Bild: © Fotolia.com/Viktor Gmyria

Intelligente Sprachsteuerung unter der Lupe

Alexa, wie sicher bist du?

Digitale Assistenten sind derzeit in aller Munde. Smart Home ist eine besonders zukunftsträchtige Branche. Vor allem Amazons Alexa, die seit Februar 2017 in Deutschland erhältlich ist, spielt hier eine besondere Rolle. Aber auch Google zieht seit August 2017 mit dem Google Home nach. Doch was ist Alexa eigentlich, was kann sie, wie funktioniert sie und wie sieht es mit der IT-Sicherheit und dem Datenschutz aus?

Alexa ist eigentlich der Alexa Voice Service (AVS)[1], ein cloudbasierter Dienst von Amazon, der Sprachsteuerung für verbundene IT-Geräte zur Verfügung stellt. Er wird vor allem im Amazon Echo und Amazon Echo Dot verwendet, kann aber prinzipiell von jedem IT-Gerät mit Mikrofon, Lautsprecher und Internetzugang benutzt werden.

Als digitale Assistentin soll Alexa dem Nutzer im Alltag helfen. Dazu kann sie zum Beispiel Musik oder Hörbücher abspielen, Wecker oder Timer stellen und Aufgaben- und Einkaufslisten sowie Kalender verwalten. Sie kann aber auch Fragen beantworten („Alexa, wie heißt die Hauptstadt von …?"), lokale Geschäfte und Restaurants finden („Alexa, welche Bäckereien sind in der Nähe?") oder Informationen zum Kinoprogramm in der Nähe ermitteln („Alexa, welche Filme laufen gerade?"). Da sie von Amazon ist, wird ein Amazon-Konto benötigt. Darüber kann sie zum Beispiel auf Amazon-Music und Audible zugreifen. Zudem kann über sie per Sprachsteuerung bei Amazon eingekauft werden.

Alexas Fähigkeiten lassen sich mit Anwendungen von Drittanbietern, sogenannten „Skills" erweitern. Es gibt unter anderem Skills für Wetterinformationen, Nachrichten, Spiele und Smart Home-Steuerung. Skills können über die Alexa-App aktiviert werden und sind dann auf allen mit dem Nutzerkonto verknüpften Alexa-fähigen IT-Geräten verfügbar. Die Alexa-App ist für iOS und Android im jeweiligen Store erhältlich und als Web-App unter alexa.amazon.de verfügbar. Über sie können die verknüpften Alexa-fähigen IT-Geräte und Skills konfiguriert und die Interaktionen mit Alexa nachverfolgt werden.

Wie funktioniert Alexa?

Mit Alexa wird per Sprache kommuniziert. Um sie zu aktivieren, muss der Nutzer ein Signalwort, standardmäßig „Alexa", sagen. Dieses Signalwort kann sich von Gerät zu Gerät unterscheiden. Es kann aber nicht frei gewählt werden, sondern muss aus einer Liste von vorkonfigurierten Wörtern bestimmt werden.[2] Manche IT-Geräte (zum Beispiel Fire TV) können Alexa auch nur per Knopfdruck aktivieren. Sind mehrere Alexa-fähige IT-Geräte in der Nähe, wählt Alexa das IT-Gerät aus, das dem Nutzer am nächsten ist.

Die Erkennung des Signalworts erfolgt lokal auf dem IT-Gerät.[3] Deshalb muss es ständig zuhören, damit es seinen Einsatz nicht verpasst. Alle Amazon Echo-Geräte verfügen aber über einen Mute-Knopf, der alle

Mikrofone deaktiviert.[4] Sobald das Signalwort erkannt wurde, wird ab einem Sekundenbruchteil vor dem Signalwort und alles danach in die Amazon-Cloud übertragen, dort verarbeitet und gespeichert und die entsprechenden Ergebnisse zurückgegeben.[5] Die eigentliche Spracherkennung und -verarbeitung erfolgt in der Amazon-Cloud. Dadurch kann Alexa ständig weiterentwickelt werden, ohne dass jedes IT-Gerät aktualisiert werden muss. Zudem wäre die komplett lokale Implementation der Sprachsteuerung nicht praktikabel.

