

AUF DURCHZUG ODER GANZ OHR?
DATENSCHUTZ BEI AMAZON ECHO UND
GOOGLE HOME

Ein Hintergrundpapier zur technischen Untersuchung



MARKTWÄCHTER
DIGITALE WELT

Kurzuntersuchung der Verbraucherzentralen
März 2018

verbraucherzentrale

Herausgeber

Verbraucherzentrale NRW e.V.

Mintropstr. 27

40215 Düsseldorf

Tel. (0211) 3809 0

Fax. (0211) 3809 172

marktwaechter@verbraucherzentrale.nrw

Text: Dr. Ayten Öksüz, Miriam Rusch-Rodosthenous

Stand: März 2018

© Verbraucherzentrale NRW e.V.

AUF DURCHZUG ODER GANZ OHR? DATENSCHUTZ BEI AMAZON ECHO UND GOOGLE HOME

EIN HINTERGRUNDPAPIER ZUR TECHNISCHEN UNTERSUCHUNG

1. Problemdarstellung

Hintergrund. Digitale Sprachassistenten halten Einzug in deutsche Haushalte. Über Sprachbefehle können Nutzer Informationen aus dem Internet beziehen, ihren Alltag organisieren (z. B. Erstellen von Einkaufslisten) oder den Assistenten für die intelligente Haussteuerung einsetzen¹ (z. B. Dimmen von Lichtern).

Für den Heimgebrauch sind digitale Sprachassistenten als Software nicht mehr nur in Smartphones, Tablets oder PCs zu finden, sondern werden zunehmend in gesonderter Hardware – meist mit Mikrofonen ausgestattete Lautsprecher – angeboten (sog. smarte Lautsprecher). Erster Anbieter von smarten Lautsprechern auf dem deutschen Markt war *Amazon* mit Amazon Echo und dem dazugehörigen Sprachassistenten Alexa.² *Google* folgte Anfang August 2017 mit seinem smarten Lautsprecher Google Home und dem dazugehörigen Sprachservice Google Assistant.³ Seitdem bilden die beiden Unternehmen ein marktbeherrschendes Duopol für smarte Lautsprecher.⁴ So zeigt eine Studie des US-Beratungsunternehmens *Strategy Analytics: Amazon* und *Google* beherrschen aktuell zusammen über 90 Prozent des weltweiten Marktes für smarte Lautsprecher.⁵

Immer mehr Technologie-Unternehmen ziehen nach und wollen in den Markt der smarten Lautsprecher einsteigen (siehe Tabelle 1). Dafür nutzen viele der Unternehmen die Dienste von *Amazon* oder *Google*, indem sie den digitalen Sprachassistenten von einem der beiden Anbieter in die hauseigenen Lautsprecher verbauen (z. B. ist im Sonos One von *Sonos* Alexa integriert). Andere wiederum setzen auf ihre eigenen digitalen Sprachassistenten wie beispielsweise *Apple* mit seinem Sprachassistenten Siri.

¹ Bundesverband Digitale Wirtschaft (2017).

² Pakalski (2017).

³ Bager (2017).

⁴ Z. B. Strategy Analytics (2017); Strathmann (2018).

⁵ Strategy Analytics (2017).

Entwickler (Sprachassistent)	Sprachassistent (Software)	Verbaut im smarten Lautsprecher (Hardware)	Hersteller (Smarter Lautsprecher)	in D erhältlich
Amazon	Alexa	Amazon Echo, Echo Dot, Echo Plus, Echo Spot, Echo Show	Amazon	✓
		Lenovo Smart Assistant	Lenovo	X
		Sonos One	Sonos	✓
		Ultimate Ears Blast, Ultimate Ears Megablast	Ultimate	✓
		Onkyo P3	Onkyo	✓
		Allure	Harman Kardon	✓
		Medion Life P61110	Medion	✓
		[...]		
Apple	Siri	Homepod	Apple	X
Blackberry	Blackberry Assistant!	-	-	-
Google	Google Assistant	Google Home, Google Mini	Google	✓
		Sony-LF-S50G	Sony	✓
		JBL Link10, JBL Link20, JBL Link300, JBL Link500	JBL	✓
		Tichome Mini	Mobvoi	X
		Onkyo G3	Onkyo	✓
	[...]			
	Google Now	-	-	-
IBM	Watson	-	-	-
Lenovo	CAVA	-	-	-
Microsoft	Cortana	Invoke	Harman Kardon	X
Samsung	Bixby	Vega*	Samsung	X
	SVoice	-	-	-

Tabelle 1. Marktüberblick digitale Sprachassistenten und smarte Lautsprecher (eigene Recherche⁶)

Datenschutz und Datensicherheit. Digitale Sprachassistenten, wie sie in smarten Lautsprechern verbaut sind, lösen bei Verbrauchern die Sorge aus, durch die smarten Alltagshelfer abgehört zu werden. Das zeigen

⁶ Recherchezeitraum: 25.01.-05.03.2018; * Vega ist Medienberichten zufolge in Planung, aber noch nicht auf dem Markt erhältlich. Die Tabelle erhebt keinen Anspruch auf Vollständigkeit.

