Frag deinen Kühlschrank!

Smart Home. Haustüren, Heizsysteme, Waschmaschinen und Toiletten: Im intelligenten Haushalt sind alle Geräte mit dem Netz verbunden. Klingt praktisch, hat aber seine Kehrseite.

Das Internet der Dinge (Internet of Things – IoT) ist ein unaufhaltsamer Trend. Er führt dazu, dass nicht mehr nur Computer, Handy und Tablet mit dem Internet verbunden sind. In der Endstufe der IoT-Ära sollen alle uns umgebenden Geräte internetfähig sein. Und wenn man sich die Praxis ansieht, hat das Spektakel schon längst begonnen: Lautsprecher, die uns über das Wetter informieren und auf Zuruf die gewünschte Musik spielen. Fernseher, die unsere Sehgewohnheiten kennen, und Autos, die die optimale Route heraussuchen – das alles ist schon Realität. Ob Drucker, Kameras, Uhren, Babyfone oder die Stromnetze – die neue Generation der Gerätschaften ist smart und kommuniziert untereinander. Sie denkt mit und vollzieht ihre Arbeitsschritte automatisch.

Im Jahr 2020 soll es schon über 50 Milliarden IoT-Geräte geben, schätzen Experten. Wagen wir einen Streifzug durch ein smartes Haus, das auf Wunsch und bei ausreichend dicker Brieftasche schon heute in dieser Form irgendwo stehen könnte.

Optimiert und komfortabel

Die Eingangstür lässt sich per Handy oder über ein Erkennungssystem – etwa den Scan des Gesichts, der Iris oder eines Fingerabdrucks – öffnen. Im Innenraum sind die Licht- und Temperaturverhältnisse an die Vorlieben der Bewohner angepasst. Morgens erstrahlt aktivierendes blau-weißes Licht. Abends verwandelt es sich in einen orangen Ton und sorgt für Entspannung. Das intelligente Heizsystem, zum Beispiel jenes der Google-Tochter Nest Labs, passt Temperatur und Luftfeuchtigkeit den jeweiligen Wünschen an. Verlassen alle das Haus, wird die Temperatur gesenkt. Der moderne Stromzähler, ein Smart Meter, meldet den Verbrauch im 15-Minuten-Takt und hilft beim Energiesparen.

In der Wohnküche steht ein Lautsprecher, etwa von Amazon Echo (mit Sprachassistentin Alexa) oder Google Home (mit dem Google Assistant). Er ist eine wichtige Schnittstelle und mit allen Haushaltsgeräten verbunden. Das Gerät liest den Bewohnern maßgeschneiderte Nachrichten vor und beantwortet Fragen. Der vernetzte Kühlschrank (hier ist Samsung bis dato Vorreiter) erstellt die Einkaufsliste selbst und spielt auf seinem Bildschirm Videos für Kochrezepte ab. Kameras filmen den Innenraum. Waschmaschinen, Backöfen oder Kaffeeautomaten – Anbieter wie Bosch haben für jedes Gerät bereits eine vernetzte Version parat und häufig wird schon einer der oben genannten Sprachassistenten direkt in die Geräte eingebaut.

Neunmalkluge Zahnbürsten

Im Badezimmer ist die Zahnbürste neunmalklug geworden. Via Bluetooth ist sie mit einer App verbunden und erklärt einem, wie und wie lange das Gebiss noch poliert werden muss. Kein Witz: Auf dem US-Markt gibt es sogar schon ein Modell mit einem integrierten Programm, das die Zahnputzdaten an die jeweilige Versicherungsgesellschaft überträgt. Die soll dann für extra fleißiges Putzen Rabatte gewähren. Und wer glaubt, Toiletten könnten nicht mehr, als man gemeinhin von ihnen erwartet, der irrt. Der Sanitäranlagenhersteller Duravit hat ein WC vorgestellt, das zum Untersuchen von Urin verwendet kann. Die Entnahme der Probe funktioniert automatisch.

Im Kinderzimmer wird das schlafende Baby gefilmt und kann am Bildschirm des Babyfons beobachtet werden. An der Matratze haben die Eltern Sensoren anbringen lassen, die die Vitalfunktionen des Nachwuchses überwachen. Unter anderem können so Herzschlag und Puls im Auge behalten werden. Das Spielzeug ist ebenso smart. Eisenbahnen und Bücher geben nicht mehr nur ein paar einprogrammierte Geräusche von sich. Dank Internetverbindung und Spracherkennungssoftware können sie Fragen beantworten (und schon die Kleinsten mit Reklame beglücken). Wobei hier zumindest im Fall der smarten Puppe Cayla die Bundesnetzagentur in Deutschland ein Machtwort gesprochen hat. 2017 veranlasste sie das Verbot von Cayla und dem Roboter I-Que.

Die Zeiten, in denen das Schlafzimmer ein intimer Rückzugsort vor der ganzen Welt war, sind im smarten Zuhause auch vorbei. Schließlich gilt es, den Schlaf zu optimieren. Der Matratzenbezug „Eight Sleep" aus den USA untersucht die Qualität der Nachtruhe, indem er 15 Faktoren, die diese beeinflussen, unter die Lupe nimmt: Temperatur, Lärm, Aufsteh- und Zubettgehzeiten und so weiter. Aus all den Faktoren errechnet das System eine Punktzahl, die angibt, wie gut der Schlaf ist. Die Weckanlage bimmelt folglich nicht einfach punktgenau zur immer gleichen Uhrzeit. Sie weckt mit sanften Licht- und Geräuschimpulsen – und das nur dann, wenn die Person sich in einer Leichtschlafphase befindet.

