Norbert Pohlmann

Chancen und Risiken von Smart Home

Die Art und Weise wie wir leben und wohnen hat sich in den vergangenen Jahren stark verändert, daraus haben sich einige neue Trends für den häuslichen Alltag ergeben. Dies ist unter anderem darauf zurückzuführen, dass das steigende Umweltbewusstsein viele Handlungsentscheidungen beeinflusst. Zudem bedingt die demografische Entwicklung, dass nach neuen Lösungsansätzen für ein eigenständiges Leben im Alter gesucht werden muss. Mittlerweile ist auch das Homeoffice so etabliert, dass daraus neue Gegebenheiten für das heutige und künftige Arbeiten von Zuhause resultieren, die technologische Veränderungen notwendig machen. Insgesamt wird ein Wandel hin zum smarten Zuhause als Chance gesehen, diesen aktuellen Herausforderungen zu begegnen. Aber was bedeutet Smart Home tatsächlich im täglichen Leben und wie wird dieses in der Zukunft gestaltet werden? Für die Einschätzung hier gilt es, die Vorteile von Smart Home ebenso zu betrachten, wie mögliche Risiken und was berücksichtigt werden muss, um Schäden zu vermeiden. Denn nur so lässt sich eine Akzeptanz in der digitalen Zukunft zu erzielen [1].

1 Einführung

Smart Home ist der Obergriff für die Ausgestaltung von Wohnräumen, in denen Haushalts- und Multimedia-Geräte interagieren und intelligent gesteuert werden, um insgesamt die Wohn- und Lebensqualität zu erhöhen, aber ebenso die Sicherheit sowie die Effizienz der Energienutzung zu verbessern. Durch die Smart Home-Technologie werden Alltagsvorgänge automatisiert und Smart Home-Geräteeinstellungen, zum Beispiel von Heizung, Licht und Lautsprechern per Smartphone problemlos von zu Hause, aber auch von unterwegs an die persönlichen Bedürfnisse angepasst. Die Steuerung über Sprachbefehle oder Handzeichen gewinnt bei Smart Home zunehmend an Bedeutung.

2 Smart Home Ökosystem

Smart Home kann als Ökosystem betrachtet werden, weil verschiedenste Parteien am Smart Home-System beteiligt sind und miteinander interagieren. Das Ökosystem Smart Home lässt sich in verschiedene Anwendungsbereiche unterteilen. Siehe Abb. 1.

Abb. 1 | Smart Home Ökosystem

Smart Home-Gegenstände / Smart Home-Geräte in diesem Ökosystem sind unter anderem: Heizung, Lampen, Jalousien, Lautsprecher, Staubsauger, Rasenmäher, Kühlschränke, Herde, Kaffeeautomaten, Waschmaschinen, Trockner, Sprachassistenten, Rauchmelder, Schalter, Steckdosen, TC, Radio, Fenster, Türen, Schließanlagen.

Smart Home-Infrastruktur besteht unter anderem aus: Hausvernetzungen, lokalen Smart Home-Zentralen, zentralen Cloud Smart Home-Diensten.

Norbert Pohlmann

ist Professor für Informationssicherheit und Leiter des Insti-tuts für Internet-Sicherheit – if(is) an der Westfälischen Hoch-schule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.
E-Mail: pohlmann@internet-sicherheit.de

Smart Home-Bediengeräte sind: Smartphone, Tablets, Sprachassistenten (mit Mikrofon und Lautsprecher), Touchdisplay, Gesten- und Geruchsensoren.

2.1 Anwendungsbereich: Energiemanagement

Das Thema erneuerbare Energie spielt im Smart Home Bereich eine besondere Rolle: Solar-Anlagen, Wärmepumpen oder Biomasse-Kessel arbeiten zusammen mit den vorhandenen Energie-Infrastrukturen und schaffen einen flexiblen Energiemix. Durch intelligente Kontrollsysteme kann der Energieverbrauch in einem smarten Zuhause über den Zeitablauf analysiert und für die konkreten Bedürfnisse und Gegebenheiten eines Haushaltes optimiert werden. Es wird zum Beispiel das Heizverhalten auf Basis von Gewohnheiten analysiert, um entsprechend intelligent, angemessen und sparsam heizen zu können. Die Heizkostenersparnis liegt dabei teilweise über 30 Prozent. Die festgelegte Heizleistung kann jedoch, bei spontanen Planänderungen, mithilfe von Apps flexibel, auch von unterwegs, anpasst werden.

