Vom Wohnzimmer aus das Kinderzimmer im Blick zu behalten, kann Eltern ein sicheres Gefühl vermitteln. Doch wer schaut sonst noch zu?

Bild: Your Best Digs. CC BY 2.0, Flickr

Forum Smart Home 2019

Wie sicher ist die vernetzte Wohnung?

Smart Homes sollen Komfort und Sicherheit bieten. Wenn plötzlich eine unbekannte Stimme aus dem Überwachungssystem ertönt, wird das moderne Wohnerlebnis aber schnell ungemütlich. Wie das «Forum Smart Home» zeigte, können einfache Massnahmen viel bewirken, doch oft fehlt das Risikobewusstsein.

Von Nadine Siegle

Einen Knopf zu drücken und ‹Licht an› zu befehlen, ist kein bisschen effizienter als einen gewöhnlichen Lichtschalter zu betätigen», betonte Reiner Hoffmann, Verkaufsleiter bei der Feller AG, am diesjährigen «Forum Smart Home» von Electro Suisse. Eine Wohnung ist noch lange nicht intelligent, wenn das Licht oder die Storen per Sprachbefehl gesteuert werden können. «Die Lösungen müssen mehr können, sie müssen wirklich intelligent sein», so Hoffmann. Das tönt logisch, doch in der Faszination um moderne Haushaltstechnologien scheinen diese Überlegungen regelmässig in den Hintergrund zu treten. So wurde auch in Basel immer wieder die Frage aufgeworfen: Sind Smart-Home-Lösungen nur Spielereien?

Auf einem Markt mit etlichen Anbietern von Einzellösungen erstaunt es kaum, dass die heutigen Anwendungen eher Spielerei-Charakter haben. In den meisten Wohnungen, die mit irgendeiner Form von intelligentem System ausgestattet sind, wird dieses derzeit vor allem für die Beleuchtung oder die Musiksteuerung per Sprachbefehl genutzt. «Amazon Echo oder Google Home haben für den Endbenutzer sicherlich ihre Berechtigung», ist Hoffmann überzeugt. Doch die Skepsis überwiegt: «Sind das wirklich smarte Systeme? Oder sind sie bloss nebeneinander existierende Lösungen für Teilprobleme?» Hoffmanns Fragen werfen vor allem mehr Fragen auf: Was soll das Smart Home überhaupt können? Welche Probleme haben diese «Lösungen» denn zu «lösen»? Einigkeit besteht darüber, wem ein intelligentes Zuhause dienen soll: Dem Menschen, der darin wohnt. Es geht um Komfort bei gleichzeitiger Ressourcenschonung. Noch etwas, das eigentlich logisch tönt. Selbstverständlich ist es aber nicht: «Unternehmen arbeiten stets an der Optimierung ihres Produkts. Doch erst am Ende stellen sie sich die Frage, was denn der Kunde überhaupt will», bedauert Markus Kramer, Associate Professor in Brand Management an der Cass Business School in London. Er plädiert für die umgekehrte Denkweise: Nicht die Technologie solle im Vordergrund stehen, sondern der Mensch und seine Bedürfnisse. Ist die Steuerung der Storen über modernste Technologien für den Anwender etwa zu kompliziert, wird er seine Fenster weiterhin manuell abdunkeln. Für Kramer bedeutet das: Die Technologie soll für den Benutzer quasi unsichtbar sein. Die Geräte müssten lediglich intuitiv bedient werden können.

Einfachheit als oberstes Gebot

«Wenn man sich nach einem Unfall oder einer Operation nicht bewegen kann, ist es optimal, das Licht und die Storen per Smartphone vom Sofa aus steuern zu können. Aber auch ein 80-Jähriger muss diese Funktionen in seiner Wohnung bedienen können», betont Ivo Bracher, Geschäftsführer und Verwaltungsratspräsident der Solothurner Immobilienanlagefirma Bonainvest Holding AG. Es braucht also einfach bedienbare Lichtschalter und Steuerungen. Das Tochterunternehmen Bonacasa AG hat in den letzten Jahren verschiedene Technologien im Smart-Home-Bereich in Musterwohnungen verbaut und getestet. Die Bedürfnisse älterer Menschen flossen dabei genauso in die Entscheidungen ein wie diejenigen jüngerer Generationen. Bracher ist überzeugt: «Wenn wir für die nächsten 50 bis 100 Jahre bauen, können wir uns nicht nur auf eine bestimmte Zielgruppe ausrichten.»

