-Smart Home-

Auswirkungen von Smart Home Technologien im privaten Bereich

Forschungsfrage

Welche sozialen, politischen und ethischen Auswirkungen können Smart-Home-Technologien im privaten Einsatz mittel- und langfristig haben?

Das Projekt fokussiert sich dabei auf den Einsatz von Smart-Home Technologien im engeren Sinn, d.h auf den Einsatz solcher Technologien im privaten Wohnbereich.

Definition

Elektronische Systeme, die in Wohnungen und Häusern Haushaltsgeräte, Unterhaltungselektronik, Haushalts-installationen, digitale Assistenten und Sicherheitstechnik vernetzen, automatisieren, und remote über das Internet zugänglich machen [1].

Methode

Methode "Szenarioentwicklung" unter Berücksichtigung gesellschaftlicher Entwicklungsdimensionen.

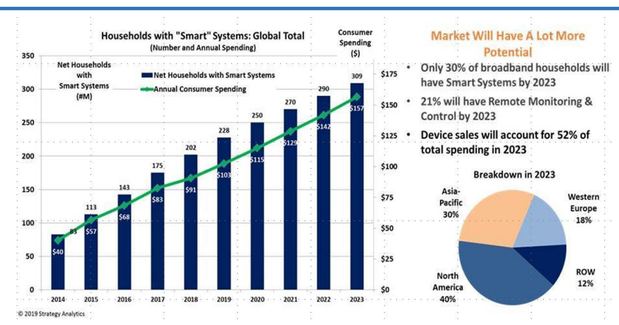
„Quantitative Daten und Information werden mit qualitativen Informationen, Einschätzungen und Meinungen verknüpft, so dass als Ergebnis detaillierte Beschreibungen einer bzw. mehrerer möglichen Zukunftssituationen unter ganzheitlichem Aspekt entstehen“ [2. S. 12]

Schritt 1: Horizon Scanning

(Extrapolierung des aktuellen Trends)

Extrapolation des aktuellen Trends

- Smart Home-Technologien werden voraussichtlich vermehrt zum Einsatz kommen [6], [9], [10]
- Bei unveränderten Rahmenbedingungen werden die aktuell bereits bestehenden Datenschutz- und Sicherheitsprobleme weiter zunehmen. [3], [4], [5]
- Inkompatibilitäten zwischen den Herstellern bewirken ein "Lock in" der Anwender auf bestimmte Hersteller (mit allen damit verbundenen praktischen und ökonomischen Effekten). [9]



Datenschutz

- Smart-Speaker
  - Abhören von privaten Gesprächen [14]
- Smart-TV
  - Überwachung des Videokonsums,
  - Abhören von privaten Gesprächen
  - heimliche Videoüberwachung [15], [17]
- "Smarte" Internet-Sicherheitsanlagen
  - Heimliche Videoüberwachung [4]

Persönliche Sicherheit

- Smart-Locks
  - Gefahr des Hackens [11], [12]
  - Gefahr, aussperrt zu werden [12]
- Alarmanlage mit Internetanschluss
  - viele Alarmanlagen mit Internetanschluss können einfach deaktiviert werden [3], [4]
- Smart-Meter
  - Hacking: Gefahr für Grid-Stabilität [4]

Obsoleszenz

- Smart-Speaker
- Smart-TV
- Smart-Bulbs

Funktionieren allesamt nicht mehr (oder nur eingeschränkt), wenn der Hersteller die Server nicht mehr betreibt. [16], [18], [19]

Schritt 2: 360° Envisioning

(Langzeitwirkung, Identifikation Schlüsselfaktoren)

