INHALTSVERZEICHNIS

WAS GEHT ÜBERHAUPT?

SCHRITT FÜR SCHRITT ZUM EIGENEN SMART HOME

SYSTEME IM ÜBERBLICK

VOM SMARTEN GERÄT ZUM SMARTEN GEBÄUDE

Die Vorsilbe „smart“ wird seit einigen Jahren geradezu inflationär gebraucht. Auf das Smartphone folgten der Smart-TV und die Smartwatch. Lautsprecher mit Sprachsteuerung heißen Smart Speaker, Dosierautomaten für Hunde- und Katzenfutter Smart Feeder. Ja selbst Wasserkocher, Zahnbürsten und Fieberthermometer nehmen das Attribut in Anspruch, irgendwie smart zu sein. Nicht selten erschöpft sich dieser beworbene Vorteil in Vernetzung. Die Geräte sind per Funk steuerbar, über eine Onlineverbindung können sie Informationen austauschen, digitale Medien und neue Software aus dem Internet nachladen.

Als kleinster gemeinsamer Nenner trifft das auch auf viele Smart-Home-Produkte zu, die mittlerweile unsere Wohnungen bevölkern. All die vernetzten LED-Lampen, Raumthermostate, Türschlösser und WLan-Kameras haben eines gemeinsam: Ihr Bedienkonzept basiert auf dem Smartphone. Die App des Herstellers hilft bei der Installation der Geräte und assistiert später im Alltag. Sie macht das gedruckte Handbuch überflüssig – sofern der Anbieter sein Software-Handwerk versteht und dem Gerät nicht einfach ein billig zugekauftes Programm überstülpt.

Fast immer handelt es sich bei diesen Produkten um Insellösungen. Sie kümmern sich um ein Gewerk, wie Fachleute am Bau sagen würden. Das kann zum Beispiel die Licht- oder Heizungssteuerung sein. Es gibt Spezialisten, die das Haus überwachen, Musik wiedergeben den Rasen mähen oder die Blumen bewässern. Je mehr davon zusammenkommen, desto aufwendiger und unübersichtlicher wird die

Funkthermostate wie das Wiser-System von Eberle regeln die Raumtemperatur.

Überwachungskameras wie die Nest Cam von Google behalten die Wohnung im Blick.

Steuerung. Denn proportional zu den Geräten steigt die Zahl der Apps auf dem Smart-phone. Timer sind über viele Programme verteilt und müssen dort mehrfach eingestellt werden, wenn etwa das Bad morgens zur selben Zeit warm, hell erleuchtet und aufmunternd beschallt sein soll. Mit jeder neuen Insellösung wächst der Wunsch, die Technik zu vereinheitlichen und zusammenzufassen.

Womöglich sind Sie bereits an diesem Punkt angekommen. Vielleicht lesen Sie dieses Buch aber auch in kluger Voraussicht – oder mit der Vorahnung, dass smarte Produkte allein Sie nicht weiterbringen werden. Dann ist es an der Zeit, über ein vernetztes Gebäude nachzudenken, ein Smart Home, das diesen Namen wirklich verdient. Es führt verschiedene Aufgaben unter einer Steuerlogik zusammen. Das Ganze ist dabei mehr als die Summe seiner Teile, weil die Geräte zusätzliche Aufgaben übernehmen können. Ein Fensterkontakt ist Teil der Alarmfunktion und drosselt gleichzeitig die Heizung, wenn gelüftet wird. Lautsprecher dienen der Unterhaltung, spielen aber auch Warntöne und Durchsagen ab.

Der Unterschied besteht im ganzheitlichen Ansatz. Während smarte Insellösungen meist zweckgebunden und nach aktuellem Bedarf angeschafft werden, beginnt die Planung eines Systems am anderen Ende der Investition: dem Vollausbau. Wer weiß, wo er hinwill, kann gleich von Anfang an den richtigen Weg einschlagen. Dabei macht es einen Unterschied, zu welchem Zeitpunkt die Installation stattfindet. Geschieht sie im Rohbaustadium, beziehungsweise während einer grundlegenden Gebäudesanierung? Dann sind Operationen am offenen Mauerwerk meist kein Problem. Oder soll sie lieber nachträglich in der möblierten Wohnung passieren, quasi minimalinvasiv wie bei einem ambulanten medizinischen Eingriff?

Systeme wie Digitalstrom lassen sich auch nachträglich in eine vorhandene Elektroinstallation integrieren.

Gebäudenetzwerke im Vergleich

Technologie	Drahtlos (Funkbus)	Stromnetz (Powerline)	Verkabelt (Installationsbus)
Definition	Die Smart-Home-Geräte kommunizieren per Funksignal miteinander.	Geräte nutzen das vorhandene Stromnetz (230 Volt) zur Kommunikation.	Die Steuersignale laufen über eigene (Bus-)Leitungen in den Wänden.
Besonders geeignet für	Nachrüstung	Nachrüstung	Neubau / Sanierung
Installationsaufwand	Gering	Mittel	Hoch
Do-it-Yourself-Potenzial	Hoch	Gering	Gering
Einstiegskosten	Eher gering	Mittel	Eher hoch
Störanfälligkeit des Netzwerks	Mittel	Gering	Sehr gering
Schrittweiser Aufbau	Problemlos, auch nachträglich	Problemlos, auch nachträglich	Schwierig (Basisinstallation muss stehen)
Typische Standards	Bluetooth, EnOcean, Homematic IP, KNX RF, Loxone Air, Thread, Z-Wave, Zigbee, WLan	Digitalstrom, KNX PL	Homematic IP wired, KNX TP, LCN, Loxone, MyGekko

tet. Im Smart Home konnte sich die Methode bislang dagegen kaum durchsetzen, von den erwähnten Beispielen abgesehen. Das hängt mit der Gebäudetechnik zusammen, die traditionell aus Hardware besteht. Lichtschalter oder Rollläden haben normalerweise keine Folgekosten. Und fest montierte Sensoren oder Aktoren sind nicht so leicht zu wechseln, wie ein Streaming-Abo, falls der Anbieter seine Gebühren erhöht. Das lässt viele Heimvernetzer vor wiederkehrenden Zahlungen zurückschrecken.

