Sicherheitstipps 07.06.2018 16:30

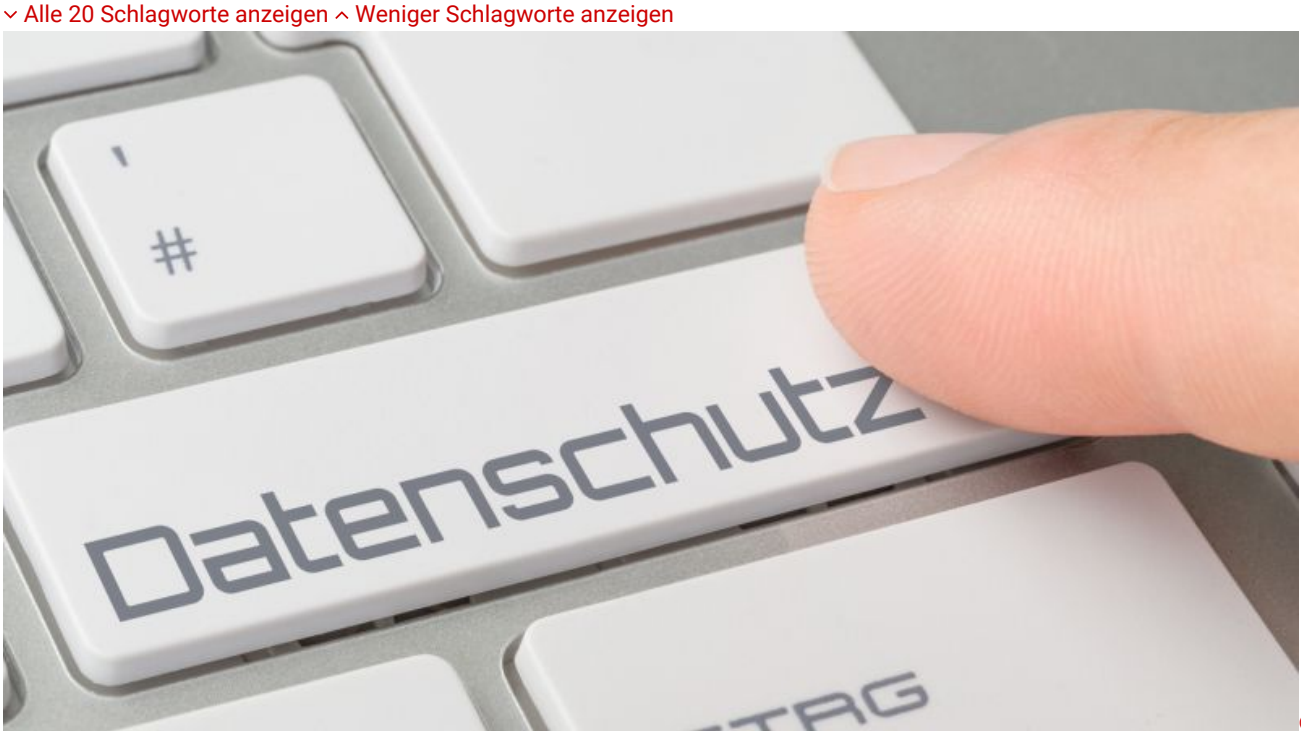
So schützen Sie sich vor Sicherheitslücken im Smart Home

Das Interesse an Heimautomation ist groß. Mit steigender Konnektivität der Geräte steigt oftmals aber auch das Sicherheitsris sich sowohl als Hersteller, als auch als Nutzer vor diesen Risiken schützen können.

Von Magdalena Ott

Sicherheit IT Smart Home Amazon KWR M-smart Marius Marek Barbara Kuchar Anna Mertinz DSGVO Datenschutz Nutzer Net Handy Alexa Recht & Normen Gebäudeautomation

Alle 20 Schlagworte anzeigen Weniger Schlagworte anzeigen



Das Kaufinteresse an smarten Heimassistenten steigt. Gleichzeitig haben die Nutzer aber Angst, dass persönliche Daten durcl gelangen.

