Die smarte Kapitulation

Das vernetzte Haus wird mit Apps und dem Smartphone gesteuert. Die Ideen sind hochfliegend. Wer ans Sparen und mehr Effizienz denkt, hat jedoch die Ziele von Google & Co. nicht verstanden.

Von Michael Spehr und Lukas Weber

Mehr Komfort und Lebensqualität, ein Zugewinn an Sicherheit und eine effizientere Energienutzung: Das smarte und intelligent gesteuerte Heim der Zukunft verspricht ein neues Wohnen im Zeitalter der vernetzten Systeme. Unter dem Begriff Smart Home versammeln sich unterschiedliche Ansatzpunkte für eine Automation nicht nur der Gebäudetechnik, sondern auch von Lampen, Steckdosen und Kühlschränken bis hin zur Unterhaltungselektronik und Sicherheitstechnik sowie Gartengeräte. Alle Komponenten kommunizieren untereinander und mit Apps, sie sind aus der Ferne programmierbar und so smart, dass man angeblich den feinen Luxus der cleveren Steuerung nicht mehr missen möchte.

Sogar ganz neue Szenarien der Fürsorge stellte unlängst der hessische Energieversorger Mainova in einem Musterhaus bei Bad Vilbel vor: Wird die Kaffeemaschine der Großmutter morgens nicht wie gewohnt eingeschaltet, löst die Anlage einen Alarm aus. Man könne dann bei älteren alleinstehenden Personen anrufen oder einen Nachbarn vorbeischicken, um zu sehen, ob alles in Ordnung ist. Die fürsorgliche Behütung im vernetzten Zuhause kann indes auch zur Falle werden, wie unlängst erlebt: Der Freund weilte in Amerika, und die Partnerin zu Hause hatte kalte Füße. Die Heizung höherzustellen, war ihr nicht möglich, denn die hochintelligente Anlage hatte ihren App-Zugang aus welchen Gründen auch immer gesperrt. So half in diesem Falle nur eine besondere Art der Fernwärme: Er stand nachts in New York auf und programmierte kurzerhand mit seinem Handy die Heizung für sie in Neu-Anspach um. Die kuriose Episode zeigt, welche Herausforderungen mit dem vernetzten Heim einhergehen können – und dass eine gewisse Zurückhaltung angesagt ist, wenn es darum geht, die langlebige Welt des Wohnens mit der schnellen des Smartphones zu verbinden.

Die Ideen rund ums Smart Home sind nicht neu. Dass der vernetzte Kühlschrank die schwindenden Milchvorräte erfasst und nachbestellt, machte schon vor Jahrzehnten als Idee die Runde. Neu ist nunmehr die Systemintegration und die übergreifende Steuerung aller elektrischen und elektromechanischen Systeme in einem Gebäude. Die Vernetzung reicht von einzelnen Komponenten über Elektrogeräte bis hin zu jenen Heimapparaten, die schon lange verbunden sind, Stichwort: Audio- und Videosysteme. Wenn alles unter einem Dach zentral verwaltet und gesteuert wird und die Anbindung ans Internet vorhanden ist, liegt in den entsprechenden Szenarien der Mehrwert sofort auf der Hand: Nicht nur beim Energie-Management des Anwesens, sondern zum Beispiel auch bei der Sicherheit: Das offenstehende Fenster wird automatisch verschlossen, sobald der letzte Bewohner das Haus verlassen hat. Dank Biometrie und Anwesenheitsdetektoren steuert das Smart Home die Zugangskontrolle mitsamt Pin-Code oder einem Scan von Fingerabdruck und Gesicht. Bei Einbruch, Brand oder Wasserschäden werden entsprechende Maßnahmen automatisch eingeleitet.

Das Smart Home der Zukunft lässt sogar die Immobilie hinter sich und bezieht das Auto mit ein. Der Verband der deutschen Automobilindustrie hat sich unlängst der Eebus-Initiative für das vernetzte Zuhause angeschlossen, weil auch das Auto über Einträge im Terminkalender der Hausbewohner energietechnisch optimiert fahren soll und zudem das Laden von Elektromobilen nur in einer „intelligenten“ Netzinfrastruktur mit entsprechender Informationstechnik erfolgen könne.

Doch die Tücken der schönen neuen Welt liegen im Detail: Welchen Standards gehorcht das Smart Home? Die Frage nach Protokollen und Übertragungswegen ist die entscheidende. Hier wird das Rennen um die Hausautomation gewonnen. Gewiss: Ein übergreifender Standard wie die Mobilfunk-Normen könnte die nächste Stufe der Entwicklung zünden. Aber klar ist, dass die großen IT-Matadore kein Interesse an offenen, transparenten und kompatiblen Systemen haben. Denn sie wollen ihre eigenen Plattformen und Ökosysteme aufbauen, die wie App-Stores funktionieren und eine Monetarisierung über Hardware, Software, Lizenzgebühren und natürlich Nutzerdaten erlauben. Die Nutzerdaten haben allerhöchste Priorität. Wer den Zugang zum Kunden hat, übernimmt nicht nur die Kontrolle der Heizung oder des Kühlschranks, sondern öffnet die Haustür sperrangelweit für alle künftigen digitalen Geschäftsmodelle. Dabei geht es nicht allein darum, dass der defekte Kühlschrank selbsttätig anbietet, den passenden Kundendienst zu alarmieren, sondern vielleicht auch, den Fitness-Kurs im Studio um die Ecke zu buchen, wenn Kühlschrankinhalt und die Auskünfte der Digitalwaage signalisieren, dass die Probleme der Hausbewohner schwerwiegender sind.