Ein automatisiertes Haus basiert inzwischen aber auch auf einiger Software. Die zunehmende Vernetzung – von der Abzugshaube bis zur Waschmaschine – erhöht den Entwicklungsaufwand. Selbst Jahre nach dem Kauf, wenn das Gerät beim Kunden steht, können Sicherheitsupdates und App-Aktualisierungen nötig werden. Solange der Hersteller seine Entwicklungskosten über den Verkauf neuer Produkte gegenfinanzieren kann, ist alles in Ordnung. Gelingt das nicht mehr, müssen die Kundinnen und Kunden für den Unterhalt aufkommen; sei es per Wartungsvertrag, Softwareabo oder bezahlte Upgrades, die neue Funktionen versprechen. Selbst scheinbar kostenlose Dienste wie Alexa oder der Google Assistant gibt es nicht umsonst. Wer sie verwendet, bezahlt dafür mit seinen Daten.

In unserem Rechenbeispiel stattet eine Wohngemeinschaft ihr Zuhause mit smarter Technik aus.

Rechenbeispiel: günstiges Smart Home in der WG

Die Ausgangssituation: Eine vierköpfige Wohngemeinschaft möchte ihre Räume energiesparend ausstatten. Smart-Home-Produkte sollen verhindern, dass die Heizung bei gekippten Fenstern weiterläuft. Auch vergessen die Wohnenden gelegentlich, das Licht und andere elektrische Verbraucher auszuschalten. Da es sich um keine Luxus-WG handelt, steht nur ein begrenztes Budget zur Verfügung.

Die Aufgabe: Jedes der vier Wohn-/Schlafzimmer soll einen Heizkörperregler mit Fensterkontakt bekommen – außerdem ein fernbedienbares Verdunkelungsrollo und eine schaltbare Steckdose. LED-Streifen am Bett und ein dimmbares Raumlicht sorgen für individuelle Beleuchtung. Das Licht- und Heizungskonzept setzt sich in der gemeinsamen Wohnküche fort. Außerdem sind Funktaster neben der Tür und

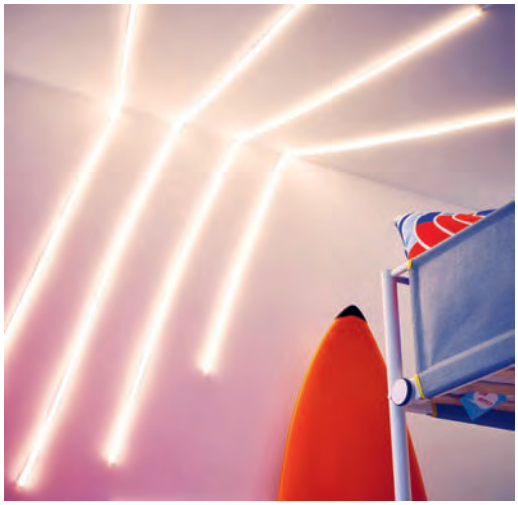
an zentralen Stellen geplant, die „Alles aus" schalten oder programmierbare Szenen starten.

Die Lösung: Das preiswerte Funksystem Ikea Home Smart (siehe Seite 231) erfüllt einen Großteil der Voraussetzungen. Seine Zentrale, das Trådfri-Gateway, steuert drahtlos Leuchtmittel, Zwischenstecker und die akkubetriebenen Rollos der Serie Fyrtur. Mit den Rollos liefert Ikea eine batteriebetriebene Funkwippe, die bereits gekoppelt ist. Sie muss für die Integration zurücksetzt werden, was den Installationsaufwand erhöht. Danach lässt sich die Beschattung aber sowohl individuell per Fernbedienung als auch zentral über das Trådfri-Gateway steuern. Zum Schalten und Dimmen des Lichts gibt es weitere Funkfernbedienungen in den Räumen. Da Ikea bislang keine Heizungsregelung fürs Home Smart anbietet, übernimmt ein zweites System diese Aufgabe: Homematic IP von EQ-3 (siehe Seite 227). Im

Das bezahlt die Wohngemeinschaft

	Anzahl	Einheit		Einzepreis	Netto	Brutto
Basisinstallation	1	Stk.	Ikea Trådfri Gateway	16,81	16,81	20
	1	Stk.	Homematic IP Starter Set Raumklima	83,99	83,99	100
Zentralfunktionen	4	Stk.	Ikea Szenen-Taster	5,04	20,16	24
	2	Stk.	Ikea Bewegungsmelder	8,40	16,80	20
	6	Stk.	Ikea Fernbedienung	8,40	50,40	60
Beleuchtung	8	Stk.	Ikea E27-Lampe warmweiß	10,92	87,36	104
	5	Stk.	Ikea LED-Streifen warmweiß	16,80	84,00	100
	6	Stk.	Ikea GU10-Lampe warmweiß	6,72	40,29	48
Beschattung	4	Stk.	Ikea Rollo Fyrtur, 1m breit	108,40	433,60	516
Steckdosen	4	Stk.	Ikea Zwischenstecker	8,40	33,60	40
Heizung	5	Stk.	Homematic IP Heizkörperthermostat	33,53	167,65	200
	5	Stk.	Homematic IP Tür-/Fensterkontakt	20,97	104,85	125
			Summe		1 139,51	
			MwSt. 19 %		216,51	
			Materialkosten		1 356,02	**1 356 €**
Installation	10	Std.	Eigenleistung		0,00	0
			Installationskosten		0,00	0 €
			Gesamtkosten			**1 356 €**