Albtraum für Datenschützer

Was auf den ersten Blick nach jeder Menge Komfort klingt, hat bei genauerem Hinsehen seine Schattenseiten: Die Bewohner eines solchen Hauses werden permanent überwacht. Unternehmen wie Google oder Amazon, die ebendiese Services ermöglichen, protokollieren sorgfältig mit, was sich in diesen vier Wänden abspielt – und sammeln dabei einen enormen Datenwust auf ihren Servern und Clouds. Wenn sie auf Kooperationspartner zurückgreifen müssen (etwa, indem sie Musik oder Filme abspielen), geben sie diese Daten sogar an Dritte weiter.

Selbst wenn sich Geräte wie die smarten Lautsprecher im Ruhezustand befinden,

MEHR ZUM THEMA

Handbuch Datenschutz. Erfahren Sie, wo die Datenkraken in unseren Alltag eingreifen und was Sie tun können, um Ihre Privatsphäre zu bewahren (www.konsument.at/hb-datenschutz).

Foto: Zapp2Photo, Andrei Mayatnik/Shutterstock.com

ist nicht sicher, ob sie nicht dennoch heimlich mithören. Darf man einem ehemaligen Mitarbeiter von Amazon Glauben schenken, dann lauscht zumindest Alexa ständig. Dadurch könne sie ihr Sprachverständnis und ihre Sprechkompetenz noch schneller verbessern, so das Argument.

Generell werden die Nutzer in Datenschutzfragen im Ungewissen gelassen. In den entsprechenden Bestimmungen beteuern die Unternehmen gern, wie sehr ihnen das Thema am Herzen liege. Wenn es dann aber um Details dazu geht, was mit den Daten geschieht, halten sie sich mithilfe schwammiger Klauseln und vager Formulierungen bedeckt. Gleichzeitig lassen sie sich allerhand genehmigen. Google zum Beispiel lässt sich in den Nutzungsbedingungen seiner Lautsprecher das Recht einräumen, Daten aus unterschiedlichen Quellen zusammenzuführen. Dass die Firma dadurch imstande ist, noch präzisere Nutzerprofile zu erstellen, liegt auf der Hand.

Dabei ist Google noch sehr darauf bedacht, nicht mit einem Datenskandal oder einer Datenpanne negativ in der Öffentlichkeit aufzufallen. Zu viel stünde für den Internetriesen auf dem Spiel, während all die kleineren Anbieter von Smart-Home-Geräten, die nicht so sehr im Fokus der Aufmerksamkeit stehen, ihre gewonnenen Daten in der Werbewirtschaft zumindest theoretisch zu Geld machen könnten.

Steuerbar = fremdsteuerbar

Ein weiteres Problem ist der Umstand, dass alle übers Netz steuerbaren Geräte gleichzeitig immer auch fremdsteuerbar sind. Je mehr davon der Einzelne nutzt, desto mehr Einfallstore bieten sich für Hacker bzw. Einbrecher. Sogenannte White Hats (Hacker, die sich auf Sicherheitstests von Systemen spezialisiert haben) haben mehrfach bewiesen, dass zum Betätigen so mancher Türöffner-Anlage nur mittelmäßiges Programmier-Geschick erforderlich ist. Wie schlecht es um die Sicherheit von Gesichts- und Fingerabdruckkennungen bestellt ist, das hat sich beispielsweise beim iPhone gezeigt. Auch wenn es mitunter ein etwas aufwendiger Vorgang ist, haben IT-Spezialisten letztlich das System überlistet.

Eine Beleuchtungsanlage, die weiß, wann die Bewohner außer Haus sind, ist ein erstklassiger Informant für einen Dieb. Auch die Spracherkennungssysteme in smarten Lautsprechern (und somit die Steuerungszentralen) werden immer wieder gehackt. Forschern ist es im Labor gelungen, deren Steuerung sogar über für menschliche Ohren unhörbare Signale zu übernehmen.

Einer Studie aus den USA zufolge haben Cyberkriminelle Smart-Home-Geräte längst als Angriffsfläche von IT-Netzwerken entdeckt. Bei 96 Prozent der untersuchten Produkte gab es mindestens eine kritische Schwachstelle.

Im smarten Haushalt wird der bis dato mehr oder weniger geschützte räumliche Privatbereich Teil des Internets. Daten werden gesammelt, die mitunter intimste Angelegenheiten betreffen. Der technikverliebte Bewohner nimmt all das in Kauf – ohne sich auf gesetzliche Rahmenbedingungen verlassen zu können, die Angelegenheiten das Internet der Dinge betreffend regeln. Denn derzeit stehen wir erst am Anfang.

Rat und Hilfe für Verbraucher in Europa ECC-Net
Finanziell unterstützt durch die Europäische Union

Dieser Artikel wurde aus den Mitteln des Verbraucherprogramms der Europäischen Union (2014 – 2020) gefördert.