ANNA
Das vernetzte Leben

Dossier

VERNETZTES WOHNEN

INHALT

ÜBER DIESES DOSSIER

Wer das Wort „Künstliche Intelligenz“ hört, denkt oft an Science-Fiction und die Machtübernahme der Maschinen. Auch Algorithmen, also komplexe Handlungsanweisungen für Computer, werden häufig als bedrohliche Macht dargestellt.

Doch im Alltag hat die Technik eine andere Gestalt: Digitale Sprachassistenten in Smartphones und Lautsprechern beantworten zum Beispiel die Frage, wie das Wetter wird oder suchen eine Zugverbindung heraus; ein vernetzter Thermostat nutzt unterschiedliche Daten, um die Raumtemperatur zu regeln.

Dennoch bleibt häufig verborgen, was im Hintergrund passiert, wenn solche lernenden und vernetzten Systeme aktiv sind. Zum Beispiel, welche Daten dabei gesammelt werden und was in diesen Daten steckt. Ein weiterer Aspekt ist die Sicherheit vernetzter Geräte: Viele Produkte sind alles andere als „smart“ und können allenfalls für einen kurzen Zeitraum sicher betrieben werden.

Um diese und andere Themen geht es im Projekt „ANNA – Das vernetzte Leben“ von iRights e.V., das im Dezember 2017 gestartet ist. In unterhaltsamen fiktionalen Geschichten und informativen Beiträgen widmet es sich der Bedeutung von Algorithmen und Künstlicher Intelligenz im Alltag. Es wird vom Bundesministerium der Justiz und für Verbraucherschutz gefördert.

Auf → annasleben.de finden Sie Geschichten aus Annas Leben, in Form von Videos, Audio-Beiträgen und Kurzgeschichten. Dieses Dossier bietet begleitende Hintergrundinformationen über technische, rechtliche und gesellschaftliche Aspekte des Themenschwerpunktes „Vernetztes Wohnen“ sowie praktische Tipps. Es soll dazu beitragen, Chancen und Risiken besser beurteilen zu können, um Verbraucherinnen und Verbraucher beim informierten Umgang mit den neuen Produkten und Diensten zu unterstützen.

VERNETZTES WOHNEN

HEIM, HERD – UND SMARTE APPARATE

Mit Geräten wie Sprachassistenten, Saugrobotern oder vernetzten Glühbirnen erobert die Digitalisierung einen besonderen Lebensbereich: unsere eigenen vier Wände. Welchen Nutzen sie bieten und welche möglichen Risiken man beim Einsatz beachten sollte, darum geht es in diesem Dossier.

In den fiktionalen Geschichten auf → annasleben.de setzt sich die Hauptfigur Anna immer wieder mit Situationen auseinander, in denen Technologien wie Algorithmen und Künstliche Intelligenz einen Einfluss auf ihr Leben haben. Neuerdings merkt sie diese Auswirkungen ziemlich direkt, in ihren eigenen vier Wänden: Smart Home-Geräte bringen die neuesten technischen Entwicklungen in unser persönlichstes, ganz privates Lebensumfeld.

Keine Frage: Intelligente, vernetzte Apparate im Haushalt können Nutzen bringen, aber sie bergen auch Risiken. Häufig bleibt verborgen, was im Hintergrund passiert, wenn solche lernenden und vernetzten Systeme aktiv sind. Was beispielsweise in den Daten steckt, die diese Hausgeräte sammeln, ist uns häufig gar nicht bewusst. Auch in punkto Sicherheit sind viele der Produkte auf dem Markt alles andere als „smart“.

Geräte wie Sprachassistenten machen deutlich, wie beinahe selbstverständlich Künstliche Intelligenz (KI) und maschinelles Lernen bereits in unserem Alltag angekommen sind. Für Anna bedeutet das, dass sie zwar viele neue Helfer hat – keine Menschen, sondern computergesteuerte Assistenten. Aber damit die ihr tatsächlich helfen, muss Anna sie erst einmal bändigen. Genau wie Anna sollten sich Verbraucherinnen und Verbraucher damit auseinandersetzen, wie diese Geräte funktionieren, welche Chancen und Risiken mit ihnen verbunden sind – und worauf man bei der Nutzung besonders achten sollte.

TECHNIK

WAS MACHT SPRACHASSISTENTEN KLUG?

Sprachassistenten zeigen, wie Künstliche Intelligenz und maschinelles Lernen bereits in den Alltag eingezogen sind. Doch welche Technologien stecken dahinter? Und sind die Geräte wirklich so smart, wie es scheint?

