SMART HOME – NUTZUNG DER GERÄTE IN ÖSTERREICH UND ASPEKTE DER SICHERHEIT UND REGULATION DER DATENSAMMLUNG

Edith Huber / Bettina Pospisil / Walter Seböck / Peter Kieseberg / Albert Treytl

Autor 1: Senior Researcher, Donau Universität Krems
Dr. Karl Dorrek Str. 30, 3500 Krems an der Donau, AT
edith.huber@donau-uni.ac.at; https://www.donau-uni.ac.at

Autor 2: Researcher, Donau Universität Krems, Zentrum für Infrastrukturelle Sicherheit
Dr. Karl Dorrek Str. 30, 3500 Krems an der Donau, AT
bettina.pospisil@donau-uni.ac.at; https://www.donau-uni.ac.at

Autor 3: Ass. Prof., Donau Universität Krems, Zentrum für Infrastrukturelle Sicherheit
Dr. Karl Dorrek Str. 30, 3500 Krems an der Donau, AT
walter.seboeck@donau-uni.ac.at; https://www.donau-uni.ac.at

Autor 4: Institutsleiter Institut für IT Sicherheitsforschung,
Heinrich Schneidmadl-Straße 15, 3100 St. Pölten, AT
peter.kieseberg@fhstp.ac.at, https:/fhstp.ac.at

Autor 5: Senior Researcher, Donau Universität Krems, Department für integrierte Sensorsysteme
Viktor Kaplan Straße 2 – Bauteil E.Dr. Karl Dorrek Str. 30, 3500 Krems an der Donau, AT
albert.treytl@donau-uni.ac.at; https://www.donau-uni.ac.at

Schlagworte: ***Datenschutz, Cybersicherheit, Cybercrime, IoT, Home Automatisation***

Abstract: *Es steht außer Zweifel, dass das Internet der Dinge (IoT) und seine Anwendung in Heimautomationssystemen (HAS) eine Vielzahl an neuen Diensten ermöglichen wird. Immer mehr österreichische Haushalte setzen daher vermehrt auf HAS-Geräte im Haushalt, dabei findet man Anwendungen vom internetfähigen TV bis hin zum Tierfutternapf. Aber wie sieht es mit der Aufklärung der Nutzer*innen über die Verwendung ihrer Daten und mit der Sicherheit dieser Systeme aus? Im Rahmen dieses Vortrags werden die Ergebnisse einer österreichweiten repräsentativen Studie dargestellt, die sich unter anderen dieser Forschungsfrage widmen.*

1. Einleitung

HAS-Anwendungen[1] können sich dynamisch an den aktuellen Kontext anpassen, automatisiert Entscheidungen treffen und das Situationsbewusstsein ihrer Nutzer*innen verbessern. Dabei ist jedoch die Gewährleistung der Sicherheit dieser Geräte eine besondere Herausforderung.[2] In privaten Haushalten werden sie vor allem zur Einsparung von Energie und zur Erhöhung von Komfort und Sicherheit eingesetzt.[3] IoT-basierte HAS zählen zu den bedeutendsten (zukünftigen) Komponenten der Digitalisierung, die unmittelbar direkt die Privatsphäre von vielen Menschen berühren. Durch die zunehmende Integration der HAS in unser tägliches Leben, stellen sie ein attraktives Ziel für kriminelle Angreifer*innen dar. HAS können genutzt werden, um die Bewohner*innen auszukundschaften und so in weiterer Folge kriminelle Handlungen wie Einbruch, Identitätsdiebstahl, Stalking oder Erpressung durchzuführen.

---

1 Im Rahmen dieses Artikels werden die Begriffe HAS, Smart Home Automation Systems (SHAS) und SMART HOME als Synonyme verwendet.

2 Pirbhulalp et al.: A novel secure IoT-based smart home automation system using a wireless sensor network. Sensors 17(1), 69 (2016).

3 Wilson et al.: Benefits and risks of smart home technologies. Energy Policy 103, 72-83 (2017).

Angesichts dieser Bedrohungslage, stellen sich folgende Forschungsfragen:

– Welche HAS-Geräte finden sich in den österreichischen Haushalten?
– Welche Risiken ergeben sich aus dem Besitz dieser HAS-Geräte für die Besitzer*innen?
– Wie wurden die Besitzer*innen dieser Geräte über die Verwendung ihrer Daten informiert?

