

SMARTHOME

Der Saugroboter als Tür-Öffner

Technik für das Smarthome ist sicherlich praktisch, doch sie kann auch als Ziel für Cyberattacken dienen. Es gibt aber Möglichkeiten, sich zu schützen.

VON MARKUS STREHLITZ

Das Smarthome bietet seinem Bewohner viele Vorteile. Intelligente Heizkörperthermostate helfen beim Energiesparen. Digitale Sicherheitssysteme schützen das Haus, wenn der Eigentümer auf Reisen ist.

Doch dafür müssen die Geräte oder Sensoren Daten austauschen. Und alles, was sich mit dem Internet verbindet, ist immer auch ein potenzielles Ziel für Online-Angriffe. Saugroboter, Videokameras oder andere Komponenten des smarten Hauses können als Hintertür für Cyberkriminelle dienen.

Das Problem entsteht vor allem, wenn die Geräte mit ihren Herstellern kommunizieren und somit selbstständig über das Internet Daten austauschen. Während ein Privatanwender Sicherheitsfunktionen auf seinem Router, der für den Internetzugang zuständig ist, aktivieren kann, ist dies bei den Smarthome-Geräten nicht möglich. Sie lassen sich zum einen nicht vom Anwender konfigurieren, zum anderen verfügen sie nur über wenig Rechenleistung, sodass keine Sicherheitssoftware nachträglich installiert werden kann.

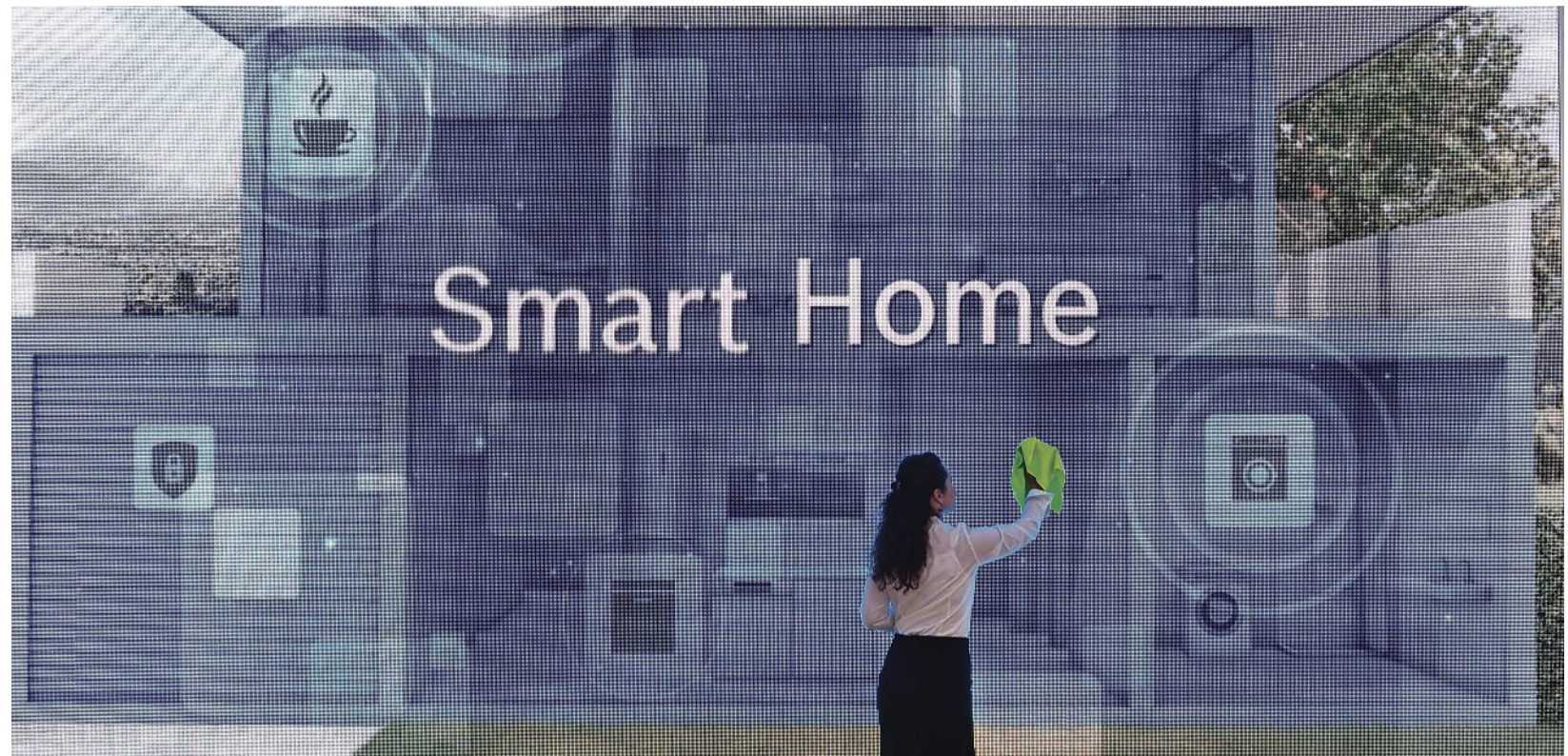
Grundsätzlich sei zwar ein Privathaus ein eher unbedeutendes Ziel für einen Hacker, meint Florian Kirchbuchner, Leiter der Abteilung „Smart Living and Biome-

