Smart Home: Sicherheitsrisiken kennen und Gefahren vorbeugen

Verbraucherzentrale NRW gibt Tipps zum richtigen Einsatz intelligenter Geräte in den eigenen vier Wänden

Rollläden, die bei Sonnenaufgang automatisch hochfahren, Saugroboter, die während der Arbeitszeit die Wohnung saugen und wischen und Heizungen, die flexibel Temperaturen senken und wieder aufheizen – im Smart Home ist das möglich und lässt sich bei Nutzung von entsprechenden Apps auch von unterwegs steuern. Die intelligente Vernetzung von Geräten kann dem Komfort dienen, aber je nach Nutzerverhalten auch Energie sparen und die Sicherheit erhöhen. Es gibt allerdings auch Risiken. „Smarte Geräte sammeln sehr viele Daten, aus denen sich ein ziemlich genaues Bild vom Zuhause und den dort lebenden Personen ergibt", sagt Ayten Öksüz, Datenschutzexpertin der Verbraucherzentrale NRW. „Problematisch wird es, wenn nicht nur die Hersteller der Smart Home-Geräte, sondern auch Cloud-Betreiber oder Anbieter sozialer Netzwerke Zugriff auf die gesammelten Daten haben. „Eine weitere Gefahr birgt der potentielle Angriff Krimineller auf das Smart Home. „Hacker können sensible Informationen ausspähen, sich Zugang zu persönlichen Daten und Bankkonten verschaffen und Geräte manipulieren", so Öksüz. Die Expertin gibt Tipps, wie smarte Geräte sicher eingesetzt werden können.

- **Über Datenschutz und IT-Sicherheit der Geräte informieren**
  Die Nutzung von Smart Home-Produkten ist häufig mit einer umfangreichen Erhebung und Verarbeitung personenbezogener Daten verbunden. Für Verbraucher:innen ist dabei oft nicht klar, welche Daten genau erhoben werden und über welche Sensoren Smart Home-Geräte wirklich verfügen. Anhand der übermittelten Daten können umfassende Nutzungsprofile erstellt werden. Darüber hinaus werden Daten nicht nur vom Smart Home-Anbieter selbst, sondern oftmals auch von Drittanbietern verarbeitet. Dazu gehören zum Beispiel Cloud-Betreiber, auf deren Servern die Daten gespeichert werden. Außerdem können in die Apps zur Steuerung der Smart Home-Geräte Drittanbieter eingebunden sein, sodass Daten auch an soziale Netzwerke wie Facebook gehen können. Auch was die IT-Sicherheit betrifft, ist für Verbraucher:innen oft nur schwer einschätzbar, wie sicher einzelne Smart Home-Geräte vor Angriffen seitens Krimineller sind. Eine Orientierung bietet das IT-Sicherheitskennzeichen des Bundesamts für Sicherheit in der Informationstechnik (BSI). Hersteller versichern damit, dass ihr Produkt gewissen grundlegenden Anforderungen des BSI entspricht. Es handelt sich allerdings um eine Selbsterklärung des Herstellers ohne konkrete technische Überprüfung durch das BSI. Aber auch nach Kauf und Einrichtung der Geräte

Verbraucherzentrale
Nordrhein-Westfalen e.V.

Verbraucherarbeit im Kreis Kleve
mobil & digital

Tel. (0211) 54 2222 11
service@verbraucherzentrale.nrw
www.verbraucherzentrale.nrw/kleve

können Sicherheitslücken auftauchen. Deshalb sollten die Geräte und auch die dazugehörigen Apps immer auf dem neuesten Stand sein und verfügbare Updates zeitnah installiert werden.

- **Datenschutzfreundliche Einstellungen vornehmen**
  Bei der Einrichtung der Geräte sollten möglichst datensparsame Einstellungen vorgenommen werden. Ist beispielsweise die Standort-Erfassung über die App oder das Mikrofon für die Nutzung des Smart Home-Geräts nicht nötig, sollten diese jeweils deaktiviert werden. Über die Einstellungen lassen sich Zugriffsberechtigungen auch im Nachhinein anpassen.
- **Starkes Passwort wählen**
  Smart Home-Geräte sollten mit starken Passwörtern geschützt werden, die mindestens acht Zeichen lang sind und aus Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen bestehen. Lange Passwörter ab 20 Zeichen können auch weniger komplex sein. Standardpasswörter sollten unverzüglich geändert werden. Eine Zwei-Faktor-Authentifizierung erhöht die Sicherheit beim Zugriff auf smarte Systeme. Dabei werden zwei Schritte zur Authentifizierung der Nutzer:innen durchgeführt. Hierfür gibt es verschiedene Verfahren: Nach Eingabe des Passworts im Benutzerkonto kann der Anbieter zum Beispiel einen Code an das Smartphone schicken, der zusätzlich eingegeben werden muss.
- **Separates WLAN einrichten**
  Das Smart Home sollte nicht mit demselben WLAN wie der heimische PC, Laptop oder das Smartphone verbunden sein. Am Router kann dafür ein separates Netzwerk für Smart Home-Geräte eingerichtet werden. Auf diese Weise erhält ein Angreifer nicht automatisch Zugriff auf alle mit dem WLAN verbundenen Geräte, wenn er in das Smart Home-System eingedrungen ist und umgekehrt.
- **Rechte von Gästen achten**
  Auch die Rechte von Gästen, Besuchern oder anderer im Haushalt lebender Personen müssen gewahrt werden. Denn auch diese haben ein Recht darauf, selbst zu entscheiden, wer was wann über sie weiß. Wer etwa einen digitalen Sprachassistenten oder ein Gerät mit Videoaufzeichnung aktiv nutzt, während weitere Personen im Haus sind, sollte diese zumindest darauf hinweisen.

Weiterführende Infos und Links:

- Mehr zur Sicherheit von Smart Home Systemen unter:
  www.verbraucherzentrale.nrw/node/6882