Schliesslich gelangt man zur Frage, wie vernetzt und intelligent eine Wohnung oder eine geplante Überbauung sein soll – von niederschwelliger Vernetzung einzelner Funktionen bis hin zu einem «Rundum-Sorglos-Paket» ist fast alles möglich. Neben Steuerungsmöglichkeiten per App – etwa für die Beleuchtung oder Heizung – sind vernetzte Angebote mit Videotürsprechanlagen, Licht- und Rollladenszenarien, Ferienfunktionen, Rauchmeldern oder Notruf-Knöpfen denkbar.

Dabei dreht sich vieles um das Thema Sicherheit in den eigenen vier Wänden. Möglich wäre beispielsweise auch eine Alarmierungsfunktion für Notfälle, wenn sich jemand in der Wohnung aufhält, aber 14 Stunden lang keinen Schalter mehr betätigt hat. «Als meine Grossmutter im Bad gestürzt ist, trug sie ihr Alarmierungsarmband nicht. Sie war sich zu chic dafür. Glücklicherweise kam die Spitex nach dreieinhalb Stunden ohnehin vorbei und hat sie gefunden», sagt Bracher erleichtert. «Andere haben weniger Glück und liegen drei Tage da, bis jemand sie findet.» Ein eingebauter Alarmierungsmechanismus würde zumindest nach einer gewissen Zeit Hilfe rufen.

Unabhängig davon, für welche Lösungen man sich beim Bau entscheidet, auch für Bracher steht die Einfachheit an erster Stelle: «Ein roter Knopf für ‹Ich verlasse die Wohnung›, ein gelber für ‹Ich bin hier›, so simpel muss es sein. Das Smartphone kann das alles auch, aber es muss auch ohne Handy einfach zu bedienen sein.» Die Erfahrung habe zudem gezeigt, um Nutzungsbarrieren abzubauen müsse man die Bewohner in die Funktionen einführen und ihnen die neuen Möglichkeiten aufzeigen.

Stiefmütterlicher Umgang mit Risiko

Zwar geht es bei Smart Homes nicht nur um das Wohnen im Alter, die Geschichte von Brachers Oma zeigt jedoch: Bei intelligenten Wohnsystemen sind Komfort und Sicherheit eng miteinander verknüpft. Doch mit der Sicherheit ist es so eine Sache. Mit Smart-Home-Lösungen werden Sensoren und Kameras zum gewohnten Umfeld, Alexa und Siri zu hilfsbereiten Mitbewohnerinnen. Doch würde man menschliche WG-Genossen tolerieren, die einem rund um die Uhr belauschen?

Der 90-jährigen Grossmutter mag schneller geholfen sein, wenn sie stürzt. Das Neugeborene kann über das multifunktionale Babyfon sicherlich gut überwacht oder gar mit der eigenen Stimme aus dem Nebenzimmer beruhigt werden. Doch diese Systeme bieten auch Angriffsflächen für Hackerangriffe. Hier orten Experten grossen Handlungsbedarf: «Das Thema wird heute leider noch etwas stiefmütterlich behandelt», bedauert Daniel Berchtold, Mitgründer der Walliser Hooc AG, die sich auf Fernzugriff-Lösungen spezialisiert hat. Ein Grund, weshalb Smart-Home-Systeme häufig einfacher zu hacken sind, als viele Nutzer denken, sind sie selbst. «Der Endkunde möchte auf die gesammelten Daten und die Steuerung von überall Zugriff haben.» Das bedarf einer Verbindung, durch die Daten ins Netzwerk hinein wie auch hinaus fliessen. Man spricht dabei vom sogenannten Ingress und Egress Traffic. «Bei einer typischen Internet-of-Things-Anwendung wird ein Sensor in der Wohnung platziert, der von dort Daten nach draussen sendet», erklärt Berchtold. Der Ingress Traffic kommt von aussen nach innen, etwa durch Fernzugriffe auf die Smart-Home-Steuerung.

Webcam: Einfallstor für Einbrecher?