1.1. Methodik

Zu Beantwortung der Forschungsfragen wurde ein quantitatives Forschungsdesign herangezogen. Die Datenerhebung fand mittels Onlinebefragung repräsentativ für Österreich statt. Dabei wurden im März 2020 insgesamt (n=) 1.007 Männer und Frauen im Alter von 16 – 69 Jahren befragt. Die Ausfülldauer des Fragebogens betrug rund 20 Minuten. Die Datenauswertung wurde mithilfe der Statistiksoftware SPSS durchgeführt. Dabei wurden sowohl Häufigkeitsauszählungen als auch Zusammenhangsmaße berechnet.

2. HAS in Österreichs Haushalten

Prognosen verdeutlichen, dass der Umsatz von Smart Home Geräten bis 2025 in Österreich auf über 600 Million Euro steigen wird.[4] Somit werden die österreichischen Haushalte zunehmend mit internetfähigen Haushaltsgeräten versorgt. Dabei können mobile und stationäre HAS unterschieden werden, sowie jene, die sowohl mobil, also auch stationär zum Einsatz kommen. In den österreichischen Haushalten finden sich am häufigsten Smart TVs (n=583) und Sprachassistenz-Systeme (n=299). Danach folgen internetfähige Überwachungskameras (n=116) und Beleuchtungssysteme (n=87). Am seltensten sind über das Internet steuerbare Pflanzenbewässerungssysteme (n=26), Kühlschränke (n=24), Tierfutternäpfe (n=24) sowie Swimmingpools (n=16) zu finden. Nichtsdestotrotz zeigte die Studie, dass nicht alle Geräte, die besessen werden, auch im gleichen Ausmaß genutzt werden.

2.1. Nutzungsverhalten

Während sich bei rund 70 % (n=698) mindestens ein HAS Gerät im Haushalt befindet, nutzt nur rund die Hälfte der Befragten (49 %), diese auch im Alltag. Die Wahrscheinlichkeit das HAS Gerät im Haushalt auch tatsächlich zu nutzen, ist beispielsweise bei Überwachungskameras (78 %), Beleuchtungssystemen (78 %); und Heizungssystemen (76 %) verhältnismäßig höher als bei Smart TVs (64 %) und Sprachassistenten (66 %). Besonders gering ist die Nutzungswahrscheinlichkeit bei Tierfutternäpfen (29 %); Kaffeemaschinen (31 %); Waschmaschinen (35 %) und Kühlschränken (38 %). Dabei lassen sich Zusammenhänge spezifischen dem Besitz, der Nutzung der Geräte und den demografischen Merkmalen der Österreicher*innen erkennen. Diese Merkmale typischer Nutzer*innen werden im Vortrag näher diskutiert und dargestellt.

2.2. Sicherheit

Aber wie wahrscheinlich ist es, dass Hacker die Kreditkartendaten, die hinter der smarten Waschmaschine liegen hacken?

Grundsätzlich gibt es einige prominente Probleme in Bezug auf die Sicherheit von HAS. Das grundlegendste Problem ist sicher, das viele Systeme und Protokolle ursprünglich nur mit sehr geringem Bewusstsein für Security konzipiert wurden[5] und entsprechend Security als Feature erst nachgerüstet wurde (bspw. KNX). Dies ist immer sehr problematisch, da man dazu tiefgreifende Änderungen in ein fertiges System einbringen muss.

Problematisch ist auch der Verbau besonders günstiger Standardkomponenten, wie bspw. Chips mit standardmäßig angeschalteten, ungesicherten drahtlosen Schnittstellen und die fehlende Notwendigkeit der Konfiguration von Sicherheitseinstellungen. Angriffe auf Grund nicht gesetzter Passwörter bzw. nicht geänderter

[4] Statista / Digital Market Outlook, Prognose zum Smart Home Umsatz nach Segmenten in Österreich für die Jahre 2017 bis 2025.
[5] Treytl et al., Security Measures in Automation Systems – a Practice-Oriented Approach 10th IEEE International Conference on Emerging Technologies and Factory Automation Proceedings, 2005, 2, 847-855.