tric Technologies“ am Fraunhofer-Institut für Graphische Datenverarbeitung (IGD). Aber wenn Mitarbeiter wie zur Zeit verstärkt im Homeoffice arbeiten, könnte ein Angreifer über ein vernetztes Gerät auch Zugang zum heimischen Computer bekommen und darüber dann ins Firmennetz gelangen.

Für größer erachtet Kirchbuchner allerdings die Gefahr, dass ein gehacktes Gerät für sogenannte Botnetz-Angriffe missbraucht wird. Dabei kapern Kriminelle eine große Zahl von fremden Rechnern, um sie für ihre Attacken zu nutzen. Dass die Gefahr von Online-Angriffen auf das smarte Heim real ist, zeigt der Fall eines Ehepaars aus Göttingen, über den die „Hannoversche Allgemeine“ berichtet hat. Über die Internetverbindung der Eheleute war Geld von einem gehackten Konto abgebucht worden. Zugang hatten sich die Cyberkriminellen über ein Smarthome-System verschafft.

Datenaustausch mit dem Hersteller

Die grundsätzliche Gefahr lässt sich reduzieren, indem Nutzer den Datenaustausch der Geräte mit dem Hersteller deaktivieren. „Jeder Anwender sollte sich fragen, ob eine solche Verbindung notwendig ist“, so Kirchbuchner. „Brauche ich zum Beispiel einen Staubsaugroboter, der Bilder



Ein intelligentes Haus unterstützt seine Bewohner in vielerlei Hinsicht, kann aber auch Einfallstor für Hacker sein. Foto: Soeren Stache/dpa-tmn

meiner Wohnung aufnimmt?“ Der Nachteil: Der Anwender kann dann unter Umständen bestimmte Komfortfunktionen nicht mehr nutzen. Dazu zählt etwa, dass eine Heizungsanlage das Heim schon vorwärmt, weil sie dank der Geodaten des Nutzers weiß, dass sich dieser auf dem Weg nach Hause befindet.

Eine andere Möglichkeit, die Sicherheit zu erhöhen, wäre eine zentrale Steuerung des Smarthomes, wie dies etwa große Anbieter wie Google oder Apple ermöglichen. Dadurch lässt sich immerhin die Zahl der möglichen Einfallstore minimieren, weil nicht jedes einzelne Gerät nach draußen kommuniziert. Stattdessen gibt es nur eine Steuerungseinheit, die am besten von einem vertrauenswürdigen Hersteller bezogen wird.

