Unter Smart Home versteht man einen Haushalt, bei dem Haushaltsgeräte (z. B. Kühlschrank, Waschmaschine, Staubsauger), Geräte der Hausautomation (z. B. Heizung, Beleuchtung, Belüftung), Unterhaltungselektronik bzw. Kommunikationseinrichtungen (z. B. TV, Spielekonsolen) und Geräte der Steuerungs-Assistenz (z. B. Alexa, Google Home) vernetzt sind und zu „intelligenten" Gegenständen werden. Durch die Vernetzung dieser und die Kombination mehrerer solcher Gegenstände werden neue Funktionen und Dienste möglich, die gegenüber dem einzelnen Gegenstand einen Mehrgewinn bieten. Die Gegenstände können aus dem Smart Home oder aus der Ferne zentral gesteuert werden.

Diese neue Technologie bringt eine Reihe von Verbesserungen mit sich:

- Erhöhung von Wohn- und Lebensqualität z. B. automatisierte Beleuchtungssteuerung oder beim Kühlschrank durch das Erkennen von Engpässen bestimmter Produkte und das automatisierte Bestellen.
- 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 („Anwesenheitssimulation" und Alarmfunktion).
- Vereinfachte Bestell- und Steuerungsprozesse z. B. mit Hilfe von Sprachassistenten durch einfache Bestellungen im Internet per Stimme oder durch die Steuerung der Geräte im Haushalt via Smartphone und Tablet.
- Automatisierte Nutzung von Haushaltsgeräten abhängig von der Verfügbarkeit von eigen erzeugter Energie oder abhängig von einem variablen Energiepreis.

Viele Nutzer gehen davon aus, dass Ihre Geräte bereits per Default – also vor dem Kauf – vom Hersteller bezüglich des Schutzes Ihrer Privatsphäre bzw. Sicherheit eingestellt werden. Nicht jeder Hersteller hat aber ein Interesse daran, dass die Geräte zum maximalen Schutz der Privatsphäre eingestellt werden. Zum einen sind manche Hersteller an den zusätzlichen Daten interessiert. Zum anderen geht maximale Privatsphäre bzw. Sicherheit manchmal mit Einbußen in der Funktionalität einher. Da man vorher nicht weiß, wie die Einstellung des Herstellers zum Thema Privatsphäre bzw. Sicherheit ist, sollte man sich bei der Konfiguration mit den Einstellungen beschäftigen. Nur so kann sichergestellt sein, dass die Konfiguration Ihre Präferenzen widerspiegelt.

Alle diese Konsequenzen sind Beispiele, die bereits in der Praxis aufgetreten sind. Das Gefährliche beim Sammeln und Auswerten von Daten und Informationen über das eigene Nutzungsverhalten ist, dass heute noch nicht absehbar ist, was künftig alles aus den Daten abgeleitet werden kann: Zum Beispiel, welche Krankheiten eine Person hat oder der Wahrheitsgehalt von Aussagen, die Sie anderen Menschen gegenüber machen. In diesem Faltblatt genannte Sicherheits- bzw. Privatsphärerisiken betreffen nicht nur Sie, sondern Sie als Besitzer des Smart Home setzen auch Ihre Gäste vielen dieser Risiken aus.

Kontakt

Karlsruhe 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

www.secuso.aifb.kit.edu
facebook.com/secuso
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

Deshalb ist es wichtig, dass Sie sich bei der Konfiguration Ihres Smart Homes ausreichend Zeit nehmen, um die Konfiguration hinsichtlich Sicherheit und Privatsphäre durchzuführen. Außerdem sollten Sie während der Nutzung des Smart Homes etwaige auftretende Meldungen sorgfältig lesen und entsprechend den Handlungshinweisen handeln.

In diesem Faltblatt erhalten Sie Informationen über Sicherheits- und Privatsphärerisiken bzw. deren Konsequenzen.

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 und 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 und 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 und 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. Manchmal werden nachträglich durch ein Update Funktionen aktiviert, die Ihre Daten in Zukunft erheben. Die Zustimmung zu diesen zusätzlichen Daten versteckt sich manchmal tief in den neuen Vereinbarungen und ist nicht immer klar erkenntlich.

Ihre Nutzungsgewohnheiten werden aus diesen Daten abgeleitet (z. B. an welchen Tagen Sie wann Licht und Heizung einschalten, wann Sie Wäsche machen, welche Lebensmittel Sie online einkaufen oder Ihre Präferenzen bei Sendungen). So können die Hersteller umfangreiche Nutzungsprofile von Ihnen erstellen. Diese werden von den Herstellern Ihrer Geräte oder den App-Herstellern auf Ihren Geräten u. a. dafür verwendet, die Dienste zu verbessern.

Wenn die gesammelten Daten und die erstellten Nutzungsprofile allerdings in die Hände Dritter geraten oder von dem Hersteller entgegen der Vereinbarung für weitere Zwecke verwendet werden, kann Ihnen auf vielfältige Art und Weise Schaden entstehen.

Beispiele für konkrete Konsequenzen aus beiden Risiken:

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

Ihre personenbezogenen Daten (z. B. Ihre politischen, religiösen oder ethisch-moralischen Einstellungen, abgeleitet aus von Ihnen getätigten Suchanfragen) 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 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 Gesundheitsdaten können, wenn sie an Ihre Bank weitergegeben werden, dazu führen, dass Sie schlechtere Konditionen für einen Kredit erhalten.

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

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

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 personenbezogenen Daten (Namen, Adresse, Geschlecht oder Bankdaten) können genutzt werden, um Ihre digitale Identität zu übernehmen und in Ihrem Namen unangemessene Inhalte 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. Außerdem können Konflikte mit Freunden entstehen, wenn vertrauliche Inhalte veröffentlicht werden.

Ihre Audio- oder Videodaten können, wenn sie bei Dritten laden, 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.

Diese Konsequenzen treten ein, wenn Dritte an Ihre Daten, Informationen oder Nutzungsprofile gelangen. Dies geschieht weil,

- Sie dies dem Hersteller der Smart Home-Geräte oder der App explizit (ggf. unbewusst) erlaubt haben.
- Sich kriminelle Mitarbeiter des Herstellers finanziell bereichern möchten und daher die Daten unerlaubterweise kopieren und an Dritte weitergeben bzw. verkaufen.
- Hacker Sicherheitslücken in den Systemen und/oder Servern der Hersteller ausnutzen und sich so Zugriff auf die Daten, Informationen bzw. Nutzungsprofile verschaffen. Dann können Hacker diese selbst nutzen, um Ihnen zu schaden, sie veröffentlichen oder Sie damit erpressen, dass sie diese Daten, Informationen und Nutzungsprofile veröffentlichen oder sie an Dritte verkaufen.