Weitere Beispiele im Bereich Energiemanagement:

- smartes Heizkörperthermostat
- vernetzte Heizsysteme mit Energie- bzw. Wärmespeicher
- Stromfresser identifizieren und optimieren, um Strom zu sparen
- ausgeklügelte Beleuchtung, die sich an die Lichtbedingungen und Lebensverhältnisse anpasst, um Energie zu sparen, …

Unterschiedliche Parteien, die in diesem Anwendungsbereich beteiligt sind:

- Energiekonzerne , Stadtwerke, …
- Hersteller von Anlagen für die Generierung erneuerbarer Energie
- Hersteller von Heizungs- und Haushaltsgeräten, …

Prinzipielle Risiken:
Durch die verschiedenen Energiequellen müssen unterschiedliche Parteien über definierte Schnittstellen zusammenarbeiten, die auch ein Ziel für Angreifer darstellen. Sabotagemöglichkeiten, um den Bewohnern zu schaden sind hier zum Beispiel, das Absperrventil öffnen, um einen Wasserschaden herbeizuführen oder auch gleichzeitig Heizen und Kühlen, um hohe Kosten zu verursachen. Doch auch die Bewohner können in diesem Anwendungsbereich Manipulationen vornehmen mit dem Ziel Strom, Wasser, Gas usw. zu verbrauchen, ohne dafür zu bezahlen.

2.2 Anwendungsbereich: Entertainment und Kommunikation

Smarte Entertainment-Systeme und eine nahtlose Kommunikation ermöglichen es, verschiedene Entertainment-Geräte gleichzeitig aus der Ferne zu steuern und Inhalte simultan wiederzugeben. Beispiele sind Musik, die automatisch nur dort abgespielt wird, wo sich die Bewohner gerade aufhalten, oder eine Lautstärkeregelung, die sich an die jeweilige Person anpasst. Mit Bluetooth-Lautsprechern und Multiroom-Systemen können Lieblingsplaylists nach Belieben entweder per App oder Sprachbefehl ausgewählt und individualisiert gehört werden.

Weitere Beispiele im Bereich Entertainment und Kommunikation:

- intelligente Steuerungen von Multimedia-Systemen und -Geräten
- Einbettung von Unterhaltungssystemen auf verschiedenen Geräten
- Smart-TV, Heimkino, …

Unterschiedliche Parteien, die in diesem Anwendungsbereich beteiligt sind:

- Elektronikhersteller
- Hersteller von Unterhaltungselektronik (Audio, Video, TV etc.), …

Prinzipielle Risiken:
Durch die grundsätzliche Option, die Entertainment-Systeme auch aus der Ferne steuern zu können, wird es Dritten möglich, diese mittels Manipulation auch zu Zweckentfremden, also beispielsweise von außerhalb die Bewohner dadurch zu belästigen, dass ihre Musikanlage auf- oder abgedreht wird oder das TV beliebig oft aus- und eingeschaltet wird.

2.3 Anwendungsbereich: Gebäude- und Wohnungssicherheit

Bei Gebäude- und Wohnungssicherheit werden die Bewohner darüber informiert, wenn sich jemand an Fenstern oder Türen zu schaffen macht aber auch, wenn der Keller mit Wasser vollläuft. Zusätzliche Angebote im Bereich Sicherheit sind biometrische Türschlösser, die mit einem Fingerabdruck elektronisch Türen und Tore für autorisierte Personen öffnen.

Weitere Beispiele im Bereich Gebäude- und Wohnungssicherheit:

- ferngesteuerte Überwachung und moderne Zugangskontrolle
- intelligente Gefahrenabwehr durch vernetzte Rauchmelder, Gasmessgeräte, Wassersensoren, …
- Tür- und Fenstersensoren, um Einbruchsversuche zu erkennen, …

Unterschiedliche Parteien, die in diesem Anwendungsbereich beteiligt sind:

- Hersteller von Sicherheitstechnik (Videokameras, Sensoren für Rauch, Gas, …, Bewegung, …)
- Hersteller von Sicherheitstechnologien (Zugangskontrolle, …)
- Telekomunikationsunternehmen, …

Prinzipielle Risiken:
Dadurch, dass Türen auch elektronisch geöffnet werden können, besteht grundsätzlich die Möglichkeit, für Angreifer diese zu hacken und so in das Haus einzudringen oder dem Bewohner den Zutritt ins eigene Haus zu versperren. In diesem Anwendungsbereich kann der Angreifer aber zum Beispiel auch durch Auslösen der Alarmsirenen oder der Rauchmelder die Bewohner verunsichern oder in Panik versetzen.

2.4 Anwendungsbereich: Hausautomation und Komfort

Intelligente Geräte wie Roboter, Waschmaschinen und sonstige smarte Haushaltsgeräte können die Hausarbeit nachhaltig erleichtern, indem beispielsweise Routine-Tätigkeiten automatisch erledigt werden. So sind Kühlschränke zukünftig in der Lage, automatisch Lebensmittel nachzubestellen oder Roboter, selbstständig das Haus sauber zu halten oder Zimmer aufzuräumen.

