Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Das Internet der Dinge sicher nutzen

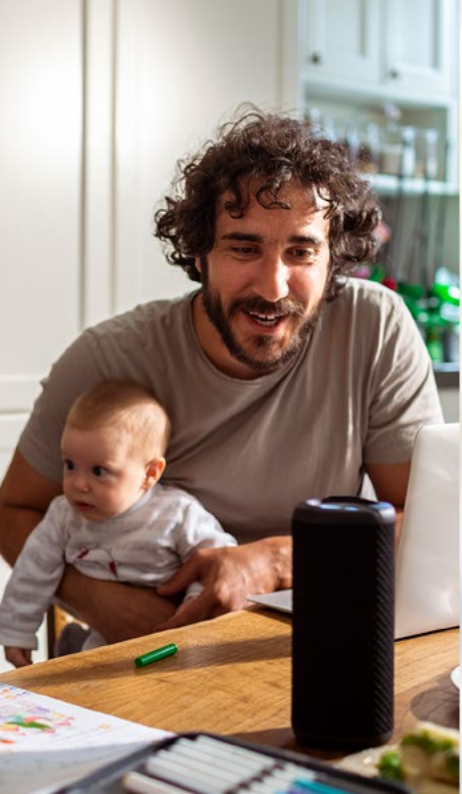
8 Tipps und Sicherheitshinweise zum Internet der Dinge

Tipps rund um das Internet der Dinge

Immer mehr Dinge in unserem Alltag sind smart, lassen sich also sowohl miteinander als auch mit dem Internet vernetzen. Man spricht daher auch vom Internet der Dinge oder auf Englisch Internet of Things (IoT). Dazu gehören beispielsweise vernetzte Fahrzeuge und intelligente Verkehrsleitsysteme oder Geräte wie Smart-TVs oder Heizungsthermostate, Rollläden und Verbrauchszähler, die dem Benutzer oder der Benutzerin das Leben erleichtern. Den Status vieler smarter Geräte können Sie jederzeit und aus der Ferne überprüfen und auch ihre Aktivitäten steuern. Doch schlecht gesicherte Geräte und Netzwerke bieten Angreifern viele Möglichkeiten, Informationen wie sensible Daten auszuspähen oder die Geräte für andere kriminelle Zwecke zu missbrauchen.

Hier haben wir einige wichtige Tipps und Informationen für Sie zusammengestellt, damit Sie Ihren Umgang mit dem Internet der Dinge möglichst sicher gestalten können. Der Fokus der Tipps liegt dabei auf dem Einsatz von vernetzten Alltagsgeräten.
Ausführliche Informationen zu den Tipps finden Sie auf den nachfolgenden Seiten dieser Broschüre sowie auf unserer Website: bsi.bund.de/smarthome

1. Aktualisieren Sie die Software Ihrer Geräte, wenn Sicherheitsupdates verfügbar sind.
2. Ändern Sie voreingestellte Standardpasswörter, nutzen Sie Passwortmanager und, falls möglich, eine Zwei-Faktor-Authentisierung.
3. Aktivieren Sie die Firewall Ihres Routers.
4. Aktivieren Sie die Verschlüsselung der Kommunikation der IoT-Geräte und verbinden Sie IoT-Geräte nur mit dem Internet, wenn ein Fernzugriff unbedingt notwendig ist.
5. Nutzen Sie, wenn möglich, ein VPN für eine gesicherte Verbindung in Ihr Heimnetz.