Option Audio	2	Stk.	Google Nest mini	49,58	99,16	118
	4	Stk.	Ikea Symfonisk Lautsprecher	83,19	332,76	396
			Summe		431,92	
			MwSt. 19 %		82,06	
			Aufpreis für Lautsprecher		513,98	**514 €**



Funkgesteuerte Rollos von Ikea verdunkeln den Raum (links). Warmweiße LED-Streifen setzen Lichtakzente in der Wohngemeinschaft.

Raumklima-Startpaket sind neben der Funkzentrale (Access Point) bereits ein Heizkörperregler und ein magnetischer Öffnungskontakt enthalten. Zugekaufte Komponenten erhöhen die Gesamtmenge auf sechs. Damit lässt sich eine automatische Heizungssteuerung einrichten – inklusive Fernbedienung von unterwegs aus. Im Prinzip könnte der Access Point von Homematic IP auch Steckdosen und Beschattung steuern. Allerdings kommt diese Lösung teurer als mit Ikea-Produkten, weshalb die WG beide Varianten kombiniert. Damit handelt es sich aber auch streng genommen um kein integriertes Smart Home mehr – eher um eine Wohnung mit smarten Geräten.

Die Funktionen: In dieser Preisklasse gibt es keine Möglichkeit, vorhandene Wandschalter intelligent zu machen. Die Ikea-Produkte werden über ihre eigenen Funkfernbedienungen gesteuert. Alle Mitbewohner erhalten zwei Exemplare – fürs LED-Licht und das Rollo in ihrem Zimmer. Weitere Funksender im Koch-/Essbereich und im Bad machen dort die Beleuchtung steuerbar. Zwei Bewegungsmelder aktivieren die Deckenlampen im Flur und WC. Hinzu kommen Shortcut-Buttons für zentrale Aufgaben. So heißen bei Ikea spezielle Batterietaster, die mit jeweils einer Smart-Home-Szene belegt sein können. Ein Exemplar neben der Tür schaltet beim Gehen alles ab. Nach dem Motto: Der Letzte macht das Licht aus. Drei weitere Buttons in der Küche, im Bad und am Esstisch aktivieren programmierbare Lichtstimmungen. Darüber hinaus steht allen WG-Mitgliedern die Ikea-App auf ihrem Smartphone zur Verfügung. Bei einem Mietwechsel können die Verbleibenden das Ex-Mitglied vom Gateway löschen. Damit entfallen auch dessen Zugriffsrechte. Mit Heizplänen arbeiten die Homematic-Thermostate weitgehend autark. Sie lassen sich in keine Szene mit den Ikea-Produkten einbinden. Über die App des EQ-3-Systems ist die Temperatur aber jederzeit individuell programmier- und regelbar.

Die Optionen: Symfonisk-Lautsprecher von Ikea bringen Musik in den WG-Alltag. Die WLan-Lautsprecher basieren auf dem Multiroom-Audiosystem von Sonos (siehe Seite 213) und werden automatisch vom Trådfri-Gateway erkannt. Damit können sie auch Teil einer Smart-Home-Szene werden und etwa auf Knopfdruck die bevorzugte Spotify-Playliste spielen. Mit dem Google Nest mini oder anderen sprachgesteuerten Smart Speakern funktioniert die Wiedergabe außerdem auf Zuruf.

Die Berechnungsgrundlage: Die Gerätekosten basieren auf handelsüblichen Produktpreisen der Hersteller (Stand: 2021). Im Rahmen von Sonderangeboten oder Verkaufsaktionen können sie niedriger liegen. Der Zeitaufwand für die Montage beruht auf Erfahrungswerten. Abweichungen nach oben oder unten sind auch hier möglich. Das kommt auf die persönlichen Fertigkeiten an.

Eine Außensirene verleiht dem Alarm Nachdruck und dient zusätzlich der Abschreckung.

- **Zwangsläufigkeit**. Um Fehlalarme zu vermeiden, erfüllen professionelle Alarmsysteme zwei Bedingungen. Erstens: Die Anlage lässt sich nur scharfschalten, wenn alle Zugänge verschlossen sind und die Sensoren ordnungsgemäß arbeiten. Zweitens: Beim normalen Betreten des Gebäudes deaktiviert sich der Alarm automatisch, damit niemand aus Versehen in einen überwachten Bereich hineinläuft. Diese sogenannte Zwangsläufigkeit ist in Anlagen mit Aufschaltung (siehe Seite 119) besonders wichtig – weil durch den unnötigen Einsatz der Notrufzentrale Kosten entstehen können.

