Quelle: Production Perig – stock.adobe.com

Sicherheitsrisiken im Smart Home

Wenn der Einbruchschutz einbricht

Egal ob intelligente Heizung, smarte Türverriegelung oder intuitives Musikstreaming – die Möglichkeiten mit smarter Technik das Zuhause zu vernetzen scheinen nahezu unbegrenzt. Ganze Geschäftszweige haben sich auf die digitale Vernetzung spezialisiert. Doch welche Sicherheitsrisiken gibt es im Smart Home und was gewährleistet Schutz?

Es klingt alles so verlockend: Man kommt nach Hause, die Wohnung ist über die App schon wohltemperiert, warmes Licht empfängt einen, denn die Zeitschaltuhr ist auf den Feierabend eingestellt. Beim ersten Schritt über die Schwelle erklingt die Lieblingsmusik, denn Siri, Alexa & Co. wissen genau, was man gerne hört. Smart Homes sollen unser Leben leichter und angenehmer machen. Sinnvolle technische Ergänzungen werden mit Smartphone, Tablet oder anderen mobilen Endgeräten bedient und kümmern sich um alltägliche Kleinigkeiten (siehe **Kasten Smart Home**). So weit, so sinnvoll.

Die erste intelligente Technik kam bereits am Anfang der Jahrtausendwende zum Tragen und belief sich dabei vor allem auf eine vernetzte Steuerung sämtlicher elektronischer Vorgänge in einem Haus. Über die Jahre hinweg wurden immer mehr technische Geräte zum Smart-Objekt gestaltet und die Vernetzung ging weiter voran. Heute hat schon jeder dritte Haushalt smarte Geräte in seinem Netzwerk. Immer mehr Möbel werden mit Technik ausgestattet und damit in die Entwicklung des IoT (Internet of Things) integriert.

Doch es geht beim Smart Home nicht nur um Bequemlichkeit, sondern auch um Sicherheit. Digitale Technologien sind seit einigen Jahren auch in der Sicherheitsbranche angelangt, sodass nicht mehr nur reine Haushaltsgeräte vernetzt werden können, sondern auch Alarmanlagen Teil von dieser Entwicklung werden – ein gutes Beispiel, um auf Sicherheitsrisiken im Smart Home einzugehen. Wie sicher ist die Vernetzung also wirklich?

Smart Home

Als smarte Technik zählen alle technischen Systeme in Wohnräumen, die für eine erhöhte Lebensqualität, mehr Sicherheit oder effizienteres Energiemanagement sorgen sollen. Dazu zählt nicht nur die Haushaltstechnik selbst, sondern beispielsweise auch Unterhaltungselektronik. Gängige Synonyme sind »Smart Living«, »Ambient Assisted Living«, »E-Home« oder »Intelligentes Wohnen«. Ein wichtiges Merkmal ist dabei die Vernetzung der verschiedenen Smart-Home-Komponenten in der Regel über WLAN, einzeln aber auch untereinander. Vor allem neuere Geräte sind mit Künstlicher Intelligenz ausgestattet, speichern und verarbeiten Daten und lernen mit jeder einzelnen Interaktion mit.

Unverschlüsseltes Smart Home

Grundsätzlich gilt in allen Bereichen der Sicherheitstechnik: eine hundertprozentige Sicherheit gibt es nicht. Hersteller von smarter Technologie setzen in ihrer Entwicklung vor allem auf eine leichte Bedienbarkeit und auf schnelle Marktfähigkeit, denn der Markt ist hart umkämpft. Dabei steht das Thema Sicherheit häufig nicht an erster Stelle. Und auch bei den Nutzern ist das Bewusstsein für Sicherheitsrisiken zu oft gering.

Das vermutlich größte Sicherheitsproblem bei Smart Homes ist die digitale Technik selbst. Die Internetverbindung wird nicht verschlüsselt hergestellt, Kameras und Mikrofone laufen permanent, es werden

durchgehend Daten auf externe Server übertragen.

Mit der zunehmenden Vernetzung sämtlicher Geräte im und um das Haus herum, müssen sich die Nutzer jedoch auch auf neue Bedrohungen einstellen: Smart-Home-Geräte bieten Kriminellen eine Plattform der besonderen Art, mit denen sie sich auf vielfältige Art und Weise Zugriff verschaffen können. Je mehr intelligente, WLAN-gebundene Technik genutzt wird, umso mehr Daten werden im Netz und auf den Servern der Hersteller gespeichert. Das macht die Nutzung solcher Systeme hoch anfällig, denn per Fernzugriff ist es für technikaffine Täter ein Leichtes, sich in die Systeme zu schalten.

Das Abhören und Ausspionieren von Daten beispielsweise über Drahtlos-Technologie wie Bluetooth ist dabei nur ein Risiko von vielen. Datenmanipulation, Veränderungen an der Gerätekennung oder dem Zertifikat und nicht zuletzt auch das Einspielen von Schadsoftware oder Viren sind Sicherheitsrisiken, die Smart-Home-Nutzer betreffen können.

Mit dem Einsatz von smarter Technik gibt der Nutzer oft unbeachtet und ohne Gedanken an die Folgen wichtige Entscheidungen ab. Etwa, wo die Daten gespeichert werden. Denn das geschieht meist auf ausländischen Servern ohne ausreichende Regularien für Datenschutz. Auch auf die Verschlüsselung der Datenübertragung hat der Nutzer selbst häufig keinen Einfluss.

