Bundesministerium
Inneres

Sicherheitsakademie

SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Jeßner, Patricia/Plattner, Georg

IoT in Österreichs Privathaushalten – eine Analyse

SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (2/2022), 61-70.

doi: 10.7396/2022_2_E

Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:

Jeßner, Patricia/Plattner, Georg (2022). IoT in Österreichs Privathaushalten – eine Analyse, SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (2), 61-70, Online: http://dx.doi.org/10.7396/2022_2_E.

© Bundesministerium für Inneres – Sicherheitsakademie / Verlag Österreich, 2022

Hinweis: Die gedruckte Ausgabe des Artikels ist in der Print-Version des SIAK-Journals im Verlag Österreich (https://www.verlagoesterreich.at/) erschienen.

Online publiziert: 09/2022

IoT in Österreichs Privathaushalten – eine Analyse

Das „Internet der Dinge“ ist gekommen, um zu bleiben. Unser vom „Internet of Things (IoT)“ geprägter Alltag wird immer digitaler, smarte Devices und innovative Technologien sind omnipräsent. Mit großem Nutzen in Sachen Komfort – und erhöhtem Risiko in Sachen Datensicherheit. Nicht nur Smartphone, iPad, Laptop & Co. sind moderne Spiegel unserer Seele, auch Smart Living öffnet Cyberkriminellen Tür und Tor zu unseren persönlichen Daten, zu unserem geistigen und materiellen Eigentum. Der smarte Kühlschrank, die ferngesteuerte Heizung und der Staubsaugroboter bedeuten für Hacking-Profis willkommene Datenlecks, die über Daheimsein und Nichtdaheimsein Bescheid geben. Die Haustür muss erst gar nicht mehr mit Gewalt aufgebrochen werden, der Code des Sicherheitsschlosses wird mit krimineller Energie und entsprechendem IT-Know-how sekundenschnell geknackt. Je komplexer und smarter unser tägliches Leben wird, desto wichtiger wird es für Nutzerinnen und Nutzer, sich neuer Risiken bewusst zu werden und mit gezielten Maßnahmen für mehr persönliche Sicherheit zu sorgen. Eine aktuelle Studie des Kuratoriums für Verkehrssicherheit (KFV) zum Thema IoT liefert Einblicke in den Informationsstand der Bevölkerung und beleuchtet Defizite, Risiken und Potenziale. Das Fazit der Fachleute: Intensivierte Information muss Konsumentinnen und Konsumenten ihre Selbstschutzmöglichkeiten aufzeigen, muss sie sicherheitsbewusst und damit fit für die Zukunft machen – damit die Chancen für Cyber Crime so gering wie möglich bleiben. Die Rolle der Exekutive ist und bleibt eine essenzielle – auch als verstärkt beworbene Anlaufstelle für von Online-Attacken betroffene Konsumentinnen und Konsumenten. Denn nur polizeilich angezeigte Schadensfälle bringen mehr Licht ins weite Dunkelfeld der Internetverbrechen – auch wenn die kriminellen Spuren im weltweiten Netz meist nur schwer zu verfolgen sind.

PATRICIA JESSNER,
Eigentumsschutz, Kuratorium für Verkehrssicherheit Wien.

GEORG PLATTNER,
Eigentumsschutz, Kuratorium für Verkehrssicherheit Wien.

1. PROBLEMSTELLUNG UND RISIKEN

Kriminalität und ihre Prävention bedeuten immer auch eine Art Katz-und-Maus-Spiel zwischen jenen, die illegale Handlungen setzen wollen, und den staatlichen Strafverfolgungsbehörden. Das bedeutet, dass Innovationen, die sich schnell weiterentwickeln, immer eine besondere Herausforderung für Strafverfolgungsbehörden darstellen. Diese müssen 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 Innova-

tionskraft nicht nur auf Seiten des Gesetzes, sondern auch auf Seiten der Kriminellen, führt zu einem ständigen Wettrennen um das nächste Schlupfloch.

