Unter Smart Home versteht man einen Haushalt, bei dem eine Vielzahl von Geräten vernetzt sind und zu „intelligenten“ Gegenständen werden. Die Liste möglicher Geräte umfasst:

- Haushaltsgeräte (z. B. Kühlschrank, Waschmaschine, Staubsauger)
- Geräte der Hausautomation (z. B. Heizung, Beleuchtung, Belüftung)
- Unterhaltungselektronik bzw. Kommunikationseinrichtungen (z. B. TV, Spielekonsolen)
- (z. B. Alexa, Google Home)

Durch die Vernetzung dieser und die Kombination mehrerer solcher Gegenstände werden neue Funktionen und Dienste möglich, die gegenüber dem einzelnen Gegenstand einen Mehrgewinn bieten.

Smart Home Anwendungen bringen daher eine Reihe von Verbesserungen mit sich:

- Erhöhung von Wohn- und Lebensqualität: z. B. automatisierte Beleuchtungssteuerung oder beim Kühlschrank durch das Erkennen von Nahrungsengpässen.
- Optimierung von Gerätenutzung: z. B. bedarfsgerechter Einsatz von Heiz- und Kühlenergie.
- Gebäudeschutz: z. B. durch individuelle Profile, die das Ein- und Ausschalten des Lichts steuern oder die Verknüpfung von Sensoren und Kameras.
- Vereinfachte Bestell- und Steuerungsprozesse: z. B. mit Hilfe von Sprachassistenten.
- Automatisierte Nutzung von Haushaltsgeräten abhängig von der Verfügbarkeit von eigenerzeugter Energie oder abhängig von einem variablen Energiepreis.

Studien zeigen, dass viele Nutzer von Smart Home Geräten und Anwendungen davon ausgehen, dass Ihre Geräte bereits per Default – also vor dem Kauf – maximalen Schutz Ihrer Privatsphäre bzw. Sicherheit bieten. Diese Annahme ist aus folgenden Gründen problematisch:

Es gibt Hersteller, die keinen maximalen Schutz bieten können oder wollen; z. B.

- sind manche Hersteller an den zusätzlichen Daten, die erhoben werden, interessiert, um diese gewinnbringend zu verkaufen;
- haben sich manche Hersteller bewusst dagegen entschieden, einen möglichst guten Schutz zu bieten, denn maximale Privatsphäre bzw. Sicherheit geht mit hohen Kosten sowie mit Einbußen in der Funktionalität einher;
- sind manche Hersteller zwar motiviert einen möglichst hohen Schutz zu bieten, aber sind wegen der Komplexität der Infrastruktur und den Möglichkeiten des Angreifers gar nicht in der Lage, dies zu leisten.

Kontakt

Karlsruher Institut für Technologie (KIT)

Institut für Angewandte Informatik und
Formale Beschreibungsverfahren (AIFB)

Forschungsgruppe Security • Usability • Society (SECUSO)

Prof. Dr. Melanie Volkamer
Kaiserstraße 89, Gbd. 05.20
76133 Karlsruhe

Telefon: +49 721 608 450 45
E-Mail: kontakt@secuso.org

secuso.aifb.kit.edu
twitter.com/secusoresearch

Herausgeber

Karlsruher Institut für Technologie (KIT)

Präsident Professor Dr.-Ing. Holger Hanselka
Kaiserstraße 12
76131 Karlsruhe
www.kit.edu

Dieser Inhalt wurde im Europäischen Union Horizon 2020 Forschungs- und Innovationsprogramm unter der Zuwendungsvereinbarung Nr. 740923, Projekt GHOST (Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control) entwickelt.

Karlsruher Institut für Technologie

aifb

Smart Home

Mehr über Sicherheits- und Privatsphärenrisiken erfahren

INSTITUT FÜR ANGEWANDTE INFORMATIK UND FORMALE BESCHREIBUNGSVERFAHREN (AIFB)

SECUSO
SECURITY · USABILITY · SOCIETY

KASTEL

Sicherheit und Privatsphäre können auf unterschiedliche Arten gefährdet werden. Im Folgen werden die unterschiedlichen Risiken erläutert:

Sicherheitsrisiken

Hacker können Ihnen auf vielfältige Art und Weise schaden: Wenn Hacker sich Zugriff auf Ihre Smart Home-Geräte verschafft haben, können diese Daten und Informationen, die in den Geräten hinterlegt oder mit diesen erzeugt werden, ausspähen. Darüber hinaus können Hacker Ihre Smart Home-Geräte dann kontrollieren und auch umkonfigurieren und so z. B.

- Kontrolle über Kameras oder andere Sensoren übernehmen (dadurch können z. B. sensible Daten wie Videos oder Fotos von Ihnen erfasst werden),
- Raumtemperaturen stark verändern (dadurch leiden z. B. Ihre Pflanzen oder Tiere im Haus),
- Kühl- bzw. Gefrierschrank abschalten oder Nahrungszubereitungsgeräte manipulieren (dadurch verderben z. B. Lebensmittel oder Wasser kann in Ihre Küche laufen),
- Rauchmelder manipulieren (dadurch werden z. B. spontan und ohne Grund laute Geräusche verursacht),
- Waschmaschinen- und Trocknerprogramme modifizieren (dadurch wird z. B. Ihre Kleidung zerstört oder Ihre Wasser- und Stromrechnung wird erhöht),
- Verbundene Geräte stark überlasten (dadurch wird die Lebensdauer verringert oder das Gerät kann sogar zerstört werden),
- Türen und Fenster öffnen (dadurch wird z. B. die Raumtemperatur beeinflusst oder Unbefugte können in Ihr Heim eindringen),
- Kontrolle über Geräte der Fernwartung z. B. Smart Meter übernehmen (dadurch können z. B. Geräte im Haus ein-/ausgeschaltet oder falsche Daten an den Versorger übermittelt werden).