Außerdem gibt es Sicherheitsprüfungen für Smarthome-Geräte, welche die Hersteller für ihre Produkte in Anspruch nehmen können. Anbieter sind Dienstleister wie etwa der VDE (Verband der Elektrotechnik, Elektronik und Informationstechnik). In diesen wird zum Beispiel geprüft, ob die persönlichen Daten geschützt sind oder ein Gerät zu leicht gehackt werden kann.

„Das senkt die Gefahr nicht auf null“, sagt Alexander Matheus, Experte für smarte Technologien und Informationssicherheit beim VDE-Institut, „aber es reduziert das Risiko eines erfolgreichen Angriffs deutlich.“ In diesen Prüfungen wird laut Matheus auch gefordert, dass ein Gerät eine gewisse Resilienz gegenüber Ausfällen besitzt – also zum Beispiel auch

nach einem Stromausfall wieder automatisch funktioniert. Verbrauchern, die sich Smarthome-Technik zulegen möchten, bieten solche Prüfungen zumindest eine gewisse Orientierung.

Und die Entwicklung geht weiter. Laut Matheus hat das Europäische Institut für Telekommunikationsnormen (ETSI) im Juni eine Norm für IoT-Geräte verabschiedet – also für Geräte im Internet der Dinge, zu denen auch Smarthome-Technik zählt. Dort werden grundlegende Anforderungen aus Sicht der Informationssicherheit für die Geräte definiert. Dazu zählt etwa, dass Passwörter vom Verbraucher selbst vergeben werden müssen. In der Norm ist auch festgelegt, dass Hersteller dem Nutzer darlegen müssen, wie lange die Software gewartet wird. Updates

sorgen schließlich dafür, eine Software auf dem aktuellen Sicherheitsstand zu halten. Doch bisher ist diese Norm für die Hersteller noch nicht bindend. Das Gleiche gilt für die Sicherheitsprüfungen.

Die Wahl des richtigen Anbieters spielt ohnehin eine wichtige Rolle, um sicher vor Online-Angriffen zu sein. Bei klassischen Herstellern müssten Nutzer vorab ihre Erlaubnis geben, ob das Gerät nach außen Kontakt aufnehmen darf, berichtet Kirchbuchner. „Das Preisschild ist immer ein guter Indikator für Sicherheit“, so der Experte. Will heißen: lieber auf Billiggeräte verzichten, die nach Hause funken, ohne den Anwender vorher zu fragen. Das Label „Made in Germany“ oder „Made in Europe“ sei in diesem Kontext ein hilfreiches Qualitätsmerkmal, so Kirchbuchner.

Frischlucht per Sprachbefehl

Lüftungsanlagen waren selten so wichtig wie zur Zeit. Sie lassen sich intelligent steuern.