Im Besonderen ist jede technologische Entwicklung, die in der breiten Bevölkerungsmasse Anwendung findet, von diesem Risiko betroffen. Denn je mehr Menschen eine Technologie nutzen, umso größer ist auch die Gefahr, dass einige unbedarft und sorglos damit umgehen und es somit Verbrecherinnen und Verbrechern besonders leicht machen. Dies ist bereits nachvollziehbar an den nach wie vor sehr stark steigenden Zahlen der Cyberkriminalität im Allgemeinen. Seit der Einführung des Privat-PCs ist es nicht nur die Innovationsfähigkeit der Kriminellen, sondern auch die Sorglosigkeit der Nutzerinnen und Nutzer, 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 tritt auch in Österreich seinen Siegeszug an. 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: Cyberkriminelle müssen sich nicht mehr an der Sicherheitstüre abmühen, um in ein Haus einzudringen – stattdessen wird in das oft nur mangelhaft gesicherte System eingedrungen, und die Tür springt von selbst auf. Die Daten des Staubsaugroboters können Rückschlüsse darauf zulassen, wann eine Besitzerin oder ein Besitzer nicht zu Hause ist, eine nützliche Information für Einbrecherinnen und Einbrecher. Und ein schlecht gesicherter smarter Kühlschrank kann das Einfallstor in den eigentlich gut gesicherten Stand-PC mit sämtlichen sensiblen persönlichen Daten darstellen.

Der Begriff „Internet of Things“ (IoT) lässt sich nur schwer 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. Sie umfasst „kleine, langlebige Devices mit geringem Stromverbrauch, die in unserer Umgebung integriert sind“, so DI Mag. Georg Petzl, 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 der wichtigsten Veränderungen, die die Digitalisierung bringen wird, ist eine weitere Vernetzung von Unternehmensprozessen, sowohl für die üblichen Geschäftsbereiche (IT – Information Technology) als 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 (vgl. Verein Industrie 4.0 Österreich 2019).

Die unter dem Schlagwort IoT zusammengefassten Umwälzungen der Rolle, die digitale, smarte Technologie in unserer Gesellschaft spielen wird, gehören zu den relevantesten Themen für Unternehmen, um zukunftsfit zu werden. Eine deutsche Studie zum Thema (vgl. Vogt 2019) zeigt,

dass IoT ein sich ständig weiter entwickelnder Prozess ist, den Unternehmen durchaus aktiv durchleben, dabei aber oft 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. Ob Staubsaugroboter, automatische Heizung, Sonnenlichtsensoren, die die Jalousien automatisch senken lassen, oder smarte Fitnesstracker: IoT ist im Alltag der Menschen allgegenwärtig.

Die IT-Sicherheitsforscherinnen und -forscher Stephen Hilt, Vladimir Kropotov, Fernando Mercês, Mayra Rosario und David Sancho (vgl. Hilt et al. 2019) analysierten in einem Bericht für Trend Micro Research die Chats in fünf Untergrundforen zum Thema IoT und Cyberkriminalität. Die Untersuchungen ergaben, dass der aktuelle 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 sogenannten Brute-Force-Attacken bewerkstelligt. Dies bedeutet, dass direkt versucht wird, ein Passwort oder einen Benutzerinnen- bzw. Benutzernamen 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.

Im Bericht von Trend Micro Research wird betont, dass IoT-Geräte derzeit 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 für Cyberkriminelle extrem anwachsen. Hier wird es vor allem um Geräte gehen, die 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 Energie und würden bei Geräten mit Akkus sehr schnell auffliegen.

