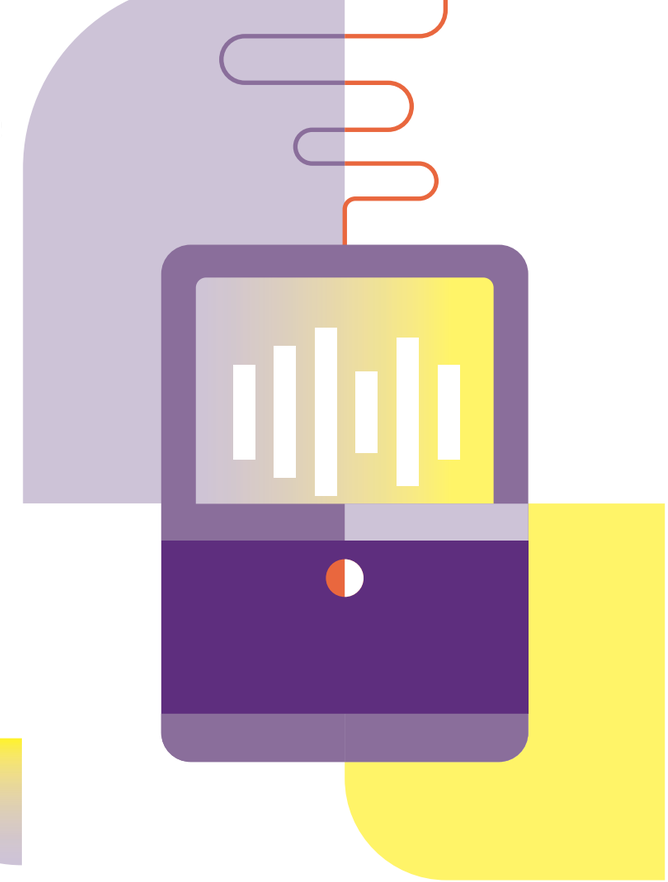
Basisschutz für Smart Speaker und Sprachassistenten – digitale Alltagsbegleiter sicher machen

Alexa, Siri oder Google – das sind nur drei Beispiele für Namen, auf die digitale Sprachassistenten hören. Sie schalten sich auf Zuruf ein und spielen zum Beispiel die gewünschte Musik ab. Dabei sind sie nicht nur auf Geräten wie etwa Smartphones installiert. Viele kennen die digitalen Begleiter vor allem von sogenannten Smart Speakern, also intelligenten Lautsprechern. Im Alltag können diese zahlreiche Informationen mithören, zum Beispiel über die Lebensgewohnheiten der Nutzerinnen und Nutzer. Ein Smart Speaker kann aber auch zum Einfallstor für Cyberkriminelle werden: Sie können versuchen, an die gespeicherten Daten zu gelangen oder in das gesamte Netzwerk einzugrinden. Umso wichtiger ist es, den Smart Speaker zu schützen.



Tipps für den sicheren Umgang mit Smart Speakern

Digitale Assistenten absichern

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

8 Tipps für einen sicheren Smart Speaker

Was im Smarthome passiert, soll auch im Smarthome bleiben. Mit den folgenden Basistipps machen Sie es Angreifenden schwer, auf Ihren Smart Speaker oder Sprachassistenten zuzugreifen.

1. Richten Sie ein seperates WLAN ein
2. Platzieren Sie Ihren Smart Speaker mit Bedacht
3. Erstellen Sie Sprachprofile für verschiedene Personen
4. Sichern Sie einzelne Funktionen mit einer PIN oder einem Passwort
5. Passen Sie die Datenschutzeinstellungen an
6. Prüfen Sie regelmäßig die gespeicherten Daten
7. Installieren Sie nur vertrauenswürdige Erweiterungen
8. Schalten Sie Ihren Smart Speaker auch mal aus

Schon gewusst?

Der Router ist das Herzstück der digitalen Vernetzung zu Hause

Kein sicheres Smarthome ohne sicheren Router. Als Knotenpunkt verbindet er Ihre Geräte sowohl mit dem Internet als auch untereinander.

Wenn es Angreifenden gelingt, in den Router einzudringen, können sie mitunter nicht nur auf das Gerät selbst zugreifen. Sie können auch verbundene Geräte unter ihre Kontrolle bringen. So gelangen sie beispielsweise an sensible Daten, die auf dem privaten Computer gespeichert sind. Erste Tipps, um Ihren Internetzugang abzusichern, finden Sie in diesem Wegweiser. Mehr Informationen rund um ein sicheres Heimnetzwerk bietet außerdem die Webseite des BSI.

Weitere Informationen

Mit digitalen Assistenten durch den Alltag

Smarthome – den Wohnraum sicher vernetzen

8 Tipps für ein sicheres Heimnetzwerk

Impressum

Herausgeber:
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 87, 53175 Bonn

Kontakt:
E-Mail: service-center@bsi.bund.de
Internet: www.bsi.bund.de
Service-Center: +49 (0) 800 274 1000

Artikelnummer:
BSI-IFB 23/152

1. Richten Sie ein separates WLAN ein

Erlangen Unbefugte Zugriff zu einem Gerät, können sie auch auf weitere Geräte im selben Netzwerk zugreifen.

