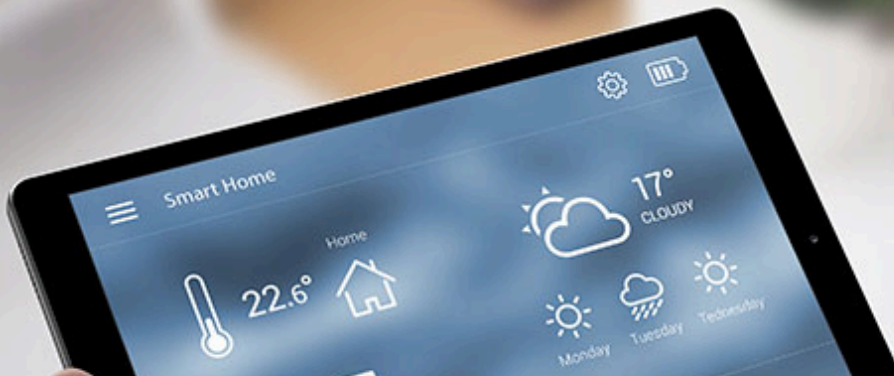




Smart Home soll sicherer werden

Smart Home-Systeme in Wohnräumen sind für viele eine Art Lebensgefühl, auf das sie nicht mehr verzichten wollen. Sieben Prozent der Deutschen nutzen bereits vernetzte Intelligenz für ihr Zuhause und steuern so Wärme, Licht und Energie auf eine komfortable Art und Weise. Welche Risiken mit dieser Vernetzung jedoch verbunden sind, ist vielen Nutzern nicht bewusst. Auch fehlen bis dato klare Anforderungen in puncto Sicherheit für diese Systeme.

Bernhard Gause, Mitglied der Geschäftsführung im Gesamtverband der Deutschen Versicherungswirtschaft (GDV) in Berlin, erläutert:



Verbraucher erwarten, dass beispielsweise alltägliche Steuerungsprozesse wie Jalousien nach Sonnenstand öffnen und schließen, oder auch die Beleuchtung je nach Tageszeit an- und abschalten sowie die Einstellung der Raumtemperatur anpassen, damit geregelt werden können. Doch die Systeme übernehmen immer mehr auch sicherheitsrelevante Funktionen, wie Einbruch- oder Brandmeldung.

Klare Anforderungen an die Cybersicherheit fehlen

Bis dato ist kein verbindlicher Sicherheitsstandard für die smarte vernetzte Intelligenz definiert. Auch Geräte, die in der unmittelbaren Privatsphäre der Verbraucher eingesetzt werden, wie internetfähige Kameras, zählen dazu. Doch gerade diese Sicherheitslücken können Kriminellen Tür und

Tor öffnen. Hausbesitzer über das Internet für eine gewisse Zeit zu beobachten und dann den richtigen Zeitpunkt für einen Einbruch zu wählen, sind heute keine Seltenheit mehr.

Um Cyberrisiken im intelligenten Haus zu minimieren, wurde jetzt von den deutschen Versicherern ein Anforderungskatalog mit den wichtigsten Eckdaten erstellt. Die zentralen Forderungen für Updates, Support, Datenschutz und neutrale Zertifizierung sind:

- Sicherheitsupdates müssen automatisch auf die Geräte geladen werden.
- Hersteller sollten die Sicherheit ihrer Produkte auch nach dem Verkauf mit einem Support und sicherheitsrelevanten Updates gewährleisten.
- Die Länge des Supportzeitraums muss auf dem Gerät für Verbraucher klar erkennbar sein.
- Hersteller verpflichten sich, Verbraucher unverzüglich und umfassend über Sicherheitslücken zu informieren, diese zu schließen und ggf. geeignete Rückrufprozesse einzurichten.

- Die Netzwerkfunktionen der Geräte müssen einfach zu deaktivieren sein.
- Die Hersteller verpflichten sich, die geltenden Datenschutzbestimmungen zu beachten, ggf. in einem eigenen Verhaltenskodex. Außerdem muss klar erkennbar sein, welche Daten für welchen Zweck wohin übermittelt und wie lange sie wo gespeichert werden.
- Um Verbrauchern die Kaufentscheidung zu erleichtern, sollten die Geräte mit einer neutralen Zertifizierung oder einem „Produktsiegel“ gekennzeichnet werden. Das Siegel muss dabei vorher festgelegte und normierte technische Mindeststandards für die Cybersicherheit erfüllen.

Bild: © Stanistic Vladimir / fotolia.com

Versicherungs- und Finanznachrichten

expertenReport



<https://www.experten.de/id/4944052/smart-home-soll-sicherer-werden/>