Apples HomePod – hier bei der Präsentation in Amerika – wird 2018 nach Deutschland kommen. Google war etwas schneller: Der smarte Lautsprecher Home ist hierzulande schon seit August erhältlich. Aber: Mehr Vernetzung heißt auch mehr Überwachung. Und mehr potenzielle Sicherheitslücken.

FOTO: PA/AP PHOTO

Die smarten Mitwisser

Sprachassistenten und vernetzte Geräte erleichtern den Alltag und bieten auch Medien neue Plattformen. Doch was wissen sie über uns?

von Sonja Peteranderl

Nachrichten sind bald überall. Smarte Autos lesen News vor, Kühlschränke geben Kochtipps, und der Badezimmerspiegel informiert über die Wettervorhersage. Wir vernetzen uns und unsere Welt. Eine zentrale Rolle spielen dabei sprachbasierte Helfer, wie sie Apple, Amazon und Google derzeit anbieten. Sie spielen Musik, suchen Nachrichten, koordinieren Termine, erledigen Einkäufe und managen andere vernetzte Haushaltsgeräte. „Sprachbefehle haben das Potenzial, bisher fragmentierte On-Demand-Erfahrungen zu verlinken, die mit vernetzten Autos, Smart Homes und Voice Assistenten auftauchen", so Francesco Marconi, Digitalstratege bei AP und Mitautor der Studie *The Future of Augmented Journalism*.

Auch deutsche Medien haben angefangen, mit sprachbasierten Oberflächen wie Amazons Alexa zu experimentieren, um Info-Angebote zu personalisieren und auf unterschiedliche Umgebungen zuzuschneiden (siehe *journalist* 05/2017). Und je vernetzter die Geräte werden, umso mehr Daten werden generiert. Der Marktforschungsgesellschaft Gartner zufolge werden rund um die Welt etwa 8,4 Milliarden smarte Geräte benutzt. Amazon veröffentlicht zwar keine Verkaufszahlen, aber Analysten von Morgan Stanley zufolge wurden allein in den USA bis Anfang Dezember 2016 elf Millionen Echos verkauft. Seit August ist Googles smarter Lautsprecher Home auch in Deutschland erhältlich, 2018 kommt noch Apples HomePod dazu.

Sprache wird das zentrale Steuerungsinstrument all dieser vernetzten Geräte. Je mehr die Helfer über Nutzer, deren Alltag, Interessen und Vorlieben wissen, desto hilfreicher sind sie. Doch werden sie damit auch zu riskanten Mitwissern? Was passiert mit den Daten?

Die Bundesdatenschutzbeauftragte Andrea Voßhoff warnt vor Assistenten wie Amazons Echo oder Google Home. „Intelligente Sprachassistenten, die ihre Umgebung ständig belauschen, sind aus Sicht des Datenschutzes kritisch zu bewerten", so Voßhoff. Bedenklich an der Speicherung von Sprachdateien in einer Cloud sei zudem, dass oft „nicht eindeutig erkennbar ist, wie und wo die aufgenommenen Daten verwendet und genutzt werden".

Problem: always on

Amazons Alexa und Apples Siri sind „always on". Allzeit bereit, um das Sprachkommando, das sie aktiviert, zu erfassen – wie „Alexa" oder „Hey Siri". In diesem Bereitschaftsmodus lausche das Mikrofon zwar kontinuierlich nach dem Aktivierungsbefehl, doch der Vorgang erfolge rein lokal, versichern die Konzerne. Es würden keine Mitschnitte der Umgebungsgeräusche übertragen. Erst auf Zuruf des Sprachkommandos werden die Stimmen der Nutzer aufgenommen, in eine Sound-Datei umgewandelt und per Cloud an die Server der Konzerne vermittelt, wo sie analysiert und verarbeitet werden, so dass eine Antwort oder Reaktion erfolgen kann.

„Man achtet beim Reden darauf, dass man auf Teufel komm raus nicht Alexa sagt, wenn man sie nicht aktivieren will", so der Datenjournalist Marco Maas, der mehrere Echos in seiner Wohnung stehen hat. Manche hat er auf andere Sperrwörter umgestellt, etwa „Computer". Dem *Time Magazin* zufolge soll Alexa künftig die Stimmen ihrer Besitzer erkennen, der Konzern arbeitet an der „Voice ID", so dass Kinder nicht einfach mit Alexa shoppen gehen oder fremde Stimmen das Gerät steuern können. In den USA hatten mehrere Echos im Januar 2017 selbstständig Puppenhäuser bestellt – weil ein TV-Sender über ein Mädchen berichtet hatte, das den smarten Lautsprecher fragt: „Alexa, kannst du Puppenhaus mit mir spielen und mir ein Puppenhaus besorgen?" Andere Echos fühlten sich angesprochen und bestellten automatisch Puppenhäuser – sofern Besitzer Onlinekäufe nicht deaktiviert oder passwortgeschützt hatten.