So wundert kaum, dass wenige Hersteller auf bewährte offene Standards wie Bluetooth, Dect oder Wireless-Lan setzen. Die neuen Protokolle für das smarte Heim werden von strategischen Wirtschaftsallianzen vorangetrieben und basieren auf Funkstandards, denn natürlich sollen sich die einzelnen Komponenten vom Heizkörperthermostat bis zur programmierbaren LED-Leuchte drahtlos untereinander austauschen.

Einer der ältesten Standards ist Zig Bee, der wiederum exemplarisch zeigt, woran es krankt: Obwohl Zig Bee schon 2002 definiert und wenig später sogar zu einer IEEE-Norm wurde, die mittlerweile von mehr als 250 namhaften Unternehmen mit Tausenden von Geräten unterstützt wird, sind weder seine Vorteile weithin bekannt, noch kann man sich darauf verlassen, dass Zig-Bee-Produkte verschiedener Hersteller reibungslos miteinander funktionieren. Zig Bee arbeitet im Frequenzbereich von 868 und 2400 Megahertz, und sein großer Pluspunkt ist die geringe Stromaufnahme. Im Schlafmodus können Geräte mit weniger als ein millionstel Ampere auskommen und damit über Jahre hinweg wartungsfrei mit einer einzigen Batterie laufen. Trotz Zertifizierung arbeiten Produkte verschiedener Hersteller oft nicht unter dem Zig-Bee-Dach zusammen, selbst wenn die Funktionalität ausdrücklich beworben wird. Denn Zig Bee fächert sich in eine ganze Familie diverser Standards auf. Allein die Hauptspezifikation Zig Bee Pro umfasst sechs Unterprofile und ein siebtes für batterielose Schalter. Ferner gibt es ein Zig-Bee-System für die Steuerung von Unterhaltungselektronik mit drei weiteren Profilen sowie ein Zig Bee IP mit Spezifikationen für das Internet der Dinge und IP V6. Ungeachtet der Zertifizierung werden Zig-Bee-Anwendungen um proprietäre Erweiterungen ergänzt, und damit ist dann endgültig das Ende der Kompatibilität erreicht.

Das neue Zig Bee 3.0 soll vieles besser machen, aber die Rivalen stehen schon Gewehr bei Fuß: Allen voran Thread, das von ARM, Samsung und der Google-Tochtergesellschaft Nest vorangetrieben wird und ebenfalls auf der IEEE-Spezifikation aufsetzt. Einige existierende Zig-Bee-Produkte wie die Hue-Lampen von Philips lassen sich mit einem Firmware-Update kompatibel zu Thread machen. Z-Wave heißt ein weiterer Standard, der von der ITU, der internationalen Fernmeldeunion, abgesegnet wurde. Insellösungen bestimmen das Bild in Deutschland. So hat beispielsweise der Energieversorger RWE sein eigenes Smart Home im Angebot, das ebenfalls im 868-Megahertz-Band mit Heizkörperthermostaten, Fenstersensoren, Bewegungs- und Rauchmeldern arbeitet. Die Basis der Deutschen Telekom und anderer für die Heimautomation heißt Qivicon und wird von mehreren Dutzend Unternehmen unterstützt, darunter Belkin, Karcher, Miele, Philips, Samsung und Vattenfall. Qivicon setzt auf den Standards Home Matic sowie Zig Bee auf und erfordert ein Abonnement.