VON MARKUS STREHLITZ

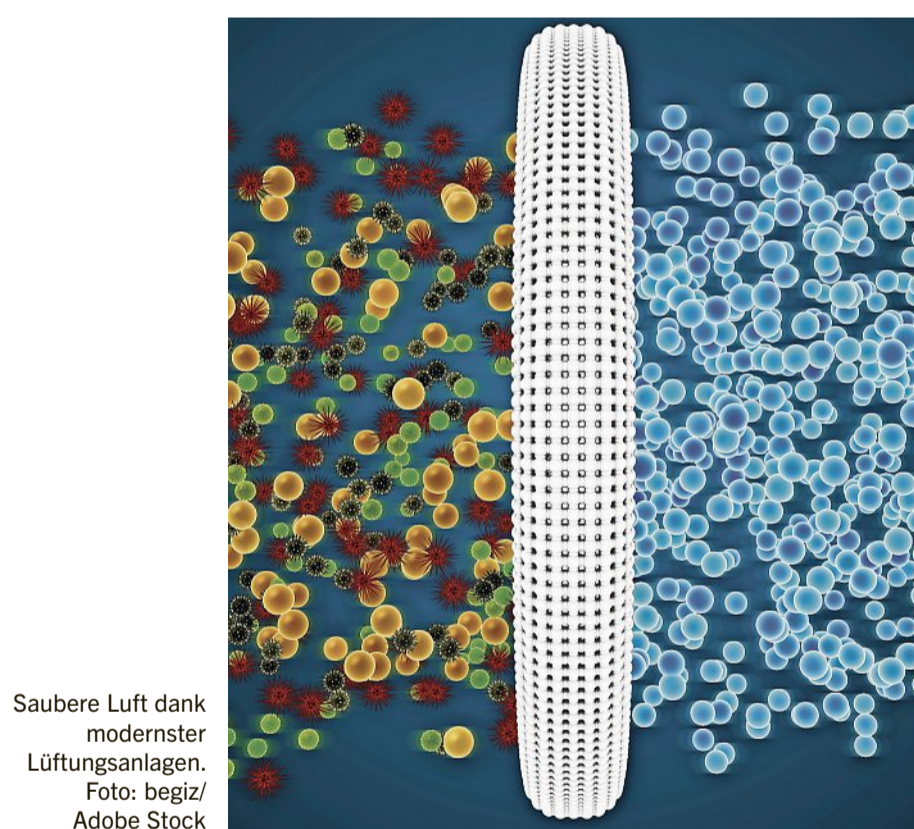
Dem Thema Lüftung kommt in diesem Herbst und Winter eine besonders bedeutende Rolle zu. Wenn wir uns alle wieder zunehmend in geschlossenen Räumen aufhalten, braucht es eine Strategie, um die Luft von potenziell virenhaltigen Aerosolen zu befreien.

Lüftungsanlagen sind dafür die beste Lösung. Das Prinzip: Die hygienisch erforderliche Luft wird von außen zugeführt, die verbrauchte Luft abgeführt – über jeweils voneinander getrennte Kanäle. Hinzu kommt häufig eine Wärmerückgewinnung. Per Wärmetauscher wird die Temperatur der Außenluft erhöht, bevor diese in den Raum strömt.

In der Regel sind diese Anlagen so eingestellt, dass ständig ein gewisser Teil an Frischluft zugeführt wird – auf Basis von Erfahrungswerten. Im Smarthome lässt sich das intelligent steuern. Grundlage dafür sind Sensoren im Haus, die Aufschluss über verschiedene Werte geben. CO₂-Sensoren etwa messen den Kohlendioxid-Gehalt in der Luft. Denn wenn dieser zu hoch ist, verursacht das nicht nur Müdigkeit oder Kopfschmerzen bei den Bewohnern. Der CO₂-Anteil der Luft sei auch „ein guter Indikator für die Virenbelastung“, wie Dirk Mobers erklärt. Mobers leitet bei der Energieagentur NRW das Themengebiet Wärme und Gebäude.

Durch die Kommunikation zwischen Sensoren und Lüftungsanlage wird letztere automatisch aktiviert, wenn frische Luft benötigt wird. „CO₂-Sensoren sind mittlerweile günstig. Und die Lüftungsanlage kann dadurch situationsbedingt reagieren“, sagt Benjamin Groß, Geschäftsführer des IT-Anbieters Softeq, der sich unter anderem mit der intelligenten Vernetzung von Geräten beschäftigt.

Daneben gibt es weitere Parameter, an denen sich der Betrieb der Lüftung orientieren kann. Auch die Zahl der Personen lässt sich als Grundlage für eine entsprechende Steuerung nutzen. Für die notwendige Frischluft in einem Raum müsse man mit 20 bis 30 Kubikmetern pro Person und



Saubere Luft dank modernster Lüftungsanlagen. Foto: begiz/Adobe Stock

Stunde rechnen, so Mobers. In einem Smarthome kann daher die Lüftungssteuerung auch mit installierten Bewegungsmeldern verknüpft werden. Wird ein Raum viel genutzt, wird auch entsprechend stärker gelüftet.