Wie wird morgen das Wetter? Wann fährt der Zug nach München? Digitale Sprachassistenten, die solche Fragen beantworten können, finden sich in immer mehr Smartphones, Lautsprechern, Laptops und anderen Geräten. Sie heißen Siri, Alexa, Cortana oder Google Assistant. Geht es nach den IT-Unternehmen, werden sie in Zukunft in immer mehr Gegenständen und Situationen anzutreffen sein.

Statt mit Tastatur oder Touchscreen bedient zu werden, hören sie auf etwas typisch Menschliches und extrem Komplexes: Sprache. Versuche, Maschinen das Hören und Sprechen beizubringen, sind nicht neu. Sie kamen bislang aber nur in wenigen, genau kontrollierten Situationen zum Einsatz, etwa in Telefonwarteschleifen. Dabei mussten sich eher die Nutzerinnen und Nutzer dem stark begrenzten Horizont der Maschine anpassen als umgekehrt.

Wie Assistenten Sprache erkennen

In den letzten Jahren wurde die Technik so weiterentwickelt, dass digitale Assistenzsysteme viele alltägliche Äußerungen identifizieren können, selbst wenn im Hintergrund die Waschmaschine läuft. Dahinter stehen mehrere Entwicklungen. Damit ein digitaler Assistent zum Beispiel die Frage nach dem Wetter beantworten kann, kommen an unterschiedlichen Stellen Techniken zum Einsatz, die zur Künstlichen Intelligenz (KI) zählen. Die dazu nötige Rechenkraft wird über das Internet bereitgestellt oder steckt im Prozessor eines Smartphones.

Wird der Assistent gefragt: „Wie wird das Wetter?“, so geht es zunächst darum, im akustischen Signal einen solchen Satz zu erkennen. Diese Spracherkennung findet häufig auf den Servern der Anbieter statt, wohin die Assistenten meist alle Daten senden, die ihnen anvertraut werden. Dazu wird die Lautfolge in ihre kleinsten Bestandteile zerlegt und nach charakteristischen Merkmalen durchsucht. Schließlich berechnet das Programm stur die Wahrscheinlichkeit, mit der es sich um eine bestimmte Wortfolge handelt.

KÜNSTLICHE INTELLIGENZ (KI)

KI ist der Versuch, Computern Dinge beizubringen, die Menschen bislang besser können. Kognitive Fähigkeiten wie das Lernen werden dabei durch Technik nachgeahmt. Das maschinelle Lernen ist ein Gebiet der KI. Ähnlich wie Wissen aus Erfahrung entstehen kann, sollen Computer aus den unterschiedlichsten Daten lernen, Muster oder Gesetzmäßigkeiten zu erkennen und Modelle zu entwickeln. Damit sollen sie auch solche Aufgaben lösen, die nicht von vornherein bekannt sind.

Der Ansatz des maschinellen Lernens besteht dabei nicht darin, den Assistenten vorab Regeln einzuprogrammieren – etwa diejenigen, wie Sprache funktioniert. Vielmehr setzt man ihnen zunächst große Datensammlungen vor, um sie zu trainieren. Maschinen lernen anders als Menschen, aber gemeinsam ist ihnen: Versuch und Irrtum macht klug. In den Datenbergen finden sie komplexe statistische Zusammenhänge, deren Struktur zum Beispiel den Regeln der Sprache folgt. Nach und nach gewinnen sie aus den Daten ein Modell. Dieser Ansatz reicht häufig bereits aus, um sie für alltägliche Aufgaben einsetzen zu können.