Smart-Home-Integration

Die vorangegangene Aufstellung zeigt: Nicht jedes Smart-Home-System mit einer Alarmfunktion taugt auch wirklich zur Alarmanlage. Tests der Stiftung Warentest stellen Lösungen unter diesem Gesichtspunkt kein gutes Zeugnis aus (test 08/2018). Das gilt besonders für preiswerte Funksysteme. Do-it-Yourself-Produkte bieten in der Regel weder Zwangsläufigkeit noch Sabotageschutz. Und von einer Notstromversorgung kann schon gar nicht die Rede sein. Teilweise ist die Steuerzentrale auch abhängig vom Cloudserver des Anbieters, sodass ohne Internet gar nichts mehr geht. Wenn also Sicherheit auf der Prioritätenliste sehr weit oben steht, sollte das bei der Planung berücksichtigt werden.

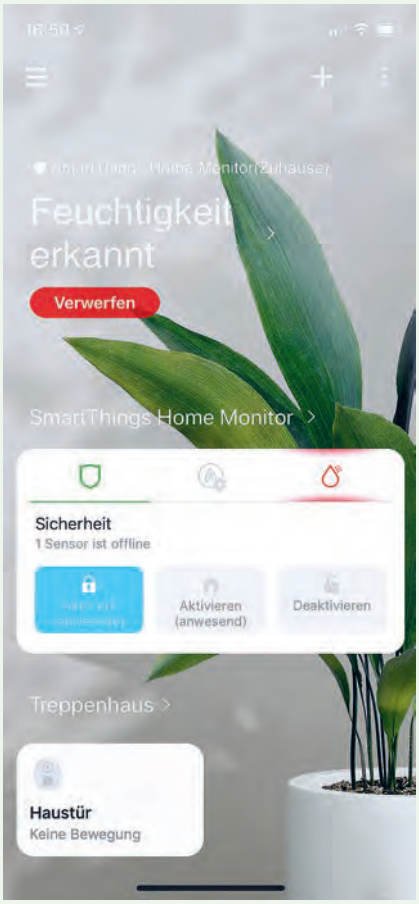
Als Anhaltspunkt gibt es seit Ende 2019 eine weitere Norm, die DIN VDE V 0826–1. Sie stellt Mindestanforderungen an Smart-Home-Lösungen, die der klassischen Sicherheitstechnik entsprechen. Um normgerecht zu sein, müssen sie zum Beispiel über hinreichende Verschlüsselung und einen Sabotageschutz verfügen. Vom Fachbetrieb verlangt die Norm entsprechende Qualifikationen und die genaue Dokumentation der Arbeiten.

Einige Hersteller, die aus dem klassischen Einbruchschutz kommen, haben ihre Systeme um Smart-Home-Funktionen erweitert. So bietet Lupus Electronics zu seinen Alarmanlagen etwa Zubehör wie Funksteckdosen, Heizkörperregler und Schaltaktoren für Licht und Rollläden an. Je nach gewünschter Sicherheit gibt es einfache Lösungen auch zur Eigenmontage, etwa von Abus, Egardia, Gigaset und Lupus. Umgekehrt übernehmen Smart-Home-Anbieter wie Bosch und EQ-3 Funktionen aus der Sicherheitsbranche. Ein Beispiel sind die Betriebsarten Vollschutz und Hüllschutz. Ist der Vollschutz aktiv, beteiligen sich alle installierten Sensoren an der Überwachung, innen wie außen. Der Hüllschutz kontrolliert dagegen nur die Außenhülle des Gebäudes, also potenzielle Einbruchstellen wie Türen, Fenster und Oberlichter. Das geschieht normalerweise mithilfe von Öffnungskontakten und Glasbruchsensoren. Bewegungsmelder in den Räumen bleiben ausgeschaltet, damit sich Personen und Tiere im Haus frei bewegen können.

Richtig geplant und ausgeführt, kommen professionelle Smart-Home-Systeme einer zertifizierten Alarmanlage sehr nahe. Sicherheitsmodule, etwa für KNX, überwachen Sensorleitungen auf Manipulation und können Sabotage erkennen. Allerdings sind die Chancen gering, eine VdS-Zulassung oder ein vergleichbares Zertifikat für solche Installationen zu bekommen. Der Versicherung wird es im Zweifelsfall egal sein, ob ihr Kunde selbst etwas zusammenschraubt oder einen Fachbetrieb damit beauftragt hat. Der umgekehrte Weg führt schon eher ans Ziel: Über ein KNX-Modul lassen sich

Typische Alarmsensoren

- **Öffnungssensoren** registrieren, wenn eine Tür oder ein Fenster aufgemacht wird. Meist handelt es sich um Magnetkontakte, auch Reed-Schalter genannt. Manche Modelle arbeiten stattdessen optisch mit einer Infrarotlichtschranke oder nutzen die Funktechnik RFID (Radio Frequency IDentification).
- **Glasbruchsensoren** reagieren auf eingeschlagene Scheiben. Aktive Melder bestehen aus einem Ultraschallsender, der die Glasfläche in Schwingungen versetzt, und einem Empfänger, der diese Vibrationen auswertet. Bei einem Bruch ändert sich das Schwingungsverhalten und der Sensor löst Alarm aus. Passive Melder erkennen stattdessen die typischen Erschütterungen brechenden Glases. Akustische Sensoren sind auf das Klirren splitternder Scheiben spezialisiert.
- **Rauchwarnmelder** arbeiten normalerweise mit Lichtschranken: Der Strahl einer Infrarot-LED durchquert eine Messkammer und trifft auf eine Fotodiode. Rauchpartikel in der Luft streuen das Licht und lösen Alarm aus. In Europa seltener anzutreffen sind Ionisationsrauchmelder. Sie messen die Leitfähigkeit der Luft mit einem radioaktiven Element. Der strahlende Stoff ist Sondermüll, was seine Entsorgung aufwendiger macht.
- **Wärmemelder** erfassen steigende Raumtemperaturen mit einem Heißleiter. Der Fühler ändert unter Hitzeeinfluss seinen elektrischen Widerstand. Um Feuer im Haushalt festzustellen, reagiert er zu träge. Es gibt aber Kombigeräte, die Heißleiter mit einem Rauchsensor kombinieren. Solche Brandmelder eignen sich auch für Küche und Bad, wo Dampf oder Qualm sonst leicht zu Fehlalarmen führt.
- **Wassermelder** stellen fest, wenn irgendwo Feuchtigkeit austritt. Meist geschieht das über Metallkontakte, die vom Wasser kurzgeschlossen werden. Die Kontakte befinden sich entweder am Melder selbst, dann liegt er auf dem Boden (Abbildung unten), oder am Ende einer längeren Sensorleitung. Einige wenige Modelle arbeiten auch mechanisch mit einem Quellmittel. Es dehnt sich bei der Berührung mit Wasser aus und schließt den elektrischen Kontakt.