Weitere Beispiele im Bereich Hausautomation und Komfort:

- ferngesteuerter Ofen/Herd, vernetzte Waschmaschinen

- Rasenmäher-Roboter
- Einkaufsautomatisierung (z.B. „DASH Buttons"), …

Unterschiedliche Parteien, die in diesem Anwendungsbereich beteiligt sind:

- Hersteller von Küchengeräten, weißer Ware, Gartenmaschinen, …
- Elektronikersteller
- Einzelhandelsunternehmen, …

Prinzipielle Risiken:
Generell besteht im Rahmen der Manipulationsmöglichkeiten über den Kühlschrank ein erhöhtes Gefahrenpotential, auch wenn sich dieses im ersten Augenblick nicht unmittelbar erschließt. Tatsächlich kann jedoch die Bestellung von falschen Lebensmitteln, etwa solche, auf die der Bewohner allergisch reagiert, fatale Folgen haben und schlimmstenfalls tödlich enden. Nicht so gravierend sind Angriffe, mittels derer der Kühlschrank mit Gefrierfach ausgeschaltet wird, um den Inhalt unbrauchbar zu machen oder die Angreifer eine Online-Bestellung so durchführen, dass sie die Lieferung abgreifen können, während die Kosten dem offiziellen Besteller abgebucht werden. Bei dem Einsatz von Robotern besteht zum einen die Gefahr, ausspioniert zu werden sowie zum anderen durch einen – aufgrund einer Manipulation ausgelösten – Angriff auch körperlich verletzt zu werden.

2.5 Anwendungsbereich: Gesundheit

Mit intelligenten vernetzten Gesundheitsprodukten werden dem Bewohner Gesundheitsdaten zur Verfügung gestellt, mittels derer er seine Lebensweise optimieren und somit gesünder leben kann. Zum Beispiel durch den Einsatz eines smarten WC, über das eine automatische Messung von zehn verschiedenen Werten im Urin erfolgt, die bei der Früherkennung von unter anderem Diabetes, Hepatitis, Prostataerkrankungen, Leberentzündungen, Infekten, Entzündungen oder Stoffwechselproblemen helfen können. Mittels Sensoren im Toilettenpapierhalter wird etwa anhand der Papierentnahme der jeweilige Benutzer erkannt.

Weitere Beispiele im Bereich Gesundheit:

- Überwachung und Steuerung der Luftqualität, zum Beispiel mit intelligenten Luftreiniger (Allergene, Schadstoffe, …)
- Schlaftracker zur Überwachung der Schlafqualität
- Smarte Sportgeräte, vernetzte Körperwaagen, …

Unterschiedliche Parteien, die in diesem Anwendungsbereich beteiligt sind:

- Hersteller von Haushaltsgeräten und Sanitäranlagen
- Elektronikersteller
- Hersteller von Gesundheitsprodukten, …

Prinzipielle Risiken:
Wenn Messwerte eines Bewohners manipuliert werden, kann dies gesundheitliche Probleme bei ihm verursachen und schlimmstenfalls zu körperlichen Schädigungen führen.

2.6 Anwendungsbereich: Zuhause eigenständig leben im Alter (Ambient Assisted Living)

Die Alternative auch mit fortschreitendem Alter bequem Zuhause leben zu können ist aufgrund der demografischen Entwicklung der Gesellschaft in Deutschland ein erstrebenswertes Ziel. Daraus entwickelt sich ein solider Zukunftsmarkt, da hier der Mehrwert besonders hoch ist. Unter Einsatz verschiedener Technologien wird älteren Menschen die Möglichkeit geboten, sowohl eigenständig als auch sicher in den eigenen vier Wänden wohnen zu bleiben. Dabei unterstützen zum Beispiel Kameras, Sensoren oder Roboter. Darüber wird etwa eine automatisierte Kommunikation mit den Familienangehörigen ermöglicht, die relevante alltägliche Informationen via Smartphone erhalten, zum Beispiel dass die Großmutter, wie üblich, morgens um 8.00 Uhr aufgestanden ist. Oder aber auch frühzeitig zu erkennen, ob eine Person gestürzt ist und Hilfe benötigt sowie allgemein Pflegeleistungen zu erbringen.

Weitere Beispiele im Bereich Zuhause eigenständig leben im Alter:

- automatisierte Verhaltensüberwachung
- vernetzte Notrufsysteme
- altersgerechte Assistenzsysteme, wie Warnmelder für den Herd, …

Unterschiedliche Parteien, die in diesem Anwendungsbereich beteiligt sind:

- Versicherungen
- Pflegedienste
- Gesundheitsversorger
- Wohnungswirtschaftsgesellschaften, …

Prinzipielle Risiken:
Wenn die Verhaltensüberwachung manipuliert wird, kann es zum Beispiel passieren, dass ein Sturz der betreffenden älteren Person nicht entdeckt wird. Zum anderen können die aufgezeichneten Daten missbräuchlich verwendet werden, etwa um eine Person auszuspionieren.