Verbraucherbeschwerden, die über die Beratungsstellen der Verbraucherzentralen eingegangen sind. Daher veröffentlichte der „Marktwächter Digitale Welt“ der Verbraucherzentrale NRW im Dezember 2017 einen Reaktions-Check⁷ zu Alexa – dem digitalen Sprachassistenten von *Amazon*. Dabei ging es um die Frage, inwieweit durch fehlerhafte Spracherkennung versehentliche Sprachaufzeichnungen und somit unerwünschte Datenübertragungen bei der Verwendung von Alexa möglich sind. Der Reaktions-Check hat gezeigt, dass bei der Nutzung von Amazon Echo Daten unbeabsichtigt in die Cloud, d. h. auf die Backend-Server von *Amazon*, übertragen werden könnten. Denn Alexa reagiert und zeichnet nicht nur auf, wenn das festgelegte Aktivierungswort genannt wird, sondern teilweise auch bei ähnlich klingenden Wörtern. Dadurch könnte *Amazon* als der Anbieter von Amazon Echo Einblick in die Privatsphäre erhalten, ohne dass der Nutzer dies möchte – unter Umständen bemerkt er dies nicht einmal. Vor dem Hintergrund dieser Erkenntnisse wurde anschließend eine technische Prüfung durchgeführt.⁸ Diese sollte Aufschluss darüber geben, unter welchen Bedingungen bei der Nutzung von digitalen Sprachassistenten Daten in die Cloud beziehungsweise an die Backend-Server der Anbieter gesendet werden. Darüber hinaus wurde untersucht, an welche Parteien die bei der Nutzung der Sprachassistentensysteme erzeugten Daten gesendet werden und wie sicher die Daten bei der Übermittlung vor Zugriff und Modifikation durch unbefugte Dritte sind.⁹

2. Testkonzept

Auswahl des Prüfgegenstands. Zum Zeitpunkt der technischen Prüfung (November/Dezember 2017) waren Amazon Echo und Google Home die einzigen für den Heimgebrauch auf dem deutschen Markt verfügbaren smarten Lautsprecher. Darüber hinaus sind *Amazon* (Alexa) und *Google* (Google Assistant) Marktführer für diese Produktgruppe¹⁰ und viele smarte Lautsprecher anderer Hersteller sind mit einer der beiden Sprachassistenten – Alexa oder Google Assistant – ausgestattet.¹¹ Daher wurden Amazon Echo mit dem Sprachassistenten Alexa und Google Home mit dem Sprachassistenten Google Assistant als Gegenstand der Untersuchung ausgewählt.

Prüfpunkte. Beide digitalen Sprachassistentensysteme wurden hinsichtlich der folgenden drei Aspekte untersucht:

⁷ Moll, R. und Rusch-Rodosthenous, M. (2017): Amazon Alexa: Wann ist der Sprachassistent Ganz Ohr? Ein Reaktions-Check, <https://ssl.marktwaechter.de/pressemeldung/reaktions-check-alexa-reagiert-nicht-nur-aufs-signalwort>.

⁸ Die technische Prüfung wurde von der TÜV Informationstechnik GmbH im Auftrag des Marktwächters Digitale Welt der Verbraucherzentrale NRW durchgeführt (Prüfzeitraum: 13. November – 22. Dezember 2017).

⁹ Der Fokus lag hierbei also auf der Analyse der Transportsicherheit.

¹⁰ Strategy Analytics (2017).

¹¹ Siehe hierzu auch Tabelle 1.

- 1) **Datensendungsverhalten:** Unter welchen Bedingungen erfolgt ein ausgehender Datenverkehr bei der Geräte- und App-Nutzung von Amazon Echo und Google Home?
- 2) **Kommunikationspartner:** An welche Parteien bzw. Kommunikationspartner¹² werden die bei der Nutzung der Sprachassistenzsysteme Amazon Echo und Google Home erzeugten Daten gesendet?
- 3) **Datensicherheit:** Welches Sicherheitsniveau weist das Ecosystem¹³ der Sprachassistenzsysteme auf?

Weitere Informationen zu den Zielsetzungen und zum detaillierten Testkonzept können dem Anhang entnommen werden.

3. Ergebnisse der technischen Untersuchung

1) Datensendungsverhalten

Google Assistant ist ebenfalls – wie bereits der Marktwächter-Reaktions-Check für Amazon Alexa gezeigt hat – anfällig für eine unbeabsichtigte Aktivierung der Datenübertragung. So reagierte der Sprachassistent von Google nicht nur auf das vordefinierte Aktivierungswort „Ok Google“ bzw. „Hey Google“, sondern beispielsweise auch auf die Wörter „Ok Kuchen“ und „Ok Du“ sowie auf die starke Abwandlung „Ok, gucken wir mal“. Auch reagierte der Sprachassistent auf Wortkombinationen, die im alltäglichen Sprachgebrauch häufig vorkommen wie „Ok, gut“.¹⁴