WELCHER SMART-HOME-TYP SIND SIE?

Das spielt eine wichtige Rolle bei der Auswahl des Systems. Denn viele Wege führen bekanntlich nach Rom. Wie die Reise abläuft, hängt von persönlichen Vorlieben und vom Geldbeutel ab. Es gibt zum Beispiel Pauschaltouristen, die schätzen Komplettpakete. Sie buchen im Reisebüro, um möglichst wenig organisieren zu müssen. „Urlaub von Anfang an" lautet ihre Devise. Übertragen aufs Smart Home entspricht das einer Komplettinstallation vom Fachbetrieb. Die Reiseleitung – sprich: Bauleitung – kümmert sich um alles. Bewohner checken nur noch ein und genießen den gebuchten Komfort. Bei Wünschen oder Problemen mit der Technik gibt es Ansprechpartner.

Individualreisende erreichen ihr Ziel auf eigene Faust. Sie nehmen Planung und Umsetzung selbst in die Hand. Genauso wie Heimvernetzer, die eine Do-It-Yourself-Lösung installieren. Der Eigenleistung sind dabei kaum Grenzen gesetzt, von Arbeiten am Stromnetz einmal abgesehen. Wer mag und sich auskennt, montiert nicht nur Sensoren und Aktoren, er setzt aus handelsüblichen Elektronikbausteinen auch gleich seine eigene Smart-Home-Zentrale zusammen. Frei verfügbare Open-Source-Software liefert das Programmierwerkzeug dafür.

Zwischen beiden Herangehensweisen gibt es Mischformen. So wie eine Pauschalreise nicht immer Vollpension enthalten muss, kann auch ein schlüsselfertiges Smart Home noch Raum für eigene Unternehmungen bieten. Das spart dann bares Geld, denn anders als im Reisekatalog sind die Kosten recht transparent und einfach nachzuverfolgen. Dort, wo Arbeitsaufwand entsteht, wird er auch bezahlt. Das heißt: Je mehr Sie selbst machen, desto niedriger fällt am Ende die Rechnung aus. Einen groben Überblick gibt die Tabelle „Wo fällt die Arbeit an?" (siehe Seite 157). Sie teilt Smart-Home-Lösungen in vier Kategorien ein. Systeme der Kategorie A machen am meisten Arbeit, sparen aber auch viel Geld. Von Stufe zu Stufe nimmt der eigene Aufwand ab, um am Schluss bei einer Installation zu landen, in der Sie sich um nichts mehr kümmern müssen. Kategorie D entspricht quasi dem Rundumsorglos-Paket von einer Reiseagentur.

Typ A – Tüftler

Günstiger geht es kaum: Nicht einmal 100 Euro müssen Sie für den Einstieg in die Hausautomatisierung bezahlen. So viel kostet ein Minicomputer Raspberry Pi plus USB-Stick für den Zigbee-Funkstandard (siehe „Selbstgebaut von Anfang an", Seite 267). Steuersoftware wie ioBroker oder OpenHab gibt es kostenlos zum Download im Internet. Und Zigbee-Lampen, -Bewegungsmelder oder -Zwischenstecker sind bei Ikea für zehn Euro pro Stück zu haben. Natürlich könnten Sie gleich ein betriebsfertiges Ikea-System kaufen, wären dann aber weitgehend auf die Produktauswahl der Schweden festgelegt.

Ein Selbstbau mit Open-Source-Software hält mehr Optionen offen. So lassen sich an einem Zigbee-Funkstick etwa Sensoren und Aktoren verschiedener Hersteller parallel betreiben. Es sollen andere Protokolle wie Homematic, EnOcean oder Z-Wave zum Einsatz kommen? Auch dafür gibt es Funkmodule. Die Integration ins System übernehmen Programmerweiterungen, sogenannte Adapter, Bindings oder Integrations. Derer finden sich Hunderte oder Tausende, je nach System (siehe „Selbst

gebaut …“, Seiten 271–280). Eine große Gemeinde ehrenamtlicher Open-Source-Entwickler pflegt die Plattformen und hält sie aktuell.