Doch auch für sehr viel direktere und für die Einzelperson schädlichere Missetaten können IoT-Geräte genutzt werden. Sind die Zugangsdaten erst einmal geknackt, können im schlimmsten Fall Geräte ferngesteuert und manipuliert werden. So kann dann die Einbrecherin bzw. der Einbrecher die Haustür per Mausklick öffnen, während ihre Komplizinnen oder Komplizen über die Sicherheitskameras im Haus darauf achten, dass niemand die Täterin oder den Täter bei der Arbeit stört.

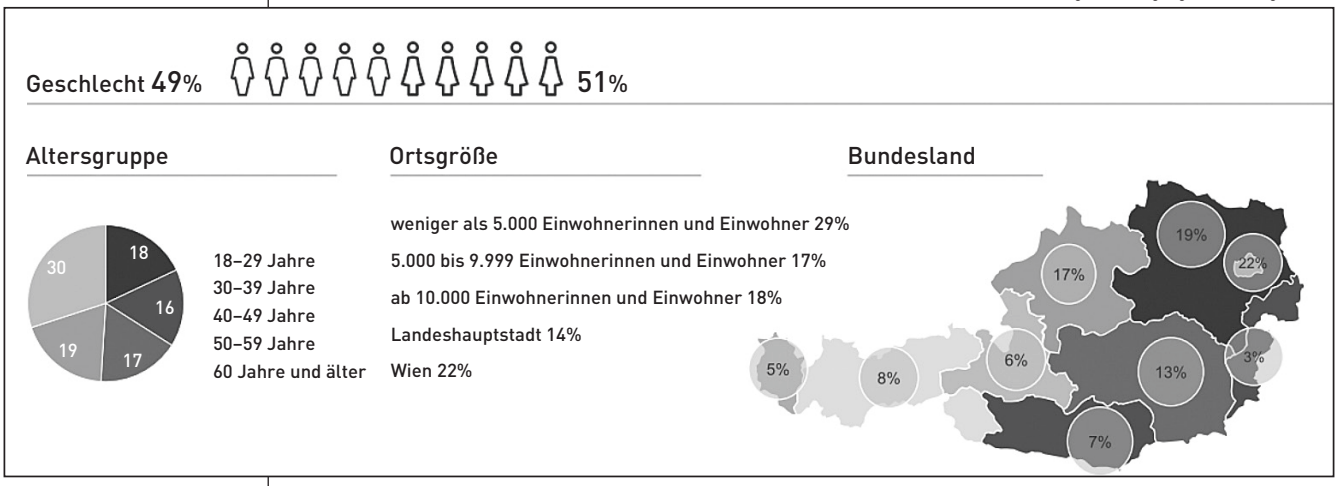
Darüber hinaus kann laut den Expertinnen und Experten davon ausgegangen werden, dass in Zukunft das Geschäft der Cyberkriminellen mit dem Zugang zu und der Ausnutzung von IoT-Geräten weiter ansteigen wird. Sei es für die bereits jetzt häufigsten Formen, wie oben beschrieben, oder für ganz neue Formen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

2. DIE KFV-ANALYSE

2.1 Methode

Eine aktuelle KFV-Studie soll einen wesentlichen Beitrag zur Prävention von Cyberkriminalität via IoT-Geräte leisten. Ausgehend vom Status quo der IoT-Nutzung in österreichischen Privathaushalten wurde über eine repräsentative Bevölkerungsbefragung die Sicherheit der österreichischen Nutzerinnen und Nutzer kritisch analysiert, um anschließend aufzuzeigen,

Quelle: eigene Befragung, Darstellung: Kantar



Sample der quantitativen Erhebung

worauf zu achten ist, um diese Innovationen möglichst sicher nutzen zu können. Mit einer Stichprobe von 1.000 Personen, repräsentativ für die online aktive österreichische Bevölkerung, wurden Nutzungsverhalten und Bewertung von IoT-Geräten in Österreich ermittelt. Für die Befragung wurde in Zusammenarbeit mit dem Marktforschungsinstitut Kantar ein Online-Fragebogen entwickelt. Die Verteilung der Teilnehmenden entsprach anhand der demografischen Marker Geschlecht, Alter und Wohnort einer repräsentativen Quotenstichprobe Österreichs.