Darüber hinaus konnten die Ergebnisse aus dem kürzlich veröffentlichten Marktwächter-Reaktions-Check bestätigt werden: Alexa hat auch im Rahmen der technischen Prüfung auf Wörter reagiert, die dem Aktivierungswort ähneln. Dabei wurden bewusst Wörter gewählt, die nicht bereits Teil des Marktwächter-Reaktions-Checks waren. So reagiert Amazons Sprachassistent beispielsweise auch auf „Alexandra“ (für „Alexa“), „Gecko“ für („Echo“) und auch starke Abwandlungen wie „Ham wa schon“ (umgangssprachlich für „Haben wir schon“ – „Amazon“). Bei allen drei Testwörtern hat Alexa fälschlicherweise reagiert. Zudem konnte für Amazon Echo festgestellt werden, dass eine vermutlich zufällige Aktivierung der Sprachaufzeichnung sowie die Verarbeitung dieser – auch ohne Nennung des Aktivierungswortes oder eines ähnlich klingenden Wortes – stattfinden kann.¹⁵

Die Analyse des Datenverkehrs hat ergeben, dass sowohl bei Amazon Echo als auch bei Google Home zwischen den relevanten Komponenten innerhalb des Ecosystems (Hersteller-App, Sprachassistent und

¹² Mit Parteien bzw. Kommunikationspartner sind hier die involvierten Backend-Server von Google und Amazon sowie mögliche Drittanbieter-Server gemeint.

¹³ Ecosystem meint hier die Gesamtheit der relevanten Komponenten des Sprachassistenzsystems, d. h. Hersteller-App, Sprachassistent und Backend-Server; siehe auch Anhang, Abbildung 2.

¹⁴ Die getesteten Wörter bzw. Wortkombinationen sind hier exemplarisch aufgeführt. Für die Liste aller getesteten Wörter siehe Anhang, Tabelle 2.

¹⁵ Hierzu gab es laut technischem Gutachten eine zufällige Beobachtung, bei der Alexa Daten aufgezeichnet und an die Server des Anbieters übertragen hat, obwohl weder das Aktivierungswort noch ein dem Aktivierungswort ähnlich klingendes Wort genannt wurde. Alexa hat also bei bloßem Vorhandensein von Nebengeräuschen reagiert. Die beobachtete Fehlfunktion könnte bspw. auf einen Fehler in der Firmware, ein ähnlich klingendes Geräusch innerhalb der Fehlertoleranz oder die zugrundeliegende Erkennungsmethodik (Eigenschaft neuronaler Netze) zurück zu führen sein.

Backend-Server der Anbieter) stets – d. h. in allen Testszenarien¹⁶ – ein gewisses „Netzwerkrauschen“¹⁷ besteht. Es werden also auch Daten an die Backend-Server der Anbieter übertragen, obwohl das Mikrofon am Lautsprecher deaktiviert ist, sich das Gerät im empfangsbereiten Zustand (Standby-Modus) befindet oder das Aktivierungswort nicht genannt wurde. Dabei ist aufgefallen, dass sich das Datensendungsverhalten¹⁸ zwischen den Szenarien „bei deaktiviertem Mikrofon“ und „im Standby-Modus“ grundsätzlich nicht stark voneinander unterscheidet – lediglich die Kommunikationspartner variieren: So werden beispielsweise im Standby-Modus andere Server angesprochen als im Szenario „Mikrofon deaktiviert“.¹⁹ Hierbei werden neben den erwarteten Internetverbindungstests²⁰ auch verschlüsselt Daten übertragen. Aufgrund der vorhandenen TLS-Transportverschlüsselung, die über einen Man-in-the-Middle-Angriff²¹ innerhalb der WLAN-Infrastruktur nicht umgangen werden konnte, können allerdings keine Aussagen darüber getroffen werden, welche Daten genau an die Backend-Server der Anbieter übertragen werden.

2) Kommunikationspartner

Die technische Prüfung hat ergeben, dass die Datenkommunikation von den lokalen Komponenten des Sprachassistenzsystems (Hersteller-App und Sprachassistent) hauptsächlich zu den zentralen Internetdiensten der Anbieter erfolgt (d. h. Backend-Server von *Google* bzw. *Amazon*).²² Dabei handelt es sich größtenteils um Server, die für die Erbringung der Leistung beziehungsweise für die eigentliche Funktion der Sprachassistenzsysteme notwendig sind. Es werden aber auch Daten an Server übermittelt, um das Nutzungsverhalten zu analysieren und statistisch zu verarbeiten (bspw. www-google-analytics.l.google.com²³).²⁴ Die daraus gewonnenen Erkenntnisse können zum einen dafür genutzt werden, den Dienst (u.a. auch die Spracherkennung) zu verbessern, zum anderen aber auch ein domainübergreifendes Tracking²⁵ des Nutzers ermöglichen. Darüber hinaus konnte festgestellt werden, dass während der Inbetriebnahme von Google Home Daten an Server übermittelt wurden, die zur Auslieferung und Erfolgsmessung von Internetwerbung eingesetzt werden (sog. Adserver²⁶, wie z. B. ad.doubleclick.net²⁷). Es wäre also auch denkbar, dass bei der Nutzung von Google Home Daten dazu

¹⁶ Siehe Anhang, Prüfpunkt 1).

¹⁷ Das bedeutet, dass bei der Überwachung des Netzwerk-Traffics Datenverkehr festgestellt werden konnte.

