Gefahren für smarte Geräte

Vernetzte Geräte im Haushalt sollen den Alltag erleichtern. Mit der Zunahme der Zahl der Geräte steigen die Sicherheitsrisiken.

Smart Homes – Haushalte auf Basis digital vernetzter Geräte – sollen zu einer Erhöhung der Wohn- und Lebensqualität, Sicherheit oder effizienteren Energienutzung beitragen. Die Nutzung von Haushaltsgeräten, Fenstern, Türen, Licht und Alarmanlagen über Handy oder Computer birgt auch Risiken. Über Vorzüge und Risiken vernetzter Systeme diskutierten Experten des *österreichischen Versicherungsverbandes VVO,* des *Kuratoriums für Verkehrssicherheit (KFV)* und des Bundeskriminalamts (BK) am 15. November 2018 in Wien. „Smart Homes sind auch in Österreich kräftig auf dem Vormarsch und aus den Haushalten der Zukunft nicht wegzudenken", sagte Mag. Rémi Vrignaud, Vorstandsvorsitzender der *Allianz-Gruppe* in Österreich und Vizepräsident des *österreichischen Versicherungsverbandes VVO*. Über das Internet gesteuerte Anlagen böten zwar viel Komfort, jedoch auch eine Angriffsfläche für Cyber-Kriminelle. „Deshalb sollte man alles dafür tun, um seine Komfortzone sicher zu machen", sagte Vrignaud.

Othmar Thann, KFV, Rémi Vrignaud, VVO, Leopold Löschl, Bundeskriminalamt, Louis Norman-Audenhove, VVO.

Prävention durch Information. „Der kontinuierliche Anstieg der Zahl an Cybercrime-Fällen wird durch die stark zunehmende Anzahl von vernetzten Geräten verstärkt und bietet ein attraktives Angriffsziel für Kriminelle", sagte Mag. Leopold Löschl, Leiter des *Cybercrime-Competence-Centers* des Bundeskriminalamts. „Jedes mit dem Internet verbundene Gerät kann über das Internet angegriffen werden." Schwachstellen seien WLAN-Heimnetzwerke oder Router, über die sich die vernetzten Geräte und Systeme mit dem Internet verbinden. Cyber-Kriminelle würden über das Heimnetzwerk Zugriff auf vernetzte Geräte und Systeme erlangen und könnten zum Beispiel Alarmanlagen oder Überwachungskameras deaktivieren. Beim Kauf von smarten Geräte sollte nicht nur auf Design und Funktionalität, sondern vor allem auf Sicherheit geachtet werden. Etwa in Form einer fachkundigen Installation und Wartung. Löschl rät zu überdenken, ob wirklich alles vernetzt sein müsse. Sprachgesteuerte Geräte zum Beispiel hören zu, was gesprochen wird. Es sollte daher überlegt werden, wo diese Geräte aufgestellt und wann sie eingeschaltet werden.

KFV-Studie. Laut einer Umfrage des *Kuratoriums für Verkehrssicherheit* stehen die befragten Österreicher dem Thema Smart Home in Bezug auf Sicherheitsfragen eher skeptisch gegenüber. Für den Großteil der Befragten überwiegen die Gefahren gegenüber dem Nutzen. Die Angst vor der „Verselbstständigung der Geräte" wird als einer der häufigsten Gründe (46 %) für die Verunsicherung angegeben. 64 Prozent fühlen sich durch Smart-Home-Technologien überwacht. Jeder Zehnte hatte bereits mit Fehlfunktionen zu tun, wobei drei Prozent davon auf sicherheitsrelevante Vorfälle wie Datendiebstahl zurückzuführen waren. 47 Prozent schätzten den Nutzen von smarten Geräten höher als deren potenzielle Gefahren ein. „Smarte Geräte kommen im Alltag der Österreicher an, aber es herrscht eine gewisse Skepsis", sagte Dr. Othmar Thann, Direktor des *KFV*.

„Bewusst und gezielt eingesetzt können Smart Devices eine Entlastung im Alltag darstellen. Um Sicherheitsrisiken so gut wie möglich zu minimieren, empfiehlt es sich, gezielt Informationen einzuholen und sich abzusichern", sagte Thann. Das *KFV* hat eine interaktive Online-Plattform entwickelt. Unter *www.sicherheit-mit-zukunft.at* haben Interessierte die Möglichkeit, den eigenen persönlichen Nutzertyp herauszufinden und die richtigen Tipps zu erhalten, um sicher und smart zu leben.

SMART-HOME-GERÄTE

Sicherer Umgang

- Auf Kompatibilität neuer und bestehender Geräte untereinander achten.
- Fachpersonal mit IT-Sicherheitsexpertise aufsuchen.
- Auf Nachhaltigkeit und Support achten, anstatt Billigprodukte zu kaufen.

Beim Datenschutz genauer hinsehen.

- Nutzungsvereinbarungen lesen.
- Auf technische Möglichkeiten und Softwarelösungen der Geräte achten.
- Konfigurationen aktiv betreiben und Settings datenschutzfreundlich einstellen.

Hacker-Angriffe erschweren

- Gebrauchsanleitungen lesen.
- Ein überlegtes Passwortmanagement einsetzen.
- Smart Devices ausschalten, wenn man außer Haus ist.

FOTO: VVO/APA-FOTOSERVICE/HAUTZINGER