Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

BfDI

Datenschutz kompakt

18. Mai 2017

diesmal:
Sprachassistenten

Was sind digitale Sprachassistenten?

Mehr und mehr Firmen bieten digitale Sprachassistenten an als App, eingebaut in Smartphones, Tischlautsprechern oder Spielzeugen. Diese Programme können gesprochene Worte analysieren. Statt Befehle in ein Smartphone zu tippen, werden diese einfach ausgesprochen. Das soll den raschen Zugriff auf Informationen und eine deutlich leichtere Bedienung vieler technischer Geräte ermöglichen. Aber auch diese neue Technik ist nicht ohne Risiko. Dieses Infoblatt klärt hierüber auf und gibt Tipps zum datenschutzfreundlichen Umgang mit Sprachassistenten.

Wie funktionieren Sprachassistenten?

Sprachassistenten hören permanent die Umgebung ab und zeichnen Befehle über Mikrofone auf. Wird der Assistent durch ein Aktivierungswort gestartet, beginnt der eigentliche Verarbeitungsprozess. Die Befehle werden über das Internet an die Server des Herstellers gesendet und dort durch komplexe Software analysiert und verarbeitet. Das Ergebnis wird zurückübermittelt und als Sprachnachricht ausgegeben oder es löst eine Aktion aus. Nun kann ein konkreter Befehl erteilt werden, etwa ein Lied abzuspielen oder die Wettervorhersage vorzulesen. Meist werden weibliche Stimmen genutzt, da Nutzerinnen und Nutzer auf diese positiver reagieren. Wurden digitale Sprachassistenten bisher meist als Zusatzfunktion in Smartphones integriert, werden nun auch eigenständige Produkte vertrieben. Sie ähneln kleinen, unauffälligen Lautsprechern. Mit ihrer Hilfe sollen langfristig auch Haushaltsgeräte wie Heizung oder Kaffeemaschine per Sprachbefehl gesteuert werden können.

Welche datenschutzrechtlichen Risiken bestehen?

Sprachassistenten sind dauerhaft mit dem Internet verbunden und können von Angreifern abgehört und manipuliert werden. So kann die Aktivierung des Assistenten durch einen Schlüsselbegriff gestört werden. Anfällig sind selbst Systeme, die nur auf bestimmte Stimmen reagieren. Mit moderner Technik lassen sich aus gespeicherten Sprachbefehlen neue Befehle generieren. Da viele Sprachassistenten für bequemes Online-Shopping direkt auf Zahlungsdaten der Nutzerinnen und Nutzer zurückgreifen, können manipulierte Sprachbefehle auch zu finanziellen Verlusten führen.

Auch die Sicherheit der in der Cloud gespeicherten „gesprochenen“ Daten lässt sich nicht zu hundert Prozent garantieren. Nahezu wöchentlich werden neue Fallbeispiele für Hacks und Identitätsdiebstähle bekannt. Dabei müssen Sprachbefehle aus technischer Sicht nicht unbedingt in die Cloud übertragen und dort gespeichert werden. Die Daten sollten daher das Gerät nicht verlassen und nach kurzer Zeit (weniger als 15 Minuten) wieder überschrieben werden. Bedenklich an der Speicherung von Sprachdateien in einer Cloud ist auch, dass oft nicht eindeutig erkennbar ist, wie und wo die aufgenommenen Daten verwendet und genutzt werden. Fraglich ist auch, ob die von den Anbietern erhobenen Sprachdaten durch Nutzerinnen und Nutzer später wieder gelöscht werden können. Nutzer solcher Assistenzsysteme sollten daher genau darauf achten, wo und wie die vom Hersteller der Assistenten aufgezeichneten Daten gespeichert und verwendet werden.

Gespeicherte Sprachinformationen können mit Daten aus anderen Online-Quellen zu detaillierten Nutzerprofilen für Marketing und Marktforschung zusammengeführt werden. Da Sprachassistenten auf vielen Smartphones vorinstalliert sind und sich entweder gar nicht oder nur umständlich abschalten lassen, besteht auch die Möglichkeit, die Geräte jederzeit zu lokalisieren. Aus dem Einsatz eines Sprachassistenten ließe sich womöglich schließen, wann eine Wohnung leer steht oder wo ein Auto geparkt wird. Schließlich könnten im öffentlichen Raum über Sprachassistenten in Smartphones selbst Daten von unbeteiligten Dritten aufgezeichnet werden. Sind die Sprachassistenten in einen Haushalt integriert, speichern sie eventuell auch persönliche Informationen von Besuchern.

Datenschutzfreundlicher Umgang mit Sprachassistenten

Die Nutzung von Sprachassistenten kann hilfreich und komfortabel sein. Nutzerinnen und Nutzer müssen sich aber über die „Dauerüberwachung“ im Klaren sein und sich mit den damit verbundenen Nachteilen beschäftigen. Auch sollten sie Familie, Freunde und Besucher auf die Verwendung digitaler Sprachassistenten aufmerksam machen, damit diese Personen ihr Verhalten entsprechend anpassen können. Hersteller solcher Assistenzsysteme sollten transparent darüber aufklären, wie aufgezeichnete Daten auf inländischen oder ausländischen Cloud-Servern gespeichert werden, wie die Daten genutzt werden und ob sie gelöscht werden können.

Darüber hinaus sollten Hersteller darauf achten, Assistenzsysteme optimal zu schützen, sodass diese möglichst nicht gehackt werden können. Bereits bei der Entwicklung sind daher datenschutzrechtliche Vorgaben zu beachten („privacy by design“). Beim Verkauf der Geräte und der Software sollten Hersteller dann Datenschutzfunktionen vorab aktivieren („privacy by default“). Der integrierte Sprachassistent im Smartphone sollte nicht, wie derzeit regelmäßig der Fall, bei der erstmaligen Anwendung einer Smartphone-App ohne Zutun des Nutzers aktiviert werden. Zumindest sollten die Betreiber aktiv darauf hinweisen und die Nutzerinnen und Nutzer über die Verarbeitung persönlicher Daten durch Sprachassistenten aufklären.