Smart-Home-Anwendungen

Hilfreiche Unterstützung oder doch vollkommene Überwachung?

Seit 2018 hat sich die Zahl der deutschen Haushalte mit Smart-Home-Anwendungen fast verdoppelt und lag im Jahre 2022 laut einer Umfrage schon bei 43%. Dabei erweist sich das Bild vom intelligenten Haus, in dem jeder Handgriff automatisch geschieht, geprägt durch Film und Fernsehen, oft als übertrieben.

Denn „smart“ bedeutet in diesem Zusammenhang eigentlich nur, dass die Geräte untereinander kommunizieren und gesammelte Daten austauschen. Viele Menschen leben daher in einem vernetzten Zuhause, ohne es wirklich zu wissen. Oft haben Fernseher, Router oder die Spielekonsole schon entsprechende Verbindungen untereinander oder zum hausinternen WLAN.

Das IoT bildet sich heraus

Dieses beginnende Netz aus internetfähigen Geräten nennt sich auch Internet der Dinge. So kann beispielsweise das Anschalten der Nachttischlampe am Morgen dafür sorgen, dass die Kaffeemaschine in der Küche ein weitergeleitetes Signal erhält und damit beginnt, einen Espresso aufzubrühen. Dabei ist es wichtig, im Kopf zu behalten, dass Smart Homes zu circa 80 Prozent auf IT-Systemen beruhen und nur ungefähr 20% des Aufwands wirklich auf die Elektroinstallation abfallen. Immer wieder kommt es vonseiten der Interessierten daher auch zu Bedenken in Bezug auf die Sicherheit und den Datenschutz bei der Anwendungen von intelligenten Geräten, da sich durch die Nutzung immer auch eine digitale Tür in die eigenen vier Wände öffnet.

Sicherheit als Kernthema

Zwar entwickeln sich Nachhaltigkeit und der Wunsch, Energie zu sparen, immer mehr zu einem überzeugenden Argument für die Umstellung oder den Bau eines Smart Homes, aber für viele steht immer noch das Bedürfnis nach mehr Sicherheit in den eigenen vier Wänden an erster Stelle. Durch den anhaltenden Siegeszug des intelligenten Zuhauses rückt für viele Anwenderinnen und Anwender auch das Thema „Datenschutz“ stärker in den Fokus. Für 83% der Interessierten hat sich dies zu einem der wichtigsten Kriterien im Kaufprozess entwickelt und steht damit sogar knapp vor dem Preis.
Hersteller und Dienstleister stellen sich daher vermehrt der Herausforderung, den Komfort mit dem Schutz der Privatsphäre sinnvoll zu verbinden. Dabei beschränkt sich dieser nicht mehr ganz so neue Trend der hausinternen Vernetzung nicht nur auf eine scheinbar junge Zielgruppe. Nutzerinnen und Nutzer entsprechender Anwendungen lassen sich in allen Generationen finden – egal ob Gen Z oder Babyboomer. Von der Lampe über die Heizung bis zum Mähroboter im Garten – intelligente Geräte bilden aufgrund der Vielzahl an Produkten, Apps und Service-Leistungen einen stetig wachsenden Marktsektor.

Schutz durch Anonymität?

Durch die Europäische Datenschutz-Grundverordnung (EU-DSGVO) sichert die Europäische Union seit Mai 2018 den Schutz personenbezogener Daten innerhalb ihrer Grenzen. Hersteller müssen dadurch offenlegen, wie sie die im Alltag gesammelten Informationen verwenden. Daher empfiehlt es sich für Anfänger und Skeptiker, auf europäische Produkte zurückzugreifen, da diese strengeren Regulierungen unterliegen. Gerade bei internetfähigen Geräten fallen häufig große Datenmengen an, weshalb es für die Steuerung klare Regeln und Verordnungen zur angemessenen Handhabung braucht.
Dabei macht es auch einen Unterschied, ob die Speicherung lokal oder über eine Cloud stattfindet. Vor allem spezielle Smart-Home-Geräte, wie beispielsweise ein Sprachassistent, dürfen in der Regel nur Daten erhe-

Autor:
Carsten Müller
Geschäftsführer
GST Müller GmbH & Co. KG
www.gst-mueller.de

ben, die sie für den Betrieb benötigen. Weniger ist mehr, lautet die Devise. Für den reibungslosen Einsatz müssen außerdem nicht alle in diesem Zusammenhang gesammelten Daten unbedingt eine zugehörige Personalisierung erhalten. Durch mehr Anonymität bei der eigentlichen Sammlung besteht die Chance, die Privatsphäre des Anwenders zusätzlich zu schützen. Wer bei seinem Smart-Home auf Nummer sicher gehen möchte, kann auch auf das Prinzip der Datensouveränität zurückgreifen, um somit in gewissen Bereichen ein geschlossenes System zu erschaffen. Damit lässt sich die Weitergabe an Dritte an so mancher Stelle vermeiden.

Keine Chance für Hacker & Co.?