Zusätzlich wurden zwei Experten zum Thema IoT befragt. Die Interviews mit Jaro Krieger-Lamina, wissenschaftlicher Mitarbeiter am Institut für Technikfolgenabschätzung der Österreichischen Akademie der Wissenschaften, und Georg Petzl, Chief Security Office Magenta, wurden in explorativer Form geführt. Die vorgegebenen Themen waren Internet of Things in Österreich, Sicherheit und Cyberkriminalität im Zusammenhang mit IoT sowie gesellschaftlicher Fortschritt und IoT. Die Interviews wurden so geführt, dass zwar Leitfragen dem Gespräch eine semistrukturierte Form gaben, in weiterer Folge jedoch vor allem die Aussagen der Experten das Gespräch leiteten.

2.2 Status quo von IoT in Österreich

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

Nach der Beantwortung erfolgte im Fragebogen eine Definition des Begriffs IoT: Als „Internet der Dinge“ wird die Vernetzung verschiedener Geräte im Internet bezeichnet. Diese Geräte sind smart, kommunizieren also miteinander und können selbstständig Aufgaben für die Nutzerin oder den Nutzer erledigen. Nach Klärung des Begriffs geben 36 % der Befragten an, derartige Geräte (Smartphones wurden dezidiert als nicht gemeinte Geräte erwähnt) zu nutzen, 56 % verneinen dies, und 8 % enthalten sich der Antwort. Im Vergleich zu einer im Jahr 2017 durchgeführten Bevölkerungsbefragung des KFV ging die Zahl der Nutzerinnen und Nutzer von IoT-Geräten um neun Prozent zurück (2017: 45 %). Dies ist jedoch mit der Tatsache erklärbar, dass in der Befragung aus dem Jahr 2017 das Smartphone als Teil des Internet of

Things betrachtet wurde (vgl. Prinzellner/Pilgerstorfer 2018).

Die Differenzen zwischen den Subgruppen (Geschlecht, Alter, Ortsgröße) verringern sich gegenüber der spontanen Abfrage deutlich, 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 selbst.

Gründe für die Anschaffung gibt es viele, es überwiegt jedoch die Erleichterung des Alltags. Diesen Beweggrund geben zwei Drittel der Befragten an. Dieses Nutzungsverhalten schätzt auch Georg Petzl in gleichartiger Weise ein. Angesprochen darauf, welche Arten von Geräten im IoT-Bereich in Zukunft große Rollen spielen werden, meint Petzl: „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 sie ist schon sehr viel weiter als das, was bisher auf dem Markt zu kaufen und auch für den Enduser von praktischem Nutzen ist.

Wenig überraschend gestaltet sich die Verteilung der konkreten Nutzung von IoT-Geräten. Die gängigsten IoT-Geräte kann man dem Bereich Smartes IT-Equipment zuordnen (92 %). Hier ist das bei weitem am meisten genutzte Gerät der smarte Fernseher (70 % der Nutzerinnen und Nutzer 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 Nutzerinnen und Nutzer von IoT-Geräten nutzen Devices dieser Kategorie). Hier dominiert der Staubsaugroboter, gefolgt von smarter Beleuchtung und smarter Kaffeemaschine.

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

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

Nach wie vor denkt knapp die Hälfte der Österreicherinnen und Österreicher nicht daran, sich (weitere) IoT-Geräte anzuschaffen. Hier ist ganz klar zu erkennen, dass jene Menschen, die bereits IoT-Geräte in ihren Alltag integriert haben, bei weitem motivierter sind, sich weitere Geräte zuzulegen. Die Hürde, sich ein erstes smartes Gerät anzuschaffen, scheint nach wie vor hoch zu sein. Darüber hinaus ist auch hier, wie bei fast allen Digitalisierungsthemen, eine große Alterskluft zu erkennen: je jünger die Befragten, desto höher ist deren Bereitschaft, sich (weitere) IoT-Geräte anzuschaffen. Ältere Personen sind hingegen weit zurückhaltender.