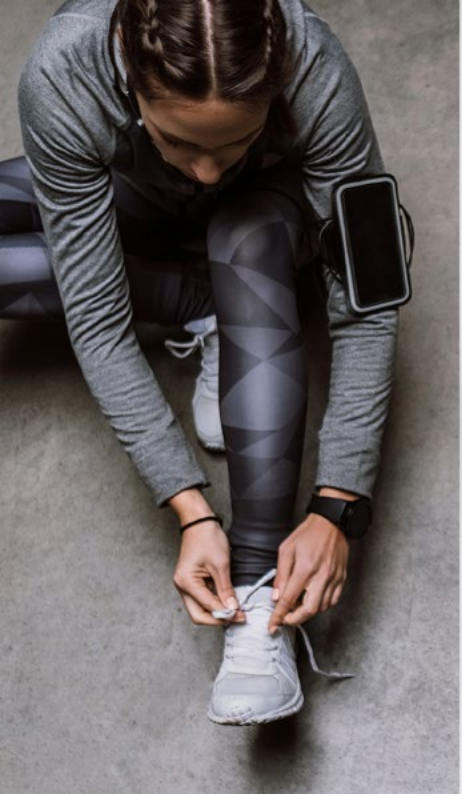


6. Richten Sie möglichst ein separates WLAN für Ihre IoT-Geräte ein.
7. Verhindern Sie den physischen Zugriff auf Ihre Geräte durch Dritte.
8. Bedenken Sie, dass durch IoT-Geräte möglicherweise persönliche Daten an Dritte weitergegeben werden. Machen Sie sich bewusst, welche Risiken mit der Nutzung von IoT-Geräten einhergehen und wägen Sie diese für sich persönlich ab.

Was ist das Internet der Dinge?

Der Begriff Internet der Dinge oder im Englischen Internet of Things (IoT) steht für eine vernetzte Welt aus smarten Geräten. Diese Geräte, auch IoT-Geräte genannt, verhalten sich wie Computer und kommunizieren lokal oder über das Internet miteinander. So sollen sie unseren Alltag einfacher, bequemer und effizienter machen. Sie generieren Daten, z. B. indem sie die Temperatur und Helligkeit in einem Raum messen und auf dieser Grundlage verschiedenste Vorgänge wie etwa die Regulierung der Heizung automatisieren. Dies kann auch beinhalten, dass sie die Daten mit weiteren hilfreichen Informationen anreichern.

Häufig sendet das Gerät dabei Informationen an eine Cloud. Darunter versteht man einen internetbasierten Speicherplatz. Dort werden die Daten aufbereitet, zugänglich gemacht oder dienen als Grundlage für weitere Dienstleistungen. Es existieren aber auch rein lokal arbeitende Systeme, die sich beispielsweise im eigenen Heimnetz befinden, aber keine direkte Verbindung zum Internet haben.



Wo werden IoT-Geräte eingesetzt?

Wearables, Smarthome, Industrie 4.0 und Smartcity stehen als Begriffe beispielhaft für Einsatzgebiete von IoT-Geräten.

Wearables

Zu den Wearables (sinngemäß: „Tragbares“) zählen IoT-Geräte, die häufig direkt am Körper eingesetzt oder getragen werden. Das kann beispielsweise ein Fitnesstracker sein. In vielen Fällen sieht er aus wie eine Armbanduhr, kann aber neben der Zeit auch die Anzahl der Schritte sowie die Vitalfunktionen anzeigen. Weitere Beispiele sind Smartwatches, aber auch Kleidungsstücke mit elektronischen Komponenten zur Musikwiedergabe. Häufig sind Wearables nicht direkt mit dem Internet, sondern über Bluetooth oder NFC (Near Field Communication) mit einem Smartphone oder Tablet verbunden, mit dem Sie das Wearable steuern und Daten abrufen können.

Smarthome

Der Bereich Smarthome umfasst alle Geräte, deren Einsatzgebiet sich in Ihrem Wohnraum befindet. Es gibt Systeme, die automatisch Fenster, Türen und Rollläden öffnen bzw. schließen – sogenannte Hausautomatisierungstechnik. Zum Smarthome zählen aber auch Haushaltsgeräte wie Kühlschränke, die Sie über deren Inhalt auf dem Laufenden halten, oder Unterhaltungselektronik wie Smart-TVs und vernetzte Lautsprecherboxen mit digitalen Sprachassistenten. Oft lassen sich diese Systeme von überall aus steuern. Ein Smarthome kann Ihnen beispielsweise helfen, Energie zu sparen, indem sich die Heizung beim Öffnen des Fensters automatisch ausschaltet. Einige Geräte dienen lediglich dem persönlichen Komfortgewinn, wie zum Beispiel das Ein- und Ausschalten von Musik oder Licht per Sprachsteuerung.

