+energieinfo!

Smart Home Technologien: Schutz vor Hackerangriffen

Die Energieversorgung Alzenau informiert

Smart Home Technologien bieten eine Vielzahl von Möglichkeiten, Energie im eigenen Haus zu sparen. Via App-Steuerung und durch die Vernetzung verschiedener Geräte lässt sich der Energieverbrauch effizienter gestalten und somit kann man sowohl Kosten sparen als auch die Umweltbelastung reduzieren. Allerdings gibt es auch Risiken im Hinblick auf Datenschutz und Cybersicherheit, die es zu beachten gilt.

Wichtig zu wissen: Unzureichend geschützte Smart-Home-Systeme können anfällig für Hackerangriffe sein, die nicht nur die Privatsphäre gefährden, sondern auch Zugriff auf sensible Informationen oder die Kontrolle über Geräte erlangen können.

Die größten Risiken

1. Smart-Home-Geräte sammeln statistische Daten. Es besteht damit auch das Risiko, dass Daten von Unternehmen für kommerzielle Zwecke genutzt werden, wenn die entsprechenden Datenschutzrichtlinien nicht ausreichend sind.
2. Virtuelle Gefährdung: Wenn Smart-Home-Geräte nicht ausreichend abgesichert sind, könnten Fremde von extern Zugriff erlangen. Sie könnten beispielsweise Kameras hacken, Türschlösser manipulieren oder einen Sicherheitsalarm deaktivieren.
3. Smart-Home-Geräte können anfällig für Trojaner sein, die versuchen, Geräte zu kontrollieren, Daten zu stehlen oder das Netzwerk zu beeinträchtigen.

Das können Sie tun:

1. Seriöse Hersteller und keine No-Name-Marken wählen: Entscheiden Sie sich für Produkte von vertrauenswürdigen Herstellern. Bekannte Marken investieren oft mehr in Sicherheitsmaßnahmen und bieten regelmäßige Updates an, um Schwachstellen zu beheben.
2. Aktuelle Software und Firmware verwenden: Stellen Sie sicher, dass Sie stets die aktuelle Version der Software und Firmware für Ihre Smart-Home-Geräte installiert haben. Aktualisierungen beheben oft bekannte Sicherheitslücken und verbessern die Gesamtsicherheit.

3. Starke Passwörter verwenden: Ändern Sie die Standardpasswörter Ihrer Smart-Home-Geräte und verwenden Sie starke, einzigartige Passwörter. Hierbei helfen Passwort-Generatoren aus nicht cloudbasierten Passwort-Managern.
4. Netzwerksicherheit gewährleisten: Schützen Sie Ihr Smart Home Netzwerk durch die Verwendung einer verschlüsselten Verbindung (z.B. WPA2 oder WPA3) und einer sicheren Wi-Fi-Kennung (SSID). Vermeiden Sie die Verbindung zu öffentlichen Wi-Fi-Netzwerken, da diese ein höheres Risiko darstellen können.
5. Separates Gastnetzwerk einrichten: Richten Sie ein separates Gastnetzwerk ein, um Ihre Smart-Home-Geräte vom Hauptnetzwerk zu isolieren. Dadurch wird verhindert, dass Angreifer auf andere Geräte in Ihrem Netzwerk zugreifen können, falls ein Gerät kompromittiert wird.

Foto: stock.adobe.com