Befragt 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. Den größten Nutzen sehen die Befragten in Sachen Kindersicherheit und Einbruchsschutz. Die geringsten zu-

gedachten 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 seien. In dieser Kategorie sind 37 % der Meinung, dass die Geräte nur „teils, teils“ helfen, weitere 17 % gehen davon aus, dass sie „weniger“ oder „gar keinen“ Nutzen bringen.

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

Weit weniger gewillt sind die Befragten zu einer 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. Auch in dieser Hinsicht spricht sich mehr als die Hälfte der befragten Personen dagegen aus.

2.3 Sicherheit und Risiko

2.3.1 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 Sorge des Herstellers für eine vernünftige Update-Policy meist nicht weit her (vgl. Petzl 2021). Dies wäre laut Petzl natürlich ein beidseitiges Problem. Denn solange die Kundinnen und Kunden nicht bereit wären, für Qualität auch entsprechend zu bezahlen, und solange diese Lücke rechtlich nicht geschlossen wird, würden Herstellerinnen und Hersteller auch keine Notwendigkeit sehen, ihre Geräte regelmäßig und langfristig upzudaten.

Im Bereich der Passwortsicherheit sieht Petzl das Problem etwas komplexer. Hier sei vor allem problematisch, dass das von Herstellerinnen und Herstellern gewählte Passwort oft auch mit der Firmware verknüpft ist und dies zu Problemen in der Programmierung führen könne. Generell sieht der Experte Passwörter als eher kleinen Hebel in der Erhöhung der Sicherheit von IoT-Geräten, da hier andere Themen wie geschützte Netzwerke wichtiger wären. Die österreichischen Nutzerinnen und Nutzer 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 über diese Möglichkeit schlicht nicht Bescheid.

In Bezug auf Updates sieht die Situation auf den ersten Blick besser aus als befürchtet. Immerhin 39 % der befragten Nutzerinnen und Nutzer geben an, dass auf all ihren Geräten die Möglichkeit besteht, unbegrenzt Sicherheitsupdates zu erhalten.

44 % geben an, dass dies entweder nur bei manchen Devices oder nicht zeitlich unbegrenzt der Fall ist. Auch hier stechen die elf Prozent der Unwissenden negativ heraus.

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 der Befragten an, auf allen Geräten sichere Passwörter zu verwenden. Weniger gut ist die Update-Disziplin der Nutzerinnen und Nutzer: Nicht einmal die Hälfte der befragten Österreicherinnen und Österreicher führt regelmäßig Updates durch. Dieses mangelnde Bewusstsein spiegelt sich auch in weiteren Studien des KFV zu anderen Cybersicherheitsthemen wider. Updates sind immer noch für eine allzu große Zahl der Österreicherinnen und Österreicher kein zentraler Punkt in ihrer Cybersicherheitsplanung. Ein weiteres Drittel verwendet schlicht die Einstellungen der Herstellerinnen und Hersteller oder Händlerinnen und Händler.

Nur 22 % 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 Cyberexpertinnen und Cyberexperten genannt werden, werden nur von einer kleinen Minderheit der Nutzerinnen und Nutzer angewendet.

Im Bereich der Maßnahmen, die den Nutzerinnen und Nutzer beim Kauf oder vor Verwendung mittels Produktinformation genannt wurden, ist ebenfalls deutliches Verbesserungspotenzial zu erkennen: So haben fast jede fünfte Herstellerfirma bzw. die beteiligten Vertriebsunternehmen keinerlei Sicherheitsmaßnahmen genannt. Auch bei Updates und Passwörtern waren die oben genannten zurückhaltend: Nur knapp mehr als die Hälfte empfahl regelmäßige Softwareupdates, weniger als die Hälfte schlug die Änderung des Ursprungspasswords 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 die Endnutzerin oder der Endnutzer mit einem Gerät ausgestattet, von dem sie oder er 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 Fachleute den Käuferinnen und Käufern ein gutes Basisinformationspaket zu deren persönlichem Schutz mitgeben können.