Industrie 4.0

Der Einzug von digital vernetzten Geräten in die Industrie wird häufig als die vierte industrielle Revolution bezeichnet – nach den Dampfmaschinen, den Fließbändern und den Mikrochips. Der Grundgedanke von Industrie 4.0

besteht darin, dass Menschen, Maschinen, Produkte und Logistik direkt und in Echtzeit Informationen untereinander austauschen und so die Produktivität und Effizienz weiter erhöhen. Produktionsschritte können durch die digitale Vernetzung besser abgestimmt und somit die Auslastung von Maschinen besser geplant werden. Auch die Logistik profitiert davon, denn Algorithmen können ideale Lieferwege berechnen oder selbstständig Ware nachbestellen.

Smartcity

Smartcity ist ein Sammelbegriff für Konzepte, die das Leben in einer Stadt angenehmer, sicherer und energieeffizienter gestalten sollen. Die Verkehrsinfrastruktur, die Energie- und Wasserversorgung, die Beleuchtung und das städtische Datenmanagement sind Bereiche, in denen das Internet der Dinge in Städten und Gemeinden häufig zum Einsatz kommt.

So könnte zum Beispiel eine smarte Verkehrssteuerung Teil einer Smartcity sein. Bei Großveranstaltungen würde diese für einen verbesserten Verkehrsfluss sorgen, bei punktuell erhöhten Emissionswerten eine Temporegulierung oder Umleitungen zur Entlastung des betroffenen Bereichs veranlassen.

1

Aktuelle Software und Sicherheitsupdates

Schon vor dem Kauf eines IoT-Geräts sollte darauf geachtet werden, dass der Hersteller Softwareupdates über die zu erwartende typische Nutzungsdauer des Geräts bereitstellen wird. Erkundigen Sie sich für jedes Gerät, ob und wie die Updates durchgeführt werden. In den meisten Fällen geschieht das automatisch oder manuell über eine zugehörige App oder die Weboberfläche des Gerätes. Aktivieren Sie nach Möglichkeit automatische Updates bei Ihrem Gerät, um dessen Sicherheitsfunktionen stets aktuell zu halten. IoT-Geräte, für die keine Updates angeboten werden, stellen ein Sicherheitsrisiko dar. Bei ihnen bleiben Schwachstellen offen und können ausgenutzt werden, Fehler in der Software können nicht korrigiert werden. Angreifer können sich auf diese Weise Zugang zu den Geräten verschaffen und sie möglicherweise fremdsteuern. Wenn Ihr Gerät nicht mehr mit Sicherheitsupdates versorgt wird, sollten Sie es austauschen.

2

Zentrale Firewall und Routersicherheit

Die Firewall in Ihrem Router schützt Ihr Heimnetzwerk vor Angriffen über das Internet. Überprüfen Sie, ob Ihr Router eine Firewall integriert hat und aktivieren Sie diese.

Schützen Sie auch Ihren Router, indem Sie das dort voreingestellte Passwort ändern, verfügbare Updates einspielen und auf aktuelle Firmware achten.

Das Aktivieren der Firewall sowie die Änderung des Passworts können Sie in den Einstellungen des Routers vornehmen. Im Handbuch Ihres Routers ist die Internetadresse (oftmals eine IP-Nummer) vermerkt, die Sie aus Ihrem LAN bzw. WLAN heraus aufsuchen müssen, um direkten Zugriff auf den Router zu erhalten.

