Bundesamt
für Sicherheit in der
Informationstechnik

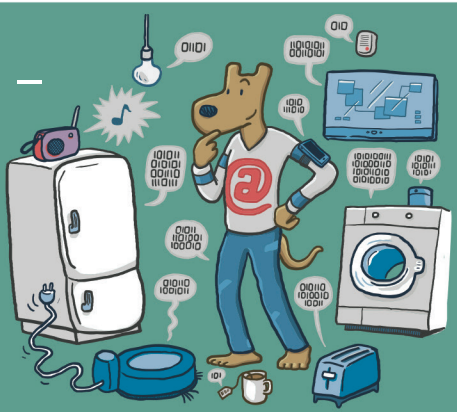
BSI FÜR BÜRGER

INS INTERNET - MIT SICHERHEIT

Internet der Dinge – aber sicher!

Basisschutz leicht gemacht

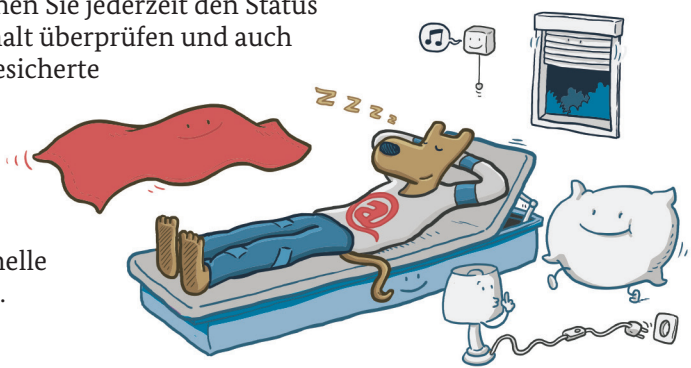
Tipps und Hinweise zum
Internet der Dinge



www.bsi-fuer-buerger.de www.facebook.com/bsi.fuer.buerger

1 Internet der Dinge – mit Sicherheit!

Die zunehmende Vernetzung von Alltagsgegenständen schreitet rasant voran. In immer mehr Haushalten befindet sich ein Smart-TV und viele weitere Dinge wie Heizungsthermostate, Rollläden und Verbrauchszähler werden smart, also vernetzt. Unterwegs können Sie jederzeit den Status smarter Geräte im Haushalt überprüfen und auch steuern. Doch schlecht gesicherte Geräte und Netzwerke bieten Angreifern viele Möglichkeiten, Informationen auszuspähen oder die Geräte für andere, kriminelle Zwecke zu missbrauchen.



Nachfolgend haben wir hier einige wichtige Tipps und Informationen für Sie zusammengestellt, um Ihren Umgang mit dem Internet der Dinge möglichst sicher zu gestalten. Der Fokus der Tipps liegt dabei auf dem Einsatz von vernetzten Alltagsgeräten.

Beachten Sie auch unsere Broschüren zum Thema „In die Cloud – aber sicher!“, „Surfen, aber sicher!“ und „Sicher unterwegs mit Smartphone, Tablet & Co“. Dort finden Sie nützliche Tipps zum Basisschutz Ihrer Geräte und zur Absicherung Ihrer Daten, die auch im Internet der Dinge wichtig sind.

2 Was ist das Internet der Dinge?

Der Begriff Internet der Dinge oder Internet of Things (IoT) steht für eine vernetzte Welt aus smarten Geräten. Diese IoT-Geräte verhalten sich wie Computer und sind lokal oder über das Internet mit anderen Geräten vernetzt. So sollen sie unseren Alltag einfacher, bequemer und effizienter machen. Sie automatisieren verschiedene Vorgänge oder reichern diese mit hilfreichen Informationen an.

Häufig sendet das Gerät dabei Informationen an eine Cloud. Dort werden die Daten aufbereitet, zugänglich gemacht oder dienen als Grundlage für weitere Dienstleistungen.

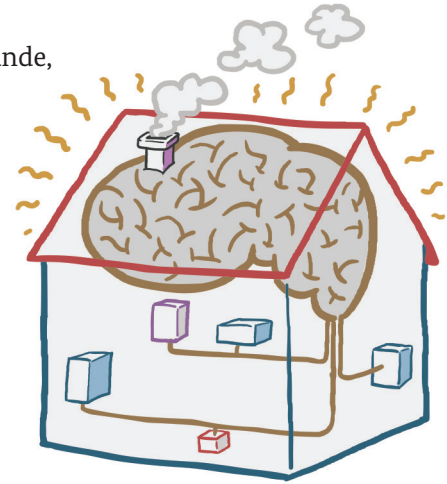
3 Wo werden IoT-Geräte eingesetzt?