Eine Umfrage der Deutschen Energie Agentur dena zeigt: Verbraucher sind sehr interessiert an smarten Lösungen für Zuhause schlecht über Sicherheitsrisiken informiert. Konkret bemängeln mehr als 60 Prozent der Befragten unzureichende Information Sicherheit, Anwendungsfelder, Produktangebote und Kosten beim Thema Smart Home und vernetzte Haushaltsgeräte. TGA kl Risiken auf und erklärt, wie Nutzer und Hersteller sich davor schützen können.

Wie kann es zu Sicherheitsrisiken kommen?

„Ganz grundsätzlich hängt die Sicherheit im Smart Home von den verwendeten Geräten und deren Art zu kommunizieren ab. P Kabelverbindungen miteinander interagieren sind natürlich sicherer, als jene, die eine WLAN-Verbindung nutzen“, erklärt Marius Smart-Home-Anbieters M-Smart, im Interview mit TGA. Tatsächlich ist im Smart Home das größte Sicherheitsrisiko meist nich versteckt, sondern im genutzten Netzwerk. Auch teure und hochwertige Smart Home-Produkte können zum Risiko werden, we gewöhnlichen Router nach außen kommunizieren. „Viele Geräte kommunizieren heute über eine App, wodurch das häusliche N Daten ins Internet gelangen“, erklärt Marek weiter. Über die Datenverbindung wird natürlich auch Hackern der Zugriff auf smart „Verwendet man ein smartes Heizsystem oder eine intelligente Lichtsteuerung, dann geht einem ein Hacker wahrscheinlich nu

Temperatur erhöht oder das Licht ein- und ausschaltet. Bei der Nutzung von Sicherheitssystemen kann es aber sogar zu Einbri
Beispiel elektronische Türen geöffnet werden", warnt der Smart Home-Experte.
Dabei kann es nicht nur offline zu Sicherheitsrisiken kommen: Durch nicht bedachte Installationsfehler können wichtige Kabel
Sicherheitssystem von außen zugänglich sind. Auch bei KNX-Installationen gilt es vorsichtig zu sein. Häufig sind Wetterstatior
Gegensprechanlagen mit einem KNX-Bus verbunden, wodurch auch diese Leitungen von außen erreicht werden können. „Das i
oft nicht bedenken. So kommt es aber ganz schnell zu erheblichen Sicherheitslücken", so Marek.

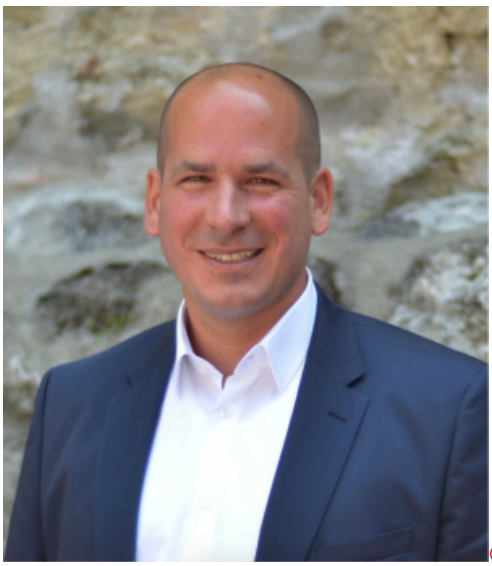
Wie kann ich mich als Nutzer schützen?
Alle smarten Geräte werden von den meisten Nutzern über einen Router und ein Netzwerk gesteuert. Dabei werden die WLAN-
Besucher weitergegeben. Dadurch kommt es zu einem erhöhten Risiko: Schafft ein Hacker es, sich in das Handy des Besucher
nur auf dessen Daten zugreifen, sondern auch auf die des eigenen WLANs. Deshalb empfiehlt es sich, ein Gäste-WLAN einzuri
in ein getrenntes Netzwerk zu hängen und von außen nur über sichere VPN-Verbindungen zu steuern. „Gewöhnliche Router sin
Hat man einmal den Masterkey eines Anbieters rausgefunden, können schnell 100.000 Haushalte geknackt werden", so Mariu
größeren Installationen lohnt es sich deshalb einen Profi zu Rate zu ziehen. Ist man IT mäßig gut abgesichert, ist eine smarte T
normale Tür der gleichen Sicherheitsklasse."