3 Lösungsvarianten von Smart Home-Systemen

Bei Smart Home-Systemen gibt es viele diverse Lösungsvarianten. Grundsätzlich gilt, dass ein Smart Home-System dann besonders effizient und komfortabel ist, wenn möglichst alle Smart Home-Gegenstände miteinander verknüpft sind, die Smart Home-Infrastruktur also nachvollziehbare Mehrwerte schafft. Im Rahmen der Umsetzung gibt es generell die nachfolgend aufgeführten Ansätze:

3.1 Offene Lösung

Offene Smart Home-Systeme haben einen Standard, der von verschiedenen Anbietern für Smart Home-Lösungen unterstützt wird. Somit können verschiedene Smart Home-Anwendungen von unterschiedlichen Herstellern miteinander kombiniert und ergänzt werden. Dadurch lassen sich mehrere parallel operierende Insellösungen vermeiden, die mit jeweils unterschiedlichen Apps bedient werden müssen. Offene Smart Home-Systeme sind flexibel, vielfältig und zukunftsorientiert. Digitale Assistenten wie Alexa sind ein Beispiel für offene Systeme.

3.2 Geschlossene / System-gebundene Lösung

Geschlossene oder System-gebundene Smart Home-Systeme sind nicht kompatibel mit den Smart Home-Lösungen anderer An-

bieter. Wenn es von einem Anbieter keine technische Lösung für eine bestimmte Anforderung gibt, kann nicht auf die Anwendung eines anderen Herstellers zurückgegriffen werden. Daher können in der Regel nur die Anwendungen von einem einzigen Hersteller genutzt werden. Bei der Nutzung einer geschlossenen Lösung ist die Auswahl der Smart Home-Geräte zwar eingeschränkt, dafür agieren sie perfekt miteinander. In der Regel sind geschlossene Lösungen eher kabelgebunden und weder sehr flexibel noch vielfältig.

4 Digitale Assistenten als Mittelpunkt von Smart Home

Digitale Assistenten spielen im Smart Home-Bereich eine wichtige Rolle. Dabei ist Amazon mit Alexa der größte Player in diesem Bereich. Aber auch Google Home und Apple HomePod spielen eine zunehmend große Rolle.

Alexa ist ein Cloud-basierter Dienst von Amazon, der eine Sprachsteuerung für die unterschiedlichsten Funktionalitäten zur Verfügung stellt. Alexa ist mit einem Mikrofon sowie einen Lautsprecher ausgestattet und mit dem Internet verbunden. Als digitaler Assistent soll Alexa dem Nutzer im Alltag helfen. Dazu kann Alexa neben der Beantwortung von Google-Fragen, zum Beispiel Musik oder Hörbücher abspielen, einen Wecker oder Timer stellen und Aufgaben- und Einkaufslisten sowie Kalender verwalten, aber auch Smart Home-Gegenstände steuern [2].

Alexas Fähigkeiten lassen sich zudem mit Anwendungen von Drittanbietern, den sogenanntenSkills erweitern. Es gibt u.a. Skills für Wetterinformationen, Nachrichten, Spiele und Smart Home-Steuerung. Siehe Abb. 2.

Damit mit Alexa per Sprache kommuniziert werden kann, lässt sie sich problemlos mit einem Signalwort, standardmäßig „Alexa“, aktivieren. Die Erkennung des Signalworts erfolgt lokal auf dem Gerät (zum Beispiel Amazon Echo). Nach der Aktivierung wird alles aufgezeichnet und die Sprachinformation in die Amazon-Cloud übertragen. Dort wird diese verarbeitet, gespeichert und die entsprechenden Ergebnisse zurückgegeben. Die eigentliche Spracherkennung und -verarbeitung erfolgt somit in der Amazon-Cloud. Bei der Sprachverarbeitung prüft Alexa, ob sie die Anfrage des Nutzers selbst bearbeiten kann (integrierter Skill) oder ob der Nutzer implizit einen externen Skill angesprochen hat. Falls der Nutzer implizit einen externen Skill angesprochen hat, zerlegt Alexa die Anfrage in ein generalisiertes Format. Der Skill erhält lediglich textuelle Daten, keine Audiodaten. Falls dem Skill noch Informationen fehlen, kann er diese mittels Alexa abfragen lassen. In der Cloud besteht die Möglichkeit, dass alle Daten mittels künstlicher Intelligenz analysiert und bewertet werden.

Ein wichtiger Anwendungsfall von Alexa ist das Steuern der vernetzten Smart Home-Gegenstände, auch mittels der speziellen Smart Home Skills. Bei deren Nutzung wird auf einen Dienst des Smart Home Skill-Anbieters zurückgegriffen. Dies setzt voraus, dass der Skill-Anbieter vom Internet aus Zugriff auf den Smart Home-Gegenstand hat, der Smart Home-Gegenstand also Cloud-Controlled ist. Dabei zerlegt Alexa die Anfrage in eine Aktion zum Beispiel „einschalten“ und einen Identifier, der den Smart Home-Gegenstand (Küchenlicht) bezeichnet, der anzusteuern ist. Diese Informationen werden zusammen mit Authentifikationsinformationen des Nutzers an den Smart Home Skill gesendet. So aktiviert kommuniziert im Weiteren der Smart Home Skill mit der Device Cloud des Nutzers und löst dort die entsprechende Aktion aus (Küchenlicht einschalten). Siehe Abb. 3.