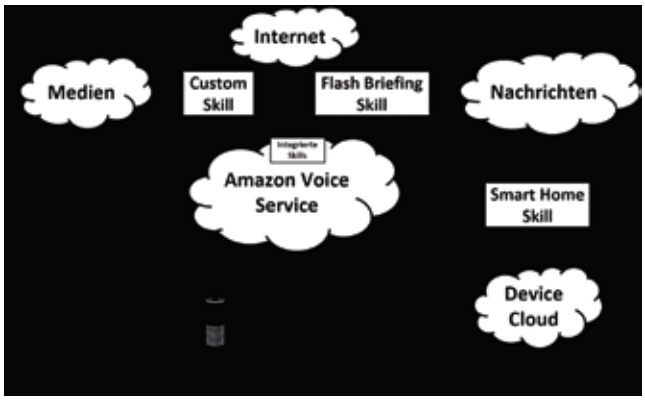

Abbildung 1: AVS Systemarchitektur

Bei der Sprachverarbeitung prüft Alexa, ob sie die Anfrage des Nutzers selber bearbeiten kann (integrierter Skill) oder ob der Nutzer implizit einen externen Skill angesprochen hat. Falls der Nutzer implizit einen externen Skill angesprochen hat, zerlegt Alexa die Anfrage in ein generalisiertes Format. Der Skill erhält lediglich textuelle Daten, keine Audiodaten. Falls dem Skill noch Informationen fehlen, kann er durch Alexa nachfragen lassen.

Im Grunde ist Alexa also ein cloudbasierter IT-Dienst von Amazon, der prinzipiell von jedem IT-Gerät mit Mikrofon, Lautsprecher und Internetzugang benutzt werden kann. Dazu müssen die Entwickler des IT-Gerätes lediglich die Alexa Voice Service API ansprechen.

Alexa und das Smart Home

Ein wichtiger Anwendungsfall von Alexa ist das Steuern der vernetzten IT-Geräte eines Smart Homes bzw. des Internet of Things (IoT). Dazu gibt es spezielle Skills, die Smart Home Skills. Wird ein solcher Skill benutzt, wird auf einen Dienst des Smart Home Skill-Anbieters zurückgegriffen.[6] Dies setzt voraus, dass der Skill-Anbieter vom Internet aus Zugriff auf das Smart Home-Gerät hat, das IT-Gerät also cloud-controlled ist. Dabei zerlegt Alexa die Anfrage in eine Aktion, zum Beispiel „anschalten" und einen Identifier, der das Gerät bezeichnet, das gesteuert werden soll. Diese Informationen werden zusammen mit Authentifikationsinformationen des Nutzers an den Smart Home Skill gesendet. Daraufhin kommuniziert dann der Smart Home Skill anhand der Authentifikationsinformationen mit der Device Cloud des Nutzers und löst dort die entsprechende Aktion aus.

Einige Smart Home-Geräte, zum Beispiel Philips Hue-Geräte mit einer Hue-Bridge oder Belkin Wemo-Geräte, können von manchen Alexa-fähigen IT-Geräten, zum Beispiel dem Amazon Echo, nativ erkannt und gesteuert werden. Die Erkennung kann über die App oder per Sprachbefehl initiiert werden. Daraufhin sucht das IT-Gerät im lokalen Netzwerk nach unterstützten Smart Home-Geräten.

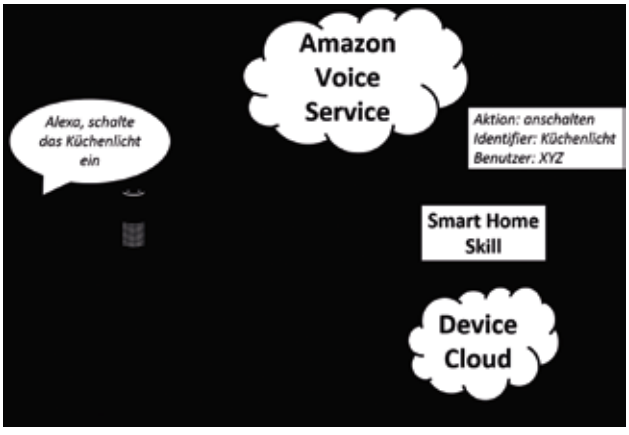

Abbildung 2: Ablauf eines Smart Home Skills

Viele weitere Smart Home-Geräte und Hubs implementieren die Philips hue API oder emulieren eine Hue-Bridge oder ein Wemo-Gerät, wodurch sie von Alexa zwar als Hue- bzw. Wemo-Geräte erkannt werden, sich aber dennoch kontrollieren lassen.