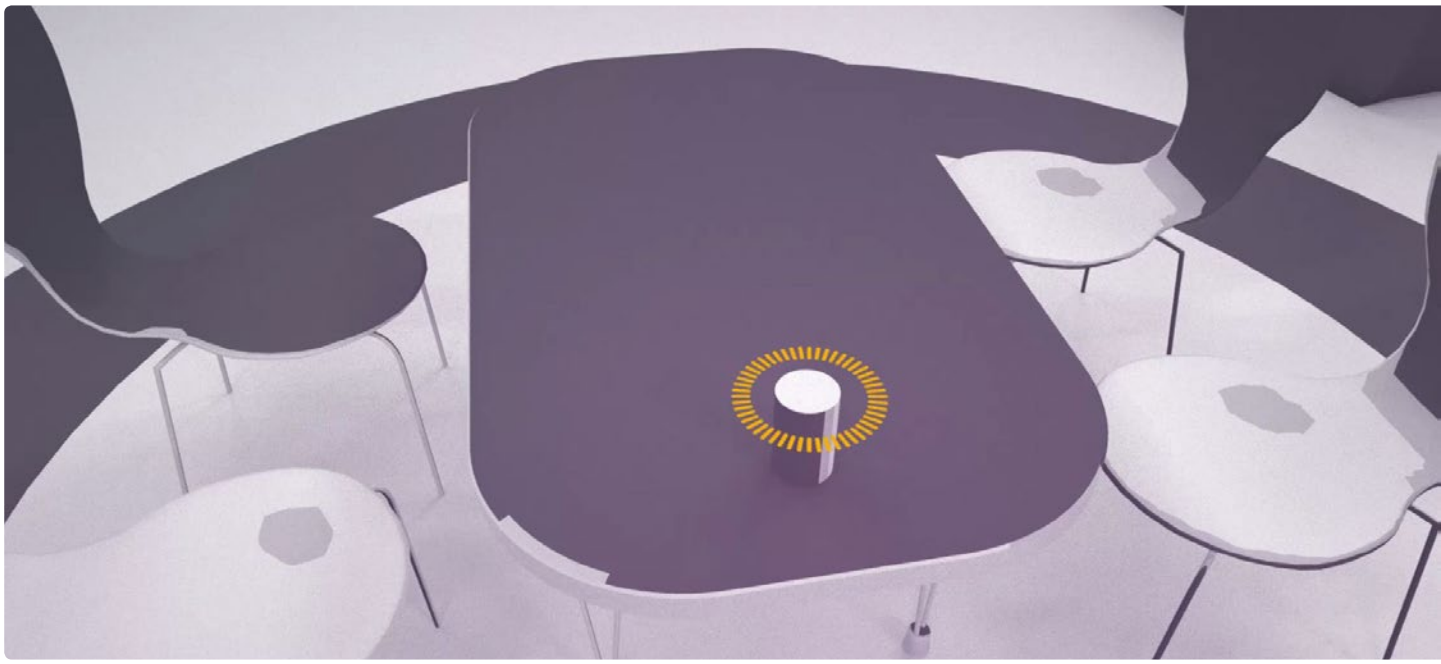
Kontext erkennen

Doch mit Spracherkennung allein ist es nicht getan. Um eine passende Antwort zu liefern, muss der Assistent erkennen, welche Absicht eine Nutzerin oder ein Nutzer mit dem geäußerten Satz verbindet. Sprache ist zudem vieldeutig: Ohne Kontext lässt sich ein Satz oft nicht deuten. Derzeit mobilisieren die IT-Unternehmen sämtliche Kräfte, den Assistenten solche Fähigkeiten beizubringen.

Ein Beispiel: Fragt jemand in Hamburg den Assistenten zuerst nach einem Zug nach München, anschließend nach dem Wetter, so geht es womöglich um das Wetter in München. Um Allgemeinwissen nachzuvollziehen, werden die Assistenten mit großen Faktendatenbanken verknüpft, etwa Googles „Knowledge Graph“ oder Microsofts „Satori Knowledge“. Auch die Nutzerinnen und Nutzer liefern den Anbietern stetig Daten zurück, mit denen die Assistenten dazulernen.

ANNA IST VERSCHWUNDEN

Als die besorgten Nachbarn Annas smarte Geräte um Hilfe bitten, geben sie bereitwillig Auskunft über Annas Leben. Warum das Ganze aus dem Ruder läuft und ob die Sache ein glückliches Ende findet – davon erzählt die Kurzgeschichte → **„Anna und der Bankraub“.**



Intelligenz bleibt beschränkt

Trotz aller technischen Entwicklung bleiben die Fähigkeiten der Assistenten auf wenige, genau abgegrenzte Bereiche und Lebensaspekte beschränkt. Das gilt auch für die Entwicklung der KI insgesamt. Literatur und Kino haben schon lange eine allgemeine KI erdacht, die beliebige menschliche Aufgaben übernehmen kann. Immer wieder schien es manchen Forscherinnen und Forschern, als stünde die Informatik kurz vor dem Durchbruch zu einer solchen „Superintelligenz". Doch immer wieder stellte sich heraus: Die Prognose fußte auf falschen Annahmen, war zu optimistisch.

Je mehr die digitalen Assistenten allerdings über ihre Besitzerin oder ihren Besitzer wissen, desto eher können sie selbsttätig aktiv werden. Sie warnen dann etwa vor Stau auf dem Weg zur Arbeit, noch bevor man sich auf den Weg gemacht hat. Eine Suchmaschine zu bedienen, könnte bald altmodisch erscheinen.

CASSANDRA, LASS DAS!

Dass es mit der „Intelligenz" ihrer neuen Haushaltshelfer nicht zum Besten bestellt ist, merkt Anna ziemlich schnell. Ob sie es schafft, das Heer aus sprachgesteuerten Lampen, Saugrobotern und anderen Assistenten zu bändigen, kann man im Kurzfilm → **„Vernetztes Wohnen"** herausfinden.