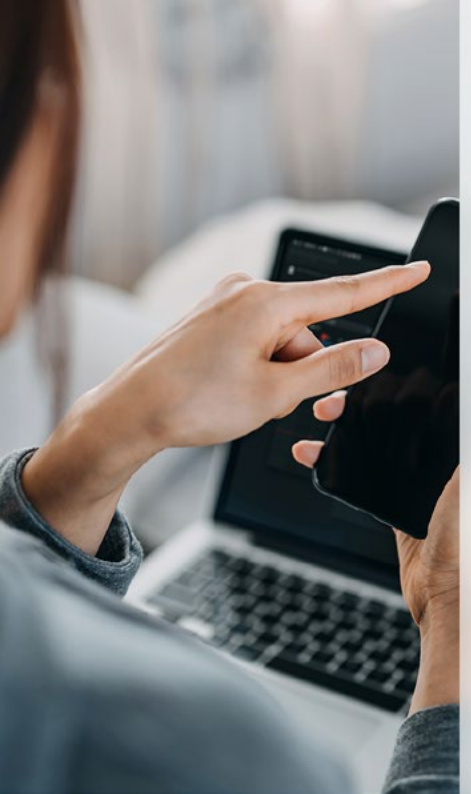
3

Keine Standardpasswörter verwenden

Ein viel genutztes Einfallstor für Angreifer sind an das Internet angeschlossene Geräte, die keinen Passwortschutz besitzen oder nur mit voreingestellten Standardpasswörtern geschützt sind. Solche Geräte sind besonders anfällig für das unbefugte Aufspielen von Schadsoftware. Infizierte Geräte können beispielsweise Teil eines Botnetzes werden: Das ist ein Netzwerk aus sehr vielen Geräten, das Angreifer per Fernsteuerung zusammenschließen und für verschiedene Aktionen nutzen können. In den meisten Fällen ist es sehr schwer nachzuvollziehen, ob ein Gerät mit Schadsoftware infiziert ist. Achten Sie daher darauf, dass Sie beim erstmaligen Anschließen eines IoT-Geräts ein eigenes, individuelles Passwort setzen. Geben Sie Ihre Passwörter niemals an Dritte weiter.

Worauf Sie beim Erstellen eines sicheren Passwortes achten sollten:

- Sie müssen sich ein Passwort gut merken können.
- Je länger das Passwort ist, desto besser.
- Das Passwort sollte mindestens acht Zeichen lang sein. Für die Absicherung eines WLAN werden mindestens 20 Zeichen empfohlen.
- Für ein Passwort können in der Regel alle verfügbaren Zeichen genutzt werden, also Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen.
- Das vollständige Passwort sollte nicht im Wörterbuch vorkommen. Gängige Zahlenfolgen oder Tastaturmuster kommen ebenfalls als sicheres Passwort nicht in Frage.
- Einfache Ziffern oder Sonderzeichen vor oder nach einem normalen Wort zu ergänzen, ist nicht empfehlenswert.



- Ein Passwortmanager kann die Handhabung unterschiedlicher Passwörter erleichtern.
- Wird eine Zwei-Faktor-Authentisierung angeboten, können Sie damit den Zugang zu Ihrem Gerät zusätzlich absichern. Dabei wird neben der Passworteingabe ein zusätzlicher Faktor abgefragt, beispielsweise in Form einer Hardware-Komponente, die als Schlüssel fungiert. Das können das Smartphone, eine Chipkarte oder ein spezieller USB-Stick sein. Auch ein Fingerabdruck oder eine vom Anbieter versendete SMS mit einem Einmalcode kann als zweiter Faktor genutzt werden.

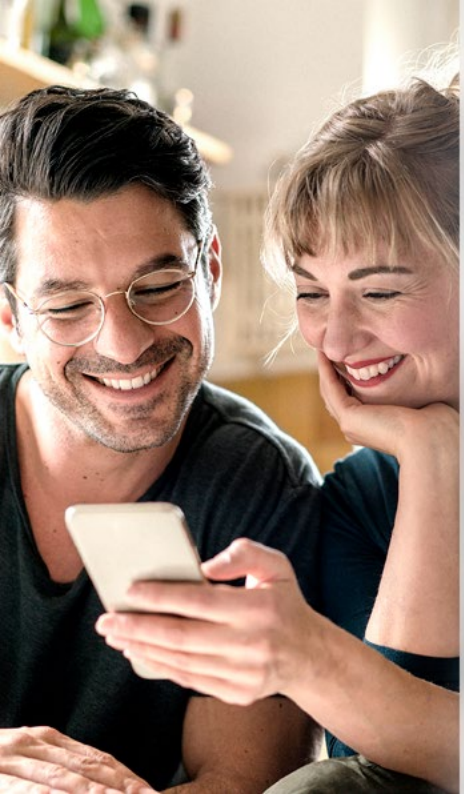
Weitere Hinweise zu sicheren Passwörtern bieten wir auf unserer Website **bsi.bund.de/account-schutz**.