Diese «Türen» zwischen den eigenen Systemen sind keine anonymen Zugänge, die lediglich der Nutzer kennt und verwendet. Berchtold zeigt anhand von «Shodan», einer Suchmaschine für das Internet der Dinge, weshalb man sich dieser Risiken bewusst sein sollte: «Mann kann sich Shodan so vorstellen, als ob jemand von Tür zu Tür spaziert, anklopft und schaut, ob jemand aufmacht und wenn ja, wer das ist und was man sonst noch so erfährt.» Die Suchmaschine frage den jeweiligen Router nach seinen Ports und speichere die Antworten, die vom Router zurückkommen. «Shodan speichert alles auf einer Datenbank, die für jeden einsehbar ist. Darin findet man alle Geräte, welche die Suchmaschine bis heute ausfindig gemacht hat.» Von da gelange man mit wenigen Klicks in eine beliebige Webcam, Überwachungskamera oder sonstige von Shodan gefundene Geräte. «Die meisten Kameras haben lediglich Standardpasswörter hinterlegt. Es ist also ein Leichtes, in sie einzudringen. So schnell dient eine

> «Wenn im Netzwerk nur ein kleiner Teil, wie der Staubsaugerroboter, schlecht geschützt ist, ist das komplette Netzwerk schlecht geschützt.»
>
> **Daniel Berchtold,**
> Mitgründer und Mitglied der Geschäftsleitung, Hooc AG

Kamera, die mich eigentlich schützen sollte, auch dem Einbrecher», so Berchtold.

Die Vorstellung ist beängstigend. Doch was kann wirklich passieren, abgesehen davon, dass jemand statt durchs Fenster durch die Webcam in die Wohnung schaut? «Wenn im Netzwerk nur ein kleiner Teil schlecht geschützt ist, ist im Grunde genommen das komplette Netzwerk schlecht geschützt.» Das kann wegen kleinen Lücken im Staubsaugerroboter oder im smarten Fernseher der Fall sein. Die Technologie vieler Steuerungen im Haus sei bereits veraltet, so Berchtold. Auch wenn man sich mit modernen Firewalls oder Virenscannern abzusichern versuche, seien sie ein Risiko. Wer ein kleines Türchen findet, kann sich Zugriff auf alles verschaffen, was damit vernetzt ist.

Beispiele von Hackerangriffen auf Private in ihren eigenen vier Wänden gibt es genug. Bekannt sind etwa Geschichten, in denen sich ein Unbekannter Zugriff auf das Babyfon oder Überwachungskameras verschaffte und plötzlich mit dem einschlafenden Kind oder dem Babysitter sprach. Das sind schockierende, aber vergleichsweise «kleinere» Eingriffe, wenn man an Hackerangriffe auf Energieversorger oder gar Atomkraftwerke denkt – alles bereits vorgekommen.

So wird das Smart Home sicherer

«Aus der Praxis wissen wir: Wer beim Endkunden Smart-Home-Installationen macht, kann realistischerweise keine riesige IT-Infrastruktur aufbauen», so Berchtold. Sicherheitsvorkehrungen wie bei einem Atomkraftwerk wären in einem Smart Home wohl unverhältnismässig. Doch Berchtold ist überzeugt, mit wenigen Massnahmen könne man schon viel bewirken.

› **Sichere Passwörter:** «Es tönt lachhaft, aber das ist tatsächlich wichtig.» Es gebe immer noch Geräte, die vor der ersten Nutzung keine zwingende Passwortänderung verlangen. Die Devise lautet: «Standardpasswörter immer ändern.»

› **Aktualisierte Systeme:** Sicherheits-Updates und Patches müssen eingespielt werden. «Als Integrator könnte man auch über ein Abo für den Kunden nachdenken, wie man es von Virenscanner-Abos für den PC kennt», so Berchtold.

› **Vertraute Hardware:** Mit dem Einsatz von bekannter Hardware, fahre man besser, ist Berchtold überzeugt. «Vielleicht ist der Staubsaugerroboter mit der Kamera aus China nicht das ideale Produkt, um es zuhause am WLAN anzuhängen.» Bei vertrauten Hardware-Anbietern könne man eher davon ausgehen, dass deren Produkte von vielen anderen ebenfalls geprüft wurden und Probleme allenfalls bereits ans Tageslicht gekommen wären.

› **Getrennte Netzwerke:** Geräte können auch in einem separaten, von anderen Systemen abgekoppelten Netzwerk zusammengeschlossen werden. «Das ist in der Gebäudeautomation mittlerweile schon fast zu einem Standard geworden», sagt Berchtold. Möglich wäre, zwei Netzwerke einzurichten. Eines für Geräte, bei denen ein Zugriff nicht ganz so dramatisch wäre. Und ein sichereres für all jene Systeme, in denen sich Daten befinden, die definitiv nicht gestohlen werden oder abhanden kommen sollen. Je mehr IT-Kenntnisse vorhanden sind, desto mehr Möglichkeiten gibt es dafür.

› **Verschlüsselung:** «Wenn man von aussen auf Systeme zugreifen möchte, sollte dieser Zugriff verschlüsselt sein», betont Berchtold. Ein virtuelles privates Netzwerk, kurz VPN, sei ein sehr gutes Mittel dazu.