Umso verwunderlicher ist die Antwort der Österreicherinnen und Österreicher auf die Frage, ob sie mit den erhaltenen Informationen zufrieden waren: über zwei Drittel der Befragten gaben an, dass dies der Fall war. Hier herrscht also augenscheinlich eine große Diskrepanz zwischen dem, was aus Cybersicherheitsperspektive notwendig wäre, und dem, was die Nutzerinnen und Nutzer sich von den entsprechenden Expertinnen und Experten erwarten.

Der Wunsch nach mehr Unterstützung ist trotzdem erkennbar. Jeweils etwa die Hälfte der Befragten wünscht sich mehr Unterstützung durch den Staat oder durch die Herstellerfirmen und den Verkauf. 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.

2.3.2 Illegale Zugriffsversuche und verursachter Schaden

17 % der Nutzerinnen und Nutzer 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 all jene Betroffenen sind, die einen solchen Zugriffsversuch auch bemerkt haben.

Von jenen Personen, die einen illegalen Zugriff bzw. Zugriffsversuch erlebt haben, erlitten 55 % 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.

Jene 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.

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 Täterinnen und Täter gefasst werden. Zum anderen liegt es auch daran, dass die Menschen einen nicht erfolgreichen Zugriffsversuch oder einen erfolgreichen ohne Schaden nicht als anzeigewürdig ansehen. Doch fast alle würden es zum Beispiel zur Anzeige bringen, wenn an der eigenen Wohnungstüre eindeutige Einbruchsspuren sichtbar sind, auch wenn das Türschloss dem Einbruchsversuch standgehalten hat. Diese Fahrlässigkeit in der Anzeigemoral führt auch dazu, dass die Polizei große Schwierigkeiten hat, Kriminalitätstrends festzustellen und entsprechend zu reagieren.

Generell ist zu sagen, dass die Zahl der Personen, 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 Widerstands, 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 Nutzerinnen und Nutzer massiv anwächst, wird es für Cyberkriminelle sehr viele kaum geschützte Wege in Wohnungen, Häuser, Eigentum und private Daten der Österreicherinnen und Österreicher geben.

3. CONCLUSIO

Zusammenfassend lässt sich feststellen, dass IoT in Österreich langsam beginnt, den Mainstream zu erobern. Doch nach wie vor sind die meisten Nutzerinnen und Nutzer 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 „smarter“

Geräte und des Internet of Things wird die heimische Technik zum Angriffsvektor für Kriminelle. Um dieser Gefahr nicht schutzlos ausgeliefert zu sein, wird es notwendig sein, das Schutzniveau nachhaltig zu steigern.

Das IoT ist gekommen, um zu bleiben. 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. Das IoT wird den Menschen viele Dinge im Alltag und in der Arbeit erleichtern und hat noch großes Potenzial, das unter anderem durch den neuen Mobilfunkstandard 5G entfaltet werden kann. Doch mit großem Potenzial im positiven Sinn geht immer auch kriminelles Potenzial einher. In dieser Hinsicht 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.

Für das KFV sind in diesem Zusammenhang drei Maßnahmen zentral, um die Österreicherinnen und Österreicher fit für die Zukunft im Internet der Dinge zu machen und sie bestmöglich zu schützen:

Schulung des Verkaufspersonals

Nicht nur die Nutzerinnen und Nutzer selbst sollten dazu angehalten werden, ihre IoT-Geräte entsprechend vor Fremdzugriffen zu sichern. Die Prävention beginnt bereits im Vorfeld, beim Verkauf und bei der Beratung. Im Rahmen der Befragung wurde offensichtlich, dass in puncto Informationsstand noch Luft nach oben ist. Verkaufspersonal und Beratung bzw. Inbetriebnehmerin und Inbetriebnehmer müssen den Endnutzerinnen und Endnutzern mehr Informationen geben, wie sie sich selbst schützen können, wo die Gefahren liegen und was im Falle eines Sicherheitsvorfalls zu tun ist.

