KFV-Umfrage: Hauptgrund für die Nutzung smarter Anwendungen daheim ist die Erleichterung des Alltags.

# Smart – aber sicher?

**Die Studie der Projektpartner BMI und KFV „Internet of Things in österreichischen Privathaushalten: Nutzung, Sicherheit und Kriminalität“ liefert Einblicke in persönliche Meinungen, Einstellungen und in den Informationsstand der Bevölkerung – und deckt Sicherheitsdefizite und -potenziale auf.**

Der gläserne Mensch liefert Daten auf Schritt und Tritt. Unser vom Internet of Things geprägter Alltag wird immer digitaler, smarte Devices und innovative Komfort-Technologien sind omnipräsent. Das Internet der Dinge ist gekommen, um zu bleiben: Auch in Österreich hat diese revolutionäre Entwicklungsstufe der Digitalisierung bereits Einzug gehalten. Sensoren vernetzter digitaler Systeme sammeln, kommunizieren, analysieren und handeln basierend auf Informationen, ohne aktives menschliches Zutun. Diese automatisiert agierenden Helferlein bedeuten hohen Komfort – allzu oft auf Kosten der Sicherheit. Das Internet der Dinge öffnet Cyber-Kriminellen Tür und Tor zu unserer Privatsphäre und unserem materiellen und geistigen Eigentum.

**Neue Chancen, neue Risiken.** Die smarten Dinge des Lebens sind zwar eine Zeitersparnis und bieten Luxus, doch sie sind auch Spiegel unseres Alltags. Der smarte Kühlschrank, die ferngesteuerte Heizung und der Staubsaugroboter liefern Hackern Datenlecks. Je komplexer und smarter unser tägliches Leben wird, desto wichtiger wird es für Nutzer/-innen, sich neuer Risiken bewusst zu werden und mit gezielten Maßnahmen für mehr persönliche Sicherheit zu sorgen. Denn je mehr Menschen eine Technologie anwenden, desto größer ist die Gefahr, dass Kriminelle bei sorgloser Nutzung von Daten und Kanälen leichtes Spiel haben. Cybercrime ist leicht umsetzbar, oft schwer verfolgbar und boomt.

**IoT in Haushalten.** Wie schützen wir uns vor Datendiebstahl? Sind wir in Sachen Smart Living schon fit für die Zukunft? Das Bundesministerium für Inneres (BMI) beteiligte sich an einer Studie des *Kuratoriums für Verkehrssicherheit (KFV):* „Internet of Things in österreichischen Privathaushalten: Nutzung, Sicherheit und Kriminalität“. Diese liefert Einblicke in persönliche Einstellungen und in den Informationsstand der Bevölkerung – und deckt Sicherheitsdefizite und -potenziale auf.

## Informationsstand und Nutzungsverhalten

- *Wissen um das Internet der Dinge:* Die KFV-Umfrage zeigt: Besonders hoch ist der subjektive Kenntnisstand zum Thema IoT bei Männern, Personen unter 40 Jahren und im städtischen Bereich.
- *Anschaffung smarter Systeme:* Hauptgrund für die Nutzung smarter Devices daheim ist die Erleichterung des Alltags – diesen Beweggrund geben zwei Drittel der Befragten an.
- *Nutzung von IoT-Geräten:* Die gängigsten IoT-Geräte sind dem Bereich

Foto: HQUALITY/Stock.adobe.com

**KFV-Studie: Fast die Hälfte der Befragten nutzt intelligente Sicherheitssysteme wie smarte Überwachungskameras.**

IT- Equipment zuzuordnen (92 %), das populärste digitale Tool ist der smarte Fernseher (70 %). An zweiter Stelle rangieren smarte Haushaltshilfen (68 %). Die Riege digital gesteuerter Haushaltshilfen dominiert der Staubsaugroboter, gefolgt von smarter Beleuchtung und smarter Kaffeemaschine.