Alexa und die Sicherheit …

Ein wichtiger Punkt bei solchen vernetzten IT-Geräten ist die IT-Sicherheit: Nicht nur die IT-Sicherheit des IT-Gerätes an sich, sondern auch die IT-Sicherheit der Cloud und der Verbindung dorthin sowie die IT-Sicherheit der Skills.

… des Gerätes

Die IT-Sicherheit der IT-Geräte hängt dabei vom jeweiligen Hersteller ab. Daher werden im Folgenden die Echo-Geräte von Amazon betrachtet. Die Echo-Geräte benutzen Linux als Betriebssystem. Amazon bietet einen Teil des Source Codes der Firmwares der Echo-Geräte nach Firmware-Version geordnet als Archive zum Download an.[7] Diese Archive enthalten allerdings nur die Teile des Source Codes, deren Lizenzen eine Offenlegung des benutzten Source Codes bzw. der Modifizierungen des Source Codes fordern. Die von Amazon selbst geschriebenen Komponenten und vor allem die Integration der einzelnen Komponenten sind nicht enthalten.

Die IT-Geräte führen so wenig wie möglich lokal aus. So findet zum Beispiel die Konvertierung von Text zu Sprache in der Amazon-Cloud statt, sodass Angreifer keine Fehler in der Text-to-Speech-Software auf dem IT-Gerät ausnutzen können, um dieses zu übernehmen. Dadurch werden außerdem die Anforderungen an das IT-Gerät minimiert, sodass Alexa auf einer Vielzahl von IT-Geräten genutzt werden kann.

Bei den 2015er und 2016er Versionen des Amazon Echos ist es möglich, das IT-Gerät über Debug-Pins am Boden des IT-Gerätes von einer SD-Karte zu booten. Forschern von MWR InfoSecurity ist es dadurch gelungen, eine Reverse Shell (eine Art Trojaner) auf dem Amazon Echo zu installieren.[8] Zusätzlich installierten sie ein Skript auf dem Amazon Echo, das kontinuierlich den internen Audio-Buffer an einen externen Server streamt. Die Forscher von MWR InfoSecurity bestätigen aber, dass der Mute-Knopf die Mikrofone wirklich ausschaltet und dann keine Audiodaten mehr aufgenommen und in die Cloud gesendet werden. Für diesen Angriff muss der Angreifer jedoch physischen Zugang zum Amazon Echo haben und den Boden des Gerätes entfernen, um auf die Debug-Pins zugreifen zu können.

... der Cloud

Die Echo-Geräte benutzen derzeit ausschließlich TLS 1.2-Verbindungen und AVS erlaubt generell nur HTTPS-Verbindungen. Dadurch können nur die Endpunkte der Kommunikation, also das Alexa-fähige IT-Gerät und die Server von Amazon die Inhalte der Kommunikation einsehen und kein Dritter im selben Netzwerk oder auf dem Weg kann die Daten mitlesen oder verändern. Auch die Suche nach verfügbaren Updates und deren Herunterladen ist verschlüsselt.

Die Alexa-Apps für Android und iOS sind lediglich Browser und greifen auf dieselben Dateien und Daten wie die Alexa-Web-App zu. Daher kann Amazon neue Funktionen und Updates sehr schnell an alle Nutzer verteilen, da diese nicht die App aktualisieren müssen, sondern bei der nächsten Nutzung direkt die aktuellen Dateien und Daten benutzt werden. Sowohl die Dateien als auch die Daten werden per HTTPS heruntergeladen und die Kommunikation mit den Amazon-Servern zur Konfiguration der IT-Geräte und Skills läuft ebenfalls über HTTPS. Die IT-Sicherheit der Cloud-Dienste müsste durch eine Evaluierung/Zertifizierung kontrolliert und dokumentiert werden.