Womöglich sind die digitalen Assistenten daher nur Vorboten einer Entwicklung, in der die künstliche der menschlichen Intelligenz nicht gegenübersteht, sondern die Fähigkeiten und Sinne von Menschen erweitert, wie es Werkzeuge und Medien schon immer getan haben. Der Preis ist, dass die lernenden Systeme uns umso besser assistieren, je mehr sie auch permanente Datensammler sind.

DATENSCHUTZ

WELCHE DATEN SPRACHASSISTENTEN SAMMELN

Sprachassistenten lauschen stetig ihrer Umgebung. Aber welche Art von Daten sammeln sie überhaupt – und was geschieht mit diesen Daten?

Sprachassistenten gibt es nicht nur auf Smartphones und Computern, sie werden zunehmend auch in Geräte wie Lautsprecher und Spielzeuge eingebaut. Gestartet werden sie meist mit einem Aktivierungswort – je nach Anbieter und Einstellung lautet es zum Beispiel „Computer“, „Alexa“, „OK Google“ oder „Hey Cortana“. Das Mikrofon ist dauerhaft aktiv, um das jeweilige Wort zu erkennen. Laut den Herstellern werden keine Daten übertragen, solange es nicht gesprochen wird.

Nach dem Aktivierungswort zeichnet das System alle sprachlichen Äußerungen auf und verarbeitet sie über das Internet. Gespeichert werden in der Regel sowohl die Ausgangsdaten als auch die vom Assistenten gelieferten Ergebnisse. Beispiele sind die durch Spracheingaben ausgelösten Suchanfragen oder Webseiten, die als Antwort geöffnet werden.

Verknüpft werden sie mit zusätzlichen Angaben, den sogenannten Metadaten. Dazu gehört etwa die Uhrzeit der Sprachaufzeichnung oder die IP-Adresse, die ein Gerät im Datenverkehr identifizierbar macht. Die Anbieter wissen zudem, welche Hard- und Software dabei zum Einsatz kommt. Je nach Anbieter kommen weitere Daten hinzu, beispielsweise Diagnose- und Standortdaten. Die Geräte sind ständig online und können in der Regel jederzeit geortet werden.

Was machen Sprachassistenten mit den Daten?

Daten, die ein Sprachassistent erfasst, werden an die Server der Anbieter weitergeleitet. Dort werden sie gespeichert, automatisch analysiert und verarbeitet. Das Ergebnis wird an das Eingabegerät zurückgesendet. Zum Beispiel gibt der Assistent eine Sprachantwort aus, startet ein Musikstück oder löst eine andere Aktion auf dem Gerät aus. Mit den Daten werden zugleich die Fähigkeiten der Assistenzsysteme weiter trainiert.

Die Datenschutzerklärungen der Anbieter begründen meist nur allgemein, zu welchem Zweck sie Nutzerdaten erfassen, und nennen etwa die Bereitstellung und die laufende Verbesserung ihrer Dienste.

Apple beispielsweise sammelt die von Siri erfassten Daten, um die Nutzerinteressen besser kennenzulernen. Google will mit den Daten unter anderem die Suchergebnisse verbessern und zum Beispiel Verkehrsinformationen „zeitnah“ anbieten. Das Unternehmen hat seit geraumer Zeit einheitliche Regeln für seine Dienste eingeführt.

Die ursprünglich auf den E-Mail-Dienst passende Formulierung, dass auch „Inhalte“ analysiert werden, dürfte auch für den Sprachassistenten gelten. Das soll vor allem der personalisierten Werbung sowie individuell zugeschnittenen Suchergebnissen dienen. Keiner der Hersteller gibt genau an, wie lange die Daten gespeichert werden; offenbar geschieht es unbefristet.

Die Bundesdatenschutzbeauftragte Andrea Voßhoff stellte kürzlich fest, dass bei Sprachassistenten „nicht eindeutig erkennbar“ sei, „wie und wo die aufgenommenen Daten verwendet und genutzt werden.“ Das Datenschutzrecht setzt zum rechtskonformen Einsatz unter anderem voraus, dass die Nutzerin oder der Nutzer seine Einwilligung in die Datenverarbeitung erteilt und vom Anbieter detailliert erfährt, wer, was, wie und wo mit seinen Daten macht.

Auf Daten, die auf US-Servern gespeichert werden, können auch US-Behörden zugreifen. Ende 2016 werteten Strafverfolgungsbehörden zum Beispiel Aufzeichnungen von Amazon Echo aus, um ein Gewaltverbrechen aufklären zu können. Theoretisch können Sprachassistenten auch von Dritten abgehört und manipuliert werden, wenn es gelingt, die Systeme zu überlisten. Beispielsweise, indem frühere Sprachbefehle abgefangen und neu zusammengestellt werden.

Welchen Einfluss haben die Nutzerinnen und Nutzer?