Doch die fehlende Kompatibilität und die Probleme der Zusammenarbeit der Geräte verschiedener Hersteller lassen das Bild des smarten Zuhauses in eher trüben Farben erscheinen. Wie sieht es mit der Langlebigkeit der Produkte aus? Was 2014 besonders smart wirkte, mag schon 2016 nicht mehr mit iPhone & Co. zusammenarbeiten, weil der Hersteller mit seiner schmucken Insel nicht mehr am Markt ist und die alte Hardware an moderne Betriebssysteme angepasst werden müsste. Auch mit der Idee, dass digitale Messsysteme für Energie selbige und Geld sparen, ist es nicht weit her. Im Gespräch ist derzeit vor allem der Stromzähler, grundsätzlich lässt sich aber auch der Gasverbrauch smart messen. Für den schrittweisen Umstieg der Verbrauchserfassung hat der Bundeswirtschaftsminister ein Gesetzesvorhaben auf den Weg gebracht. Die Idee: Moderne Zähler berechnen nicht nur die angefallenen Kilowattstunden in der Summe, sondern können die aktuellen Verbräuche darstellen. Den Haushalten und Unternehmen gestattet das, den Bedarf einzelner Geräte zu erkennen und Stromfresser durch sparsamere Modelle zu ersetzen. Als „intelligente Messsysteme (Smart Meter)“ sind sie zusätzlich mit einem Kommunikationsmodul ausgestattet. Es kann die Daten zum Energieversorger übermitteln und erspart damit das Ablesen. Den Verbrauchern eröffnet das Smart Meter die Möglichkeit, etwa günstigen Nachtstrom zu nutzen. Der Tarif ließe sich sogar viertelstündlich den aktuellen Börsenpreisen anpassen.

Die Übertragung erfolgt über Funk, Kabel, Internet oder das Stromnetz. Der Hausbesitzer kann dann auf dem Tablet oder dem Smartphone die Informationen zum aktuellen Verbrauch abrufen und via App zum Beispiel einzelne Geräte an- oder abschalten. Größere Verbraucher, genannt werden gern Waschmaschinen und Trockner, können dann zu Zeiten niedrigen Stromverbrauchs und günstiger Tarife aktiviert werden, das soll den Bedarf gleichmäßiger verteilen und den Energieverbrauch insgesamt senken.

Das klingt gut. Stellt sich die Frage, warum fast alle, von den Verbraucherschützern über die Interessenvertreter der erneuerbaren Energien bis hin zum Bundesrat, etwas an den Plänen der Bundesregierung auszusetzen haben. Der erste Grund ist wirtschaftlicher Natur. Smart Meter lohnen sich für die meisten Haushalte nicht: Untersuchungen im Auftrag der Verbraucherzentralen zeigen, dass die Einsparungen deutlich geringer sind als die Kosten der Geräte (gestaffelt bis 100 Euro im Jahr).

Die meisten Kleinverbraucher verlagern, soweit möglich, stromintensive Tätigkeiten wie Waschen und Trocknen ohnehin in die Abendstunden und ins Wochenende, für den Gesamtverbrauch spielt das kaum eine Rolle. Und Großverbraucher wie Kühlhäuser werden bisher schon dann zugeschaltet, wenn der Strom günstig ist. Für die privaten Kunden fehlen außerdem gesplittete Tarife – aber falls es sie geben wird, ist zu erwarten, dass die Einheitstarife für Kunden ohne intelligente Steuerung teurer werden.

Der zweite Grund ist die Datensicherheit. Google und anderen geht es nicht um Strom, Wärme oder das Energiesparen, sondern um den Kunden als gläsernen Verbraucher. Aus der Nutzung einzelner Elektrogeräte lässt sich leicht und sehr detailliert auf die Lebensgewohnheiten schließen. Deshalb muss sichergestellt sein, dass die Daten nur als gesammelte Werte übertragen werden. Dazu sehen die Richtlinien des BSI unterschiedliche Muster vor, die der Kunde mit der Wahl seines Tarifs beeinflussen können soll. So wie es derzeit aussieht, sind intelligente Messsysteme für die Verbraucher eher eine Mogelpackung als nützlich. Die Steuerung der Elektrogeräte im Smart Home funktioniert jedenfalls auch ohne die ständige Datenübertragung an den Energieversorger. Von Google gar nicht zu reden.

Schließlich müssen sich alle Hersteller die Kritik gefallen lassen, dass ihre Systeme nicht sicher genug sind. Zuletzt waren in einer Studie von HP Security Research ausnahmslos alle Anlagen des vernetzten Heims über ihren Cloud-Zugang angreifbar: „Als hätten alle Erfahrungen, die während der vergangenen 25 Jahre hinsichtlich der Sicherheit gemacht wurden, nie stattgefunden.“ Einfachste Verfahren für mehr Sicherheit wie die Pflicht zu langen Kennworten, die Sperrung von Konten nach mehrfacher Falscheingabe eines Kennworts, die Zwei-Faktor-Authentifizierung, die verschlüsselte Übertragung von Daten zum Anbieter und die Prüfung von Updates auf Manipulation hin fehlten laut dieser Studie.

Angesichts überbordender Begeisterung achtet niemand auf solche Details. Wenn sich die fernbedienbare Haustür bereitwillig dem Einbrecher öffnet, weil dessen Handy mit der jüngsten Bluetooth-Hackersoftware bestückt ist, dürfte indes mancher Freund solcher Lösungen erkennen, dass ein Haus kein Spielzeug für Apps ist. Smart soll sein, dass letztlich Eigentümer und Mieter die Kontrolle über ihr Heim aufgeben. Was dort Dritte mit Apps und Daten veranstalten, bleibt vollkommen intransparent. Das kann es nicht sein.