4

Verschlüsselte Kommunikation und lokale Nutzung

Achten Sie darauf, dass Ihre IoT-Geräte sensible Informationen verschlüsselt kommunizieren. Dritte können diese Daten sonst abfangen und auslesen. Erkundigen Sie sich vor dem Kauf, ob das Gerät eine verschlüsselte Kommunikation unterstützt.

Verbinden Sie Ihr Smarthome nur mit dem Internet, wenn ein Fernzugriff unbedingt notwendig ist. In vielen Fällen reicht es aus, wenn Sie auf Ihre IoT-Geräte nur innerhalb Ihres Heimnetzes zugreifen können. Das Smartphone oder der Computer, mit dem Sie Ihre IoT-Geräte steuern, muss natürlich ebenfalls direkt in Ihr Heimnetz eingebunden sein. Einige Smarthome-Basisstationen bieten die Möglichkeit, die Kommunikation mit dem Internet zu unterbinden. Ein Gerät, welches nicht über



das Internet zugänglich ist, stellt ein deutlich geringeres Risiko dar. Für Rollläden oder Beleuchtung lassen sich beispielsweise Zeitpläne und Szenarien hinterlegen, die eine Steuerung völlig ohne Internetanbindung ermöglichen. So lässt sich etwa während eines Urlaubs die Anwesenheit von Bewohnern oder Bewohnerinnen vortäuschen.

Sofern an Ihrem Router die Einstellung UPnP (Universal Plug and Play) aktiviert ist, sollten Sie diese deaktivieren, damit Ihre IoT-Geräte nicht unkontrolliert ins Internet kommunizieren können.

5

VPN einrichten

Ein Virtuelles Privates Netzwerk (VPN) ist eine besonders gesicherte Verbindung zwischen zwei Punkten. Dabei wird ein Tunnel von z. B. einem Smartphone durch das öffentliche Internet zu Ihrem Heimnetz bzw. Ihrem Router aufgebaut.
Die Besonderheit des VPN ist hierbei, dass der aufgebaute Tunnel nur einen Eingang und einen Ausgang aufweist und so keine Daten auf dem Weg abfließen können. Zudem ist Ihr Heimnetz durch das VPN nur mit von Ihnen freigeschalteten Geräten erreichbar. Moderne Router bieten die Möglichkeit, ein einfaches VPN einzurichten.

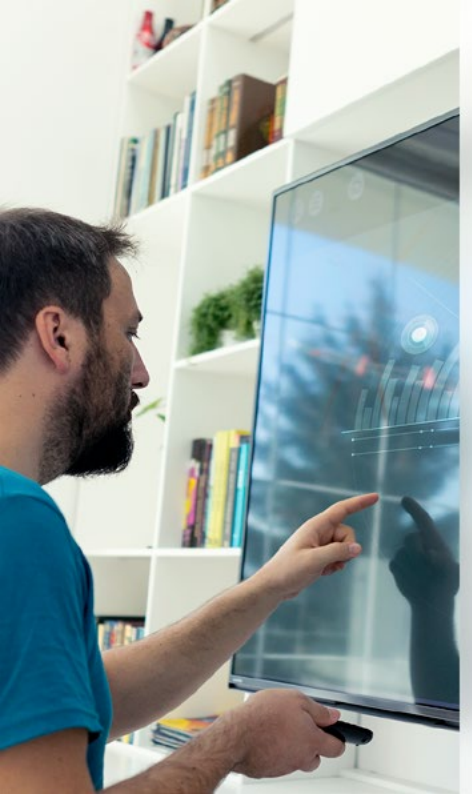
Weitere Hinweise zur Einrichtung eines sicheren VPN finden Sie auf unserer Website: bsi.bund.de/vpn

6

Separates Heimnetz

Das sogenannte Segmentieren des Netzwerkes ist in Industrienetzen bereits Standard und kann auch im Heimnetz angewandt werden. Hierbei werden die IoT-Geräte in einem separaten Netzwerk betrieben, welches keine Verbindung zu sensiblen Daten oder Geräten wie etwa Ihrem Computer hat.