Zu erwartende Auswirkungen

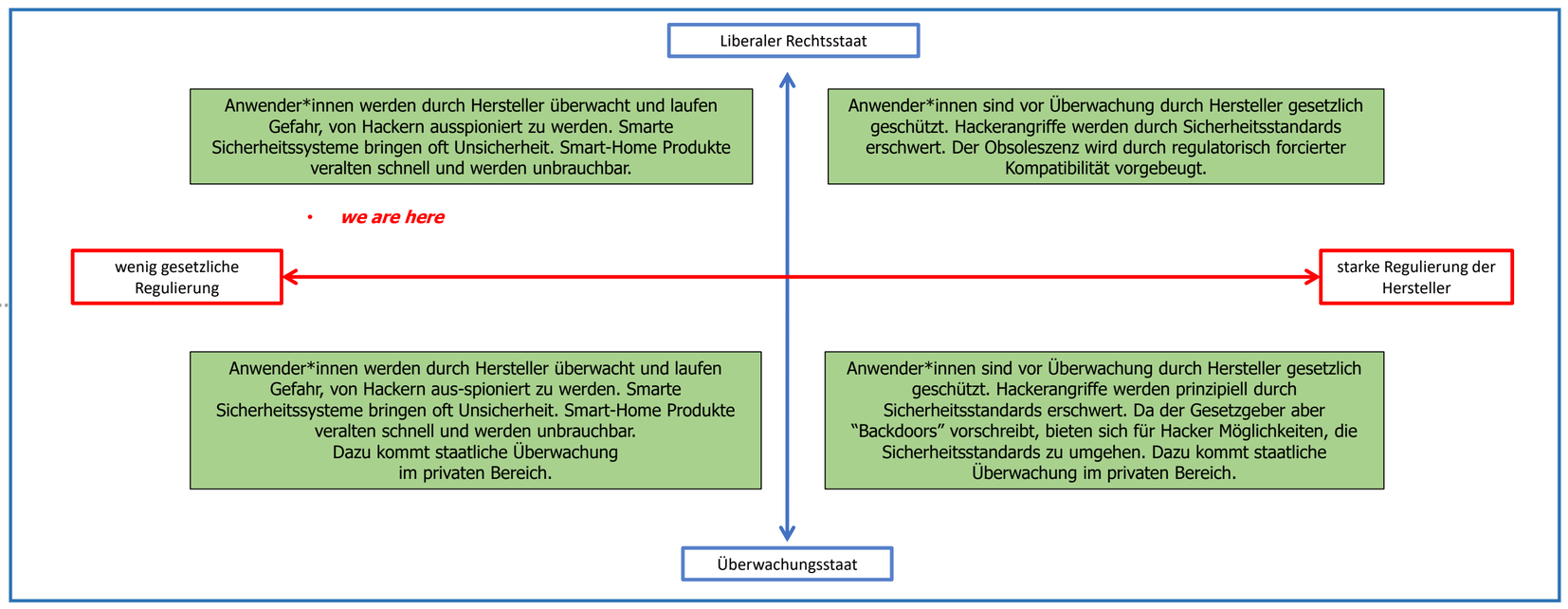
- Eindringens in die Privatsphäre von Anwender*innen durch Hersteller, staatliche Institutionen oder Hacker
- Sicherheitsprobleme ("unsichere" Sicherheitsanlagen) [3]
- Obsoleszenzeffekte [16], [18], [19]

Schlüsselfaktoren

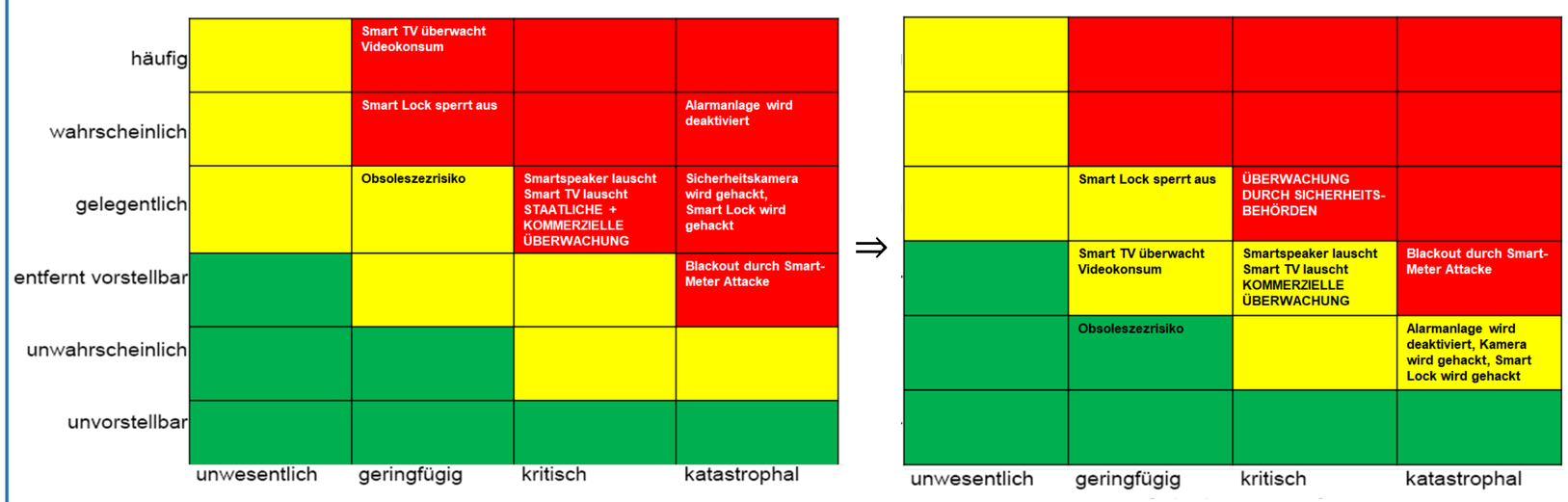
- Gesetzgebung und Regulierung (Einwirkung auf Hersteller)
- Gesellschaftliche Entwicklung (Überwachungsstaat?)
- Gesetzlicher Umgang mit Datenschutzangelegenheiten

Schritt 3: Szenarioentwicklung

(zwei „Szenario-Achsen“)



Risikoreduzierung durch gesetzliche Regulierung und Stärkung des Rechtsstaats



Reflexion und Empfehlungen

- Regulierer auf supranationaler Ebene (EU-Kommission, Internationale Normierungsinstitutionen) sollten möglichst rasch *verbindliche und durchsetzbare* Sicherheitsstandards für „Smart-Home“-Produkte verabschieden.
- Es muss beim Gesetzgeber Bewusstsein für Datensicherheitsprobleme im Zusammenhang mit Smart-Home Produkten geschaffen werden.
- Es muss Bewusstsein in der Öffentlichkeit für die Gefahr der präventiven Überwachung im privaten Bereich durch staatliche und nichtstaatliche Stellen mittels „Smart-Home“ Systemen geschaffen werden.