Teilweise lassen sich die Daten, die beim Benutzen eines Sprachassistenten gesammelt werden, einsehen und löschen. Amazon etwa bietet die Option, den Verlauf der Datenaufzeichnungen in seiner Alexa-App und auf seiner Website einzusehen. Ähnlich wie in einem Browserverlauf lassen sich einzelne Einträge entfernen. Google zeigt die Sprachaufzeichnungen unter „Aktivitäten ansehen“ an. Dort können sie angehört und einzeln entfernt werden. Ähnlich ist es bei Microsofts Cortana. In den „Privacy“-Einstellungen des eigenen Kontos gibt es die Funktion „Notizbuch bearbeiten“. Wie weitgehend die Daten letztlich auch auf den Servern der Anbieter gelöscht werden, lässt sich kaum überprüfen.

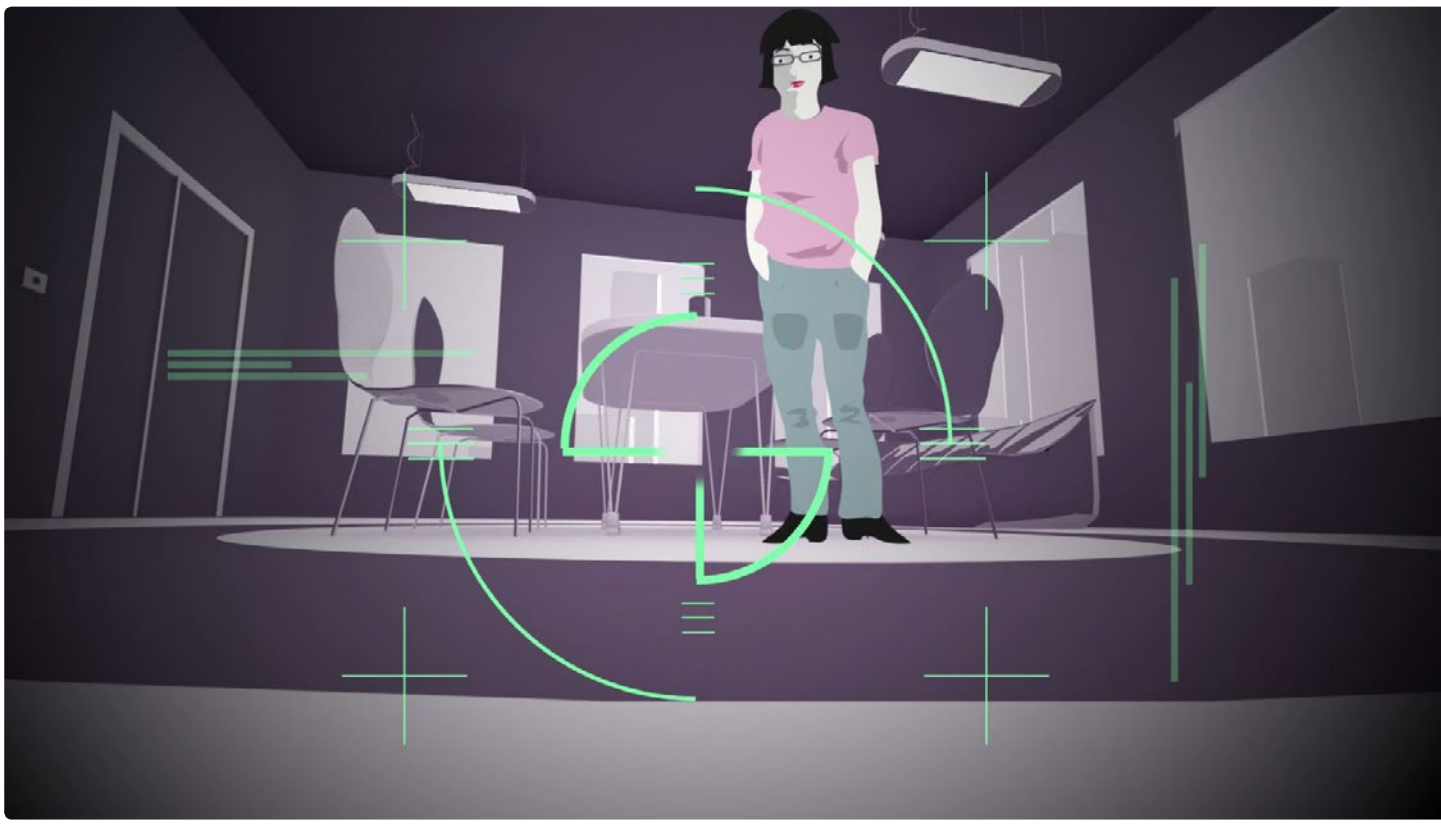
Während Amazon, Google und Microsoft also die erfassten Daten direkt einer Nutzerin oder einem Nutzer zuordnen, setzt Apple auf ein anderes technisches Design. Dort werden alle Daten nicht der Benutzerkennung „Apple ID“, sondern einer zufällig generierten

Kennziffer zugeschrieben. Wenn Siri samt Diktierfunktion deaktiviert und erneut aktiviert wird, wird die Kennung laut Datenschutzerklärung „zurückgesetzt“. Die mit der pseudonymen Kennziffer verbundenen Daten werden gelöscht und der Assistent fängt an, neu zu lernen. Somit ist die Zuordnung zu einem bestimmten Konto nicht auf direktem Weg möglich.