Risikofaktor Alarmanlage

Dies lässt sich gut am Beispiel von Einbruchschutz und smarten Alarmanlagen zeigen. Die verschiedenen Smart-Home-Komponenten in Kombination mit mobiler Steuerung per App sind von vornherein dafür prädestiniert, das eigene Zuhause mit smarter Technik zu schützen (**Bild 1**). Doch per Fernzugriff können sich Täter in die Systeme schalten und die Bewohner in ihren privatesten Momenten ausspionieren. Die genutzte »smarte« Alarmtechnik kann ausgeschaltet und der beste Zeitpunkt für einen Einbruch ermittelt werden. Auch die persönlichen Gewohnheiten oder das Nutzungsverhalten können so schnell zum Verhängnis werden.

Smart-Home-Produkte rund um die eigene Sicherheit bieten gegen diese Art des Einbruchs keinen zuverlässigen Schutz und auch die Hersteller kommunizieren die Art der Datenverarbeitung, -sicherung, und -speicherung nur selten. Generell müssen Systeme, die für die Sicherheit von Haus, Bewohnern und Sachgegenständen sorgen sollen, höheren Maßstäben genügen als simple Systeme zur Haussteuerung. Hier gilt es, dass die Systeme rund um die Uhr zuverlässig und störungsfrei funktionieren, um im Bedarfsfall wirklich zu schützen, und nicht nur Licht und Heizung zu steuern.

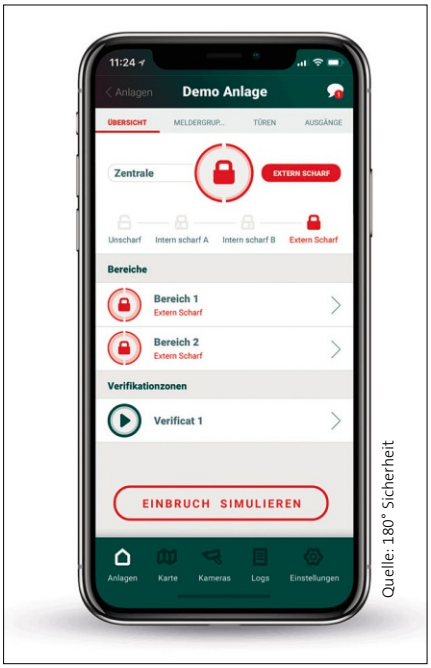

Bild 1: *Per Smartphone-App lassen sich Einbruchszenarien simulieren und potenzielle Risiken ausschalten*

Selbsteinbau durch Laien

Smart-Home-Komponenten zum Selbsteinbauen sind – da sind sich spezialisierte Errichter wohl alle einig – nicht geeignet, um verlässlichen Schutz gewährleisten zu können. Ein großer Schwachpunkt ist dabei auch die Installation, denn das Risiko einer Fehlinstallation oder Manipulation von außen ist hoch. Eine normierte Installation ist beim Selbsteinbau durch den Nutzer nahezu ausgeschlossen, und auch Sabotageüberwachung oder ähnliches ist bei den intelligenten Systemen einer Smart Home-Alarmanlage nur selten zu finden.

Auch die Art der Alarmierung spielt eine große Rolle. Wenn überhaupt, bieten die smarten Systeme eine rein akustische Vor-Ort-Alarmierung. Doch ob der Alarm dann bemerkt wird, ist fraglich. Und wenn bei einem Stromausfall der Internetrouter ausfällt, fallen natürlich auch die Alarmsignale aus.

Billige Technik als Problem

Ein maßgebliches Problem dabei ist, dass der Markt für Smart-Home-Technik von Billigware überflutet ist. Diese genügt in der Regel weder bautechnisch, noch sicherheitstechnisch den erforderlichen Standards. Die Ware ist günstig produziert und schnell installiert. Das ist es, was beim Endverbraucher zunächst zählt. Doch von Ausfallsicherheit, Datenschutz und Cyber-Sicherheit kann dabei keine Rede sein.

Errichter und Techniker kämpfen tagtäglich gegen die billige Ramsch-Ware und versuchen, die Nutzer aufzuklären und von hochwertigeren Lösungen zu überzeugen. Das kann vor allem über die Argumentationslinie der Sicherheitsrisiken und des professionellen Einbaus erfolgen. Diese Art der Aufklärung wird immer wichtiger, je mehr Smart-Home-Lösungen zum gesellschaftlichen Standard werden. Eine vergleichende Darstellung lässt keine Zweifel daran, dass professionell installierte, vernetzte und geschützte Technik einen höheren Schutz und damit die mit smarter Technik angestrebte Lebensqualität liefern kann.

Professionelle Beratung anbieten

Ziel muss sein, dass Bewohner, die sich mit dem Thema Smart Home und Vernetzung im Eigenheim auseinandersetzen, alle relevanten Faktoren bei der Entscheidung einbeziehen und sich nicht von schnellen, billigen Lösungen locken lassen. Es gibt Sicherheitsrisiken, und es ist nur eine Frage der Zeit, bis etwas passiert (siehe **Kasten Schneller Schutz vor Angriffen**). Eine ausführliche Beratung ist daher unabdingbar.

Hier sind Errichter und Elektriker gefragt, auf Kunden zuzugehen und mit individuellen Sicherheitschecks, mögliche Lücken zu identifizieren. Diese zeigen dem Kunden, welche Risiken wirklich vorherrschen und geben dem Elektro-Fachhandwerk die Möglichkeit, eine professionelle und sichere Lösung anzubieten. Ein wichtiger Faktor, um sich von billigen und unsicheren Standardlösungen abzuheben.

Schneller Schutz vor Angriffen

- Alle Smart-Home-Apps schließen
- Passwort bei webbasierten Zugangsportalen ändern
- Regelmäßige Updates der Smart-Home-Software und der Sicherheitssoftware
- Bedienung über interne, verschlüsselte Verbindung einrichten.

Autor:
Malte Tasto
Geschäftsführung,
180° Sicherheit GmbH, Düsseldorf