Abb. 3 | Ablauf eines Smart Home Skills

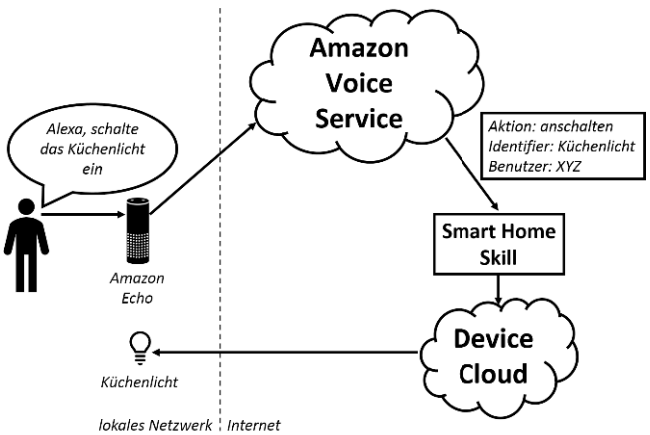
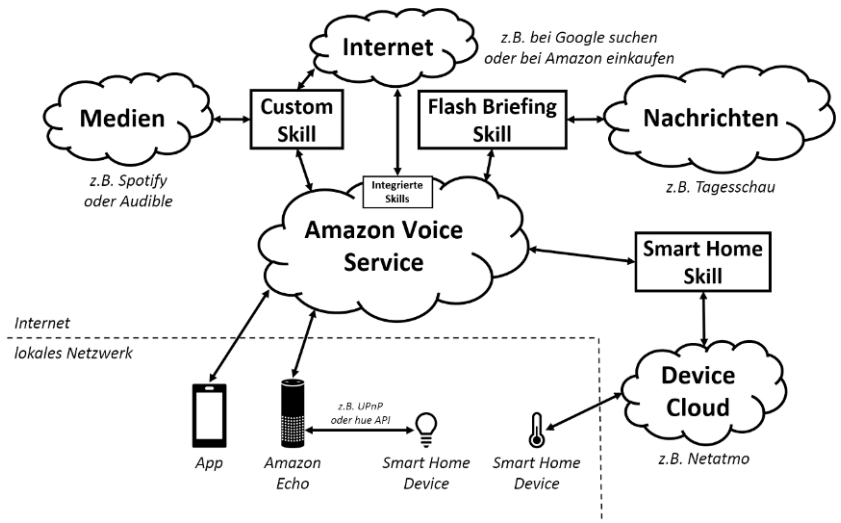


Abb. 2 | Systemarchitektur des Amazon Voice Service (AVS)



5 (Neue) Risiken bei Smart Home

Die Chancen und Anwendungsfelder von Smart Home sind vielfältig, die Risiken auch – allein unter dem Aspekt, dass die Qualität von Cyber-Angriffen zunehmend ausgereifter ist, wie auch durch den aktuellen BSI-Cyber-Sicherheitslagebericht „Die Lage der IT-Sicherheit in Deutschland 2020“ bestätigt wird. Schwachstellen in IT-Systemen stellen wegen der vorhandenen zu schlechten Softwarequalität und den nicht schnell genug durchgeführten Updates, immer noch ein sehr großes Problem dar – entsprechendes gilt auch für viele Smart Home-Produkte. Aber auch die Strategien, etwa die Distributed Denial of Service (DDoS)-Angriffe werden immer intelligenter und stellen ein be-

sonderes Risiko vor allen bei Diensten über das Internet dar. Insgesamt muss festgestellt werden, dass es keine hundertprozentige IT-Sicherheit gibt und daher erfolgreiche Angriffe auf Smart Home-Systemen nicht vollständig verhindert werden können.

6 Beispiele von neuen Angriffsvektoren

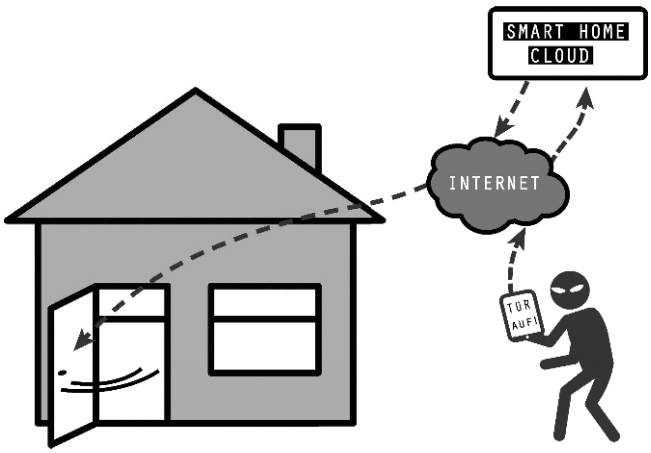
6.1 Einbruchsmöglichkeiten

Die Einbrecher kommen zukünftig nicht mehr mit der Brechstange, sondern hacken sich in das Smart Home-System ein. Dies bietet neue Möglichkeiten: Zuerst lassen sich darüber vorab problemlos die Rahmenbedingungen analysieren, indem mittels der so kompromittierten Videokamera ausgekundschaftet wird, wo die Wertgegenstände versteckt sind, wann die Bewohner in der Regel nicht zu Hause sind und welche Verhaltensweisen sie typischerweise haben. Eventuell ist es darüber sogar möglich Nutzernamen und Passwörter von wichtigen Internet-Diensten (Einkaufen, Online-Banking, …) oder Unternehmensdaten auszuspähen [3].