Viele Heimrouter bieten die Möglichkeit, ein separates WLAN einzurichten, in welchem dann nur IoT-Geräte eingebunden werden. Dieses ist logisch von Ihrem Heimnetz getrennt und stellt somit eine einfache Möglichkeit dar, Ihre IoT-Geräte in einem separaten Netzwerk zu betreiben. Für Geräte, die Zugriff auf Daten in Ihrem Heimnetz benötigen, ist die Verlagerung in ein separates Netz nicht sinnvoll.



Ein Beispiel hierfür ist Ihr Smart-TV, wenn Sie mit diesem auch auf Ihre im Netzwerk gespeicherten Mediendateien zugreifen möchten. Bietet Ihr Router keine Netzwerksegmentierung, aber ein Gäste-WLAN, so können Sie auch überlegen, ob Sie die IoT-Geräte in dieses einbinden. In dem Fall sollte das Gäste-WLAN jedoch ausschließlich für IoT-Geräte genutzt und die Zugangsdaten nicht an Dritte weitergegeben werden.

7

Physikalische Sicherheit

Achten Sie darauf, dass Fremde von außen keinen physischen Zugriff auf Ihre Geräte erhalten können. USB- oder LAN-Ports sollten nicht frei zugänglich sein, da diese Dritten als Einfallstor in Ihr Netzwerk und auf Ihre Daten dienen können.

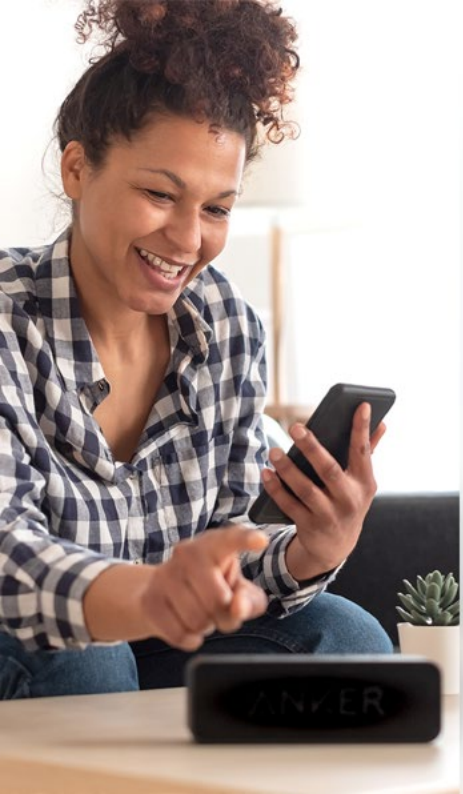
8

Bewusster Einsatz von IoT-Geräten

Machen Sie sich bewusst, wie Ihr Gerät arbeitet, welche Daten Sie mit der Nutzung Ihres Geräts generieren und wo diese gespeichert werden. Dies ist eine wichtige Grundlage für den bewussten Einsatz von IoT-Geräten.