Zuallererst lässt sich festhalten: Kein Hersteller oder Dienstleister kann einen Fremdzugriff auf die Systeme eines Smart-Homes von vorneherein komplett ausschließen. Gerade durch Schnittstellen innerhalb des Hausnetzwerks besteht immer ein gewisses Datenschutzrisiko. Vor allem ungeschützte und übereilt ins System eingeführte Geräte bergen jedoch die Gefahr, einen gewaltigen Schaden zu verursachen. Hacker-Angriffe finden dabei entweder über ein einzelnes intelligentes Gadget oder direkt über das teilweise schlecht gesicherte Heimnetzwerk statt.
In der Regel haben Angreifer bei ersterem Eingangstor zwar nur einen begrenzten Handlungsspielraum, aber trotzdem besteht so die Möglichkeit, dass Fremde die eigene Überwachungstechnik zum Ausspionieren nutzen. In manchen Fällen bietet solch eine offene „Hintertür" auch den benötigten Universalschlüssel, um in das eigentlich verriegelte Netzwerk einzudringen. Hier braucht es daher von Anfang an eine saubere Planung und die Absicherung von Schnittstellen im Zuge der Installation, um Angreifer nachhaltig von einem Eindringen abzuhalten. Wer zudem auf eine detaillierte Dokumentation der technischen Abläufe setzt, sichert sich noch zusätzlich ab. Unüberlegtes Hinzuschalten von einer Vielzahl an ungeprüften Anwendungen kann ansonsten schnell zu einer Sicherheitslücke führen.

Der Weg der Übertragung

Bei der Installation eines neuen Smart-Homes stehen Bewohner beim Übertragungsweg immer vor der Entscheidung zwischen einem Funk- oder einem Kabelsystem. Ersteres erweist sich meist aufgrund der Sensoren als flexibler, kostengünstiger und einfacher nachrüstbar, während Letzteres eine höhere Ausfallsicherheit garantiert sowie eine hohe Kompatibilität bietet. Funksysteme kämpfen oft mit der bestehenden Reichweite und Hacker haben durch offene Schnittstellen häufig mehr Angriffspunkte für eine Cyberattacke. Hier beruht der Schutzgedanke auf verschlüsselten Protokollen und regelmäßigen Updates.
Für das Verlegen der einzelnen Kabel braucht es zwar eine vorherige Planung und entsprechende bauliche Maßnahmen, aber schlussendlich bietet diese meist kostspieligere Lösung mehr Sicherheit vor unerwünschtem Fremdzugriff. Von vorneherein besteht bei beiden Optionen die Möglichkeit, die Anwendungen an gewünschte Sicherheitsstufen anzupassen und Nutzungsrechte an Bewohner zu verteilen. In der Regel erhalten hier alle Familienmitglieder einen eingeschränkten Zugang zu den Systemen, während eine einzelne Person auf die eigentliche Haussteuerung zugreifen kann.

Persönliche Anpassungen

85% der Anwender nutzen ihr eigenes Smartphone als Kontrolleinheit für ihr intelligentes Zuhause. Dabei gilt es aber einige Sicherheitsrichtlinien zu beachten. Bildschirmsperre und eine schwer zu knackendes Passwort bilden nur den Grundstein für ein entsprechendes Kontrollkonzept. Mit der richtigen Unterstützung aufseiten der Hardware steht einer sicheren und symbiotischen Zusammenarbeit der einzelnen Elemente nichts mehr im Weg. Auch die einzelnen Geräte lassen sich dadurch individuell vor Fremdzugriffen schützen. Hier spielen beispielsweise speziell eingerichtete Gastnetzwerke eine wichtige Rolle, da im Falle eines Cyberangriffs Angreifer damit nicht den vollen Zugang erhalten und Anwender somit unter anderem wichtige Daten vor Diebstahl bewahren können.
Schlussendlich muss jeder für sich selbst entscheiden, welche Anwendungen sie oder er in sein Zuhause integrieren möchte und welche Funktionen oder Berechtigungen diese innerhalb der vier Wände erhalten sollen. Hier braucht es eine individuelle Abwägung zwischen Komfort und dem rigorosen Sammeln von personalisierten Daten. Bei der Anschaffung gilt es aber darauf zu achten, dass Nutzerinnen und Nutzer die vorgegebenen Passwörter und Einstellungen durch selbst gewählte ersetzen.

Zufrieden in den eigenen vier Wänden

Zwar hegen einige Menschen noch eine gewisse Skepsis gegenüber smarten Gerätschaften in ihrem Haushalt, gleichzeitig bietet die Technik aber auch ein zusätzliches Maß an Sicherheit unter anderem durch die Integrierung von entsprechenden Alarm- und Überwachungssystemen. Ein Leben ohne smarte Technologie scheint für viele heute kaum noch vorstellbar und gerade in der Zukunft stehen die Zeichen für diesen Markt weiter auf Wachstum. In diesem Zusammenhang erweist es sich daher als entscheidend, eine bestimmte Sensibilität für die eigenen Daten zu entwickeln und sich bei Bedenken oder Fragen an einen entsprechenden Experten zu wenden. Bei einem vollendeten und gut durchdachten Smart-Home sollten Komfort, Sicherheit und Datenschutz Hand in Hand zusammenarbeiten. Wer zudem wirklich die Vorzüge eines intelligenten Zuhauses genießen möchte, der sollte nicht einfach blind Anwendungen kombinieren, sondern im Voraus und in Zusammenarbeit mit einem entsprechenden Experten ein Konzept sowie einen Geräteplan erstellen. Daran können sich auch die Installateure bei ihrer Arbeit orientieren.

Wer schreibt:

Carsten Müller ist Geschäftsführer der GST Müller GmbH & Co. KG und Experte für Smart-Home-Anwendungen. Als ausgebildeter Gebäude-System-Designer verfolgt er dabei das Ziel einer effizienten vorausgehenden Planung und Dokumentation beim Ausbau von Gebäudetechnik in Alt- und Neubauten. Unvollständige Pläne oder schlechte Absprachen führen ansonsten schnell zu Schwierigkeiten im weiteren Verlauf, die sich mit entsprechenden Nachweisen einfach vermeiden lassen. ◄