¹⁸ Anzahl und Abfolge/zeitlicher Abstand der übertragenen Datenpakete über einen gewissen Zeitraum.

¹⁹ Sichtbar durch die bei der Analyse der Kommunikationspartner festgestellten Domains.

²⁰ Bei den Internetverbindungstests wird hauptsächlich geprüft, ob der Sprachassistent mit dem Internet bzw. den Servern des Anbieters verbunden ist.

²¹ Siehe hierzu auch den Punkt 3) Datensicherheit.

²² Das bedeutet, dass Drittanbieter-Server, zumindest was die direkte Kommunikation zwischen Hersteller-App bzw. Sprachassistenten und Backend Server betrifft, größtenteils nicht involviert sind. Das schließt aber nicht aus, dass Google oder Amazon Daten an Drittanbieter weiterleiten könnten.

²³ Domain von Google Analytics, ein Datenanalysewerkzeug von Google, mit dem ein umfassendes Benutzerprofil von Besuchern einer Webseite erstellt werden kann, vgl. https://www.google.com/intl/de_de/analytics/.

²⁴ Sichtbar durch die bei der Analyse der Kommunikationspartner festgestellten Domains.

²⁵ Nutzerdaten werden über mehrere Domains oder Subdomains hinweg für die Analyse aufgezeichnet und segmentiert, vgl. z. B. Tusche (2017).

²⁶ Für Definition eines Adservers vgl. z. B. Bundesverband Digitale Wirtschaft e.V. (2018).

²⁷ Domain von Doubleclick Ad Exchange, der Werbemarktplatz von Google zum Kauf und Verkauf von Werbung. Werbetreibende Drittanbieter können diesen Markt nutzen, um im Internet Gebote für Display-Werbung (eine Form der Bannerwerbung im Internet,

genutzt werden könnten, die über den *Google*-Dienst Doubleclick ausgelieferte Internet-Werbung zielgerichteter auf den Nutzer zuzuschneiden.

Auch *Amazon* hält sich die Möglichkeit offen, die Daten, die bei der Nutzung von Amazon Echo entstehen, für individualisierte Werbung einzusetzen: Denn bereits bei der Ersteinrichtung des Sprachassistenten (Erstellung des Benutzerkontos) muss man den Bestimmungen zu Cookies und Internet-Werbung zunächst zustimmen, um den Dienst überhaupt nutzen zu können (siehe Abbildung 1).

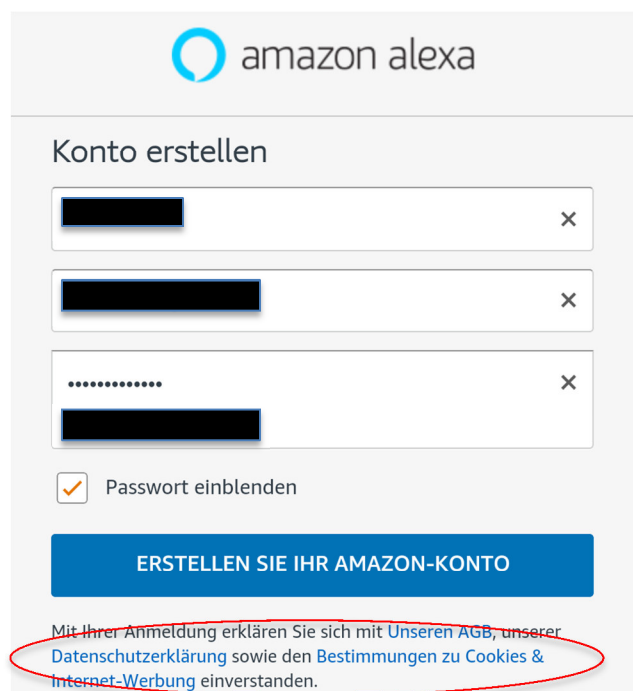


Abbildung 1. Kontoerstellung Amazon Echo

Neben den Backend-Servern der Anbieter (*Google* bzw. *Amazon*) sind bei einigen Nutzungsschritten auch weitere Server anderer Anbieter (sog. Drittanbieter-Server) involviert, die hauptsächlich beim Installationsprozess (z. B. Ausliefern eines Einführungsvideos²⁸) oder für die Funktion der Sprachassistenten notwendig sind (z. B. Beantwortung von Informationsabfragen²⁹).

Werden per Sprachbefehl Informationen abgerufen, unterscheidet sich Google Home teilweise von Amazon Echo, was das Einbeziehen von Drittanbieter-Servern betrifft: Bei Google Home werden für abgefragte Informationen wie beispielsweise Nachrichten von Informationsplattformen (z. B. heise.de) direkt als Ressourcen des Drittanbieters bezogen. Das bedeutet: Stellt der Endanwender eine Anfrage an Google Home, wie etwa „Ok Google, lies mir die letzten Nachrichten von heise.de vor“, werden die Server von

bei der grafische Werbemittel zu kommerziellen Zwecken auf Webseiten oder Apps auf Mobilfunkgeräten eingeblendet werden) abzugeben, vgl. z. B. Spiegel (2009); Ihlenfeld (2010).