Privatsphärenrisiken

Die Hersteller der Smart Home-Geräte sammeln eine Vielzahl von Daten und Informationen, z. B. Kreditkarten, Online-Einkäufe, aktuelle Raumtemperatur, getätigte Suchanfragen, Lichtaktivität, Gewicht oder innerhäusliche Bewegungen. Dies ist im besten Fall alles notwendig, um die gewünschte Funktionalität zu bieten.
Ihre Nutzungsgewohnheiten können aber auch aus diesen Daten abgeleitet werden (z. B. an welchen Tagen Sie wann Licht und Heizung einschalten, wann Sie Wäsche machen, welche Lebensmittel online einkaufen oder Ihre Präferenzen bei Sendungen). So können die Hersteller umfangreiche Nutzungsprofile von Ihnen erstellen. Diese werden von den Herstellern Ihrer Geräte bzw. ihrer Smart Home Anwendungen dafür verwendet, die Dienste zu verbessern.
Wenn die gesammelten Daten und die erstellten Nutzungsprofile allerdings in die Hände Dritter geraten (z. B. weil Kriminelle sich in die Systeme des Herstellers hacken i. d. R. weil diese nicht ausreichend geschützt sind) oder von dem Hersteller entgegen Ihrer Erwartungen für weitere Zwecke verwendet werden, kann Ihnen auf vielfältige Art und Weise Schaden entstehen.

Beispiele hierfür sind:

Die Kombination von Lichtaktivität, Temperaturregelung und Stromverbrauch können genutzt werden, um gezielt Einbrüche durchzuführen.

Ihre Gesundheitsdaten (z. B. Krankenakte, aktuelle Blutdruckwerte, einzunehmende Medikamente) können, wenn sie an Ihren derzeitigen oder potenziellen Arbeitgeber weitergegeben werden, dazu führen, dass Sie schlechtere Chancen bei der Bewerbung auf einen neuen Job haben oder dass Sie gekündigt werden.

Ihre Gesundheitsdaten können, wenn sie an Ihre Bank weitergegeben werden, dazu führen, dass Sie schlechtere Konditionen für einen Kredit erhalten.

Ihre persönlichen Präferenzen können, wenn sie an andere Unternehmen weitergegeben bzw. verkauft werden, genutzt werden, um Sie gezielt in Ihrer Kaufentscheidung zu beeinflussen oder Produkte, die Sie sehr wahrscheinlich kaufen werden, teurer zu machen.

Ihre Daten über Ihre Wohnverhältnisse (z. B. durch Kartographierung Ihrer Wohnung) können genutzt werden, um Rückschlüsse auf Ihre finanzielle Situation zu ziehen und somit zu teureren Zinsen z. B. im Versandhandel führen.

Ihre Lokationsdaten können, wenn sie bei Dritten landen, dazu führen, dass Sie ein Opfer von Stalking werden.

Ihre Präferenzen bzgl. Sendungen im Fernsehen und Internet und Ihre Kommunikationsdaten können dazu genutzt werden, Sie in Ihren Entscheidungen z. B. bei politischen Wahlen gezielt zu beeinflussen.

Die Kombination von Präferenzen der Ernährung, Bestellungen und Lichtaktivität können, wenn sie an Ihre Versicherung weitergegeben werden, genutzt werden, um Sie in der Gestaltung Ihres Lebens einzuschränken, wenn Sie nicht in einen schlechteren Tarif eingestuft werden möchten.

Ihre allgemeinen personenbezogenen Daten (z. B. Namen, Adresse, Geschlecht oder Bankdaten) können, wenn sie bei Dritten landen und zu einem Profil verknüpft werden, genutzt werden, um Ihre digitale Identität zu übernehmen und unangemessene Inhalte in Ihrem Namen zu veröffentlichen, gefährliche Nachrichten (z. B. Phishing Nachrichten oder Nachrichten mit gefährlichen Anhängen) in Ihrem Namen zu verschicken oder finanzielle Transaktionen in Ihrem Namen durchzuführen.

Ihre Audio- oder Videodaten können, wenn sie bei Dritten landen, dazu führen, dass Sie sich nicht mehr ungestört in Ihrem Heim fühlen. Dadurch können Sie sich selbst in Ihren Tätigkeiten/Verhalten einschränken oder eingeschränkt fühlen.

Das Gefährliche beim Sammeln und Auswerten von Daten und Informationen über das eigene Nutzungsverhalten ist, dass heute noch nicht absehbar ist, was zukünftig alles aus den Daten abgeleitet werden kann, z. B. welche Krankheiten eine Person hat oder der Wahrheitsgehalt von Aussagen, die Sie anderen Menschen gegenüber machen.

Oben genannte Sicherheits- bzw. Privatsphärerisiken betreffen nicht nur Sie, sondern Sie als Besitzer des Smart Home setzen auch Ihre Gäste vielen dieser Risiken aus.