Der so vorbereitete Kriminelle kann dann den idealen Zeitraum für einen erfolgversprechenden Einbruch wählen, indem er sicherstellt, dass tatsächlich niemand zu Hause ist.

Das Öffnen der Tür über die gehackte Smart Home-Infrastruktur (Cloud) ist dann ebenso potenziell möglich. Siehe Abb. 4. Der eigentliche Einbruch mit den Diebstahl der Werte kann dann risikoärmer, zielgerichteter und erfolgreicher durchgeführt werden.

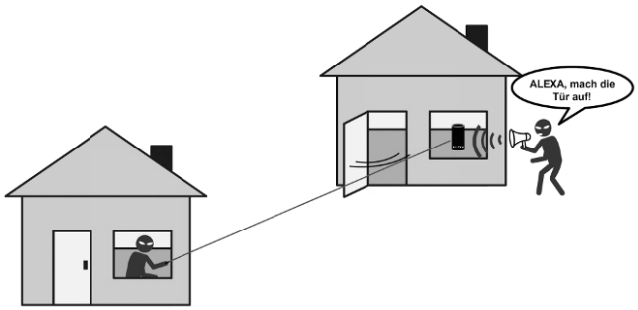
Abb. 4 | „Modere Einbrecher“



6.2 Manipulationsmöglichkeiten von Alexa

In mehreren Fällen ist es bereits vorgekommen, dass Alexa sich angesprochen fühlt, obwohl der Nutzer dies nicht beabsichtigt hatte. Dies liegt zum einen an den hervorragenden Mikrofonen sowie der entsprechenden Spracherkennung und zum anderen an dem Umstand, dass Alexa eher auf uneindeutige Ansprachen reagiert, als einen Befehl zu ignorieren. Hinzu kommt, dass es möglich ist, Alexa auch auf eine größere Distanz, zum Beispiel von außen durch ein Fenster, Befehle zu geben. Dies ermöglicht somit Einbrechern zum Beispiel Haustüren zu öffnen oder Jalousien hochfahren zu lassen, wenn diese Smart Home-Anwendungen vorhanden sind. Aus diesem Grund muss darauf geachtet werden, dass Alexa stets ausgeschaltet ist, wenn niemand zu Hause ist. Siehe Abb. 5, rechts oben.

Abb. 5 | Angriffe auf Alexa



„Light Command“-Angriff

Sprachbefehle an Alexa und Co. müssen nicht unbedingt per Sprache übertragen werden. US-Forscher haben aufgezeigt, wie mithilfe eines Lasers aus bis zu 110 Metern Entfernung Alexa und Co. sich von außen steuern lassen. Ebenfalls mit einem Laser lässt sich die Membran eines Mikrofons zum Schwingen bringen, mit den Schwingungen können Töne bis hin zu Sprachbefehlen erzeugt werden. Mit diesen, für Menschen nicht hörbaren Sprachbefehlen können die digitalen Sprachassistenten im Sinne eines Angreifers manipuliert werden [4]. Siehe Abb. 5, links unten.

6.3 Unsichere Smart Home-Gegenstände

Die Hersteller von Smart Home-Gegenständen, etwa Videokameras, stellen teilweise immer noch IT-Technologie zur Verfügung, die bei Weitem nicht die Cyber-Sicherheitsanforderungen erfüllen. Wenn einfache Videokameras über das Internet gehackt werden können, ist das vordergründig ein Problem des jeweiligen Anwenders, denn Angreifer können über entsprechende Schwachstellen Einblicke seiner Wohnräume erhalten. Das verletzt erst einmal die Persönlichkeitsrechte des Bewohners und erhöht die Wahrscheinlichkeit eines Einbruches, wenn dieser nicht zu Hause ist.

Ein weitaus größeres Problem für alle anderen ist jedoch ein anderes: Angreifer haben sehr viele Videokameras und weitere Smart Home-Gegenstände, die mit dem Internet verbunden sind, wie Drucker, Föne oder Kaffeemaschinen fremdgenutzt, um die Infrastruktur des Internets insgesamt erfolgreich mithilfe von DDoS bis zu 1,5 Terabit/s anzugreifen. Dadurch wird das Internet sehr verletzlich, ist nicht mehr verlässlich und gefährdet somit die Digitalisierung [5].