Mehr zum Thema
App der Woche31.07.2018 14:31
Alles unter Kontrolle mit der Smart Control App
Fortschreitendes Wachstum26.07.2018 06:30
Haus- und Gebäudetechnik erzielt starkes Umsatzplus
Vernetzte Heimausstattung12.07.2018 15:48
Darum lohnt es sich, die eigenen Produkte mit Google Home und Alexa vernetzbar zu machen

Was passiert, wenn es dennoch zu Sicherheitslücken kommt?
Die neue Datenschutzgrundverordnung DSGVO zwingt Hersteller zu einem sensibleren Umgang mit vertraulichen Daten, was N
automatisch entlastet, wie Anna Mertinz, Arbeitsrecht- und Datenschutzrecht-Expertin bei Karasek Wietrzyk Rechtsanwälte KW
persönlichen Umfeld gilt die Datenschutzgrundverordnung grundsätzlich nicht. Bei diesem sensiblen Thema geht es unter and
Sicherheitsrisiken kommuniziert werden. Beispielsweise: Womit darf ich rechnen, wenn ich so ein Produkt kaufe?" Deshalb sol
Herstellerinformationen eines smarten Produktes genauestens durchlesen, um über alle möglichen Risiken informiert zu sein.
„Produkte wie Alexa können in einem gewissen Rahmen selbst konfiguriert werden. Nach der DSGVO müssen sie jedoch so vo
Nutzerdaten im geringst erforderlichen Umfang verarbeitet werden. In diesem Rahmen stimmt der Nutzer auch der Datenverw
Kuchar, IP/IT-Spezialistin bei KWR. Kommt es dann zu Sicherheitsproblemen, stellt sich eine Reihe zivilrechtlicher Fragen: Wur
falsch konfiguriert oder war es bereits im Vorhinein mangelhaft?

Um mögliche Klagen abzuwenden, sollten auch Hersteller einiges beachten: Die smarten Produkte müssen alle vorgegebenen
dem Stand der Technik einhalten. Hersteller könnten Haftungsausschlüsse aufnehmen, um auf der sichereren Seite zu sein", e
„Mit einer gewissen Restunsicherheit müssen die Hersteller jedoch trotzdem rechnen, da es sich im Endeffekt immer um eine
handelt."

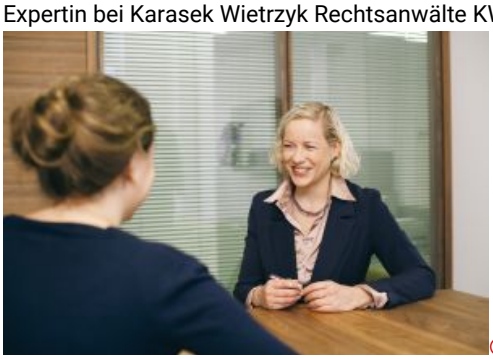
Folgen Sie TGA auf Twitter: @TGAmagazin
Folgen Sie der Autorin auf Twitter: @Ott_Magdalena


© www.m-smart.eu

„Ganz grundsätzlich hängt die Sicherheit im Smart Home von den verwendeten Geräten und deren Art zu kommunizieren ab", e
Geschäftsführer Marius Marek im TGA-Interview.


© KWR

„Im privaten und persönlichen Umfeld gilt die Datenschutzgrundverordnung grundsätzlich nicht", erklärt Anna Mertinz, Arbeitsr Expertin bei Karasek Wietrzyk Rechtsanwälte KWR.


© KWR

„Produkte wie Alexa können in einem gewissen Rahmen selbst konfiguriert werden. Nach der DSGVO müssen sie jedoch so vo Nutzerdaten im geringst erforderlichen Umfang verarbeitet werden. In diesem Rahmen stimmt der Nutzer auch der Datenverw Kuchar, IP/IT-Spezialistin bei KWR.

MEHR VON TGA

GEBÄUDETECHNIK
Facility Management
Energie & Umwelt
Gebäudeautomation

SANITÄR

BRANCHE
Deals & Projekte
Köpfe & Karrieren
Marketing & Vertrieb Digital
Events

DOSSIERS
White Paper
Handwerker-Hattricks Bad-Storys
Recht & Normen

Impressum | Kontakt | Erklärung zum Datenschutz

Crafted by imverlag in Vienna, Austria