So viel Flexibilität hat allerdings ihren Preis – auch wenn er nicht auf der Geräterechnung auftaucht. Als Smart-Home-Tüftler oder -Tüftlerin bezahlen Sie für zusätzlichen Komfort mit Ihrer Zeit. Der Raspberry Pi ist keine Smart-Home-Zentrale, die man nur ans Stromnetz anschließt, eine App installiert und dann sofort mit der Anmeldung von Funklampen loslegen kann. Im Auslieferungszustand verfügt der Kleinstrechner nicht einmal über ein Betriebssystem. Erst mit einer kleinen SD-Speicherkarte, die am PC oder Mac bespielt wird, erhält die zigarettenschachtelgroße Box ihre Software. Anleitungen für das sogenannte Flashen von SD-Karten gibt es im Internet.

Wo fällt die Arbeit an?

Typ	Beschreibung	Beispielhafte Systeme	Eigenleistung Das können Sie selbst machen	Fremdleistung Das erledigen andere
A	**Eigenbau mit Open-Source-Software**	**Home Assistant, ioBroker, Node RED, OpenHab**	Planung Hardware installieren Systemsoftware installieren In Betrieb nehmen Basisprogrammierung Szenen / Regeln ändern	230-V-Installation
B	**Do-it-Yourself-System mit Funkzentrale**	**Bosch Smart Home, Homee, Homematic IP, Magenta SmartHome, SmartThings**	Planung Hardware installieren In Betrieb nehmen Basisprogrammierung Szenen /Regeln ändern	230-V-Installation Systemsoftware vorinstalliert
C	**Schlüsselfertiges Smart Home**	**Digitalstrom, eNet Smart Home, Homematic IP wired, KNX, Loxone**	Kabel verlegen / Dosen setzen Evtl. Basisprogrammierung Szenen / Regeln ändern	Planung Hardwareinstallation Systemsoftware installieren In Betrieb nehmen Basisprogrammierung
D	**Full-Service-Installation**	**KNX, LCN, Loxone**	Kabel verlegen / Dosen setzen	Planung Hardwareinstallation Systemsoftware installieren In Betrieb nehmen Basisprogrammierung Szenen / Regeln ändern

Produkte wie ein smarter Lautsprecher mit Videochat-Funktion sammeln zwangsläufig auch personenbezogene Daten.

Timer für die Rollläden lassen Rückschlüsse auf den Tagesablauf zu.

Rein technisch ist es möglich, dass IoT-Plattformen solche Daten sammeln und auswerten, und sei es nur, um ihre eigene Servicequalität zu verbessern. Wenn Befehle über die Cloud laufen, können sie Niederschlag in Log-Dateien auf dem Server finden. Ob solche Daten privat bleiben, hängt von Faktoren ab, die aus der Ferne schwer zu beurteilen sind: Wie gut verschlüsseln die Anbieter ihre Übertragung? Haben Mitarbeiter Zugriff auf die Informationen oder nur die Kunden selbst? Wird der Datenpool in regelmäßigen Abständen gelöscht? Wo auf der Welt steht das Rechenzentrum und welche Datenschutzbestimmungen gelten dort? Wie gut hat der Anbieter die Cloud gegen Angriffe von außen abgesichert?

Klar ist: Einen hundertprozentigen Schutz vor Hackern und Cyberkriminellen gibt es nicht. Die Cloud-Rechner professioneller Anbieter wie Amazon, Bosch, Microsoft, Telekom & Co. dürften Angriffe aber besser verkraften als ein Selbstbau-Server, der mit offenen Ports im Internet hängt und keine Softwareupdates erhält. In den Unternehmen kümmern sich große Abteilungen um IT-Sicherheit und sind es normalerweise gewohnt, Serverattacken abzuwehren. Wer jede Gefahr ausschließen will, muss mit dem Smart Home offline bleiben. Er sollte dann aber auch keine Apps oder Programme installieren, die eine Hintertür ins heimische Netzwerk öffnen (siehe „Das kleine Einmaleins der Smart-Home-Sicherheit“, Seite 305). Wie oft heißt es abzuwägen – zwischen den Vorteilen, die eine Lösung bringt, und den Risiken, die mit ihr verbunden sind. Manchmal triumphiert dabei der Komfort über alle Datenschutzbedenken. Wäre es anders, hätten Social-Media-Angebote wie Facebook, TikTok und WhatsApp wahrscheinlich nicht mehrere Milliarden Nutzer in aller Welt.

Smarte Displays und Apps

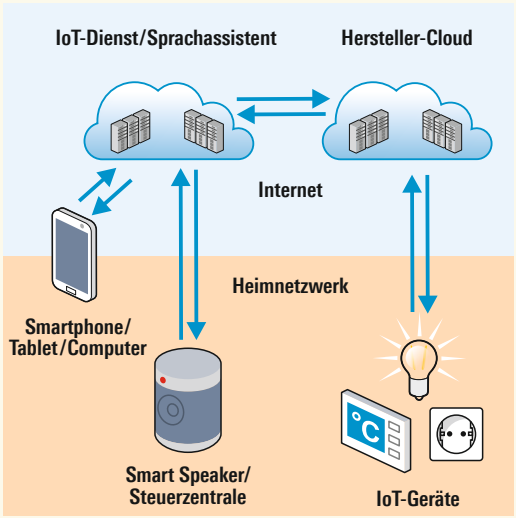
Eine noch junge Produktgruppe ist durch das Internet der Dinge überhaupt erst möglich geworden: smarte Displays. Als vernetzte Bildschirme zeigen Sie Fotos aus der persönlichen Cloud-Bibliothek. Sie liefern Nachrichten und Kochrezepte oder starten Videoanrufe per Sprachbefehl von der Küchenarbeitsplatte aus. Nach dem Motto: „Alexa, ruf‘ Oma an“, sie weiß bestimmt, wie lange das Schokoladensoufflé im Ofen bleiben muss.