... der Skills

Für die IT-Sicherheit der Skills sind deren Entwickler zuständig, jedoch stellt Amazon einige Anforderungen an die bereitgestellte Schnittstelle. So müssen zum Beispiel alle Skill Endpoints nur über HTTPS angesprochen werden. Bei einem Smart Home Skill muss der Service zur Verknüpfung der Accounts auch über HTTPS angesprochen werden. Außerdem müssen Skills bei jeder Anfrage verifizieren, dass die Anfrage vom Alexa Voice Service kommt. Um den Entwicklern die Arbeit zu vereinfachen, bietet Amazon das Hosten von Skills auf Amazon Web Services (AWS) an. Wie die Skill Endpoints nach dem Erhalt der Anfrage weiter verfahren, ist deren Entwicklern überlassen. Da alle eingehenden Anfragen von Amazon signiert sind und verifiziert werden müssen, können Skills die meisten Angriffsversuche einfach ignorieren, wodurch ihre Angriffsfläche erheblich verringert wird.

Alexa und Datenschutz

Ein weiterer wichtiger Punkt bei digitalen Assistenten mit Sprachsteuerung ist der Datenschutz. Die größten Bedenken bezüglich Datenschutz bereitet die Tatsache, dass Alexa ständig zuhört. Dies ist jedoch für die Funktionsweise von Alexa unerlässlich und Paketmitschnitte zeigen, dass Amazons Aussage, dass nur in die Cloud gestreamt wird, sobald das Signalwort erkannt wurde, stimmt. Ein weiterer Beweis hierfür ist die Tatsache, dass das Amazon Echo noch auf das Signalwort reagiert, wenn es keine Internetverbindung hat, dann aber nur eine Fehlermeldung ausgibt. Im Standby sendet das Amazon Echo nur periodisch Pakete, die viel zu klein und viel zu selten für Datenübertragungen sind und als Keep-Alive dienen. Auch andere digitale Assistenten wie zum Beispiel Siri oder Ok Google, die in Smartphones integriert und daher ständige Begleiter sind, funktionieren so.

Der nächste Punkt betrifft die erfassten Daten. Das Streamen der Audiodaten in die Cloud erfolgt verschlüsselt, was bedeutet, dass kein Unbefugter sie mitlesen kann. In der Cloud werden diese Daten dann verarbeitet und für unbestimmte Zeit gespeichert. Zu den Daten gehören die aufgezeichnete Audiodatei, der erkannte Text, der Zeitpunkt und die Antwort von Alexa. Diese erfassten Daten können über die Alexa-App eingesehen bzw. angehört und auch gelöscht werden. Zudem kann hier ein Feedback gegeben werden, ob Alexa den Befehl richtig verstanden und ausgeführt hat. Auf www.amazon.de/mycd unter „Meine Geräte" können alle Sprachaufnahmen gleichzeitig gelöscht werden. Bloomberg und Wired berichten[9], dass diese Daten anonymisiert benutzt werden, um Alexas Verständnis von Dialekten und Umgangssprache zu verbessern. Leider gibt es derzeit keine Opt-out-Möglichkeit von dieser Verwendung und keine Möglichkeit, das Speichern in der Cloud generell zu deaktivieren.

Abbildung 3: „Alexa, mach die Tür auf"!

Skills erhalten nur von Alexa verarbeitete Daten, keine textuellen oder akustischen Rohdaten. Das bedeutet, dass ein Skill nur weiß, dass er angesprochen wurde und was der Nutzer von ihm möchte, aber nicht, was genau der Nutzer gesagt hat.

Hin und wieder kommt es vor, dass Alexa sich angesprochen fühlt, obwohl der Nutzer das nicht beabsichtigte. Hieran sind die hervorragenden Mikrofone und Spracherkennung und der Umstand, dass Alexa sich lieber ohne Grund angesprochen fühlt, als einen Befehl zu ignorieren, schuld. Echo-Geräte (Echo und Echo Dot) besitzen am oberen Rand einen LED-Ring, der über seine Farbe den aktuellen Zustand anzeigt. Zudem können die Geräte so eingestellt werden, dass sie Signaltöne abgeben, wenn sie sich angesprochen fühlen oder aufhören Audiodaten zu streamen.

Es ist aber auch möglich, Alexa zum Beispiel durch ein Fenster Befehle zu geben. So könnte ein Einbrecher zum Beispiel sich selbst die Türe öffnen oder Jalousien hochfahren lassen, wenn die Smart Home-Anwendungen entsprechend vorhanden sind.