Wearables, Smart Home, Industrie 4.0 und Smart City stehen als Begriffe beispielhaft für einige der Einsatzgebiete von IoT-Geräten. Nachfolgend finden Sie Begriffserklärungen sowie jeweils einige Beispiele dazu.

Wearables
Zu den Wearables (sinngemäß: „Tragbares“) zählen IoT-Geräte, die mehr oder weniger direkt am Körper eingesetzt werden. Dazu zählen Fitnesstracker, Smartwatches und auch Kleidungsstücke mit elektronischen Komponenten zur Musikwiedergabe, Kommunikation oder Überwachung der Vitalfunktionen. Häufig lassen sich Wearables über Bluetooth oder NFC (Near Field Communication) mit dem Smartphone verbinden.

Smart Home

Der Bereich Smart Home umfasst alle Gegenstände, deren Einsatzgebiet sich in Ihrem Wohnraum befindet und somit einen besonders sensiblen Bereich darstellt. Das betrifft Haustechnik, Haushaltsgeräte sowie klassische Unterhaltungselektronik im Haus. Es gibt Systeme, die automatisch Fenster, Türen und Rollläden öffnen bzw. schließen, Kühlschränke, die Sie über deren Inhalt auf dem Laufenden halten, oder Multimedia-Anwendungen, die Sie von überall aus steuern können. Ein Smart Home kann Ihnen helfen Energie zu sparen, z. B. indem sich die Heizung beim Öffnen des Fensters automatisch ausschaltet.



Die meisten Tipps dieser Broschüre zielen darauf ab, private Anwendungen im Bereich Smart Home sicherer zu machen.

Industrie 4.0
Der Einzug von digital vernetzen Geräten in der 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.

Smart City
Smart City ist ein Sammelbegriff für Konzepte, die das Leben in einer Stadt bequemer, 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.

4 Tipps rund um das Internet der Dinge

Aktuelle Software und Sicherheitsupdates
Schon vor dem Kauf eines IoT-Geräts sollte darauf geachtet werden, dass der Hersteller Softwareupdates über einen längeren Zeitraum bereitstellt. Erkundigen Sie sich für jedes Gerät, ob und wie die Updates durchgeführt werden. In den meisten Fällen geschieht das automatisch oder manuell über die entsprechende App oder Weboberfläche des Gerätes. Aktivieren Sie nach Möglichkeit automatische Updates bei Ihrem Gerät, um dessen Sicherheitsfunktionen stets aktuell zu halten.

Keine Standardpasswörter verwenden

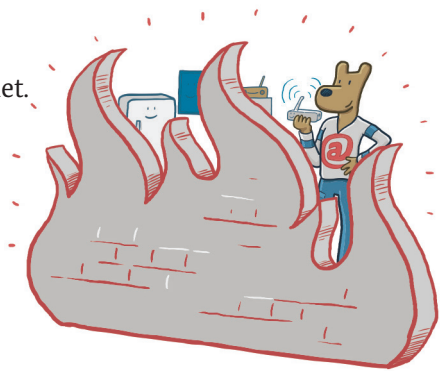
Ein viel genutztes Einfallstor für Angreifer sind an das Internet angeschlossene Geräte, die keinen Passwortschutz besitzen oder nur mit voreingestellten Standardpasswörtern geschützt sind. Achten Sie darauf, dass Sie beim erstmaligen Anschließen eines IoT-Geräts das Standardpasswort durch ein eigenes, individuelles Passwort ersetzen. Das Passwort sollte mindestens acht Zeichen lang sein, nicht im Wörterbuch vorkommen und aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern bestehen.

Info

Weitere Hinweise zu sicheren Passwörtern bieten wir auf unserer Webseite *www.bsi-fuer-buerger.de/Passwoerter*.

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.



Verschlüsselte Kommunikation
Achten Sie darauf, dass Ihre IoT-Geräte nicht unverschlüsselt mit dem Internet und im Heimnetz kommunizieren. Die Verschlüsselung sollte möglichst über HTTPS bzw. TLS erfolgen, um eine abhörsichere Kommunikation sicherzustellen. Erkundigen Sie sich vor dem Kauf, ob das Gerät eine verschlüsselte Kommunikation unterstützt.

Auf lokale Nutzung beschränken

Verbinden Sie Ihr Smart Home nur mit dem Internet, wenn ein Fernzugriff unbedingt notwendig ist. In vielen Fällen reicht es aus, wenn Ihre IoT-Geräte nur innerhalb Ihres Heimnetzes zugreifbar sind. Das Smartphone oder der Computer, mit dem Sie Ihre IoT-Geräte steuern, muss natürlich ebenfalls direkt in Ihr Heimnetz eingebunden sein. Einige Smart Home Basisstationen bieten einen Schalter, um die Kommunikation mit dem Internet zu deaktivieren. Ein Gerät, welches nicht über das Internet zugänglich ist, stellt ein deutlich geringeres Risiko dar.