²⁸ Hierbei wird das Einführungsvideo nicht von den Backend-Servern des Anbieters selbst sondern von einem Drittanbieter-Server aus abgespielt.

²⁹ Dieses konkrete Beispiel trifft nur auf Google zu, siehe nachfolgenden Absatz.

heise.de und eventuell weitere involvierte Drittserver zur Erfüllung dieses Dienstes direkt angefragt. Diese Drittanbieter erhalten dann ebenfalls bis zu einem gewissen Grad personenbezogene Daten wie beispielsweise die aktuelle IP-Adresse des Endanwenders, um den Dienst ausführen zu können. Im Gegensatz dazu laufen derartige Anfragen bei Amazon Echo zentral über *Amazon*. Somit kanalisiert *Amazon* diese Kommunikation über die Server von *Amazon*, sodass auch bei Informationsabfragen keine Drittanbieter direkt involviert sind. Das bedeutet: Stellt der Endanwender eine Anfrage an Alexa, wie etwa „Alexa, lies mir die letzten Nachrichten von heise.de vor“, werden erst die *Amazon*-Server kontaktiert. *Amazon* leitet dann die Anfrage an den Drittanbieter zur Beantwortung weiter und schickt wiederum das Ergebnis an den Sprachassistenten. Der Drittanbieter hat dann keine Informationen darüber, welcher Endanwender genau welche Anfragen gestellt hat.³⁰

Sobald mehr Daten zeitkritisch übertragen werden müssen, beispielsweise beim Streaming eines Radiosenders, werden die Daten bei beiden Plattformen direkt vom Drittanbieter abgerufen. Folglich werden auch hier zu einem gewissen Grad personenbezogene Daten wie beispielsweise die aktuelle IP-Adresse des Endanwenders offengelegt.

3) Datensicherheit

Das Datensicherheitsniveau der Sprachassistenzsysteme entspricht zum Zeitpunkt der Testdurchführung dem Stand der Technik und kann insgesamt als vergleichsweise hoch eingestuft werden. Der Großteil der Kommunikationsverbindungen zur Datenübertragung zwischen den Komponenten des Ecosystems (Hersteller-App, Sprachassistent und Backend-Server der Anbieter) sind mittels TLS³¹-Tunnel kryptografisch geschützt. Die Transportverschlüsselung konnte über einen Man-in-the-Middle-Angriff³² in der WLAN-Infrastruktur nicht umgangen werden, da der Kommunikationspartner nur vertrauenswürdige und keine selbstgestellten Zertifikate akzeptiert.³³

Insgesamt konnten hauptsächlich folgende Schwachstellen identifiziert werden: Bei der Kommunikation zwischen der Hersteller-App und dem Sprachassistenten werden Klartextprotokolle verwendet und somit Daten ohne Transportverschlüsselung übertragen. Bei Google Home handelt es sich hierbei um die SSID³⁴ und das Passwort des WLANs sowie um Daten, die bei der Durchführung bestimmter System-Aktionen wie „Trennung vom WLAN“, „Lautstärkenänderungen“ oder „Neustart des Assistenten“ ausgetauscht werden. Unabhängig davon, dass die Kommunikationsverbindung zwischen Hersteller-App und dem Sprachassistenten als solche nicht durch eine Transportverschlüsselung geschützt ist, wird hier – im

³⁰ Damit kann aber nicht ausgeschlossen werden, dass Amazon im Hintergrund Daten an Drittanbieter weiterleitet.

³¹ TLS steht für Transport Layer Security (ehem. bekannt unter der Bezeichnung Secure Sockets Layer (SSL)) und ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung, z. B. Oppliger (2009).

³² Hierbei wurde versucht, einen Man-in-the-Middle-Proxy in der WLAN-Infrastruktur zwischen die Kommunikationspartner zu positionieren, um den verschlüsselten Datenaustausch zu entschlüsseln, im Klartext mitzulesen und mit einem selbst generierten Zertifikat wieder verschlüsselt an das ursprüngliche Ziel weiterzuleiten.

³³ Ein Reverse Engineering (Kompromittieren des zugrundeliegenden Server-Zertifikats des Herstellers inklusive des geheim gehaltenen Schlüsselmaterials) wurde aufgrund des möglichen Verstoßes gegen bestehende Schutzrechte nicht durchgeführt.

³⁴ SSID steht für „Service Set Identifier“. Hierbei handelt es sich um den Namen von einzelnen WLAN-Netzwerken, z. B. Freist (2015); Klucznik (2018).

Gegensatz zur SSID – das WLAN-Passwort selbst durch eine Content-Verschlüsselung geschützt übertragen. Bei Amazon Echo werden lediglich die SSID und das Passwort des WLANs während der ersten Inbetriebnahme ohne Transportverschlüsselung übermittelt. Auch hier wird allerdings das WLAN-Passwort selbst verschlüsselt übertragen, während die SSID des WLANs ungeschützt übertragen wird. Ein potentieller Angreifer könnte durch die fehlende Transportverschlüsselung der Kommunikationsverbindung die gesendeten Informationen mitlesen. Mit dem Wissen über die Inhalte der Datenpakete³⁵ könnte dieser beispielsweise im Falle von Google Home die oben aufgeführten Aktionen ohne zusätzliche Authentifizierung durchführen (bspw. Trennen des Sprachassistenten vom aktiven WLAN). Hierfür muss sich der Angreifer in dem WLAN des Sprachassistenten befinden. Die Anbindung des Sprachassistenten an möglicherweise unsichere Netze, wie beispielsweise ein offenes Gäste-WLAN, könnte ein Sicherheitsrisiko für Nutzer darstellen.