Ein Sicherheitsforscher hat vorgeführt, wie sich Amazons Echo in ein Abhörgerät verwandeln lässt – Angreifer müssen dafür vor Ort Zugriff auf das Gerät haben. Sprachassistenten lassen sich auch auf der Sound-Ebene manipulieren: Forscher der UC Berkeley und der Georgetown University konnten den Google-Assistenten austricksen, indem sie Sprachbefehle wie „Ok Google" so veränderten, dass menschliche Teilnehmer sie kaum wahrnehmen konnten – während der digitale Assistent die Befehle in 95 Prozent der Fälle verstand.

Im Alexa-Nutzerkonto können Nutzer nachvollziehen, welche Sprachbefehle übertragen wurden und einzelne oder alle Interaktionen löschen. Das könne allerdings „das Alexa-Erlebnis mindern", so Amazon – denn personalisierte Vorschläge kann die Software eben nur liefern, wenn sie genug Informationen über Nutzungsmuster besitzt.

Marco Maas sieht keinen Anlass, seine Interaktionen zu löschen. Alexa sei für ihn einfach ein intelligenter Lichtschalter. „Es werden die Sachen abgespeichert, die ich dort reinspreche und ich kann sie abhören“, sagt er. Alexa, mach das Licht aus! Alexa, wie ist mein Weg zur Arbeit? Alexa, was gibt es Neues an Nachrichten? „Du redest wie mit einem doofen Assistenten“, so Maas. „Die ganzen Horrorszenarien sind Unfug. Alexa hört nicht die ganze Zeit mit.“ Um Alexa so zu manipulieren, dass man die ganze Zeit mithören kann und Amazon nichts davon mitbekäme, bräuchte es schon einen „Megahack“ irgendeines Geheimdienstes.

Polizeit „verhört“ Echo

In Einzelfällen interessieren sich tatsächlich Ermittler für Daten, die smarte Geräte speichern. Nach einem Mordfall 2015 im US-Bundesstaat Arkansas wurden auch Daten von Amazons Echo ausgewertet. Amazon hatte sich erfolgreich gegen die Herausgabe der Daten gewehrt, allerdings stimmte der Verdächtige letztlich zu. Die Ermittler werteten auch einen vernetzten Wasserzähler aus, der frühmorgens einen hohen Wasserverbrauch registriert hatte – möglicherweise ein Hinweis auf eine nächtliche Putzaktion.

Im Rachen der Algorithmen

Die Auswertung der meisten Nutzerdaten ist eher kommerziell interessant. „Mit Dutzenden von täglichen Interaktionen wächst ein Archiv heran. Wenn man sich die Daten und Zeiten ansieht, etwa wie ich Alexa gefragt habe, John Lennon zu spielen, meiner Einkaufsliste Knoblauch hinzuzufügen, oder das Wetter in Baja California zu checken, wohin ich in den Urlaub fahren wollte“, beschreibt *Guardian*-Reporter Rory Carroll seinen Alexa-Test. „Banale Fußnoten des Alltags, aber potenziell lukratives Wissen für einen Handelsgiganten, der ‚Everything-Store‘ genannt wird.“ Ihm sei bewusst, dass Alexa seine Gedanken und Anfragen in die Cloud lade, wohl „in den Rachen von Amazons Algorithmen“ – aber sie sei eben nützlich.

Welche Algorithmen genau bei der Auswertung angewandt werden, bleibt unklar – oft auch, wie Drittanbieter die Daten weiterverwerten. Amazon weist darauf hin, dass das Unternehmen keinen Einfluss darauf habe, welche Daten von Drittfirmen gesammelt werden. Kunden sollten Dienste nur nutzen, wenn sie mit deren Datenschutzerklärungen einverstanden seien. Für Alexa sind jetzt schon mehr als 10.000 sogenannte Skills, Anwendungen, verfügbar. In Zukunft könnten vermehrt sprachbasierte Werbung und „Branded Skills“ ausgespielt werden – etwa Rezeptvorschläge von Lebensmittelkonzernen.

Je mehr Geräte vernetzt sind, desto exakter lassen sich Profile und Bewegungsdaten erstellen. Eine smarte Wohnung verrät viel über ihre Bewohner – wie die von Marco Maas, der in seiner Wohnung 130 vernetzte Geräte betreibt. „Durch Anhänger am Schlüsselbund weiß meine Wohnung, wer wann reinkommt und rausgeht“, sagt Maas. „In Kombination mit den Bewegungsmeldern könnte man auch herausfinden, wann diese Leute aufstehen und ins Bett gehen.“ Anbieter von Software und Hardware könnten so die Tagesrhythmen der Bewohner rekonstruieren.

Maas ist bewusst, dass sich sein Alltag auf Basis der Daten sehr genau nachvollziehen lässt. „Ich bin jemand, der sich beruflich viel mit Daten beschäftigt, von daher war es wenig überraschend – aber es war beeindruckend zu sehen, dass diese Daten tatsächlich so anfallen, wie man es erwartet und man daraus Profile erstellen kann.“

Dass die Firmen so viele persönliche Daten über ihn besitzen, stört ihn nicht. „Wir müssen diese Prozesse besser verstehen. Es führt kein Weg

FOTO: AMAZON

Wer hört neben Alexa noch zu? Amazons Echo ist „always on“. Das könnte ein Einfallstor für Angreifer sein.

daran vorbei, diese Daten zu erheben", sagt Marco Maas. Mit seinem Nachrichtenprojekt *xMinutes* will er Nutzern die richtige Nachricht zur richtigen Zeit anbieten, auf Basis von Wifi-Verbindung, GPS-Funktion, Leseverhalten und lokalen Interessen. „Wir müssen uns nur Gedanken darüber machen, auf welche Art wir Daten speichern und wie wir mit den Daten aus Sicht einer Privatsphäre umgehen", sagt Maas.