Hier muss darauf geachtet werden, dass Alexa ausgeschaltet ist, wenn niemand zu Hause ist. Der Zustand des Mute-Knopfs der Echo-Geräte wird nach einem Neustart wieder auf den Wert davor gesetzt. Dadurch ist es nicht möglich, die Mikrofone von außen durch einen kurzen Stromausfall einzuschalten. Derzeit ist es nicht möglich, die Mikrofone per Sprachbefehl zu deaktivieren. An Echo-Geräten selbst kann nicht ohne Weiteres erkannt werden, ob es ausgeschaltet ist oder sich im Standby-Modus befindet. Dies ist nur zu erkennen, wenn die Power-LED im unteren Bereich über dem Stromanschluss betrachtet wird. Die Verbraucherzentrale NRW rät Besitzern solcher digitalen Assistenten mit Sprachsteuerung, Familienmitglieder und Gäste im Vorhinein auf das IT-Gerät hinzuweisen oder die Mikrofone zu deaktivieren.[10]

Forscher des Computer Science Department der Princeton Universität haben ein Amazon Echo und andere Smart Home-Geräte auf Bedenken hinsichtlich der Privatsphäre untersucht.[11] Dabei fanden sie heraus, dass sich auch bei verschlüsselten Verbindungen Rückschlüsse auf das IT-Gerät und das Nutzungsverhalten ziehen lassen. Da Alexa jedoch fast ausschließlich mit der Amazon-Cloud kommuniziert, kann aus den Verbindungen nur begrenzt abgelesen werden, welche Skills genutzt werden. Lediglich bei Skills, die Audiodateien nachladen, zum Beispiel einigen Nachrichten-Skills, wie „Tagesschau in 100 Sekunden", kann deren Nutzung erkannt werden.

Vor- und Nachteile von Alexa

Alexa ist als digitale persönliche Assistentin konzipiert. Aufgrund ihrer Entwicklung als cloudbasierter Dienst, der ständig weiterentwickelt und verbessert wird, und der präzisen Spracherkennung und -verarbeitung kann sie diese Aufgaben auch sehr gut erfüllen. Ihre Vielseitigkeit und vor allem ihre Erweiterbarkeit durch Skills sowie ihr Einsatz in Produkten von Drittanbietern sind ihre größten Vorteile.

Dabei sind die Anforderungen an die Skills und die Produkte der Drittanbieter einfach gehalten und die Schnittstellen gut dokumentiert, wodurch Skill- und Produktentwickler schnell und einfach neue Skills und Produkte für Alexa entwickeln können. Auch die Echo-Geräte sind schnell und vor allem einfach einzurichten. Zugleich ist Amazon auf den Schutz der Daten seiner Kunden bedacht und liefert den Skills nur die wirklich nötigen Daten über deren Nutzer. Durch die Integration ins Smart Home kann aus Alexa in Amazon Echo-Geräten eine zentrale Steuereinheit für das Smart Home werden, mit allen Vor- und Nachteilen.

Alexas Rolle als digitale persönliche Assistentin ist bisher leider auch ihr größter Nachteil. Wer keine Verwendung für einen persönlichen Assistenten hat, wird auch nicht viele Anwendungsfälle für Alexa finden.

Auch Personen, die viel Wert auf ihre Privatsphäre legen und den großen, datensammelnden Konzernen eher skeptisch gegenüberstehen, halten eher Abstand zu Alexa, da sie auf die Amazon-Cloud angewiesen ist und alle Befehle in der Cloud speichert. Zudem ist es am Anfang ungewohnt, mit Alexa zu reden und ihr Befehle zu geben. Anfänger versuchen meist, einfache, grobe Befehle zu geben, anstatt normal mit ihr zu reden, wobei sie natürliche Sprache besser versteht als vereinfachte.