Referenzen

[1] M. Chana, D. Estève, C. Escriba und . Campo, “A review of smart homes—Present state and future challenges” in “Computer Methods and Programs in Biomedicine”, Vol 91, Issue 1, July 2008, Pages 55-81
[2] O. Albers, A. Broux, “Zukunftswerkstatt und Szenariotechnik: ein Methodenbuch für Schule und Hochschule“, Beltz, 1999.
[3] J. Merkert und S. Hansen, “Smart Alarm - Sechs vernetzte Alarmanlagen im Test” in c’t 3/2017, S. 90
[4] N. Jurran, “Hintereingang inklusive - Fatales Sicherheitsleck beim Smart-Home-System von Loxone” in c’t Magazin für Computertechnik 19/2016, S. 72
[5] O. Ur-Rehman, N. Zivic und C. Ruland, "Security issues in smart metering systems," 2015 IEEE International Conference on
Smart Energy Grid Engineering (SEGE), Oshawa, ON, 2015, pp. 1-7, doi: 10.1109/SEGE.2015.7324615.
[6] N. Balta-Ozkana, B. Botelerb, O. Amerighic, “European smart home market development: Public views on technical and economic aspects across the United Kingdom, Germany and Italy”, doi: 10.1016/j.erss.2014.07.007
[7] T. Hargreaves, C. Wilson (2017) Perceived Benefits and Risks of Smart Home Technologies. In: Smart Homes and Their Users. Human–Computer Interaction Series. Springer, Cham. DOI: 10.1007/978-3-319-68018-7_3
[8] A. Jacobsson, M. Boldt, B. Carlsson, A risk analysis of a smart home automation system, Future Generation Computer Systems, Volume 56, 2016,
S. 719-733
[9] S. Kozubaev, F. Rochaix, C. F. DiSalvo, C. A. LeDantec. Spaces and Traces: Implications of Smart Technology in Public Housing.
Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, May 2019, Paper No.: 439, S. 1–13, DOI: 10.1145/3290605.3300669
[10] W. Ablondi, J. Narcotta, “2019 Global Smart Home Forecast - September 2019”,Strategy Analytics Report September 2019
[11] C. Dardaman, Breaking & Entering with Zipato SmartHubs, https://blackmarble.sh/zipato-smart-hub/
[12] E. Fernandes, J. Jung and A. Prakash, "Security Analysis of Emerging Smart Home Applications," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2016, pp. 636-654, doi: 10.1109/SP.2016.44.
[13] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," in IEEE Security & Privacy, vol. 7, no. 3, pp. 75-77, May-June 2009, doi: 10.1109/MSP.2009.76.
[14] J. Lau, B. Zimmerman, F. Schaub, “Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers”, Proceedings of the ACM on Human-Computer Interaction, November 2018, Article No.: 102, doi: 10.1145/3274371
[15] S Lee, S Kim : “Hacking, surveilling and deceiving victims on smart tv”, Blackhat Briefing 2013 (2013)
[16] Jonas: “Das wars: Keine Unterstützung mehr der 1. Philips Hue Bridge Generation” https://www.smartlights.de/licht/philips-hue/das-wars-keine-unterstuetzung-mehr-der-1-philips-hue-bridge-generation/ (Mai 2020)
[17] B. Michéle and A. Karpow, "Watch and be watched: Compromising all Smart TV generations," 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, 2014, pp. 351-356, doi: 10.1109/CCNC.2014.6866594.
[18] M. Moon: “Samsung's older smart TVs are losing remote control app support”, https://www.engadget.com/samsung-killing-smart-view-app-103148010.html
[19] A. Villas-Boas: “Netflix will soon stop working on some older Samsung smart TVs”, Nov, 2019, https://www.businessinsider.de/international/netflix-stop-working-old-samsung-smart-tvs-december-1-2019-11

WS 2020/21 - Folgen des technischen Fortschritts

Einführung in die Theorie und Praxis der Technikfolgenabschätzung (TA)

Gruppennummer: Gruppe J

Gruppenmitglieder:
Helmut Hörner, Dragan Božic

TU WIEN TECHNISCHE UNIVERSITÄT WIEN

ÖAW ITA INSTITUT FÜR TECHNIKFOLGEN ABSCHÄTZUNG