• *Smarte Sicherheitssysteme:* Fast die Hälfte der vom KFV befragten Nutzer/-innen nennt intelligente Sicherheitssysteme wie smarte Überwachungskameras ihr Eigen.

• *Hohe Hürde für Neueinstieg:* Fast die Hälfte der österreichischen Bevölkerung denkt derzeit (noch) nicht daran, sich IoT-Geräte anzuschaffen – ein Hinweis auf die noch immer hohe Hürde, sich ein erstes smartes Gerät zuzulegen.

• *Je jünger, desto IoT-affiner:* Je jünger die Befragten sind, desto höher ist deren Bereitschaft, (weitere) IoT-Geräte zu erwerben.

## Sicherheit und Risiko

• *Passwörter und Updates:* Fast zwei Drittel der österreichischen IoT-Nutzer/innen geben an, auf allen Geräten Passwörter zu verwenden. Die Update-Disziplin lässt zu wünschen übrig: Nicht einmal die Hälfte der Befragten führt regelmäßige Updates durch.

• *Wunsch nach mehr Information:* Sicherheitsmankos gibt es beim Kauf smarter Geräte zu beanstanden. Jede(r) fünfte Verkäufer(in) nennt beim Verkaufsgespräch keinerlei Sicherheitsmaßnahmen. Jeweils rund die Hälfte der befragten Konsument/innen wünscht sich mehr Information vonseiten des Staates bzw. durch Industrie und Handel.

• *Hacking-Attacken:* 17 Prozent der vom KFV befragten Personen geben an, auf smarten Devices bereits einen illegalen Zugriffsversuch erlebt zu haben. Mit dem Schrecken kamen 55 Prozent der Betroffenen davon, ein Viertel der Hacking-Opfer hatte finanziellen Schaden zu beklagen. Bei weiteren fünf Prozent der Geschädigten kam es zu Datendiebstahl.

• *Polizeiliche Anzeigen:* Ein Drittel der von illegalen Zugriffsversuchen betroffenen Personen zeigte den Vorfall polizeilich an. In puncto Anzeigemoral ist Luft nach oben. Mut zur Transparenz sind allerdings ein Muss, um Strafverfolgung und Präventionsarbeit maßgeblich zu erleichtern. Nur polizeilich angezeigte Schadensfälle bringen mehr Licht ins weite Dunkelfeld von Internetverbrechen.

## Cybercrime-Prävention

• *Einrichtung smarter Geräte durch Profis:* Professionelle Installation, persönliche Beratung über notwendige Sicherheitsmaßnahmen und die Änderung vorgegebener Standard-Passwörter sind empfehlenswert.

• *Eigenes Netzwerk für IoT-Geräte:* Mit einem eigens für IoT-Devices installierten Netzwerk wird unerwünschter Zugriff auf private Daten erschwert.

• *Regelmäßige Updates:* Schutz vor Fremdzugriff erfordert regelmäßige Software-Updates. Finger weg von Geräten ohne Update-Möglichkeit.

• *Großer Wert – großer Preis:* Beim Kauf smarter Technik lohnt es sich, auf Qualität zu achten. Sicherheit kostet: Eine einmalige Investition kann spätere größere finanzielle Verluste verhindern.

• *Attacken zur Anzeige bringen:* Alle illegalen Zugriffe – auch Zugriffsversuche – sollten unbedingt angezeigt werden. Jede Anzeige erleichtert der Polizei die Erkennung von Tatmustern und Trends und das Setzen entsprechender Verfolgungsmaßnahmen. Darüber hinaus können spezifische Warnhinweise an die Bevölkerung weitere Cyber-Attacken verhindern. *Patricia Jeßner*

*Studie: www.kfv.at/wp-content/uploads/2022/07/Projektbericht_Cybercrime-IoT_21.pdf*
*Folder: www.kfv.at/wp-content/uploads/2022/06/KFV_Folder_IoT-5G_HP.pdf*

FOTO: PHONLAMAIPHOTO /STOCK.ADOBE.COM