Rechtliche Rahmenbedingungen seien dafür mit der neuen Datenschutzgrundverordnung für die EU geschaffen worden: „Ich glaube, dass dieses Gesetz die Lösung ist, weil es zentrale Punkte aus Konsumentensicht berücksichtigt", so Maas. „Ich muss als Anbieter meinen Nutzer darüber informieren, welche Daten ich zu welchem Zweck erhebe, speichere und weitergebe. Ich kann keine AGB mit einem Häkchen mehr zeigen, sondern muss künftig explizit über jeden einzelnen Schritt informieren."

Wer sorgt für Updates?

Aber auch Hackerangriffe könnten die Privatsphäre im vernetzten Zuhause gefährden. Kein Gerät ist völlig sicher vor Attacken – die Frage ist eher, wie schnell Sicherheitslücken entdeckt und behoben werden können. „Aus der Datensicherheitsperspektive ist ein Amazon Voice Assistant oder Google Voice AI extrem sicher, weil die Unternehmen viel Geld reinstecken, um sie sicher zu halten", sagt Jan-Peter Kleinhans, Leiter des Projekts IT-Sicherheit bei der Stiftung Neue Verantwortung (SNV). „Und dadurch, dass sie unter voller Kontrolle eines großen Unternehmens sind, kann Amazon etwa, wenn es will, auf einen Schlag auf alle Echo-Geräte ein Update spielen, das heißt alle Geräte installieren das automatisch." Im Idealfall werden so Sicherheitslücken schnell geschlossen, nachdem sie entdeckt worden sind. Das sei ein absoluter Sonderfall, meint Kleinhans.

Bei den meisten vernetzten Geräten sind verschiedene Soft- und Hardwarehersteller sowie Zwischenhändler beteiligt – so dass sich am Ende kaum jemand verantwortlich fühlt oder kein Unternehmen Kosten und Aufwand tragen will. „Ich habe meistens einen asiatischen Hardwarehersteller, der das Produkt herstellt, der verkauft es dann weiter an alle möglichen Unternehmen, die vielleicht das Gehäuse oder die Benutzeroberfläche ein bisschen ändern, da ihren Sticker draufmachen, und es dann unter ihrem Namen an den Endkunden verkaufen", erklärt Kleinhans. „Wenn in so einem Gerät eine Sicherheitslücke gefunden wird, selbst wenn der eigentliche Hersteller diese Sicherheitslücke behebt, hat er keinerlei Kontrolle darüber, wie die Unternehmen, die das Produkt an den Endkunden verkaufen, dieses Update weitergeben."

So wie bei Android: Google bringt zwar monatlich Sicherheitsupdates heraus, aber Samsung entscheidet darüber, an welche Geräte das Sicherheitsupdate ausgespielt wird – meistens werden nur die teuren Modelle einigermaßen regelmäßig mit Sicherheitsupdates versorgt. „Im Android-Ökosystem sehen wir also ganz gut, was im größeren IoT-Ökosystem auf uns zukommt: Geräte, die niemals upgedatet werden", warnt Kleinhans. Er sieht vor allem die Gesetzgeber in der Pflicht – die Einhaltung von IT-Sicherheitsstandards müsse die Voraussetzung dafür sein, smarte Geräte zu verkaufen.

Eine Reihe von Skandalen zeigt, dass Handlungsbedarf besteht: Mirai-IoT-Botnetze kaperten etwa Hunderttausende Geräte wie Kameras oder digitale Videorekorder, um DDoS-Angriffe (DDoS= Distributed Denial of Service) zu fahren. Sicherheitsforscher haben 2016 eine Ransomware für smarte Thermostate präsentiert, die Geräte gegen Lösegeldforderung blockieren kann. Datenleaks bei smarten Sextoys, aber auch Kinderspielzeugen offenbarten ungewollte Einblicke ins Eigenheim.

Es bleibt das klassische Dilemma: Wer Komfort und Bequemlichkeit von individualisierten Angeboten nutzen möchte, bezahlt mit seinen Daten. ■

Sonja Peteranderl ist Redakteurin beim Wired Germany Magazin sowie Gründerin des BuzzingCitiesLabs und berichtet über Politik, Cyber & Crime.

FOTO: XMINUTES

FOTO: PRIVAT

FOTO: SNV

„Wir müssen Prozesse besser verstehen. Es führt kein Weg daran vorbei, diese Daten zu erheben", sagt Datenjournalist Marco Maas. Für Digitalstratege Francesco Marconi (m.) und IT-Experte Jan-Peter Kleinhans (u.) ist klar, dass die Vernetzung der Geräte immer weiter zunehmen wird.