Standardpasswörter sind noch immer leicht möglich[6]. Auch die Steuerung des HAS per App bedarf einer Überprüfung, speziell, ob die App Sicherheitslücken aufweist und die Kommunikation zwischen HAS und App gut abgesichert ist. Eine Risikoanalyse von HAS zeigt hier Risiken sowohl in der Sicherheit von Applikationen als auch Angriffsmöglichkeiten in der Authentifizierung und Zugriffskontrolle.[7] Gerade In-House-Gateways müssen hier als zentraler Angriffspunkt besonders beachtet werden.

Ein weiteres Problem liegt in der Nutzung von Anwendungen verschiedener Hersteller*innen, vor allem wenn diese über ein Bus-System oder Netzwerk betrieben werden. Hier können schon aufgrund der Schnittstellenproblematik entsprechende Sicherheitsprobleme auftreten.

Ein wesentlicher Aspekt in Bezug auf Privacy sind auch sprachgesteuerte Geräte, müssen diese doch permanent Gespräche aufnehmen, um auf die spezifischen Stichwörter zu ihrer Aktivierung reagieren zu können. Es ist schwer zu kontrollieren, was mit den aufgenommenen Gesprächen tatsächlich gemacht wird, ob diese wirklich gleich gelöscht, oder aber für weitere Analysen, bspw. zum Zweck der Optimierung des Reaktionsverhaltens des Geräts, genutzt werden, wie entsprechende Vorkommnisse immer wieder beweisen.

2.3. Verwendung der Daten

Die Verwendung der, durch internetfähige Geräte erhobenen, Daten durch deren Hersteller*innen ist schon seit Jahren ein heiß umstrittenes Thema. Durch den Einsatz meist einfacher Computerchips wird den Objekten eine eindeutige Identität zugewiesen. Durch Funk-, Bluetooth- oder andere in der Regel kabellose Verbindungstechnologien lassen sich die einzelnen Objekte digital miteinander verbinden. In einer Studie von Deloitte (2018) wurde die deutsche Bevölkerung zum Thema Sicherheit und HAS befragt. Die Ergebnisse zeigen, dass die Sorge um den Verbleib der Nutzungsdaten gegenüber möglichen Vorteilen der Geräte noch überwiegt. „*Denn obwohl das Teilen von Nutzungsdaten eine unabdingbare Voraussetzung für intelligente Smart Home Funktionalitäten darstellt, sind nur 14 Prozent der Befragten dazu grundsätzlich bereit – und 40 Prozent lehnen es sogar ab, Nutzungsdaten zu teilen. Besonders kritisch sind hier vor allem die älteren Befragten über 65 eingestellt.*“[8] Die aktuelle Studie in Bezug auf die österreichische Bevölkerung zeigt, dass sich mehr als zwei Drittel der befragten Personen (67 %) sicher sind, dass durch HAS-Geräte Daten gesammelt werden. Angesichts dessen, wünscht sich der Großteil der Befragten (90 %), eine rechtliche Regelung, die Hersteller*innen dazu verpflichtet, die Sammlung und Verwendung dieser Nutzungsdaten offenzulegen. Im Vortrag wird näher darüber informiert wann und wie sich die Österreicher*innen über die Sammlung von Daten und die Sicherheitsschwachstellen ihrer HAS-Geräte informieren.

3. Fazit

3.1. Der allgemeine Ausblick

Bereits im Jahr 2020 nutzen 37% der Verbraucher*innen[9] Smart-Home-Anwendungen. 49% dieser Verbraucher*innen würden gerne alle technischen Geräte vernetzen und digital steuern. Dieses Bedürfnis wird in Zukunft stark steigen. Das Smart Home wird mehr sein, als nur Lampen, die via App gesteuert werden, sondern Geräte werden vernetzt sein und über eine gemeinsame Plattform gesteuert werden. Smart Home wird das Leben komfortabler, sicherer und klimafreundlicher gestalten und die Möglichkeit bieten, länger selbstbestimmt alleine wohnen zu können. Funktionen werden, je nach Bedarf, als Applikation angeboten werden und so HAS flexibel erweitern.