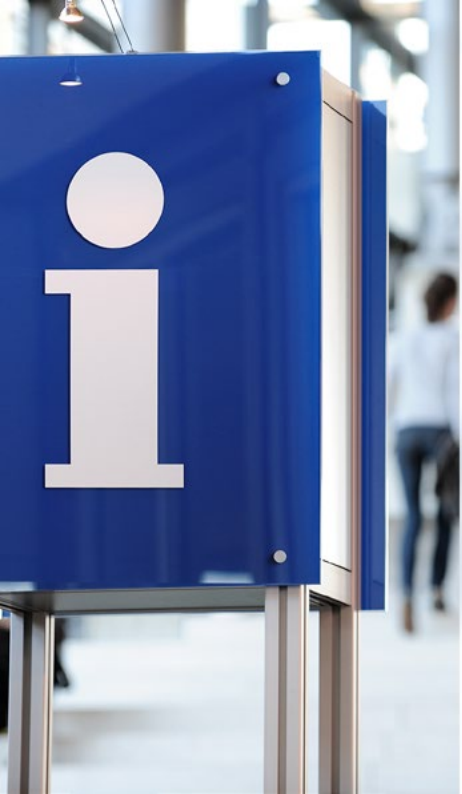
Folgende Fragen sind dabei hilfreich, das Gerät und die potentiellen Risiken seines Einsatzes besser einzuschätzen:

1. Welche Sensoren, wie z. B. eine Kamera oder ein Mikrofon, hat das Gerät?
2. Welche Daten werden aufgezeichnet und gespeichert?
3. Kann nachvollzogen werden, wo die Daten gespeichert werden?



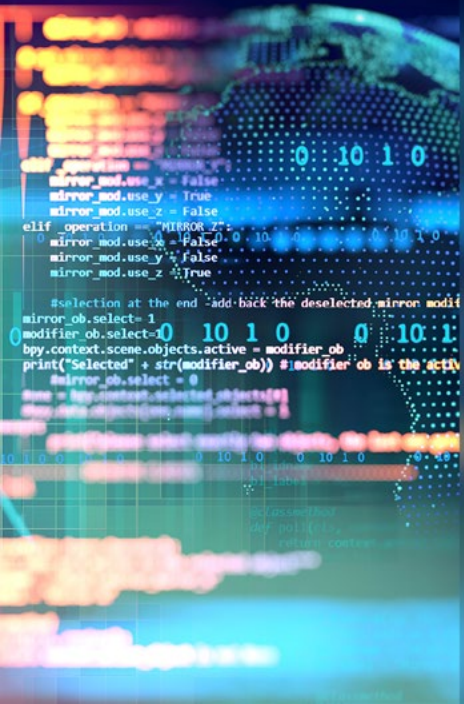
4. Werden diese Daten versendet oder mit anderen Anwendungen geteilt?
5. Welche potenziellen Risiken könnten mit der Nutzung des Geräts einhergehen und bin ich bereit diese zu tragen?

Die Antworten auf diese Fragen helfen Ihnen auch, eine Abwägung zwischen Komfort oder Funktionalität und Aspekten der Sicherheit zu treffen. Entscheiden Sie bewusst, ob Sie auf Sicherheit verzichten wollen, um bestimmte Funktionalitäten zu nutzen.



Weiterführende Informationen

- Wenn Sie mit Ihrem Smartphone IoT-Geräte steuern, sollte das mobile Gerät ebenfalls gut gesichert sein. bsi.bund.de/smartphone-sicherheit
- Auch zu digitalen Assistenten, Smart-TVs, Wearables und Smart Toys gibt das BSI Tipps und Empfehlungen für ihre sichere Nutzung. bsi.bund.de/iot



Das BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verfolgt das Ziel, die Digitalisierung in Deutschland sicher zu gestalten. Im Sinne des digitalen Verbraucherschutzes sensibilisiert das BSI die Verbraucherinnen und Verbraucher für Sicherheitsrisiken im Cyber-Raum und die sichere Nutzung digitaler Technologien. Als unabhängige und neutrale Anlaufstelle bietet es Ihnen für einen sicheren digitalen Alltag umfangreiche Informationen.

IMPRESSUM

Herausgeber:
Bundesamt für Sicherheit in der Informationstechnik – BSI
53175 Bonn

Bezugsquelle:
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189, 53175 Bonn
E-Mail: service-center@bsi.bund.de
Internet: www.bsi.bund.de
www.facebook.com/bsi_bund
Service-Center: +49 (0) 800 274 1000

Stand: März 2021
Bilder: © GettyImages
Layout und Gestaltung: Faktor 3 AG

Artikelnummer: BSI-IFB 21/254