audatis
Datenschutz und Informationssicherheit | CONSULTING

Whitepaper

Datenschutz beim Einsatz von Sprachassistenten und Kameras im Gesundheitswesen

Zusammenfassung

Beschäftigte im Gesundheitswesen müssen die Klienten oftmals in Ihren Privatwohnungen betreuen. Sprachassistenten wie Alexa, Google Assistant oder Siri haben den Einzug in den Haushalt vieler Menschen geschafft, bieten teilweise Erleichterungen und Komfort im Alltag. Allerdings hören die smarten Helfer im Regelfall auch permanent zu und zeichnen auf. Des Weiteren können Wohnungen ebenfalls mit Kameras ausgestattet sein, beispielsweise in Form eines Babyphones mit Kamera und App-Zugriff. Das Thema Datenschutz und Privatsphäre ist dabei allerdings oft heikel. Pflegekräfte könnten bei der Arbeit aufgenommen und abgebildet werden, was in der Praxis zu Fragen führt.

Problemstellung

Was für die einen Menschen mehr Komfort im Alltag bedeutet, wirft bei anderen Nutzern Fragen nach dem Datenschutz und der Privatsphäre auf, weil bei intelligenten Lautsprechern die Mikrofone in der Regel immer angeschaltet sind. Die Mikrofone der Geräte müssen ständig angeschaltet sein, da das Aktivierungswort jederzeit vom Anwender genannt werden kann und die Sprachassistenten darauf reagieren sollen. In der Regel besteht in diesem „Wartemodus“ keine Verbindung zur Cloud und die Daten werden nicht an Server des Herstellers weitergeleitet. Erst mit bestimmten Aktivierungswörtern wie beispielsweise „Alexa“, „Hey Siri“ oder „Ok Google“ wird eine Verbindung zur Cloud aufgebaut und der darauffolgende Befehl oder die Frage an Server versendet. Problematisch ist, dass die Assistenten ähnliche Worte beispielsweise aus dem Fernseher versehentlich als Aktivierungswort verstehen können und daraufhin ungewollt eine Verbindung zur Cloud aufbauen. Laut Angaben der Hersteller sammeln diese die Aufnahmen und weitere Daten, um sie auszuwerten, z. B. für Marketingzwecke und zur Verbesserung der Dienste. Kritisch sind in diesem Zusammenhang auch Berichte, nach denen Gespräche von Anwendern oder anderen Personen unwissentlich gespeichert und die Aufnahme an die Hersteller weitergeleitet wurden. Des Weiteren besteht auch die Gefahr, dass sensible Daten nicht nur beim Hersteller selber, sondern auch ggfs. bei Drittanbietern auf Servern gespeichert werden, ohne dass die betroffenen Personen davon Kenntnis erlangen. Das kann in einer Vielzahl von Situationen oder bei der Kommunikation von sensiblen Daten Unbehagen bei den anwesenden Personen auslösen.

Sollten die Mitarbeitenden Bedenken äußern, sie würden durch die Geräte ausgespäht und aufgenommen, stellt sich die Frage: Wie geht man als Einrichtung damit um?

Lösungsansatz

Die rechtliche Frage, ob Privatpersonen in der eigenen Wohnung die Nutzung beispielsweise für den Zeitraum der Betreuung durch Pflegepersonal überhaupt untersagt bzw. eingeschränkt werden kann, soll an dieser Stelle nicht weiter diskutiert werden. Vielmehr befürworten und empfehlen wir eine kommunikative Lösung, sollten Mitarbeitende entsprechende Bedenken gegenüber den Geräten äußern.

1. Aufklärung der Mitarbeitenden über die Funktionsweise der smarten Assistenten.

2. Ohne Nennung des Aktivierungsbefehls besteht keine Verbindung zur Cloud des Herstellers.

3. Mikrofon abschalten: In modernen Assistenten ist mittlerweile eine Taste verbaut, mit der die Anwender das Mikrofon komplett abschalten können.

4. Kameras verdecken: Smarte Displays wie z.B. Amazons „Echo Show“ sind mit einem manuellen Schieber ausgestattet, der ein Verdecken der Kamera ermöglicht.

5. Die Anwender einbeziehen: Mit den (privaten) Anwendern sollte das Gespräch gesucht und auf die Bedenken der Mitarbeitenden hingewiesen werden.

6. Die Anwender wiederum können folgende Maßnahmen, auch zur Wahrung Ihrer eigenen Privatsphäre umsetzen:

- Besucher darüber informieren, dass z.B. ein Lautsprecherassistent eingeschaltet ist und ggfs. auf Wunsch abschalten.
- In den Einstellungen die Nutzung der Daten zur Verbesserung der Assistenten unterbinden.
- Intelligente Lautsprecher abstellen, wenn sensible Daten oder Themen besprochen werden.
- Die Hersteller bieten über die entsprechende App in der Regel an, dass die zuletzt getätigten Anfragen gelöscht werden können.
- Im Voraus über die jeweilige Datenschutzerklärung und -bestimmungen informieren.

7. Sollen Lautsprecherassistenten & Co. innerhalb einer Einrichtung eingesetzt werden, bietet sich der Abschluss einer entsprechenden Betriebsvereinbarung an. So können die Spielregeln für beide Seiten (Mitarbeitende und Einrichtungsleitung) transparent festgelegt werden.

Autor und Ansprechpartner

Sascha Knicker
Senior Consultant Datenschutz und Informationssicherheit

Schwerpunkte: Datenschutz, TISAX, ISO 27001

Mail: s.knicker@audatis.de
Fon: 05221 87292-07

XING **Linkedin**

Gerrit Schulte
Consultant Datenschutz

Schwerpunkte: Datenschutz, Vertragsrecht

Mail: g.schulte@audatis.de
Fon: 05221 87292-11

Haben Sie noch Fragen?

Wir haben versucht alle wichtigen Aspekte in unserem Whitepaper möglichst verständlich aufzubereiten.

Sollten Sie dennoch Fragen oder Beratungsbedarf haben, nehmen Sie gerne mit uns Kontakt auf.

Dieses Whitepaper wird Ihnen von der audatis Consulting GmbH zur Verfügung gestellt und darf gerne unverändert weitergegeben oder veröffentlicht werden.

Die audatis Consulting GmbH ist als Beratungsunternehmen auf die Bereiche Datenschutz und Informationssicherheit spezialisiert und betreut Kunden im In- und Ausland bereits seit 2011.

Neben der Stellung des externen Datenschutzbeauftragten begleiten und beraten wir Unternehmen, öffentliche Stellen und kirchliche Einrichtungen bei der Umsetzung des Datenschutzes, der Informationssicherheit und der Digitalisierung.

Als Teil der audatis Group hat die audatis Consulting GmbH Ihren Sitz im ostwestfälischen Herford und betreibt eine Niederlassung in Potsdam.

audatis Consulting GmbH
Luisenstr. 1
32052 Herford
Deutschland

Fon: 05221 872 92-0
Fax: 05221 872 92-49

Mail: info@audatis.de
Web: www.audatis.de