---

6 Knieriem et.al., An Overview of the Usage of Default Passwords (extended version) Lecture Notes of the Institute for Computer Sciences · January 2018, DOI: 10.1007/978-3-319-73697-6_15.

7 Jacobson et. al., On the Risk Exposure of Smart Home Automation Systems, *2014 International Conference on Future Internet of Things and Cloud*, Barcelona, 2014, pp. 183-190, doi: 10.1109/FiCloud.2014.37.

8 Deloitte, Smart Home Consumer Survey 2018, ausgelesen am: 15.10.2020, https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/smart-home-studie-2018.html.

9 Bitkom Research Studie Smart Home 2020 / 09/2020, ausgelesen am 27.10.2020, https://www.bitkom-research.de/de/Smart-Home-2020.

3.2. Die Privatsphäre

Entsprechende Sicherheitsfunktionen sind die Grundlage für die Nutzung von Funktionen und Diensten (Services) im vernetzten Smart Home. Um Angriffe auf die Nutzer*innen zu verhindern, müssen Sicherheitsempfehlungen, wie in diesem Beitrag beschrieben, eingehalten werden. Insbesondere in Bezug auf die Privatsphäre der Nutzer*innen variiert dies aktuell jedoch stark zwischen den Anwendungen mit unterschiedlicher Datennutzung und Sicherheit. Es muss kritisch angemerkt werden, dass durch die Vernetzung persönlicher Daten eine systemisch bedingte Transparenz der Nutzer*innen geschaffen wird.

Es benötigt daher auch Normung und Prüfstellen, die ein Mindestniveau an Sicherheit und Privatsphäre garantieren. Trotzdem muss den Nutzer*innen aber bewusst sein, dass es keine absolute Sicherheit geben kann außer man verzichtet zur Gänze auf die Annehmlichkeiten des Smart Home, um z.B. das Risiko eines Datendiebstahls über das Smart Home auszuschließen.

3.3. Anforderung an Sicherheitsforschung und Regulation

Die Anforderung an die Sicherheitsforschung in diesem Bereich ist die laufende Evaluierung der Maßnahmen hinsichtlich ihrer Sicherheitsqualität. Der Beitrag der Forschung wird auch zukünftig darin bestehen, durch eine tiefgehende Analyse und Untersuchung der einzelnen Komponenten und des Gesamtsystems im Rahmen einer Risikoanalyse, Schwachstellen frühzeitig zu erkennen und neue Lösungen zu erforschen.

4. Literatur

Bitcom Research Studie Smart Home 2020/09/2020, ausgelesen am 27.10.2020, https://www.bitkom-research.de/de/Smart-Home-2020.

Deloitte, Smart Home Consumer Survey 2018, ausgelesen am: 15.10.2020, https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/smart-home-studie-2018.html

Jacobson et. al., On the Risk Exposure of Smart Home Automation Systems, *2014 International Conference on Future Internet of Things and Cloud*, Barcelona, 2014, pp. 183-190, doi: 10.1109/FiCloud.2014.37.

Knieriem et.al., An Overview of the Usage of Default Passwords (extended version) Lecture Notes of the Institute for Computer Sciences January 2018, DOI: 10.1007/978-3-319-73697-6_15

Pirbhulalp S et al.: A novel secure IoT-based smart home automation system using a wireless sensor network. Sensors 17(1), 69 (2016)

Statista / Digital Market Outlook, Prognose zum Smart Home Umsatz nach Segmenten in Österreich für die Jahre 2017 bis 2025, ausgelesen am: 13.10.2020, https://de-1statista-1com-1wy4rx2cg094f.han3.donau-uni.ac.at/prognosen/801529/smart-home-umsatz-nach-segmenten-in-oesterreich

Treytl et. al., Security Measures in Automation Systems – a Practice-Oriented Approach 10th IEEE International Conference on Emerging Technologies and FactoryAutomation Proceedings, 2005, 2, 847-855

Wilson et al.: Benefits and risks of smart home technologies. Energy Policy 103, 72-83 (2017).

5. Danksagung

Diese Arbeit wurde im Rahmen des Projektes ARES – Angriffsresiliente IoT-basierte Sensoren in der Heimautomation – durchgeführt. Dieses Projekt wird von der NFB, der Niederösterreichischen Forschungs- und Bildungsgesellschaft gefördert.