4. Fazit

Die im Rahmen dieses Berichts durchgeführte technische Prüfung hat gezeigt: Google Assistant, genau wie Alexa, reagiert nicht nur auf das festgelegte Aktivierungswort. Auch ähnlich klingende Abweichungen vom konfigurierten Aktivierungswort können zur Aktivierung der Sprachassistenten ausreichen. Darüber hinaus werden zwischen den Komponenten innerhalb des Ecosystems der Sprachassistentensysteme (Hersteller-App, Sprachassistent, Backend-Server der Anbieter) stets Daten übertragen, auch wenn der Sprachassistent im empfangsbereiten Zustand oder das Mikrofon am Gerät deaktiviert ist. Da die Daten kryptografisch geschützt übertragen werden, konnten im Rahmen der technischen Prüfung keine Aussagen zu den übertragenen Datentypen getroffen werden. Die Analyse der Kommunikationspartner hat gezeigt, dass die Datenkommunikation größtenteils nur zu den eigenen Backend-Servern von *Amazon* bzw. *Google* erfolgt. Bei Google Home sind – im Gegensatz zu Amazon Echo – Drittanbieter-Server direkt involviert, wenn der Nutzer Informationen, wie etwa Nachrichten von Informationsplattformen, abfragt. Bei zeitkritischen und größeren Datenmengen (z. B. wenn der Nutzer möchte, dass ein bestimmter Radiosender abgespielt wird) werden die Inhalte bei beiden Sprachassistenten (Google Home und Amazon Echo) direkt von den Drittanbietern bezogen. Die bei den Kommunikationsverbindungen zwischen Hersteller-App beziehungsweise Sprachassistent und Backend-Server der Anbieter festgestellten Domains deuten zudem darauf hin, dass die Daten nicht nur für die reine Erfüllung des Dienstes genutzt werden: Google bindet den Adserver „ad.doubleclick.net“ ein und Amazon holt sich bei der App-Installation das Einverständnis der Nutzer zur Verwendung von Cookies und Internet-Werbung. So besteht bei beiden Anbietern die Möglichkeit, dass die gewonnenen Daten auch für Maßnahmen im Bereich Internet-Werbung genutzt werden könnten. Daher wäre es für Verbraucher wichtig zu wissen, welche Daten genau übermittelt werden und wohin, insbesondere, wenn der Sprachassistent nicht genutzt oder das Mikrofon deaktiviert wird. Positiv hervorzuheben ist, dass die digitalen Sprachassistentensysteme von *Amazon* und *Google* ein hohes Sicherheitsniveau aufweisen was die Transportsicherheit betrifft. Die Datenübertragung zwischen den

³⁵ Das bedeutet, wenn ein potentieller Angreifer in der Lage ist, die Verschlüsselung der Datenpakete selbst, bspw. des WLAN-Passworts, zu durchbrechen.

Komponenten des Ecosystems ist größtenteils mittels TLS-Tunnel geschützt. Allerdings wird bei der Inbetriebnahme von Google Home und Amazon Echo zwar das WLAN-Passwort selbst verschlüsselt, jedoch über eine ungeschützte Kommunikationsverbindung (d. h. ohne Transportverschlüsselung) übertragen. Daher könnte die Anbindung des Sprachassistenten etwa an ein offenes Gäste-WLAN unter Umständen ein Sicherheitsrisiko für Nutzer darstellen.