Vernetzung auf allen Ebenen

Mit wenigen Sicherheitsvorkehrungen kann der Endkunde bereits deutlich geschützt werden. Berchtolds Ausführungen zeigen vor allem, wie bedeutsam IT-Kenntnisse bei Installationen in modernen Wohnungen sein können. Dies stellt Anbieter in unterschiedlichen Branchen vor neue Herausforderungen. «Im Energiebereich wissen wir, was wie miteinander funktioniert und interagiert», sagt Eike Johann, Business Developer bei der BKW Energie AG. «Wir müssen nun aber auch verstehen, was auf der Datenebene in der Erfassung und Steuerung passiert.» Die verschiedenen Gewerke müssten zusammengebracht werden. Es reiche nicht mehr, lediglich die einzelnen Systeme zu verstehen.

Das Schlüsselwort lautet Vernetzung: Geräte mit anderen Geräten, Maschinen mit Menschen, aber auch Menschen mit Menschen. «Heute plant im Gebäudebereich jeder für sich. Ein Haus wird nie zum Smart Building, wenn wir nicht gemeinsam planen», so Klaus Wächter, Global Standardization Manager bei Siemens Building Technologies. Ivo Bracher von Bonainvest betont: «Die Vernetzung aller Beteiligten muss bereits früh in der Planungsphase stattfinden.» Der Investor müsse begreifen, worum es geht. Alle Partner, vom Hauseigentümer bis zur Verwaltung, müssten ins Boot geholt werden. «Es sind viele Akteure involviert, bis man am Schluss eine stimmige Lösung hat.» Es soll schliesslich ein Haus entstehen, das sowohl in der Nutzung als auch im Unterhalt einfach zu handhaben ist. Denn auch in Sachen Instandhaltung gelte das Gebot der Einfachheit.

Bis die «Smartifizierung» der eigenen vier Wände derart fortgeschritten ist, dass man sich nicht bloss über den neuen selbstlernenden Staubsaugerroboter freut, sondern den Komfort des eigenen Smart Homes als selbstverständlich erachtet, braucht es noch einiges an Vernetzungsarbeit. «Die Systeme müssen im Hintergrund so smart funktionieren, dass sie fast unbemerkt mit mir zusammenleben», betont Markus Kramer. Die Branchenvertreter sind jedoch überzeugt, dass die Entwicklung ähnlich verlaufen wird wie beim Smartphone: Nach einer ersten Angewöhnungszeit ist es heute schon fast mit uns verschmolzen und ein Leben ohne ist kaum noch vorstellbar. ■

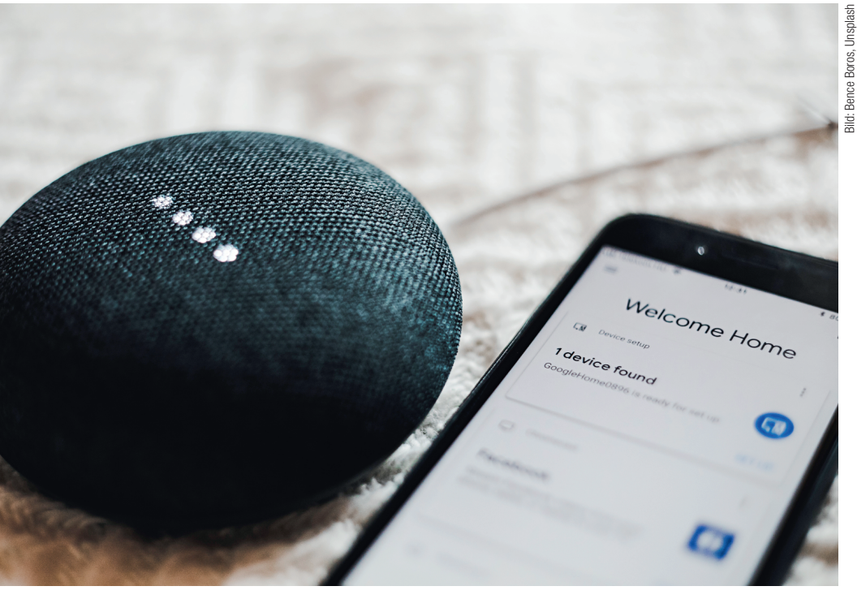

Bild: Bence Boros, Unsplash

Willkommen Zuhause: Es gibt bereits viele Anwendungen, die eine Steuerung per Smartphone zulassen. Zurzeit sind aber vor allem unabhängige Einzellösungen, etwa von Google Home, in Gebrauch.