



Smart Home aus der Angstecke holen



Ein Geist, der das Smart Home bedroht und von den drei Experten betrachtet wird.

Günter Martin, Mitglied des Vorstands der Smart Home Deutschland Initiative, Geschäftsführer CorDev GmbH

Fast die Hälfte der Deutschen ist sehr skeptisch gegenüber Smart Homes, weil sie Angst vor Hackern haben. Die Angst ist sachlich unbegründet. Dies zu sagen oder statistisch zu beweisen, reicht meist nicht aus. Die Angst sitzt tiefer. Man traut sich die digitale Teilhabe nicht zu. Weder beim Smart Home noch – und das ist schlimmer – im beruflichen und sozialen Umfeld. Dabei braucht gerade ein Smart Home kaum digitale Kompetenz, wenn es richtig gemacht ist. Es kann mithelfen, dass Nutzer Vertrauen und Selbstvertrauen in digitale Technik bekommen und so Zugang zur digitalen Teilhabe finden.

Wie kann man die Angst fundiert und überzeugend nehmen, um damit nicht nur Smart Homes voranzubringen, sondern auch mehr Menschen einen Einstieg in die digitale Teilhabe zu geben? Dazu gibt es Überlegungen aus Hersteller-, Security- und Wissenschaftssicht, die beim Smart Living Summit diskutiert wurden und in diesem Beitrag zusammengefasst sind.

Herstellersicht: Den Nutzer individuell abholen mit KI

Prof. Dr. Reiner Wichert, Professor an der Hochschule Darmstadt (Fachbereich Informatik), Gesellschafter uCORE Systems GmbH

Natürlich müssen die Systeme sicher und zuverlässig sein. Dafür gibt es Gesetze, Normen und Standards, die seitens der Hersteller eingehalten werden müssen. Hingegen ist nicht vorgeschrieben, dass der Nutzer mit dem System klarkommen muss. Tatsächlich wird der Nutzer eher außen vorgelassen.

Digitale Systeme im Wohnumfeld erfüllen häufig nicht die Anforderungen der Bewohner, was zu Unzufriedenheit führt. Heizungen werden falsch gesteuert, die Gebäudeautomation funktioniert

nicht zuverlässig und Alarmanlagen erzeugen unnötige Fehlalarme. Dadurch erscheinen Smart Home-Systeme oft nur für Technikbegeisterte sinnvoll. Ein wesentlicher Grund dafür ist, dass jedes System individuell an die Bedürfnisse und das Verhalten der Bewohner angepasst werden muss. Der Hersteller kennt weder die konkrete Situation im Zuhause noch das spezifische Nutzerverhalten und auch der Installateur kann das Verhalten nur grob einschätzen. Zudem fehlt den meisten Bewohnern die Zeit oder das Wissen, Systeme selbst zu programmieren.

Ein zentrales Problem ist das Fehlen eines allumfassenden Systems, das durch Künstliche Intelligenz (KI) die verschiedenen digitalen Elemente im Wohnumfeld miteinander verbindet. Der Einsatz von KI kann dazu beitragen, diese Systeme an die individuellen Bedürf-



nisse der Bewohner auch mit Informationen von außen, wie Wetterdaten oder Strompreisen, anzupassen und deren Effizienz kontinuierlich zu verbessern. Dafür sind jedoch umfassende KI-Modelle notwendig, die nicht nur die technischen Abläufe verstehen, sondern auch das Verhalten und die Gewohnheiten der Bewohner berücksichtigen. Ein solches System kann zur Steigerung der Energieeffizienz beitragen, indem es den Energieverbrauch optimiert. Beispielsweise kann KI durch situationsabhängige Steuerung von Heizung und Belüftung den Energieverbrauch senken, wie das uCORE Systems in Weiterstadt im dortigen Wohn- und Quartierzentrum beweisen konnte, wobei 56 Prozent Gas eingespart wurden.

Das dortige System kann auch Notfallsituationen zuverlässig erkennen und somit bei der Pflege älterer oder pflegebedürftiger Menschen eine wichtige Rolle spielen. Durch intelligente Notfallerkennung konnte die Zahl erkannter echter Notfälle um 20 Prozent gesteigert und Fehlalarme um 60 Prozent reduziert werden. Im Mittelpunkt stehen dabei die Erkennung von Stürzen, ein überlanger Badaufenthalt, kein Aufstehen morgens, keine Rückkehr in die Wohnung oder keine Rückkehr ins Bett beim nächtlichen Toilettengang, wobei das System durch einen einzigartigen Bestätigungsmechanismus der Bewohner direkt an den Hausnotruf angebunden werden darf.