Und was folgt daraus?

Mit den Sprachassistenten eröffnet sich für die IT-Unternehmen eine neue Schnittstelle, um stetig weitere Daten über die Nutzerinnen und Nutzer zu sammeln. Dazu gehören etwa Stimmprofile, die eine Sprecherin oder einen Sprecher identifizieren. Viele Informationen und Auswertungsmöglichkeiten liefern die Nutzerinnen und Nutzer allerdings bereits über die Daten, die ihr Smartphone generiert, auch wenn darauf kein Sprachassistent aktiv ist.

Die Bundesdatenschutzbeauftragte warnt vor einer „Dauerüberwachung“ durch die Assistenten und erinnert daran, dass Sprachbefehle nicht zwingend auf die Server der Anbieter übertragen werden müssen. Sie verlangt, dass die Daten „das Gerät nicht verlassen und nach kurzer Zeit (weniger als 15 Minuten) wieder überschrieben werden“ sollen. Umgesetzt wurde diese Forderung von den Herstellern bislang nicht.



LÜCKENHAFT

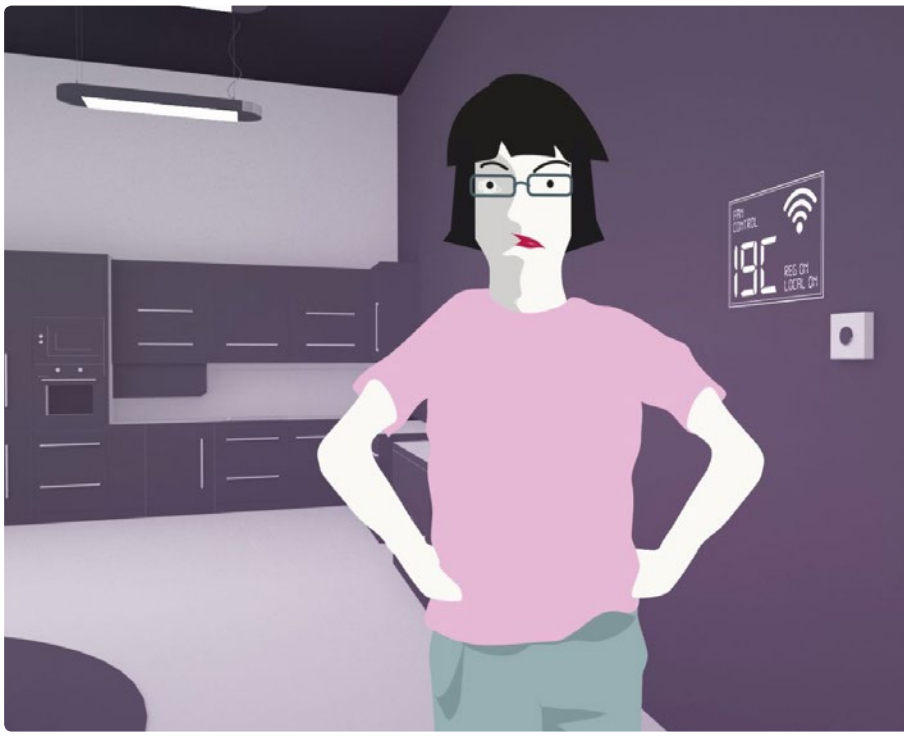
DATENSICHERHEIT IM VERNETZTEN ZUHAUSE

Intelligente und vernetzte Technologien im Haushalt können Nutzen bringen, aber auch missbraucht werden. Kriminelle könnten die Geräte kapern oder Daten abfischen. Damit das nicht passiert, sollte man die Risiken kennen und Sicherheitsvorkehrungen treffen.

Wie praktisch: Der vernetzte Thermostat passt sich flexibel daran an, wann man zu Hause ist, und heizt schon mal vor. Doch sollte Bequemlichkeit nicht auf Kosten der Sicherheit gehen. Wie jede digitale Technologie können auch vernetzte Hausgeräte missbraucht werden, etwa zum Ausspionieren der Bewohnerinnen und Bewohner oder für Angriffe auf Dritte. Zu den möglichen Angriffspunkten gehören die einzelnen Heimgeräte, der Datenverkehr und die sogenannte Cloud-Plattform im Internet, aber auch ein Smartphone, das die Hausgeräte steuert.

