Wie geht's besser?

Staubsaugerroboter vermessen mit Sensoren Wohnungen und laden das erstellte Kartenmaterial auf die Server des jeweiligen Herstellers, obwohl sie eigentlich nur auf dem Gerät selbst gespeichert werden müssten. In vielen Fällen ist es nicht unbedingt notwendig, dass gesammelte Daten der Smarthome-Geräte an den Hersteller übermittelt werden. Trotzdem werden sie in die Cloud übertragen – beispielsweise zur Verbesserung des Komforts oder um den Zugriff von verschiedenen Endgeräten aus zu ermöglichen. Smarte Hersteller sind mehr denn je gefragt, Möglichkeiten und Wege zu finden, smarte Geräte komfortabel und datensicherer zu gestalten.

Weitere Informationen

Das gemeinsame Projekt „Smart Home – aber sicher!" soll zu mehr Information und Bewusstsein im Umgang mit smarten Geräten und sensiblen Daten führen. Dieser Folder wurde von der Arbeiterkammer Niederösterreich im Rahmen ihrer Digitalisierungsoffensive in Kooperation mit der FH St Pölten, Department für Informatik & Security, erstellt. Weitere Tipps und Informationen zu digitaler Sicherheit finden Sie auf **noe.arbeiterkammer.at/digitales.**

Der Schutz von IT-Infrastrukturen und sensiblen Daten stellt Unternehmen jeden Tag vor neue technische und organisatorische Herausforderungen. Mit sechs Instituten und zwei Forschungszentren zählt die FH St. Pölten zu den forschungsstärksten Fachhochschulen des Landes. Mehr darüber unter **research.fhstp.ac.at!**

Kontakt und Information

Hotline Konsumentenberatung: 05 7171-23000
Mo bis Fr: 8 bis 13 Uhr
Mail: konsumentenberatung@aknoe.at

Kammer für Arbeiter und Angestellte für Niederösterreich
AK-Platz 1, 3100 St. Pölten

SERVICENUMMER
05 7171-0
mailbox@aknoe.at
noe.arbeiterkammer.at

ÖFFNUNGSZEITEN
Montag bis Donnerstag 8 – 16 Uhr
Freitag 8 – 12 Uhr

BERATUNGSSTELLEN	DW
Amstetten, Wiener Straße 55, 3300 Amstetten	25150
Baden, Elisabethstraße 38, 2500 Baden	25250
Flughafen-Wien, Office Park 3 - Objekt 682, 2. OG - Top 290, 1300 Wien	27950
Gänserndorf, Wiener Straße 7a, 2230 Gänserndorf	25350
Gmünd, Weitraer Straße 19, 3950 Gmünd	25450
Hainburg, Oppitzgasse 1, 2410 Hainburg	25650
Hollabrunn, Brunnthalgasse 30, 2020 Hollabrunn	25750
Horn, Spitalgasse 25, 3580 Horn	25850
Korneuburg, Gärtnergasse 1, 2100 Korneuburg	25950
Krems, Wiener Straße 24, 3500 Krems	26050
Lilienfeld, Pyrkerstraße 3, 3180 Lilienfeld	26150
Melk, Hummelstraße 1, 3390 Melk	26250
Mistelbach, Josef-Dunkl-Straße 2, 2130 Mistelbach	26350
Mödling, Franz-Skribany-Gasse 6, 2340 Mödling	26450
Neunkirchen, Würflacher Straße 1, 2620 Neunkirchen	26750
Scheibbs, Burgerhofstraße 5, 3270 Scheibbs	26850
Schwechat, Sendnergasse 7, 2320 Schwechat	26950
SCS, Bürocenter B1/1A, 2334 Vösendorf	27050
St. Pölten, AK-Platz 1, 3100 St. Pölten	27150
Tulln, Rudolf-Buchinger-Straße 27 – 29, 3430 Tulln	27250
Waidhofen, Thayastraße 5, 3830 Waidhofen/Thaya	27350
Wien, Plößlgasse 2, 1040 Wien	27650
Wr. Neustadt, Babenbergerring 9b, 2700 Wr. Neustadt	27450
Zwettl, Gerungser Straße 31, 3910 Zwettl	27550

ÖSTERREICHISCHER GEWERKSCHAFTSBUND
Landesorganisation Niederösterreich
AK-Platz 1, 3100 St. Pölten
niederösterreich@oegb.at

Facebook
facebook.com/ak.niederoesterreich

Broschüren
noe.arbeiterkammer.at/broschueren

AK-App
noe.arbeiterkammer.at/app

YouTube
www.youtube.com/aknoetube

Foto: AdobeStock

IMPRESSUM
Herausgeber, Medieninhaber und Redaktion: Kammer für Arbeiter und Angestellte für Niederösterreich, AK-Platz 1, 3100 St. Pölten
Telefon: 05 7171-0
Hersteller: Eigenvervielfältigung
Stand: 2021

SMART HOME

fh st. pölten

KONSUMENTENSCHUTZ noe.arbeiterkammer.at/konsument

Smart Home

Einleitung

Das Internet der Dinge (Internet of Things – IoT) bezeichnet die (globale) Vernetzung von Gegenständen und Geräten mit dem Internet. So können diese smarten Helfer selbstständig Aufgaben für den Besitzer erledigen oder auch über das Internet kommunizieren – das soll unseren Alltag bequemer und effizienter machen. Sprachassistenten, Haushaltsgeräte, Heizungssteuerungen, Wearables (beispielsweise smarte Uhren oder Fitnessarmbänder), TV-Geräte oder auch intelligentes Spielzeug dringen aber auch immer mehr in unsere privatesten Bereiche vor. Oft werden dabei verschiedenste Daten von Nutzer*innen erfasst, an eine herstellereigene Cloud übertragen und verwertet.