Das System wird zusätzlich im BMBF-Projekt AI4ActiveAge, das von der Hochschule Darmstadt koordiniert wird, eingesetzt. uCORE Systems ist AI4ActiveAge-Projektpartner mit dessen Expertise aus der Energie- und Bauwirtschaft und bringt alle Voraussetzungen um das Thema Digitalisierung in der Wohnungswirtschaft mit. Hier ist entscheidender Aspekt, dass beim Einsatz von Künstlicher Intelligenz im Wohnumfeld, der Schutz der Privatsphäre der Bewohner in höchstem Maße berücksichtigt wird. Um diesem hohen Anspruch gerecht zu werden, erfolgt die Auswertung aller relevanten Daten direkt auf dem zentralen Wohnungscontroller, der lokal im Haushalt installiert ist. Dies bedeutet, dass keine sensiblen Informationen an externe Server gesendet werden, wodurch das Risiko einer unbefugten Datenweitergabe oder -abfrage erheblich reduziert wird. Zusätzlich wird der Controller mit fortschrittlichen Sicherheitsmechanismen ausgestattet, die eine zuverlässige IT-Sicherheit gewährleisten. Dies umfasst Verschlüsselungstechnologien, Verhaltensanalyse von Geräten, Zugriffskontrollen und regelmäßige Sicherheitsupdates, um sowohl die Datenintegrität, den Geräteschutz, als auch die Vertraulichkeit zu schützen. Auf diese Weise kann ein hohes Maß an Daten- und Geräteschutz gewahrt werden, während gleichzeitig die Vorteile von KI-gestützten Systemen im Wohnumfeld voll ausgeschöpft werden.

In Zukunft wird erwartet, dass der Einsatz von KI zur Überwachung und Unterstützung individueller Verhaltensmuster im Wohnumfeld einen milliardenschweren Markt bildet.

Securitysicht: Vertrauen schaffen mit dem deutschen IT-Sicherheitskennzeichen

Joshu Wiebe, Referatsleiter IT Sicherheitskennzeichen bei Bundesamt für Sicherheit in der Informationstechnik (BSI)

Mit dem IT-Sicherheitskennzeichen gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Herstellern ein unkompliziertes Instrument an die Hand, um IT-Sicherheit zum Kaufargument zu machen. Sie können damit ihre Produkte auszeichnen und am Markt hervorheben. Verbraucher können so auf den ersten Blick erkennen, wenn Hersteller ihre Produkte sicher gestalten.

Gleichzeitig ist das Kennzeichen eine gute Vorbereitung auf die bevorstehende Regulierung durch den Cyber Resilience Act der EU (CRA). Die bestehenden Sicherheitsanforderungen des IT-Sicherheitskennzeichens werden sukzessive auf die Schutzziele des CRA ausgerichtet, sodass Hersteller schon jetzt damit beginnen können, diese in ihre Produktentwicklung zu integrieren. So können sich Hersteller auf die bevorstehende Regulierung vorbereiten und gleichzeitig das Vertrauen in ihre Produkte stärken. Gemeinsam mit Wirtschaft und Gesellschaft wird das BSI die Sicherheitsanforderungen des Kennzeichens im CRA-Kontext (fort-)entwickeln. Das so gewonnene Feedback kann perspektivisch als Orientierung für harmonisierte Standards oder Umsetzungsempfehlungen auf europäischer Ebene eingebracht werden.

Das BSI gestaltet mit dem IT-Sicherheitskennzeichen die internationale Labelling-Landschaft und treibt dessen Harmonisierung gemeinsam mit anderen Nationen voran. Mit der Cyber Security Agency von Singapur (CSA) hat das BSI ein Anerkennungsabkommen geschlossen. So erhalten Hersteller mit IT-Sicherheitskennzeichen unkompliziert das Cybersecurity Label aus Singapur auf Level zwei in den Produktkategorien Smarte Verbrauchergeräte und Breitbandrouter.

Im September 2024 wurde ein Letter of Intent (LoI) mit der Korea Internet & Security Agency (KISA) aus Südkorea geschlossen, um die Zusammenarbeit auf dem Gebiet der Kennzeichnung zu stärken und auszubauen.

Das deutsche Kennzeichen ist außerdem als Referenzschema im Normungsvorhaben ISO 27404 (Universal Cybersecurity Labelling Framework) benannt und damit Vorbild für andere Schemata weltweit. Derzeit kann das IT-Sicherheitskennzeichen für die Produktkategorien Breitbandrouter, E-Mail-Dienste, mobile Endgeräte, Videokonferenzdienste und die meisten IoT- und Smart Home-Produkte beantragt werden.

Bei Fragen zum Kennzeichen oder dem Antragsprozess berät das BSI gerne. Ausführliche Informationen



TECHNIK + INNOVATION

zur Funktionsweise des IT-Sicherheitskennzeichens und das Antragsverfahren gibt es auf der Website des BSI:

www.bsi.bund.de/it-sik/antrag

Info

www.bsi.bund.de/it-sik/antrag



Wissenschaftliche Sicht: Digitalkompetenz steigern

**Dr. Rahild Neuburger, Akad. Oberrätin
an der LMU Munich School of Management**

Nutzer trauen sich nicht an Smart Home und komplexere digitale Anwendungen, weil Digitalkompetenzen fehlen. Was ist das und wie kann man sie entwickeln?