Das Beispiel des Softwareunternehmens Adobe zeigt, wie groß der Nutzen eines solchen Konzepts sein kann. Das Bürogebäude am Hauptsitz der Firma ist in verschiedene Zonen unterteilt. Wenn eine von diesen länger als 15 Minuten unbesetzt bleibt, schaltet sich das System auf Heizungs-, Lüftungs- und Klimaanlage für den entsprechenden Bereich automatisch ab. Auf diese Weise konnte Adobe den Energieverbrauch um 65 Prozent reduzieren, wie Softeq auf seiner Website berichtet.

DATEN ZUM NUTZERVERHALTEN

Laut Groß ist es auch möglich, dass sich eine Anlage den Hausbewohnern anpasst. Das System sammelt dann über einen gewissen Zeitraum hinweg Daten zum Nutzerverhalten, lernt daraus und regelt seinen Betrieb so, dass dieser genau zum Bedarf passt.

Daneben lässt sich mit einer smarten Lüftungsanlage die Wartung intelligent steuern. Das Gerät misst die Menge der geförderten Luft und bestimmt daraufhin,

wann etwa eine Kontrolle des Filters nötig ist. Ist dies der Fall, gibt es per App oder E-Mail ein Signal an den Nutzer. Auf die gleiche Weise wird der Besitzer auch informiert, wenn die Anlage eine Störung hat.

Im intelligenten Zuhause kann ein Nutzer mit seinen Lüftungsanlagen auch reden. Einige Hersteller bieten mittlerweile die Möglichkeit, ihre Geräte mit digitalen Sprachassistenten wie zum Beispiel Alexa von Amazon zu verbinden. Per Sprachbefehl kann der Nutzer dann die Stärke der Anlagen regeln oder die aktuelle Luftqualität abfragen.

Auch ohne spezielles Gerät kann das System beim richtigen Lüften der Wohnung helfen. Wird etwa ein smarter Fensterkontakt mit dem Sprachassistenten verbunden, gibt Alexa Bescheid, wenn das Fenster wieder geschlossen werden sollte.

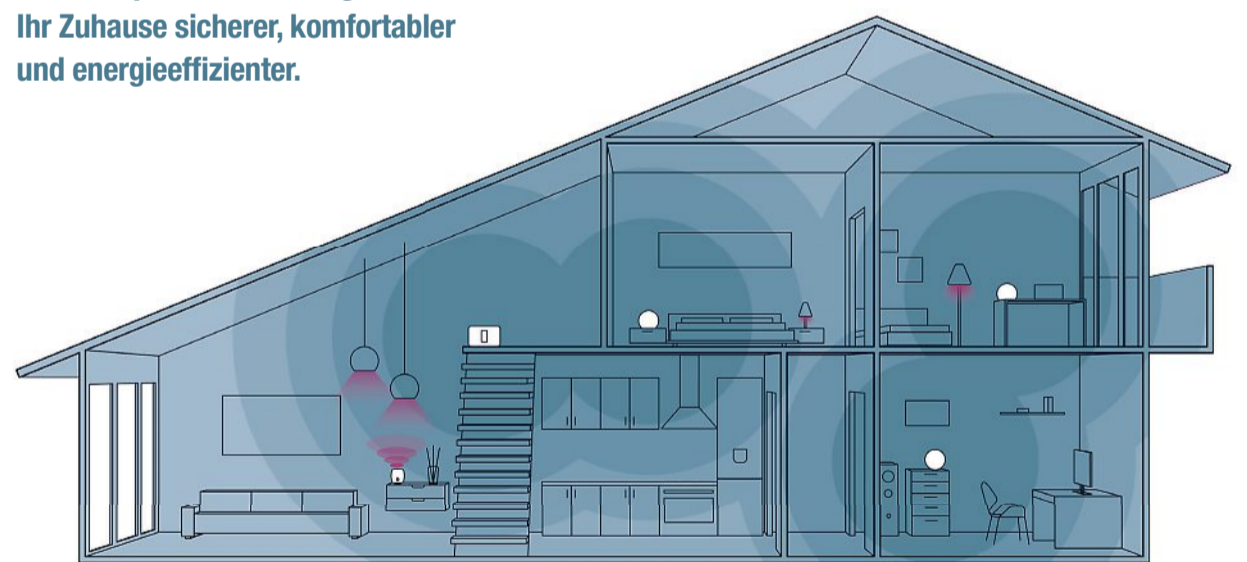
Wer solche und andere Funktionen nutzen möchte, sollte bei der Auswahl der Geräte und Systeme aber darauf achten, dass diese miteinander kompatibel sind. Denn dass alle Komponenten eines intelligenten Heims miteinander kommunizieren können, ist nicht selbstverständlich. Noch fehlt es im Smarthome an Standards. Sensoren und Lüftungsanlage müssen eben eine Sprache sprechen, um stets für die passende Menge an Frischluft zu sorgen.