Zu solch **sensiblen Geräten** zählen etwa der Computer, von dem aus Sie auf Ihr **Onlinebanking** zugreifen, Ihre **Homeoffice-Ausstattung** oder das Smartphone, auf dem **private Fotos** gespeichert sind. Um diese von Ihrem Smart Speaker und anderen Geräten Ihres Smarthomes zu trennen, richten Sie am besten ein **separates WLAN** (Gäste-WLAN) ein. In der Bedienungsanleitung Ihres Routers finden Sie eine Anleitung für das jeweilige Modell. Vergeben Sie ein **starkes Passwort**, machen Sie regelmäßig **Sicherheitsupdates** und schalten Sie die **Firewall** des Routers ein. Wenn möglich, aktivieren Sie auch die Sicherheitsprotokolle WPA2 oder WPA3.

2. Platzieren Sie Ihren Smart Speaker mit Bedacht

Jeder, der sich in der Nähe eines Smart Speakers aufhält, kann ihn ansprechen. Achten Sie darauf, dass Geräuschquellen ihn nicht unbefugt aktivieren können.

Steht ein Smart Speaker beispielsweise **neben einem geöffneten Fenster**, können Unbefugte ihn von außerhalb des Wohnbereichs steuern. Im schlimmsten Fall öffnen sie so zum Beispiel ein verbundenes smartes Türschloss. Informieren Sie sich daher über die **Reichweite Ihres Smart Speakers** und platzieren Sie ihn so, dass er nicht auf Befehle von außerhalb des Wohnraums reagiert. Beachten Sie auch **weitere Geräuschquellen**, etwa einen Anrufbeantworter oder einen Fernseher. Um das Risiko ganz auszuschalten, können Sie einige Smart Speaker zudem per Knopfdruck statt Zuruf aktivieren.

3. Erstellen Sie Sprachprofile für verschiedene Personen

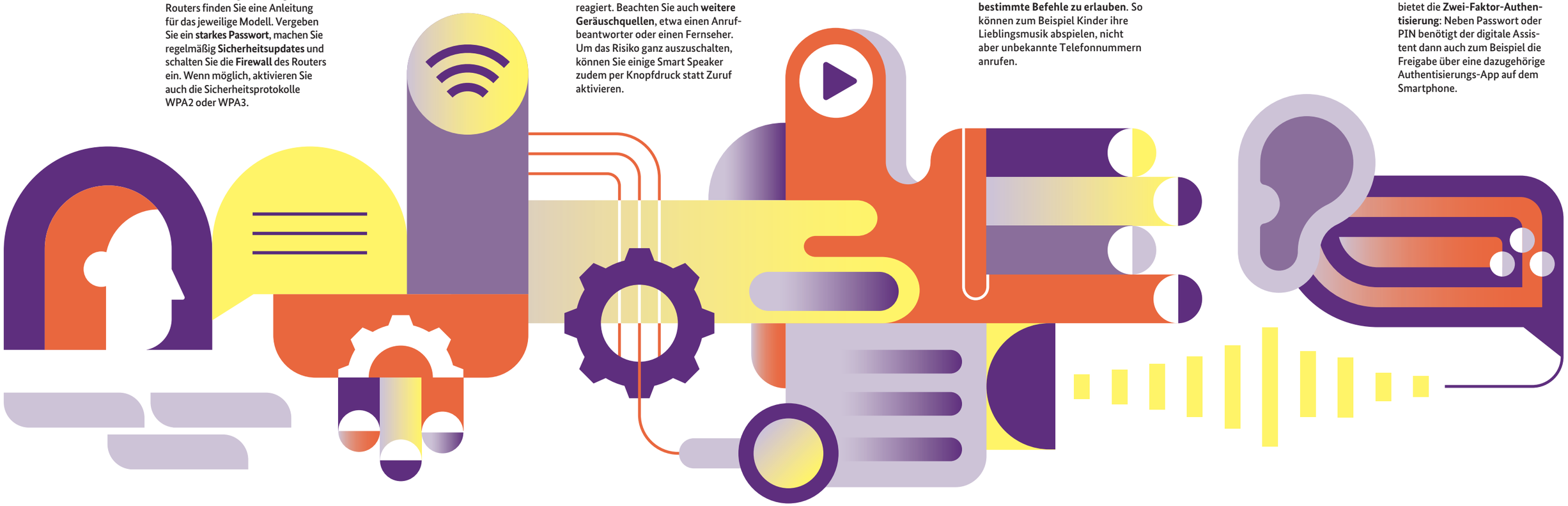
Gäste oder Kinder können den Smart Speaker natürlich ebenso nutzen. Zu einigen Funktionen sollten sie aber keinen Zugang haben.