Sofern UPnP (Universal Plug and Play) aktiviert ist, sollten Sie diesen Dienst deaktivieren, damit Ihre IoT-Geräte nicht unkontrolliert ins Internet kommunizieren können.

VPN einrichten
Ein Virtuelles Privates Netzwerk (VPN) ist eine besonders gesicherte Verbindung. Dabei wird ein Tunnel durch das Internet zu Ihrem Heimnetz aufgebaut, wenn Sie von außen auf dieses zugreifen möchten. Dadurch kann niemand Ihre Kommunikation abhören. Über ein VPN ist Ihr Heimnetz nur über die von Ihnen freigeschalteten Geräte erreichbar. Moderne Router bieten die Möglichkeit, ein VPN einzurichten. Endgeräte wie Smartphones oder Computer können sich über die in Ihrem Router eingestellten Anmeldedaten registrieren und so über das Internet eine gesicherte Verbindung zu Ihrem Heimnetz aufbauen.

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.

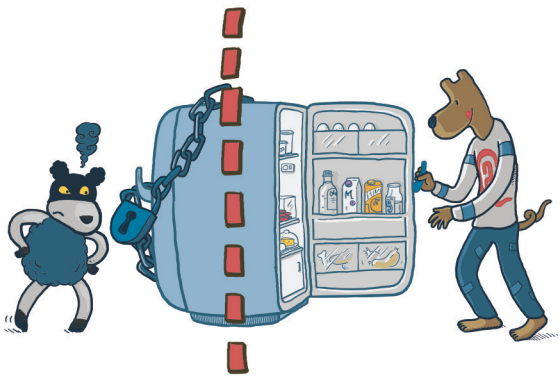
Viele Heimrouter bieten die Möglichkeit, ein separates WLAN einzurichten, in welchem dann nur IoT-Geräte eingebunden werden. Dieses ist logisch von Ihrem Heimnetz getrennt und stellt somit eine einfache Möglichkeit dar, Ihre IoT-Geräte in einem separaten Netzwerk zu betreiben. Für Geräte, die Zugriff 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 gespeicherten Mediendateien zugreifen möchten.

Privatsphäre
Erkundigen Sie sich vor dem Kauf eines IoT-Gerätes, welche Daten von Ihnen gesammelt und wie diese gespeichert werden. Seien Sie besonders wachsam, wenn personenbezogene Daten von Ihnen erhoben werden. Insbesondere dann, wenn Sie nicht für die Erbringung der Dienste erforderlich sind.

Kaufen Sie kein Produkt, bei dem nicht klar ist, welche Daten erhoben und gespeichert werden und was mit den Daten geschieht.

Physikalische Sicherheit
Achten Sie darauf, dass Fremde von außen nicht oder nur schwer auf Ihre Geräte zugreifen können. USB- oder LAN-Ports sollten nicht frei zugänglich sein, da diese einem Angreifer als Einfallstor in Ihr Netzwerk und auf Ihre Daten dienen können.

Abwägung von Sicherheit und Komfort
An vielen der hier genannten Punkte ist eine Abwägung von Komfort und Funktionalität gegen Aspekte der Sicherheit notwendig. Entscheiden Sie bewusst, ob es sinnvoll ist auf Sicherheit zu verzichten, um für Sie einen Mehrwert in der Funktionalität zu generieren.



Internet der Dinge, aber sicher!

Basisschutz im Internet der Dinge
Die BSI-Checkliste

- ✔ Aktualisieren Sie die Software Ihrer Geräte, wenn Sicherheitsupdates verfügbar sind
- ✔ Ändern Sie voreingestellte Standardpasswörter
- ✔ Aktivieren Sie die Firewall Ihres Routers
- ✔ Aktivieren Sie die Verschlüsselung der Kommunikation der IoT-Geräte
- ✔ Verbinden Sie IoT-Geräte nur mit dem Internet, wenn ein Fernzugriff notwendig ist

- ✔ Nutzen Sie VPN für eine gesicherte Verbindung in Ihr Heimnetz
- ✔ Richten Sie ein separates WLAN für IoT-Geräte ein
- ✔ Bedenken Sie die Weitergabe und den Schutz persönlicher Daten
- ✔ Verhindern Sie den physischen Zugriff auf Ihre Geräte durch Dritte
- ✔ Wägen Sie bewusst ab, wann Sicherheit wichtiger ist als Komfort und Funktionalität

NOTIZEN

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185–189, 53175 Bonn
E-Mail: mail@bsi-fuer-buerger.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de
www.facebook.com/bsi.fuer.buerger
Telefon +49 (0) 22899 9582 - 0
Service-Center: +49 (0) 800 274 1000

Stand
September 2017

Illustrationen
Leo Leowald

Artikelnummer
BSI-IFB17/254