Der Echo Show von Amazon gehört in diese Kategorie, genauso wie Googles Nest Hub und diverse Modelle von Lenovo. Vom Prinzip her handelt es sich um sprachgesteuerte Lautsprecher mit einem Touchscreen. Der digitale Assistent des Geräts nutzt das Display, um Bedienelemente anzuzeigen. Ist etwa die Temperatur in einem bestimmten Raum gefragt, erscheint gleichzeitig der Heizungsregler auf dem Display. Betätigt jemand den Knopf an der Videotürklingel von Ring (siehe Seite 213), sendet die Cloud des Amazon-Tochterunternehmens den Videostream direkt an einen Echo Show. Ohne weitere Konfiguration, nur durch die Kombination zweier IoT-Systeme, verwan-

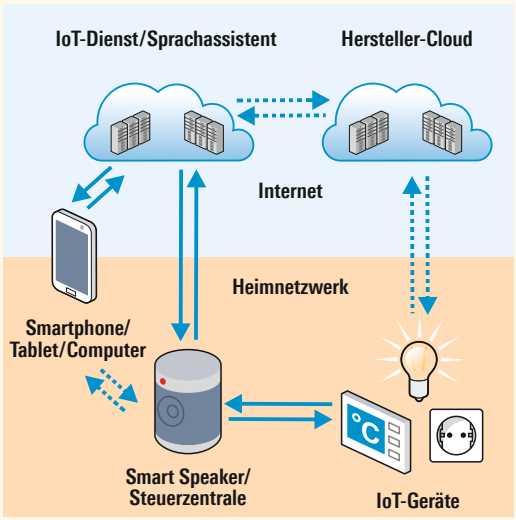
Digitale Assistenten mit Touchscreen gibt es von Google (Bild), Amazon und anderen.

Kommunikation im Internet der Dinge

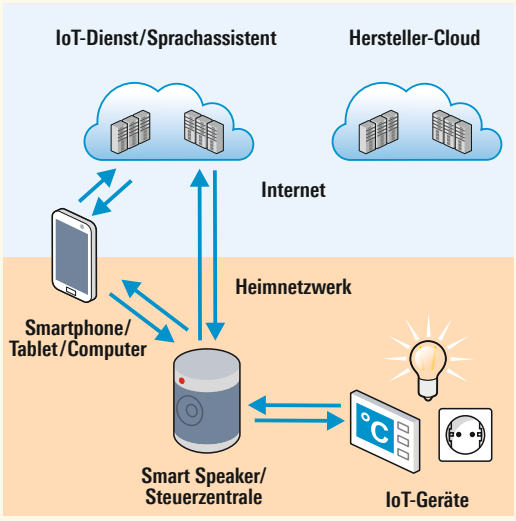
- **Cloud-zu-Cloud-Verbindung:** Der Sprachassistent oder IoT-Dienst nimmt online Kontakt zum Internetserver eines Geräteherstellers auf. Dieser leitet Steuerbefehle dann an die zu Hause installierten IoT-Produkte weiter. So funktionieren unter anderem die klassischen Alexa-Skills und Onlineangebote wie IFTTT.



- **Cloud und lokal gemischt:** Mit speziellen Zentralen oder einem geeigneten Smart Speaker kann die Steuerung zu Hause im Netzwerk stattfinden. Die Cloud-Verbindung bleibt aber trotzdem möglich. Nach diesem Prinzip arbeitet etwa der Google Assistant mit Aktionen, die für lokale Ausführung programmiert wurden. Auch der neue Smart-Home-Standard Matter (siehe Seite 53) sieht beide Wege vor.



- **Lokale Steuerung:** Eine Lösung wie Apple HomeKit nutzt die Cloud zwar für Aufgaben wie Spracherkennung, die Smart-Home-Geräte erhalten ihre Steuerbefehle aber von einer Steuerzentrale daheim im Netzwerk. So gibt es statt mehrerer Geräteverbindungen zu den Hersteller-Clouds im Idealfall nur einen Kanal ins Internet.



Prüfsiegel von angesehenen Instituten können als Orientierungshilfe dienen.

Seite 311) nimmt regelmäßig IoT-Produkte unter die Lupe und prüft ebenfalls im Herstellerauftrag. Somfy hat die aus den USA stammende Organisation Underwriters Laboratories (UL) mit dem Sicherheitscheck seiner jüngsten Smart-Home-Zentrale beauftragt.

Zusätzliche Orientierung dürfte auch das kommende, deutsche IT-Sicherheitskennzeichen geben. Es entsteht unter Federführung des Bundesamts für Sicherheit in der Informationstechnik (BSI), das im IT-Sicherheitsgesetz von 2021 zu diesem Zweck mit mehr Befugnissen ausgestattet wurde. Zwar handelt es sich dabei um kein Prüfsiegel, die Hersteller geben eine freiwillige Erklärung ab, dass ihr Produkt „für eine festgelegte Dauer bestimmte IT-Sicherheitsanforderungen erfüllt" (Paragraf 9c, IT-Sicherheitsgesetz). Aber damit existieren immerhin offizielle Mindestanforderungen. Die Grundlage bildet eine Europäische Norm, an der neben BSI und ausländischen Behörden auch Unternehmen wie Bosch, IBM und Samsung mitgearbeitet haben.