Viele Smart Speaker können zwischen unterschiedlichen Stimmen unterscheiden: Sie erkennen, von wem sie angesprochen werden, und reagieren nur auf die **Anweisungen bestimmter Personen**. Dafür muss die dazugehörige Funktion aktiviert und das Gerät mit der jeweiligen Stimme vertraut bzw. eingerichtet sein. Einige Modelle ermöglichen es auch, einzelnen Stimmen **nur bestimmte Befehle zu erlauben**. So können zum Beispiel Kinder ihre Lieblingsmusik abspielen, nicht aber unbekannte Telefonnummern anrufen.

4. Funktionen mit PIN oder Passwort sichern

Bei einigen Funktionen, etwa dem Onlineshopping, ist es besonders problematisch, wenn Unbefugte darauf zugreifen. Diese Aktivitäten können daher zusätzlich beschränkt werden.

Der Smart Speaker kann beispielsweise ein **Passwort abfragen**, um eine Bestellung zu autorisieren. Ebenso kann eine PIN eingefordert werden, um jugendgefährdende Inhalte zu beschränken. Auch der **Zugriff auf verbundene Geräte**, etwa auf die Notiz-App eines Smartphones, kann so beschränkt werden. Noch mehr Sicherheit bietet die **Zwei-Faktor-Authentisierung**: Neben Passwort oder PIN benötigt der digitale Assistent dann auch zum Beispiel die Freigabe über eine dazugehörige Authentisierungs-App auf dem Smartphone.



5. Passen Sie die Datenschutzeinstellungen an

Welche Daten Ihr Smart Speaker zu welchem Zweck speichern darf, können Sie in seinen Einstellungen ansehen und anpassen.

Damit er auf Zuruf reagiert, muss der Smart Speaker **dauerhaft eingeschaltet** sein. Einmal aktiviert, speichert das Gerät außerdem die nötigen Informationen, um einen Befehl auszuführen. Wofür diese Daten genutzt werden, erfahren Sie in der der jeweiligen Datenschutzerklärung und in den AGB. **Anstelle der voreingestellten Berechtigungen** sollten Sie diese individuell anpassen. Bei den meisten Modellen können Sie sich beispielsweise dagegen entscheiden, dass **Daten vom Hersteller ausgewertet** werden, um das Gerät weiterzuentwickeln.

6. Prüfen Sie regelmäßig die gespeicherten Daten

Um sich einen Überblick über die gespeicherten Daten zu verschaffen, lohnt es sich, diese in regelmäßigen Abständen einzusehen.

Die gespeicherten Daten finden Sie bei den meisten Modellen in den Einstellungen. Dort können Sie auch die **Datenschutzeinstellungen** anpassen oder **bereits aufgezeichnete Daten löschen**. Alternativ können Sie das gesamte Gerät oder zumindest sein Mikrofon ausschalten, wenn Sie es gerade nicht benötigen. Das kann zum Beispiel bei **vertraulichen Gesprächen** dafür sorgen, dass keine sensiblen Daten aufgezeichnet werden.

7. Installieren Sie nur vertrauenswürdige Erweiterungen

Erweiterungen bringen neue Funktionen mit sich: Sie steuern zum Beispiel das Smarthome oder erlauben es, an Videokonferenzen teilzunehmen.

Solche Erweiterungen können vom selben Hersteller wie der Smart Speaker stammen, müssen sie aber nicht. Sie werden ähnlich wie Apps für das Smartphone heruntergeladen. Einige Hersteller prüfen die für das jeweilige Modell erhältlichen Erweiterungen nur vor einer ersten Freigabe, nicht aber nach späteren Updates.
Unseriöse Anbieter können auch **im Nachgang Schadsoftware hinzufügen**. Auf diesem Weg gelangen sie zum Beispiel an gespeicherte Daten, hören Nutzerinnen und Nutzer ab oder dringen gar in das gesamte Netzwerk ein. Schauen Sie sich vor dem Download **den Anbieter der Erweiterung sowie die Datenschutzbestimmungen** genau an.

8. Schalten Sie Ihren Smart Speaker auch mal aus

Nicht immer muss der Smart Speaker mithören und mit dem Internet verbunden sein. Damit er keine Daten aufzeichnet, kann er entweder deaktiviert oder ganz ausgeschaltet werden.

Auch **in Ihrer Abwesenheit**, beispielsweise während eines Urlaubs, kann ein Smart Speaker zum Einfallstor für Cymberkriminelle werden. Außerdem gibt es Situationen, etwa **vertrauliche Gespräche**, in denen ein Smart Speaker besonders sensible Daten nicht mithören soll. Dagegen gibt es eine einfache Lösung: Schalten Sie das Gerät aus und trennen Sie es vom Strom, wenn Sie gerade keine Unterstützung benötigen oder das Mithören nicht wünschen. Viele Modelle zeigen anhand einer **LED-Leuchte** an, ob sie eingeschaltet sind.