Konsumentinnen- und Konsumentenschutz ausbauen

Auch der Konsumentinnen- und Konsumentenschutz formuliert ähnliche Forderungen, unter anderem Basisinformationsblätter für Konsumentinnen und Konsumenten zur Verfügung zu stellen, aus denen hervorgehen soll, welche Daten übermittelt und wozu diese verwendet werden.

Zertifizierungen für IoT-Geräte entwickeln

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

Die KFV-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 und soll hier immer noch nachgebessert werden. Vor allem aber wird es wohl in Zukunft auch immer schwieriger, gewisse Geräte ohne „smarten“ oder IoT-Charakter zu erwerben. Umso wichtiger ist es, mittels gezielter Präventionsarbeit ein grundlegendes Sicherheitsbewusstsein in den Köpfen der Nutzerinnen und Nutzer zu verankern und die Bevölkerung auf die Wichtigkeit polizeilicher Anzeigen auch im Onlinebereich hinzuweisen, um Licht in das große Dunkelfeld des digitalen Verbrechens zu bringen.

[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 2019). Hierfür werden die komplexen Daten von den Geräten der Minerinnen und Miner mittels Blockchain verarbeitet. Auf Grund der hohen Rechenleistung, die benötigt wird, um Cryptomining zu ermöglichen, dauert dies lange, erfordert viel Strom und ist somit mit erheblichen Kosten verbunden. Cryptomining selbst ist völlig 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.*

Quellenangaben

Hilt, Stephen et al. (2019). The Internet of Things in the Cybercrime Underground. Trend Micro Research, Online: https://documents.trendmicro.com/assets/white_papers/wp-the-internet-of-things-in-the-cybercrime-underground.pdf?_ga=2.146915956.298592428.1627969979-1463739643.1626677563 (03.08.2021).

Krieger-Lamina, Jaro (2021). Interview von Georg Plattner zu IoT und 5G 08.04.2021.

Petzl, Georg (2021). Interview von Georg Plattner zu IoT und 5G, 23.03.2021.

Prinzellner, Yvonne/Pilgerstorfer, Monika (2018). Smart Living in Österreich. Chancen, Risiken, Meinungen & Trends, KFV (Kuratorium für Verkehrssicherheit) – Sicher Leben, Bd. 15, Wien.

IT-Service Network 2019. IT-Wissen. IT-Lexikon. Cryptomining – Definition, Online: https://it-service.network/it-lexikon/cryptomining#:~:text=Als%20Cryptomining%20ist%20das%20%E2%80%9EAbsch%C3%BCrfen,Transaktionen%20aufzeichnen%2C%20verifizieren%20und%20verbuchen (02.07.2020).

Verein Industrie 4.0. Österreich (2019). Cyber-Security Leitfaden für Produktionsbetriebe. Schutz vor Cyberattacken – Mehr Wertschöpfung mit Security, Online: https://plattformindustrie40.at/wp-content/uploads/2020/05/WEB_Industrie4.0_Ergebnispapier_CyberSecurity_2019.pdf (02.07.2020).

Vogt, Arnold (2019). Das Internet der Dinge im deutschen Mittelstand: Bedeutung, Anwendungsfelder und Stand der Umsetzung, Eine Studie im Auftrag der Deutschen Telekom, Online: https://iot.telekom.com/resource/blob/data/183656/e16e24c291368e1f6a75362f7f9d0fc0/das-internet-der-dinge-im-deutschen-mittelstand.pdf (02.07.2020).