Aus diesem Grund müssen die Smart Home-Gegenstände, -Infrastruktur und -Bediengeräte sicher und vertrauenswürdig realisiert werden, damit diese nicht von außen angreifbar sind und dabei zu helfen, unsere Gesellschaft angemessen zu schützen.

6.4 Angriff auf die Privatsphäre

a.) Unerlaubter Zugriff auf Mikrofone und Kameras

Der direkte Angriff auf ein Mikrofon oder eine Kamera ermöglicht direkt ein Eingreifen in die Privatheit der Bewohner. Der Angreifer kann aus der Ferne unerlaubt jedes Wort hören oder

jede Bewegung sehen. Da immer mehr Kameras in den Smart Home-Gegenständen, wie Kühlschlank, Roboter oder Smart TV integriert sind, werden die Kameras zu einem immer größeren Risiko, unsere Privatsphäre zu stören.

b.) Unerlaubter Zugriff auf die Smart Home-Gegenstände, -Infrastruktur und -Bediengeräte, um an die Daten, mit denen ein Bewegungsprofil erstellt werden kann, zu gelangen.
Beispiele sind:

- **Stromverbrauch:**
  Der Stromverbrauch kann analysiert und dadurch das Verhalten der Bewohner ausgewertet werden. Wann schaltet er das Licht an, föhnt sich, kocht, wäscht, guckt Fernsehen, hört Musik – all das kann über den Stromverbrauch identifiziert und analysiert werden.
- **Jalousien:**
  Die Daten über die Zeiten, wann Jalousien hoch- und runtergefahren werden geben Informationen darüber, wie der Tagesablauf eines Bewohners aussieht.
- **Wasser-, Gas-, Internet-, … -verbrauchswerte:**
  Auch diese Informationen können genutzt werden, um die Aktivitäten der Bewohner zu beobachten. Wann geht jemand auf die Toilette, macht Kaffee (über den Wasserverbrauch), dreht die Heizung an, surft im Internet usw.
- **Heizkurve:**
  Auch die Heizkurve gibt Aufschluss darüber, wie die Gewohnheiten eines Bewohners sind.
- **Zugriff auf Terminkalender:**
  Hier kann leicht festgestellt werden, wann der Bewohner sein Haus, seine Wohnung verlässt, um einen Termin anderswo wahrzunehmen.

In diesem Bereich ist es besonders wichtig, dass alle Parteien dafür sorgen, dass so wenig wie möglich personenbezogene Daten generiert, verarbeitet und gespeichert werden. Außerdem müssen Smart Home-Gegenstände, -Infrastruktur und -Bediengeräte gegen den unerlaubten Zugriff durch Angreifer nach dem Stand der Technik im Bereich der IT-Sicherheit geschützt werden.

6.5 Der Verlust von Vertrauen

Da die Bewohner in der Regel nicht in der Lage sind, die Sicherheit von Smart Home-Gegenständen, -Infrastruktur und -Bediengeräten zu überprüfen, müssen Mechanismen wie Reputationssysteme und Evaluierung/Zertifizierung für die Vertrauensbildung aufgebaut und umgesetzt werden, damit eine nachhaltige Akzeptanz von Smart Home-Anwendungen zu erreichen ist [6].

6.6 Wie ist die Akzeptanz von Smart Home-Anwendungen

Die Angebote, die wir im Bereich Smart Home sehen, stellen im Prinzip Mehrwerte zur Verfügung. Ob diese jedoch tatsächlich von der Bevölkerung akzeptiert werden, ist nicht grundsätzlich anzunehmen.
Denn fraglich ist, ob ältere Menschen zukünftig von Robotern gepflegt werden wollen oder nicht eher weiterhin menschliche PflegerInnen bevorzugen, um ihr Bedürfnis nach sozialen Kontakten zu erfüllen.

Inwieweit die vielen Kameras in den Smart Home-Gegenständen mittel und langfristig von allen akzeptiert werden, ist bei dem heutigen Level der realen IT-Sicherheit unklar, wenn die Privatsphäre auf dem Spiel steht.

Aber auch, ob wir wirklich wollen, dass unsere Kühlschränke eigenständig Ware nachbestellen, muss sich noch zeigen. Das Bedürfnis, mal etwas anderes einzukaufen, macht das Leben vielfältig und zeigt uns, dass wir eine freie Wahl haben.

7 Bewertung von Chancen und Risiken

Smart Home wird in der Zukunft eine wichtig Rolle spielen, da wir damit in der Lage sind, heutigen und zukünftigen Herausforderungen zu begegnen. Auf der anderen Seite sind damit zunehmend mehr Risiken verbunden, wodurch potenziell der Akzeptanzlevel sinken kann.