Die ETSI EN 303 645 definiert Sicherheitsstandards für IoT-Geräte wie Smart-Home-Zentralen, vernetzte Hausgeräte, sprachgesteuerte Lautsprecher, Smart-TVs oder auch Fitness-Tracker. Zu den Vorgaben an die Hersteller zählen unter anderem:

- **Keine allgemeinen Standardpasswörter**. Eventuell voreingestellte Codes haben nur für das jeweilige Produkt Gültigkeit.
- **Für aktuelle Software sorgen**. Softwarekomponenten sollen aktualisierbar sein und wenn nötig Updates erhalten.
- **Sichere Kommunikation**. Geräte setzten bewährte Technik zur Verschlüsselung ein, die ebenfalls updatefähig sein muss.
- **Sichere Speicherung von Daten**. Sensible Informationen auf dem Gerät sind verschlüsselt und unzugänglich.
- **Installation und Wartung erleichtern**. Der Hersteller soll Nutzer dabei unterstützen, das Gerät sicher einzurichten und zu nutzen.

Anbieter, die das Kennzeichen verwenden wollen, müssen künftig einen definierten Support-Zeitraum für ihr Produkt angeben, in dem sie für Softwareaktualisierungen und Sicherheitsupdates sorgen. Erfüllt der Hersteller seine Zusagen nicht und wird das BSI darauf aufmerksam, kann die Behörde Warnungen herausgeben. Langfristig ist auch eine eigene Webseite denkbar, die Produkte mit ihrem digitalen Mindesthaltbarkeitsdatum auflistet.

Klassische Prüfsiegel wird das IT-Sicherheitskennzeichen jedoch nicht ersetzen. Zum einem fehlt ihm der Testcharakter. Die Herstellerangaben werden vor der Siegelvergabe nicht unter Laborbedingungen geprüft. Zum anderen gehen die Institute in ihren Untersuchungen teilweise deutlich über die EN 303 645 hinaus. Die ETSI-Norm beschränkt sich aufs Gerät. Eine VDE-Zertifizierung für Informationssicherheit berücksichtigt zum Beispiel auch die beteiligten Server und Apps. Um als echte Orientierungshilfe zu taugen, sollte das Siegel außerdem ein Veröffentlichungsdatum enthalten. Denn in der IT-Technik kann jedes Update die Produkteigenschaften ändern – und nichts ist so alt, wie die Software von gestern.

„VIELE BILLIGANBIETER SPAREN AN SICHERHEIT“

Maik Morgenstern ist Technischer Direktor des AV-Test Instituts in Magdeburg. Das herstellerunabhängige Unternehmen prüft seit mehr als 15 Jahren Produkte auf ihre IT-Sicherheit und besitzt laut eigener Aussage eine der größten Sammlungen digitaler Schädlinge weltweit. Neben Virenschutzlösungen für private und professionelle Anwendungen zählen IoT-Produkte zu den Fachgebieten. AV-Test prüft IP-Kameras und andere Smarthome-Geräte und veröffentlicht die Ergebnisse auf einem eigenen Blog (www.iot-tests.org). Die Testsiegel zählen zu den wenigen Orientierungshilfen für Endkonsumenten, wenn es um die Datensicherheit geht.

Herr Morgenstern, viele Geräte sind heute mit dem Internet verbunden. Wie groß ist die daraus resultierende Gefahr?

Fakt ist, dass viele Hersteller von Smart-Home-Produkten der Sicherheit und dem Datenschutz nicht den Stellenwert einräumen, den ein Gerät mit Internetverbindung erfordert. Seit vielen Jahren weisen wir auf diesen Missstand in den entsprechenden staatlichen und industriellen Beratungsgremien hin. Fakt ist aber auch, dass manche Gefahren eher theoretischer Natur sind.

Können Sie Beispiele nennen – wo liegen die Unterschiede?

Eine weggeworfene LED-Lampe, die das WLan-Passwort unverschlüsselt gespeichert hat, stellt ein vergleichsweise geringes Risiko dar. Angreifer müssten schon zum richtigen Zeitpunkt vor Ort sein und die Herkunft der Lampe kennen, dann den Chip auslöten und das Passwort mit entsprechender Technik auslesen – möglich, aber eher unwahrscheinlich. Anders sieht es mit Überwachungskameras aus, die offen ins Internet streamen. Auf Webseiten wie www.insecam.org kann man sehen, dass dies gar nicht so selten vorkommt. Nutzer wollen ihr Eigentum schützen, geben Angreifern aber womöglich Auskunft darüber, welche „Schätze“ in der Wohnung zu holen sind und wann sie aus dem Haus gehen. Ist der Datenverkehr dann auch noch schlecht oder gar nicht verschlüsselt, offenbaren die Kameras ihre IP-Adresse und damit den Standort. Deshalb achten wir bei unseren Tests darauf, dass mögliche Angriffsszenarien praktikabel sein müssen.

Wo lauern die die größten Gefahren?

Wie im Kamerabeispiel beschrieben, kann eine unsichere Gerätekommunikation reale Schäden verursachen. In unseren Tests gab es schon Smartlocks, die Angreifern über bekannte Sicherheitslücken Tür und Tor geöffnet hätten. Sogenannte Botnetze, in denen Geräte übers Internet zusammengeschaltet werden, sind eine reale Bedrohung – selbst wenn die Betroffenen davon nichts mitbekommen. Angreifer nutzen die Rechenpower solcher Netze für eigene Zwecke, etwa fürs Coinmining, um digitale Währungen zu schürfen. Am größten ist die Gefahr für alle aus der Ferne verwundbaren Produkte, also solche, die man massenhaft übers Internet angreifen kann. Allerdings