5. Quellenverzeichnis

- Bager, J. (2017).** Google Home in Deutschland: Eine ernstzunehmende Konkurrenz für Amazons Echo. Abgerufen von <https://www.heise.de/newsticker/meldung/Google-Home-in-Deutschland-Eine-ernstzunehmende-Konkurrenz-fuer-Amazons-Echo-3794806.html> (Stand 28.02.2018).
- Bundesverband Digitale Wirtschaft e.V. (2017).** Digital Trends – Umfrage zu digitalen Sprachassistenten. Abgerufen von https://www.bvdw.org/fileadmin/bvdw/upload/bilder/pressemitteilungen/BVDW_Digital_Trends_Sprachassistenten.pdf (Stand 06.02.2018).
- Bundesverband Digitale Wirtschaft e.V. (2018).** Glossar. Abgerufen von <https://www.bvdw.org/glossar/> (Stand 28.02.2018).
- Freist, R. (2015).** Sicherheit im WLAN - SSID senden oder nicht?. Abgerufen von <https://www.pcwelt.de/tipps/Sicherheit-im-WLAN-SSID-senden-oder-nicht-9601227.html> (Stand 28.02.2018).
- Ihlenfeld, J. (2010).** Adserver: Googles Doubleclick überarbeitet und kostenlos – Aus DART wird Doubleclick for Publishers. Abgerufen von <https://www.golem.de/1002/73310.html> (Stand 28.02.2018).
- Kluczniok, J. (2018).** WLAN: Was ist eine SSID? Begriff einfach erklärt. Abgerufen von <https://www.netzwelt.de/wlan/163450-wlan-ssid-begriff-einfach-erklart.html> (Stand 28.02.2018).
- Moll, R. und Rusch-Rodosthenous, M. (2017).** Amazon Alexa: Wann ist der Sprachassistent Ganz Ohr? Ein Reaktions-Check. Verbraucherzentrale NRW e.V. (Hrsg.). Abgerufen von <https://ssl.marktwaechter.de/pressemeldung/reaktions-check-alexa-reagiert-nicht-nur-auf-signalwort> (Stand 08.03.2018).
- Oppliger, R. (2009).** SSL and TLS Theory and Practice. Artech House, Norwood.
- Pakalski, I. (2017).** Amazon und Google setzen Standards. Abgerufen von <https://www.golem.de/news/smarte-lautsprecher-amazon-und-google-setzen-standards-1712-131618.html> (Stand 28.02.2018).
- Spiegel (2009).** Google versteigert Display-Werbung. Abgerufen von <https://www.spiegel.de/netzwelt/web/doubleclick-marktplatz-google-versteigert-display-werbung-a-649860.html> (Stand 28.02.2018).
- Strategy Analytics (2017).** Smart Speakers: Amazon and Google Share 92% of the Global Market in Q3 2017. Abgerufen von <https://www.strategyanalytics.com/strategy-analytics/news/strategy-analytics-press-releases/strategy-analytics-press-release/2017/12/14/smart-speakers-amazon-and-google-share-92-of-the-global-market-in-q3-2017-says-strategy-analytics#.WjuFVPhCUm> (Stand 06.02.2018).
- Strathmann, M. (2018).** „Alexa, spionierst du mich aus?“. Abgerufen von <https://www.sueddeutsche.de/digital/digitale-privatsphaere-alexa-spionierst-du-mich-aus-1.38427948> (Stand 04.02.2018).
- Tusche, C. (2017).** Das Google Analytics-Buch. dpunkt.verlag GmbH, Heidelberg.

Anhang

Testkonzept. Die technische Prüfung wurde von TÜV Informationstechnik GmbH im Auftrag des Marktwächters Digitale Welt im Zeitraum vom 13. November bis zum 22. Dezember 2017 durchgeführt. Die Ergebnisse wurden in Form von Videomitschnitten, Screenshots und Datenprotokoll-Exporten dokumentiert und in einem Prüfbericht aufbereitet.