Die zwei wichtigsten Fragen, die beim Betrieb eines smarten Geräts beachtet werden sollten:

- Welche Daten werden vom Hersteller selbst erfasst und wie werden diese Daten verwertet und gespeichert?
- Wie sicher sind die Geräte gegenüber Gefahren und Zugriffen Dritter – beispielsweise aus dem Internet?

Tipps vor dem Kauf:

Informieren Sie sich schon vor dem Kauf darüber, welche Daten bei einer Registrierung und der eigentlichen Nutzung des Geräts abgefragt werden. Häufig werden etwa personenbezogene Daten erfasst – darunter fallen beispielsweise Name, Geburtsdatum, Körpergröße, Geschlecht, Standort, Telefonnummer, E-Mail-Adresse etc. Denkbar ist aber auch, dass Hersteller Daten zusätzlich aus anderen Quellen wie beispielsweise sozialen Medien sammeln. Vergewissern Sie sich, ob Sie die Abläufe der Datenerfassung, -verwaltung und -verwendung verstehen und letztlich auch die Hoheit über die erhobenen und gespeicherten Daten bei Ihnen liegt (beispielsweise Löschung). Lesen Sie dazu die Datenschutzerklärung des Anbieters! Werden beispielsweise sensible Gesundheits- oder Standortdaten abgefragt, obwohl dies mit der Funktionalität der Anwendung nichts zu tun hat, oder enthalten die Unterlagen keine Information darüber, wo die Daten gespeichert werden, sieht man sich besser nach einem anderen Gerät um.
Eine kurze Recherche im Internet kann oft weitere hilfreiche Informationen zur Sicherheit liefern – beispielsweise wie lange und häufig das Gerät mit Softwareupdates versorgt wird und welche Erfahrungen andere Nutzerinnen und Nutzer damit gemacht haben.

Da die meisten Smarthome-Geräte mithilfe einer eigenen Smartphone-App gesteuert werden, sollte vor einem Kauf geprüft werden, welche Berechtigungen die App fordert. Über Berechtigungen (Permissions) wird festgelegt, auf welche Funktionen und Daten eine App auf einem Smartphone zugreifen darf. Apps werden jedoch oft mehr Berechtigungen eingeräumt, als technisch notwendig wäre (so benötigt beispielsweise eine simple Taschenlampen-App keinen Zugriff auf Standort- oder Kontaktdaten). Worauf man bei Berechtigungen auf dem Smartphone achten sollte, können Sie in dem Folder „Apps – aber sicher!“ der AK Niederösterreich in Kooperation mit der Fachhochschule St. Pölten nachlesen.

Tipps vor der Einrichtung:

Der Router ist der zentrale Knotenpunkt für den Datenverkehr in einem Haus und stellt somit das Herzstück der digitalen Vernetzung beispielsweise für Computer, Smart-TV oder auch die Heizungssteuerung dar. Schwachstellen auf dem Router sollten daher ausgeschlossen und angebotene Firmware-Updates des Herstellers zeitnah installiert werden. Um smarte Geräte getrennt von der restlichen digitalen Infrastruktur betreiben zu können, sollte dafür ein eigenes WLAN-Netzwerk im Router eingerichtet werden. Anleitungen dazu finden sich in den Beschreibungen des Herstellers. Wird für Smarthome-Geräte ein eigener Router oder Access Point (AP) verwendet, dann verhindert die Funktion „AP Isolation“, dass Geräte unerwünschte Verbindungen innerhalb des Netzwerks aufbauen können. Die Geräte können jedoch das Internet weiterhin erreichen. Sollten die Smarthome-Geräte eine direkte Verbindung zu anderen Geräten benötigen, kann diese Funktion nicht genutzt werden.

Tipps bei der Verwendung:

Hinterfragen Sie auch während des Betriebs Datenzugriffe kritisch und geben Sie nicht mehr Daten als gefordert an. Hersteller-Updates für das Gerät, eine App, Betriebssystem und Virenschutz sollten jeweils zeitnah installiert werden.

So können Sie die Sicherheit erhöhen:

TIPP

Sichere Passwörter verwenden!
Voreinstellte Zugangsdaten sind oft leicht zu knacken – ändern Sie diese daher auf sichere Passwörter und kontrollieren Sie diese regelmäßig. Denn unsichere Passwörter können Dritten leicht den Zugriff auf Kundenkonten und zugehörige Daten ermöglichen. Ein gut merkbarer Satz mit Zahlen und Fremdzeichen kann Grundlage für ein sicheres Passwort sein:
„Ich esse gerne Pizza mit 3 Zutaten, aber ohne Käse!“ I e g P m 3 Z , a o K !
„Mein Hund heißt Rosi und hat 4 Pfoten!
M H h R u h 4 P!

TIPP

Zwei-Faktor-Authentifizierung aktivieren!
Das ist eine zusätzliche Sicherheitsmaßnahme zum Schutz von Benutzerkonten. Zusätzlich zum Passwort muss beim Login eine weitere Sicherheitskomponente eingegeben werden. Beispielsweise ein PIN-Code, der auf die im Konto hinterlegte Handynummer der Nutzer*innen gesendet wird.