7.1 Chancen

Aus der Sicht der unterschiedlichen Hersteller hat der Markt von Smart Home ein hohes Wachstum in der fortschreitenden Digitalisierung. Wenn die verschiedenen Hersteller zusammenarbeiten, können sie gemeinsam einen größeren Markt mit vielen Mehrwerten schaffen. Eine globale IT-Sicherheitsarchitektur für Smart Home in Deutschland oder in der EU zu etablieren würde eine sehr gute Basis für eine sichere und vertrauenswürdige digitale Zukunft schaffen. IT-Sicherheit und die Einhaltung des Wertesystems unserer Gesellschaft kann als nachhaltiges Differenzierungsmerkmal genutzt werden, um international im Ökosystem Smart Home erfolgreich zu sein und Vertrauen und damit Nutzerakzeptanz aufzubauen.

7.2 Risiken

Der Smart Home-Markt wird durch internationale Hersteller und Diensteanbieter aus den USA und Asien dominiert, die ein anderes IT-Sicherheitsverständnis und unterschiedliches Wertesystem haben. Ein weiteres Risiko besteht darin, dass es keine Zusammenarbeit im Ökosystem Smart Home und zu den angrenzenden Ökosystemen gibt und damit die Chancen nicht voll genutzt werden können. Zudem besteht das Risiko, dass wir keine angemessene IT-Sicherheit schaffen: Damit wird es für (Cyber-)Kriminelle weiterhin möglich sein, erfolgreich zu agieren und damit sowohl das Zuhause des einzelnen Nutzers aber auch das Internet in seiner Gesamtheit zu sabotieren. Letztendlich besteht das Risiko, dass unser Zuhause nicht mehr der Ort ist, wo wir unsere Persönlichkeit frei entfalten können. Damit wird Smart Home mittel- und auch langfristig keine Akzeptanz bei den Nutzern finden.

8 Zusammenfassung und Ausblick

Wichtig ist, dass die IT-Hersteller im Smart Home-Ökosystem eine besondere Verantwortung übernehmen müssen und nur noch sichere sowie vertrauenswürdige Smart Home-Gegenstände, -Infrastruktur und -Bediengeräte zur Verfügung stellen, die den Stand der Technik im Bereich der Cyber-Sicherheit und unsere Werte berücksichtigen. Außerdem ist es notwendig, die Produkthaftung deutlich schärfer zu reglementieren, damit die IT-Hersteller und -Anbieter im Smart Home Bereich deutlich mehr Interesse daran haben, sichere IT-Lösungen anzubieten. Aber auch die Nutzer sind dazu aufgerufen, verantwortungsvoll zu handeln und die Konsequenzen ihres Handelns zu bedenken: Anzahl und Funktionalität der Smart Home-Gegenstände sollte mit Bedacht gewählt werden. Denn jeder Smart Home-Gegenstand kann Sicherheitslücken aufweisen und sensible Werte angreifbar machen. Deshalb muss dem Nutzenden bewusst sein, wie hoch das Schutzniveau seiner Smart Home-Geräte ist und wie sorgsam er bei der Verwendung sein sollte.

Eines sollte jedoch bei der Betrachtung der Chancen und Risiken von Smart Home im Fokus stehen: Privatsphäre. Diese bezeichnet den nicht-öffentlichen Bereich, in dem ein Mensch unbehelligt von äußeren Einflüssen sein Recht auf freie Entfaltung der Persönlichkeit wahrnimmt. Das Recht auf Privatsphäre gilt als Grundrecht und ist in allen modernen Demokratien verankert. Die Wohnung bzw. das Haus ist der privateste Platz, der somit einen besonderen Schutz genießen muss. Nach dem Motto „My home is my castle" sollte es für Hersteller, von den Smart Home-Gegenständen, -Infrastrukturen und -Bediengeräten verpflichtend sein, diesen besonders zu schützen, damit die Privatheit weiterhin gewährleistet ist.

Hier müssen die Smart Home-Infrastrukturen besonders sicher, vertrauenswürdig und somit wertekonform umgesetzt werden – nicht zuletzt auch, damit eine hohe Akzeptanz entstehen kann.

Literatur

[1] eco – Studie – Der deutsche Smart-Home-Markt 2017–2022 – Zahlen und Fakten https://www.eco.de/presse/studie-von-eco-und-adl-smart-home-umsaetze-verdreifachen-sich-bis-2022-auf-43-milliarden-euro/

[2] J.-H. Frintrop, N. Pohlmann: „Alexa, wie sicher bist du? – Intelligente Sprachsteuerung unter der Lupe", IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 6/2017

[3] N. Pohlmann: „Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung", Springer-Vieweg Verlag, Wiesbaden 2019

[4] Siegel Netzwelt: „Forscher hacken Sprachassistenten mit Laserattacke" https://www.spiegel.de/netzwelt/gadgets/light-commands-forscher-taeuschen-sprachassistenten-per-laser-a-1294910.html

[5] J. Hoang, O. Jötten, N. Pohlmann, C. Wojzechowski: „Internet of Things (IoT) – Herausforderung für die IT-Sicherheit", IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 3/2017

[6] U. Coester, N. Pohlmann: „Vertrauen – ein elementarer Aspekt der digitalen Zukunft", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 2/2020