Testszenario

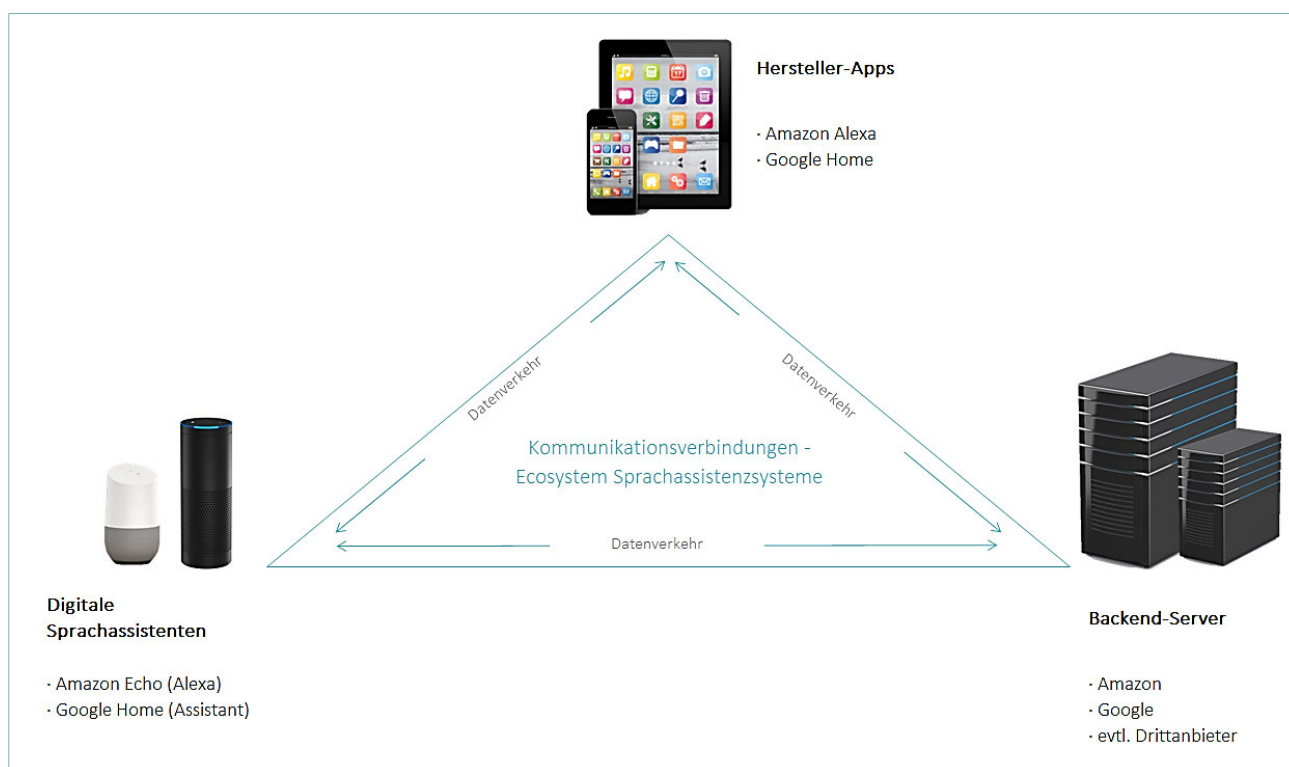


Abbildung 2. Ecosystem der Sprachassistentensysteme und relevante Kommunikationsverbindungen

Prüfpunkte

- 1) **Datensendungsverhalten.** Unter welchen Bedingungen erfolgt ein ausgehender Datenverkehr bei der Geräte- und App-Nutzung von Amazon Echo und Google Home?

Ziel. Die Analyse des Datensendungsverhaltens soll Aufschluss darüber geben, ob Daten nur dann an Anbieterserver übertragen werden, wenn das Aktivierungswort genannt wird (aktive Kommunikationsinitialisierung) oder aber auch, wenn das Aktivierungswort nicht genannt wird oder das Mikrofon deaktiviert ist (passive Kommunikationsinitialisierung)?

Hierzu wurde die Datenübertragung zwischen den unterschiedlichen Komponenten des Ecosystems (siehe Abbildung 2) für folgende Szenarien protokolliert:

- ohne Nennung des Aktivierungswortes
- bei und nach Nennung des Aktivierungswortes
- bei Nennung von Wörtern, die ähnlich wie das Aktivierungswort klingen
- bei deaktiviertem Mikrofon

- 2) **Kommunikationspartner.** An welche Parteien werden die bei der Nutzung der Sprachassistentensysteme Amazon Echo und Google Home erzeugten Daten gesendet?

Ziel. Beim Aspekt Kommunikationspartner wurde der Frage nachgegangen, ob Daten nur an die Backend-Server von *Amazon* bzw. *Google* übertragen werden, oder ob auch Drittanbieter-Server involviert sind? Zur Beantwortung der Frage wurden die Kommunikationspartner für folgende Szenarien identifiziert:

- bei Inbetriebnahme (Installation) des Sprachassistenzsystems
- bei abgeschlossener Installation und ohne Nennung des Aktivierungswortes
- bei abgeschlossener Installation und mit Nennung des Aktivierungswortes
- bei abgeschlossener Installation und mit deaktiviertem Mikrofon

3) Datensicherheit. Welches Sicherheitsniveau (Transportsicherheit) weist das Ecosystem der Sprachassistenzsysteme auf?

Ziel. Beim Aspekt Datensicherheit soll der Frage nachgegangen werden, wie sicher die Schnittstellen von Amazon Echo und Google Home vor Zugriff und Modifikation durch unbefugte Dritte sind. Der Fokus lag hier auf der Analyse der Transportsicherheit. Für die Beantwortung der Frage wurden folgende Aspekte geprüft:

- Verschlüsselung vorhanden bei der Übertragung von Daten zwischen:
 - Hersteller-App und Sprachassistent
 - Sprachassistent und Backend-Dienst der Anbieter
 - Hersteller-App und Backend-Dienst der Anbieter
- Für den Fall, dass Daten verschlüsselt übertragen werden:
 - Sicherheitsmerkmale der Transportverschlüsselung.
 - Umgehung der Verschlüsselung über einen Man-in-the-Middle-Angriff möglich?

Liste der getesteten Wörter

Technische Prüfung. Die in Tabelle 2 aufgeführten Wörter wurden unter Prüfpunkt 1) für das Szenario „Nennung von Wörtern, die ähnlich wie das Aktivierungswort klingen“ bis zu zehn Mal wiederholt. Tabelle 3 gibt einen Überblick über die im Rahmen des Marktwächter-Reaktions-Checks getesteten Wörter.

Google Home	Amazon Echo
Gugu	Alexa
Strudel	Alexandra
Bubu	Alex
Unfall	Lexa
Du	Echo
Uu	Gecko
Oo	Das Echo war schön laut
Kookle	Computer
Goo	Komm runter
Gugelhupf	Ham wa schon (ugs. für „Haben wir schon“)
Rubel	
Gurke	
Gut	
Goodie	
Gucken wir mal	
Kuchen	
Pudel	
Hodor	
U-Boot	

Tabelle 2. Im Rahmen der technischen Prüfung getestete Wörter.

Marktwächter-Reaktions-Check. Für Amazon Echo wurden im Rahmen des Marktwächter-Reaktions-Checks folgende Wörter getestet:

Alexa, Alexander, Alex, Alexis, Amazonas, Amazone, Klimazone, Echo, Echos, Tejo, Psycho, Ich schon, Micho, Computer, Computersystem, Supercomputer, Akuter Bronchitis, Komm Peter, Komm Uta, Router, Absoluter.