Digitalkompetenzen werden unterschiedlich definiert. Im vorliegenden Kontext sehen wir sie als Fähigkeiten, die eine Teilhabe an einer digitalen Gesellschaft ermöglichen. Hierzu zählen Kenntnisse wie der „Umgang mit Informationen und Daten“, „Kommunikation und Zusammenarbeit“, „Erzeugen von digitalen Inhalten“, „Sicherheit“ sowie „Probleme lösen“. Nach einer aktuellen Untersuchung des BSI gehört Deutschland im internationalen Vergleich zum Schlusslicht. Je mehr digitale und smarte Technologien im häuslichen Umfeld eingesetzt werden, desto wichtiger ist jedoch der Aufbau von Kompetenzen gerade im Bereich Sicherheit. Allerdings ist der Nutzen hier jedoch nur indirekt vorhanden. So führen Kompetenzen im Bereich Kommunikation zu einem spürbaren Mehrwert, wenn effizienter mit einer größeren Gruppe kommuniziert werden kann. Dagegen führen Kompetenzen im Bereich Sicherheit dazu, dass alle Prozesse reibungsfrei ablaufen, dass also nichts passiert. Die Effekte des Kompetenzaufbaus sind somit nicht direkt gegeben, sondern indirekt. Fehlen die Kompetenzen, kann es zu einem Ausfall oder zu Sicherheitsproblemen führen. Dies erschwert die bewusste Auseinandersetzung und den Anreiz, sich hiermit auseinanderzusetzen.

Insofern reicht die reine Entwicklung von Skills nicht. Erforderlich sind vielmehr:

(1) Aufbau von Wissen:

Zunächst gilt es, ein Bewusstsein für Sicherheitsprobleme zu schaffen und klar zu kommunizieren, warum die Auseinandersetzung mit dem Thema Sicherheit wichtig ist. Dies umso mehr, da in Deutschland 61 Prozent der befragten Personen der Meinung sind, dass dem Thema Digitalisierung zu wenig Aufmerksamkeit geschenkt wird (in anderen Ländern unter 30 Prozent der Befragten). Angesprochen sind hier insbesondere Medien, Politik, Schulen und Bildungseinrichtungen, Kommunen und Familien. Ziel muss es sein, das Bewusstsein zu schärfen, dass das Leben und Bewegen in der digitalen Welt normal ist. In der analogen Welt können wir uns einigermaßen sicher bewegen. Das selbe sollte in der digitalen Welt gelingen.

(2) Entwicklung von Fähigkeiten:

Ziel ist es, durch den Zugang zu geeigneten Weiterbildungsmaßnahmen notwendige Kompetenzen und Fähigkeiten aufzubauen. Diese betreffen insbesondere grundlegende technische Anwendungskompetenzen, Skills im Bereich von Datenschutz und Datensicherheit sowie persönliche Kompetenzen wie insbesondere Bewusstsein für Sicherheitsprobleme, Beurteilungsfähigkeit sowie selbstverantwortliches Agieren. Je problem- und zielgruppenorientierter diese Kompetenzen aufgebaut werden können, desto höher ist der Anreiz, sich damit auseinanderzusetzen. Der Einsatz technologischer Hilfsmittel wie insbesondere VR-Brillen, Micro-Learning oder individualisierte KI-gestützte Lernpfade können hier hilfreich sein.

(3) Empowerment zur Umsetzung

Schließlich gilt es, die Betroffenen zu ermutigen, sich mit Sicherheitskompetenzen auseinanderzusetzen und diese auch in ihren individuellen Gewohnheiten zu integrieren. Nur dann entfalten die gelernten Fähigkeiten aus Punkt (2) tatsächlich ihren Nutzen. Realisieren lässt sich dies durch positive Use-Cases, die den Mehrwert von Security im privaten Umfeld zeigen, finanzielle Anreize beispielsweise bei Abomodellen von Smart Home-Dienstleistungen, konkrete Unterstützungsangebote durch Unternehmen und Kommunen, benutzerfreundliche technische Lösungen, Texte und Gebrauchsanweisungen oder auch hier den Einsatz von KI, Chatbots oder neuartigen Lernformaten.

Zusammenfassend wird deutlich: Beim Aufbau digitaler Kompetenzen hat Deutschland Nachholbedarf. Dies gilt insbesondere für Kompetenzen im Bereich Sicherheit, deren positive Effekte nicht direkt erkennbar sind. Umso wichtiger sind Maßnahmen zur Schärfung des Bewusstseins, zur Entwicklung von konkreten Fertigkeiten und zur Ermutigung zur Auseinandersetzung mit relevanten Kompetenzen und deren Umsetzung in die eigenen Gewohnheiten und Verhaltensweisen. Ziel sollte bei allen Maßnahmen sein, das Selbstvertrauen der Nutzenden zu stärken, dass sie mit Smart Home-Anwendungen kompetent und sicher umgehen können. Denn die Nutzenden müssen nicht nur in die Technik, sondern auch in sich selbst vertrauen.



Ein Geist, der das Smart Home bedroht.

Fotos: Günter Martin mithilfe von KI Firefly