RATGEBER: Smartes Zuhause

ANZEIGE

Ihr Zuhause intelligent vernetzt

Ein leistungsstarkes und stabiles WLAN bietet viele Vorteile, zum Beispiel auch für Magenta SmartHome. Damit wird Ihr Zuhause sicherer, komfortabler und energieeffizienter.



Dank perfekter Heimvernetzung überall dabei

Ob Fußball schauen auf der Terrasse, Gaming auf dem Dachboden oder Homeoffice im Keller – die Mesh-Technologie macht es möglich. Denn die Mesh-Lösungen der Telekom vernetzen intelligent den Router und sorgen so für schnelles, stabiles WLAN in jedem Winkel Ihres Zuhauses. Dabei stellen mehrere Zugangspunkte ein gleichmäßiges Signal im ganzen Haus her – auch über mehrere Etagen hinweg.

Bis zu sechs Sendestationen

Als Sendestation dient der Speed Home WiFi der Telekom. Die Repeater nutzen moderne Mesh-Technologie. Dabei er-



zeugen die im Haus oder in der Wohnung aufgestellten Speed Home WiFi im Verbund mit dem Router ein konstantes WLAN-Signal. Das intelligente Netzwerk kann dabei aus bis zu sechs Speed Home WiFi Komponenten inklusive Basis bestehen – praktisch, vor allem bei größeren Wohnungen oder mehrstöckigen Häusern.

Beste Voraussetzungen für ein smartes Zuhause

Eine optimale WLAN-Abdeckung bildet die ideale Grundlage, damit Ihr Zuhause zu einem Smart Home wird. Entdecken Sie eine Vielzahl praktischer Alltagshelfer, die Ihr Zuhause noch komfortabler und sicherer machen. Sagen Sie zum Beispiel einfach, was Sie möchten – der Smart Speaker erledigt es sofort. So steuern Sie über den Sprachassistenten viele Telekom Dienste und Funktionen bequem mit Ihrer Stimme.

Smart Home erleichtert den Alltag

Mithilfe des Smart Speakers dimmen Sie auf Zuruf das Licht, wählen TV-Sender aus oder spielen Ihren Lieblingssong ab. Weitere Geräte wie Kameras, Be-

wegungsmelder oder Heizkörperthermostate sorgen für mehr Sicherheit und Energieeffizienz.



Speed Home WiFi mit Mesh-Technologie

TOP-BERATUNG UND -SERVICE

Wir entwickeln gemeinsam mit Ihnen die optimale Lösung für Ihre Wohnsituation und helfen Ihnen selbstverständlich auch bei der Einrichtung – telefonisch und auf Wunsch vor Ort.

Lassen Sie sich beraten: unter 0800 330 3000, im Telekom Shop oder unter www.telekom.de/heimvernetzung bzw. www.smarthome.de

T ERLEBEN, WAS VERBINDET.

» impressum

Produktion: STZW Sonderthemen
Anzeigen: Jürgen Mauker