Fazit

Alexa eignet sich hervorragend als digitale Assistentin. Sowohl ihre Spracherkennung als auch ihre Sprachverarbeitung sind sehr präzise und genau. Manchmal erkennt sie zwar einzelne Wörter nicht korrekt, leitet aber den korrekten Befehl durch den Kontext ab. Ihr Funktionsumfang und dadurch auch ihre Verbreitung werden in Zukunft weiter steigen. Dazu trägt auch bei, dass Alexa eigentlich nur eine API in der Cloud ist, wodurch andere Unternehmen und auch Privatpersonen ihre Produkte und IT-Geräte mit Alexa verbinden können.[12] Dadurch werden immer mehr Produkte mit Alexa kompatibel und können per Skill gesteuert werden, und immer mehr Hersteller integrieren Alex in ihre Produkte.[13]

Über die Nutzergruppen von Alexa und den Amazon Echo-Geräten lässt sich bisher nur spekulieren. Solche IT-Geräte sind noch vergleichsweise neu und viele Besitzer wollen einfach nur die Technik ausprobieren und untersuchen. Daher sind die Nutzergruppen derzeit breit gefächert, werden sich jedoch in Zukunft herauskristallisieren. So werden solche digitalen Assistenten zunehmend im Hotelwesen eingesetzt werden, da sie hier dem Zimmerservice oder der Rezeption Aufgaben abnehmen können.[14] Mit zunehmender Funktionalität und Anwendungsbereichen werden solche IT-Geräte auch in Zukunft weitere Nutzergruppen für sich erschließen können.

Das Amazon Echo ist seit Ende 2014 in den USA auf dem Markt und seit Februar 2017 in Deutschland erhältlich. Bisher hat Amazon selbst keine Verkaufszahlen bekanntgegeben, aber Marktforscher schätzen die Verkaufszahlen seit dem Verkaufsstart in den USA auf fast 11 Millionen Echo.[15] 2017 will Amazon über 10 Millionen Echo-Geräte verkaufen.[16]

Alexa und den Echo-Geräten ist anzumerken, dass die IT-Sicherheit dieser Produkte

bei ihrer Entwicklung eine große Rolle gespielt hat und auch weiterhin spielt. So ist die komplette Kommunikation der Echo-Geräte mit der Amazon-Cloud verschlüsselt und auch der Alexa Voice Service erzwingt HTTPS. Auch dürfen alle neuen Skills nur noch HTTPS unterstützen.

Der größte Kritikpunkt an Alexa und anderen digitalen Assistenten wie Siri, Cortana oder Google Now bzw. Google Assistant ist das dauerhafte Lauschen. Dies ist jedoch notwendig, da diese Assistenten sonst nicht erkennen können, wenn sie angesprochen werden. Beim Amazon Echo lassen sich die Mikrofone jedoch per Knopfdruck ausschalten und die Erkennung des Signalworts geschieht lokal auf dem IT-Gerät. Erst wenn das Signalwort erkannt wurde, werden Daten an Amazon gesendet.

Ein weiterer Kritikpunkt ist die Speicherung der Sprachdaten in der Amazon-Cloud. Alexa speichert jeden Befehl als Audiodatei mit erkanntem Text und Antwort von Alexa automatisch in der Amazon-Cloud, auch wenn sie den Befehl nicht verstanden hat oder ausführen konnte oder sie im Endeffekt gar nicht angesprochen wurde. Diese automatische Speicherung kann auch nicht vom Nutzer deaktiviert werden. Jedoch können alle Daten oder einzelne Datensätze im Nachhinein gelöscht werden. Auch ist für den Nutzer nicht direkt ersichtlich, was mit den über ihn gespeicherten Daten passiert. Amazon selbst sagt dazu, dass mit den Daten das Erlebnis des Nutzers sowie die Amazon-Dienste verbessert werden. Berichten zufolge gibt Amazon nur sehr begrenzt Daten von Alexa an Entwickler und Unternehmen heraus.[17] Zu diesen Daten gehören zum Beispiel der Wortlaut der Wörter und Sätze, die die Anfragen ausgelöst haben sowie die Anfragen an sich. Diese Daten sind für die Entwickler des Skills allerdings nur in Textform erhältlich, nicht als Audiodaten. Dadurch können sie zum Beispiel nicht benutzte Schlüsselwörter entfernen oder die Interaktion anderweitig optimieren.