Ungefragter Blick in die Wohnung

Nicht nur privat genutzte Überwachungskameras machen Fotos und laden sie in die Cloud, auch moderne Staubsaugerroboter verfügen über eingebaute Kameras. Auf ihrer Fahrt durch die Zimmer entsteht ein detaillierter Grundriss der Wohnung und ihrer Einrichtung. Einbrecher, die sich für die Ausstattung der von ihnen ausgewählten Wohnungen interessieren, könnten vorab eine Rundfahrt mit dem Staubsauger unternehmen.



Angesichts eklatanter Sicherheitsprobleme vieler Smart Home-Geräte ist dieses Szenario gar nicht so weit hergeholt, wie man denken könnte. Beispielsweise ermöglichten es bestimmte Schwachstellen bis vor kurzer Zeit, dass ein vernetzter Staubsaugerroboter des Herstellers LG von Unberechtigten ferngesteuert werden konnte. Nach Angaben des Herstellers wurden die Sicherheitslücken mittlerweile durch Software-Updates behoben. Solche Schwachstellen können auch bei vielen anderen vernetzten Geräten wie Kühlschränken, Öfen, Waschmaschinen oder Trocknern auftreten.

Überlistete Alarmanlagen

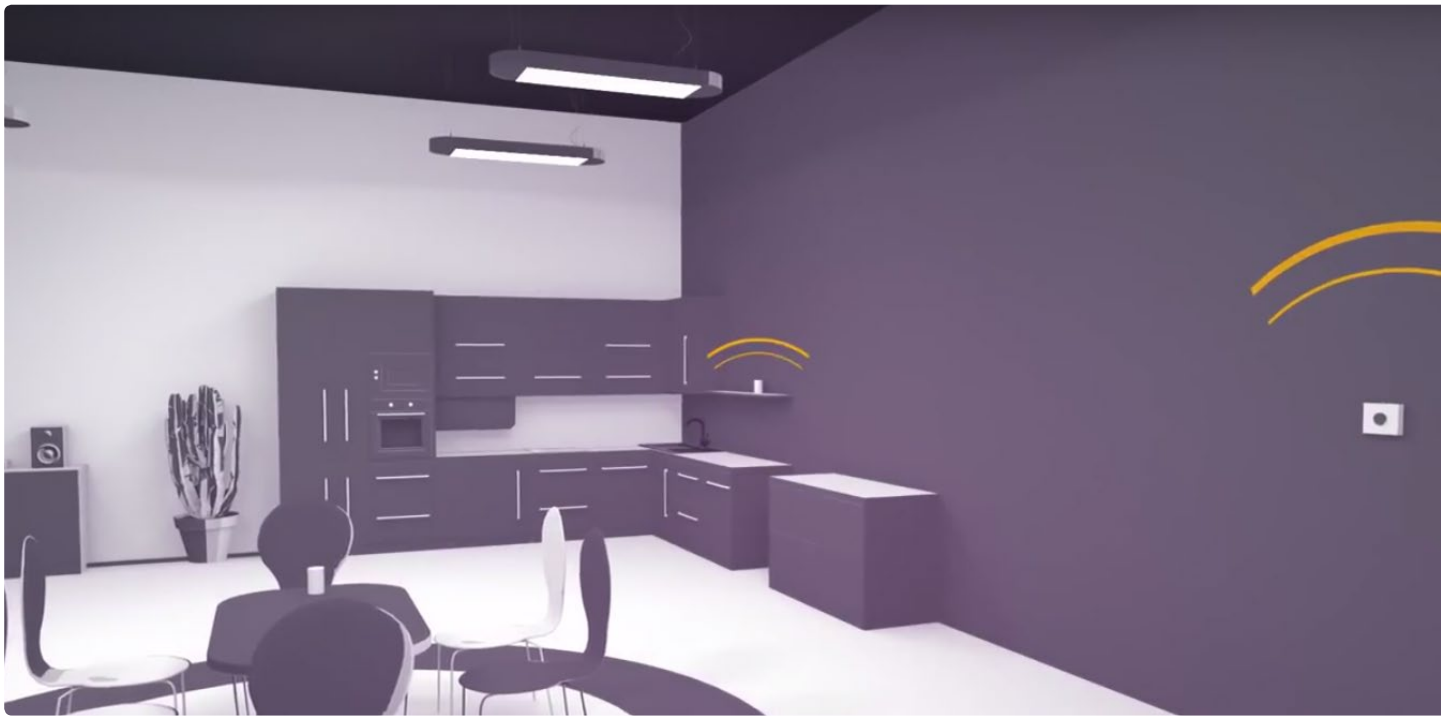
Der smarte Einbrecher kommt auf digitalen Wegen und hat noch weitere Möglichkeiten. Viele Alarmanlagen sind über kleine Fernbedienungen steuerbar und können darüber deaktiviert werden. Wie leicht sich so manche Anlage von Unberechtigten abschalten lässt, haben Sicherheitsexperten bereits demonstriert. Mit einem simplen Sender-Empfänger-Modul, das in der Umgebung der Anlage platziert wird, werden die Steuerbefehle mitgeschnitten und können anschließend nach Belieben abgespielt werden. Replay-Angriff nennen Spezialisten das.

