immer schwieriger, gewisse Geräte ohne „smarten“ oder IoT-Charakter zu erwerben. Umso wichtiger ist es, einige grundlegende Sicherheitsmaßnahmen zu treffen:



Tabellenverzeichnis

Abbildungsverzeichnis

Literaturverzeichnis

Burger, L. (2021). *Was bringt der Standard ETSI EN 303 645 für die Sicherheit von Consumer-IoT-Produkten?* Abgerufen am 03. September 2021 von itconsulting-burger.de: https://itconsulting-burger.de/etsi_303645/

Evans, D. (2011). *The Internet of Things: How the Next Evolution of the Internet is Changing Everything*. Abgerufen am 20. Juli 2021 von cisco.com: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Hilt, S., Kropotov, V., Mercês, F., Rosario, M., & Sancho, D. (2019). *The Internet of Things in the Cybercrime Underground.* Trend Micro Research. Abgerufen am 03. August 2021 von https://documents.trendmicro.com/assets/white_papers/wp-the-internet-of-things-in-the-cybercrime-underground.pdf?_ga=2.146915956.298592428.1627969979-1463739643.1626677563

Infineon. (2019). *Was Sie über das Internet der Dinge wissen müssen*. Abgerufen am 20. Juli 2021 von infineon.com: https://www.infineon.com/cms/de/discoveries/internet-der-dinge-basics/

IoT Business News. (2020). *Connected Devices Will Generate 79 Zettabytes of data by 2025*. Abgerufen am 20. Juli 2021 von iotbusinessnews.com: https://iotbusinessnews.com/2020/08/10/08984-connected-devices-will-generate-79-zettabytes-of-data-by-2025/

IT-Service Network. (2021). *Cryptomining - Definition*. Abgerufen am 03. August 2021 von https://it-service.network/it-lexikon/cryptomining

Krieger-Lamina, J. (8. April 2021). Interview: Iot/5G Jaro Krieger-Lamina. (G. Plattner, Interviewer)

Petzl, G. (22. März 2021). Interview zu IoT und 5G: Georg Petzl (Magenta). (G. Plattner, Interviewer)

Prinzellner, Y., & Pilgerstorfer, M. (2018). *Die Revolution im eigenen Heim: Keine Angst vor Smart Living!* Wien: KFV (Kuratorium für Verkehrssicherheit.

Verein Industrie 4.0. (2019). *Cyber-Security Leitfaden für Produktionsbetriebe: Schutz vor Cyberattacken - Mehr Wertschöpfung mit Security.* Wien. Abgerufen am 02. 07 2020 von https://plattformindustrie40.at/wp-content/uploads/2020/05/WEB_Industrie4.0_Ergebnispapier_CyberSecurity_2019.pdf

Vogt, A. (2019). *Das Internet der Dinge im deutschen Mittelstand: Bedeutung, Anwendungsfelder und Stand der Umsetzung.* München: Deutsche Telekom. Abgerufen am 02. 07 2020 von https://iot.telekom.com/resource/blob/data/183656/e16e24c291368e1f6a75362f7f9d0fc0/das-internet-der-dinge-im-deutschen-mittelstand.pdf

KFV (Kuratorium für Verkehrssicherheit)
Schleiergasse 18
1100 Wien
T +43-(0)5 77 0 77-DW oder -0
F +43-(0)5 77 0 77-1186
E-Mail kfv@kfv.at
www.kfv.at

Medieninhaber und Herausgeber: Kuratorium für Verkehrssicherheit
Verlagsort: Wien
Herstellung: Eigendruck
Redaktion: Dr. Georg Plattner
Grafik: KFV

SAFETY FIRST!