Alles in allem sind Alexa und die Echo-Geräte vielversprechende Produkte, deren Fähigkeiten und Nachfrage in Zukunft stetig steigen wird und die die Entwicklung digitaler Assistenten vorantreiben. Wir sollten unsere Erfahrungen mit dieser neuen Technologie machen, damit wir Kompetenzen aufbauen, die uns helfen, die Vorteile zu nutzen und die Nachteile zu vermeiden. ■

---

[1] *https://developer.amazon.com/de/alexa-voice-service*

[2] *https://www.amazon.de/gp/help/customer/display.html?nodeId=201971890*

[3] *https://www.amazon.de/gp/help/customer/display.html?nodeId=201602230 -> Häufig gestellte Fragen zu Amazon Echo, Echo Plus und Echo Dot -> 1. Wie erkennen Amazon Echo, Echo Plus und Echo Dot das Aktivierungswort?*

[4] *https://www.amazon.de/gp/help/customer/display.html?nodeId=201602230 -> Häufig gestellte Fragen zu Amazon Echo, Echo Plus und Echo Dot -> 3. Kann ich das Mikrofon an Amazon Echo, Echo Plus und Echo Dot ausstellen?*

[5] *https://www.amazon.de/gp/help/customer/display.html?nodeId=201602230 -> Häufig gestellte Fragen zu Amazon Echo, Echo Plus und Echo Dot -> 2. Wie stelle ich fest, wann Amazon Echo, Echo Plus oder Echo Dot meine Stimme in die Cloud leiten?*

[6] *https://developer.amazon.com/de/docs/smarthome/understand-the-smart-home-skill-api.html*

[7] *https://www.amazon.com/gp/help/customer/display.html?nodeId=201626480*

[8] *https://labs.mwrinfosecurity.com/blog/alexa-are-you-listening*

[9] *https://www.bloomberg.com/news/articles/2016-12-13/why-google-microsoft-and-amazon-love-the-sound-of-your-voice und https://www.wired.com/2016/12/alexa-and-google-record-your-voice/*

[10] *https://www.verbraucherzentrale.nrw/amazon-echo#dierechteandererundmoeglichermissbrauch*

[11] *https://arxiv.org/abs/1705.06805*

[12] *Siehe zum Beispiel https://www.golem.de/news/eufy-genie-anker-bietet-guenstigen-klon-des-amazon-alexa-echo-dot-an-1708-129411.html, https://www.golem.de/news/senic-covi-smarte-tischlampe-laeuft-mit-alexa-1706-128500.html, https://www.golem.de/news/triby-mit-alexa-im-test-der-lautsprecher-der-mehr-kann-als-amazons-echo-1706-128161.html und https://www.golem.de/news/avs-device-sdk-amazon-bringt-alexa-auf-raspberry-pi-und-andere-boards-1708-129547.html*

[13] *Siehe zum Beispiel https://www.heise.de/mac-and-i/meldung/Tradfri-Ikeas-Lampensystem-soll-auf-Siri-Alexa-und-Google-Assistant-hoeren-3723154.html, https://www.heise.de/newsticker/meldung/Netgear-Nighthawk-X6S-Router-Modell-mit-drei-Funkmodulen-und-Sprachsteuerung-3784638.html und https://www.golem.de/news/spracheingabe-nuki-smart-lock-laesst-sich-mit-alexa-oeffnen-1704-127513.html*

[14] *Siehe zum Beispiel https://www.theverge.com/circuitbreaker/2016/12/14/13955878/wynn-las-vegas-amazon-echo-hotel-room-privacy und https://www.bloomberg.com/news/articles/2017-03-22/amazon-s-alexa-takes-its-fight-with-siri-to-marriott-hotel-rooms*

[15] *Siehe zum Beispiel https://de.nachrichten.yahoo.com/amazon-echo-dominiert-geschäft-schlauen-haushaltshilfen-usa-153943611--finance.html und http://www.augsburger-allgemeine.de/wirtschaft/Amazon-Echo-dominiert-Geschaeft-mit-schlauen-Haushaltshilfen-in-den-USA-id41400351.html*

[16] *http://www.digitimes.com/news/a20170601PD218.html*

[17] *Siehe zum Beispiel https://www.marketingdive.com/news/amazon-releases-some-alexa-data/435706/ und http://adage.com/article/datadriven-marketing/epsilon-scramble-alexa-data-amazon/307843/*

JAN-HENDRIK FRINTROP
studiert im Master Internet-Sicherheit am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit Amazons Alexa.

PROF. DR. NORBERT POHLMANN
ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.