Eine Analyse des Computermagazins c‘t ergab, dass einige Alarmanlagen selbst aus größerer Distanz ausgetrickst werden können. Sie erlauben via Internet den Zugriff auf Protokoll- und Logdateien, E-Mail-Adressen oder Telefonnummern. Auch der Standort kann abgefragt werden. Kriminelle könnten dadurch die Gewohnheiten der Bewohnerinnen und Bewohner ausspionieren. In einigen Fällen könnten sie sogar die Anlage über das Internet abschalten, weil manche Modelle lediglich über ein Standardpasswort gesichert sind.

Viele solcher Alarmanlagen dienen auch als Schaltzentrale des vernetzten Zuhauses. Sicherheitslücken sind dadurch besonders heikel, da somit prinzipiell alles angegriffen werden kann, was mit der Anlage verbunden ist, beispielsweise Heizung, Strom oder Licht.

SMART HOME

Ein sogenanntes Smart Home besteht aus Apparaten und Hausgeräten, die mit Computerprogrammen arbeiten. Dazu gehören beispielsweise sprachgesteuerte Lampen und Heizungen, Saugroboter, die selbstständig die Wohnung reinigen, oder Sprachassistenten, die ihnen gestellte Fragen beantworten und Geräte steuern können.



Gekaperte Heimgeräte

Kriminelle interessieren sich auch aus einem anderen Grund für die vernetzten Geräte. Wenn sie mangelhaft gesichert sind, lassen sie sich leicht kapern und als Ausgangspunkt für Angriffe auf Dritte nutzen. So wurde Mitte 2016 das sogenannte Botnetz „Mirai“ entdeckt. Es bestand zu einem weiten Teil aus handelsüblichen DSL-Routern, Überwachungskameras und digitalen Videorekordern. Bei Botnetzen werden solche gekaperten Geräte zu einer Armada zusammengeschlossen, die beispielsweise Angriffe auf Webseiten oder andere technische Infrastrukturen ausführt.

Leider ist vorerst nicht zu erwarten, dass die hier geschilderten Sicherheitsprobleme vollständig verschwinden werden. Entsprechend umfangreich müssen die Sicherheitsvorkehrungen ausfallen. Auch die Bewohnerinnen und Bewohner eines vernetzten Zuhauses sollten sich darum kümmern.

SICHERHEITSLÜCKEN

Wenn vernetzte Geräte Mängel oder Sicherheitslücken haben, sollten Verbraucherinnen und Verbraucher ihre Rechte kennen. Doch in der Praxis ist es schwierig, diese auch durchzusetzen. Welche Handlungsmöglichkeiten es gibt und wo der Verbraucherschutz Verbesserungsbedarf sieht, schildert Julian Gallasch vom Bundesverband der Verbraucherzentralen im
→ **Interview auf annasleben.de.**

IMPRESSUM

Herausgeber

iRights e.V.
Projekt: ANNA – Das vernetzte Leben

Projektleitung: Philipp Otto, Gina Schad
Almstadtstr. 9/11
10119 Berlin

E-Mail: kontakt@annasleben.de
Telefon: +49 (0)30 89 37 01 03

→ www.annasleben.de

Autorinnen und Autoren dieses Dossiers: Eike Gräf, David Pachali, Christiane Schulzki-Haddouti, Uwe Sievers

Illustrationen: Óscar Valero, Fritz Gnad

Layout: Tiger Stangl

Das Projekt wird gefördert durch das Bundesministerium der Justiz und für Verbraucherschutz aufgrund eines Beschlusses des Deutschen Bundestages.

Über iRights e.V.

iRights e.V. ist ein gemeinnütziger Verein, der Informationen für Verbraucherinnen und Verbraucher zu Themen wie Urheberrecht, Datenschutz, Computersicherheit und Digitalisierung bereitstellt. Dafür betreiben wir die Informationsplattform iRights.info, Webangebote wie annasleben.de und veröffentlichen weitere Publikationen. Mit allen unseren Projekten wollen wir dazu beitragen, dass Nutzerinnen und Nutzer die Veränderungen, die die Digitalisierung mit sich bringt, besser verstehen und an der Entwicklung teilnehmen können.

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages