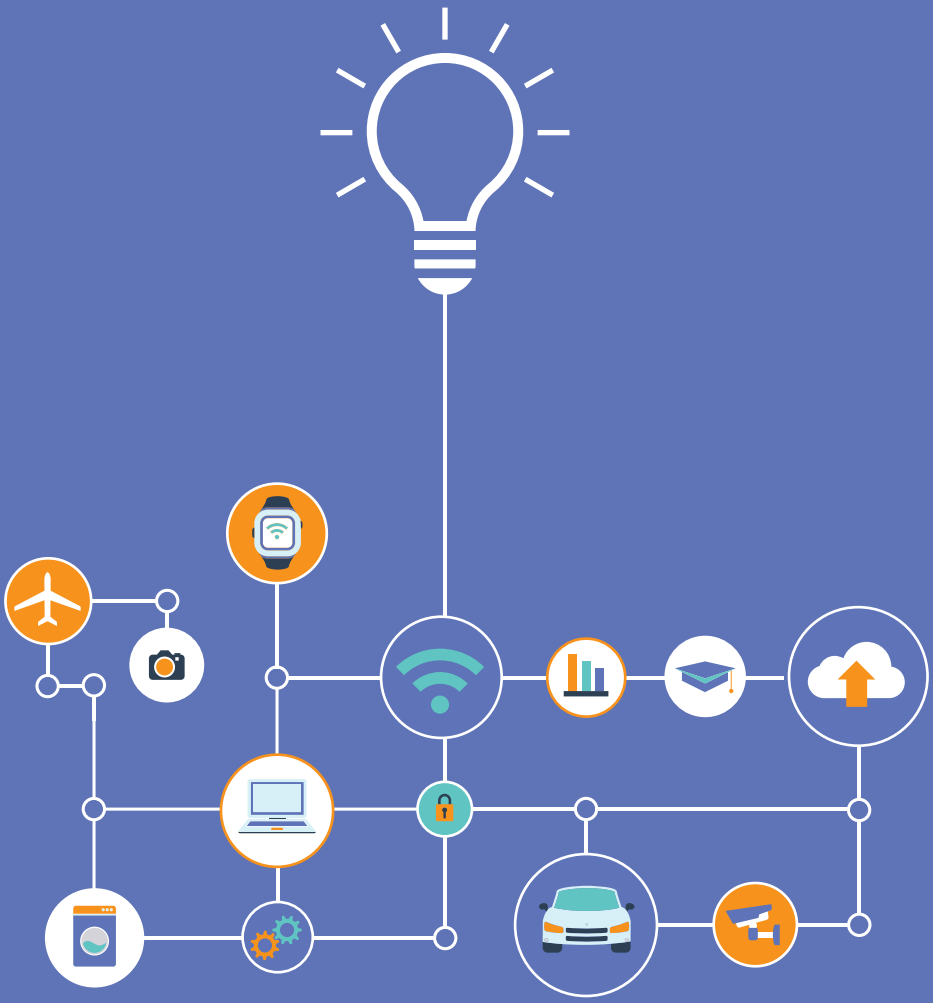
IoThink

# Tipps & Tricks

## für den sicheren Umgang mit dem IoT

iothink.at



# Inhalt


**Vorwort** ..... 4

**Gefahren** ..... 6

**Fallbeispiel** ..... 7

**Bedrohungsphänomene** ..... 8

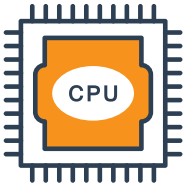
- Eavesdropping
- Man-in-the-Middle Attack
- Phishing
- Denial-of-Service
- War Driving
- Dolphin-Attacke
- Cryptojacking

**Tipps für den sicheren Umgang mit dem Internet-der-Dinge** ..... 12

1. Username und Passwort regelmäßig ändern
2. Achtung bei Smart Toys!
3. Stets sichere Netzwerke verwenden
4. Ungesicherte Verbindungen meiden
5. Wachsamkeit bei persönlichen Informationen im Internet
6. IoT-Geräte für Kinder4
7. Verwendung von 2-Faktor-Authentifizierungsmethode
8. Sicherheitsniveau beachten
9. Achtung bei Live Video Streamings
10. Frage jemanden um Rat, dem du vertraust

# Vorwort

**Das Internet der Dinge kennzeichnet ein neues Zeitalter, in dem Geräte, die traditionell offline waren, nun unzählige Daten erheben und auswerten. Vor allem bringt diese Entwicklung zahlreiche neue Möglichkeiten, die insbesondere das Leben der Menschen einfacher und angenehmer machen.**




Eine der größten Herausforderungen, die mit dieser Entwicklung einher geht, ist die Sicherheit dieser Geräte. Angesichts des rasanten Innovationsdrucks in der Branche hinken Sicherheitsstandards zum Teil hinterher. Menschen sollten primär von den Möglichkeiten durch vernetzte Technologien profitieren und sich darauf verlassen können, dass angemessene Sicherheits- und Datenschutzmaßnahmen gegeben sind - doch auch dort wo das nicht immer der Fall ist, kann der kompetente und sicherheitsbewusste Umgang mit IoT-Geräten erlernt werden.

Der vorliegende Guide bietet Eltern einen Überblick über wesentliche Phänomene und Bedrohungsszenarios im Internet of Things, sowie effektive Strategien zu deren Bewältigung. Dadurch sollen sie die Gefahren, denen ihre Kinder durch den Umgang mit IoT-Geräten womöglich ausgesetzt sind, frühzeitig erkennen und ihnen dadurch entgegenwirken können.


Internet of Things

# Gefahren

Die Nutzung von IoT-Geräten birgt, neben zahlreichen hilfreichen Funktionen, auch Gefahren über die sich vor allem Kinder und Jugendliche oftmals nicht im Klaren sind. Zum Teil werden persönliche Informationen über das Internet der Dinge für Fremde sichtbar oder auffindbar, auch kann jedoch die Steuerung von IoT-Geräten zum Teil oder gar ganz durch Unbefugte übernommen werden.


Vorsicht ist vor allem bei Geräten im Billigst-Segment geboten, da hier die Gefahr besteht, dass bereits Hintertüren eingebaut sind. Die verbauten Sicherheitssysteme können hier als mangelhaft betrachtet werden, Interessenten oder Benutzer können möglichen Gefahren jedoch entgegenwirken indem sie sich ausführlich informieren und den bewussten Umgang mit IoT-Geräten erlernen.

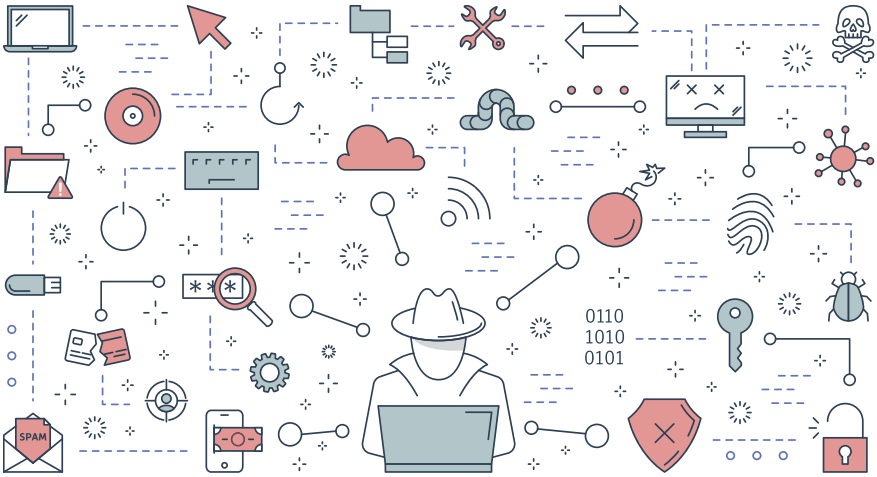
## Fallbeispiel - Puppe Cayla

Die sprechende Puppe „MyfriendCayla“ beantwortet Fragen und liest Geschichten vor. Über ein Mikrophon sowie einer Software zur Spracherkennung können Kinder auch mit ihr sprechen. Übertragen werden sämtliche Informationen an eine Drittfirma in den USA.

Die deutsche Bundesnetzagentur hat das interaktive Spielzeug „MyfriendCayla“ nun als „verbotenes Spionagegerät“ eingestuft. Hacker könnten relativ einfach Zugriff auf die aufgezeichneten Gespräche der Kinder mit der Puppe bekommen und diese verwenden um Eltern zu erpressen oder zu nötigen. Wer die Puppe besitzt, aber nicht zerstört, wird mit bis zu 25.000 Euro bestraft.

# Bedrohungs Phänomene

Der Einsatz neuer Technologien kann auch zu neuen Bedrohungsphänomene führen, wie z.B. Dolphin-Attacken bei Smart Speakern. Für einen sicherheitsbewussten Umgang mit neuen IoT-Technologien ist es unablässig, sich der häufigsten Bedrohungsphänomene bewusst zu sein. Hier wird ein Überblick über diese gegeben.



## Eavesdropping

Eavesdropping Attacken sind Angriffe, die das heimliche Abhören oder Mitlesen von Gesprächen oder Nachrichten zum Ziel haben. IoT-Geräte verfügen oftmals nicht über die Rechenleistung (oder Energie, bei Batterien) für verschlüsselten Datenaustausch im Haushalt, wodurch diese oft sehr anfällig für Eavesdropping Attacken sind.

## Man-in-the-Middle Attack

Ein Man-in-the-Middle-Attack ist ein aktiver Abhörangriff, bei dem ein Hacker Nachrichten von einem zum nächsten Opfer weiterleitet, um sie im Glauben zu lassen, dass sie miteinander kommunizieren. Da viele IoT-Produkte mit Sicherheitslücken und schlecht konfigurierten Wi-Fi-Netzwerken auf den Markt kommen, sind diese Geräte leichter für MITM-Angriffe anfällig:


## Phishing

Phishing ist ein Kunstwort, das sich aus den Worten „Passwort“ und „fishing“ zusammensetzt: Wie beim echten Fischen gibt es einen Angler (Angreifer), einen Köder (Nachricht) und einen Fisch (Opfer). Der Kriminelle verwendet hierzu Methoden, um als vertrauenswürdiger Kontakt zu erscheinen und so an wertvolle Informationen (wie z.B. Kontodaten) zu gelangen.

# Bedrohungs Phänomene

## Denial-of-Service

Ein DDoS (Distributed-Denial-of-Service) Angriff ist ein „verteilter“ Denial-of Service (DoS) Angriff, der wiederum eine Dienstblockade darstellt. Diese liegt dann vor, wenn ein angefragter Dienst nicht mehr bzw. nur noch stark eingeschränkt verfügbar ist. Auslöser ist in den meisten Fällen eine Überlastung der IT-Infrastruktur

## War Driving

Wardriving ist das systematische Suchen nach offenen oder oftmals schlecht gesicherten Wireless Local Area Netzwerks mit Hilfe eines Fahrzeugs. Ist das Netzwerk gehackt, reicht oftmals nur ein Befehl um alle angeschlossenen Geräte anzeigen zu lassen. War Driving ist eine relativ langsame Methode, um ungesicherte Gebäudeautomations-systeme aufzuspüren.

## Dolphin-Attack

Bei einer Dolphin-Attack werden Ultraschall- oder Geräuschangriffe auf Smart Speaker verwendet. Smart Speaker (wie Siri oder Alexa) können so mittels „versteckten“ Befehlen gesteuert werden. Durch den Missbrauch ihrer Funktion zur Haussteuerung können wiederum sicherheitskritische Befehle, wie z.B. das Öffnen der Haustüre oder das Wählen kostenpflichtiger Nummern ausgeführt werden.

## Cryptojacking

Beim Cryptojacking findet ein Angreifer eine Möglichkeit, die Rechenleistung fremder Computer für Cryptomining zu missbrauchen. Cryptojacking wird zunehmend auch an unsicheren und oft nicht überwachten Internet-of-Things-Geräten verwendet. Prinzipiell funktioniert Cryptojacking auf allen Arten von IoT-Geräten – auch gibt es z.B. Beweise dafür, dass Miner auf Xbox- und PlayStation-Konsolen laufen können.

# Tipps für den sicheren Umgang mit dem Internet-der-Dinge

**Die hier formulierten Tipps und Richtlinien sollen dabei helfen, das eigene Sicherheitsbewusstsein zu stärken und somit den sicheren Umgang mit IoT-Geräten in einer digitalen Welt zu erleichtern. Der Anwendungsbereich bezieht sich auf eine breite Palette von Geräten im Internet der Dinge – von Heizungssteuerungen im Smart Home, über Smart Speaker bis hin zu Smart Toys im Kinderzimmer.**

## 1. Username und Passwort regelmäßig ändern

Der Benutzername und das Passwort sollten sofort nach dem Kauf eines Gerätes geändert und danach in regelmäßigen Abständen (ca. alle 3 Monate) upgedatet werden. Ein sicheres Passwort beinhaltet Klein- und Großbuchstaben, Symbole, Zahlen oder eine PIN.

## 2. Achtung bei Smart Toys!

Smart Toys erkennen ihre Umgebung und reagieren auf Sprachbefehle oder andere Interkationen mit dem Menschen. Spielzeuge, die nicht benutzt werden, sollten stets ausgeschaltet werden. Die Inbetriebnahme sollte überdies nur in einer „sicheren“ Umgebung stattfinden, Standardpasswörter sollten stets geändert werden.

## 3. Stets sichere Netzwerke verwenden

Das verwendete Netzwerk sollte sicher sein. Dafür sollte WiFi mit starkem Passwort oder VPN benutzt werden. Es sollte überprüft werden, ob der verwendete Router eine Firewall integriert hat und ob diese aktiviert ist. Das dort voreingestellte Passwort sollte laufend geändert und verfügbare Updates eingespielt werden.

## 4. Ungesicherte Verbindungen meiden

Da ungesicherte Internet Verbindungen ein großes Risiko für Cyberangriffe darstellen, sollte man nicht über ungesicherte Bluetooth oder WLAN-Verbindungen online gehen. Die Kommunikation mit dem Internet sollte möglichst über HTTPS oder TLS erfolgen.

## 5. Wachsamkeit bei persönlichen Informationen im Internet

Es sollte stets darauf geachtet werden, welche Daten von einem IoT-Gerät gesammelt werden. Besondere Wachsamkeit ist bei personenbezogenen Daten geboten – insbesondere dann, wenn diese nicht zur Funktion des Gerätes notwendig sind. Wenn nötig, können auch frei erdachte Informationen verwendet werden.

# Tipps für den sicheren Umgang mit dem Internet-der-Dinge

## 6. Sicherheitsniveau beachten

IoT Geräte setzen ein gewisses Maß an Sicherheitsanforderungen voraus, um den Verbraucher zu schützen. Hersteller müssen Datenschutzrichtlinien für IoT-Geräte beachten. Verbraucher sollen durch den Hersteller informiert werden, wie sie die Sicherheitseinstellungen ihrer Geräte anpassen sollen.

## 7. Verwendung von 2-Faktor-Authentifizierungsmethode

IoT-Geräte, die nur durch ein Passwort geschützt sind, sind nicht sicher. Durch die Verwendung der 2-Faktor Identifizierungsmethode können sich Nutzer leicht vor Hackerangriffen schützen. Diese ermöglicht den Identitätsnachweis eines Nutzers mittels Kombination zweier unterschiedlicher, unabhängiger Komponenten.

## 8. IoT-Geräte für Kinder

Bei IoT Geräten gibt es Geräte, die auch von Kindern verwendet werden und solche, die speziell für Kinder entwickelt wurden, zum Beispiel Interaktive Spielzeuge. Da solche Geräte stark miteinander vernetzt sind, besteht die Gefahr, dass diese einfach überwacht werden können. Lauschangriffe durch intelligente Spielsachen können ein Risiko darstellen.

## 9. Achtung bei Live Video Streamings

Durch das leichte Uploaden von Videos mit einem Smartphone können ungewollte Inhalte durch Fremde oder Dritte im Internet verbreitet werden. Für mehr Sicherheit und Privatsphäre im Internet auf Sozialen Medien empfiehlt es sich, seinen Aufenthalts- bzw. Wohnort nicht anzugeben.

## 10. Frage jemanden um Rat, dem du vertraust

Wenn du dich in einer Situation befindest, in der du unsicher oder misstrauisch bist, frage jemanden um Rat dem du vertraust – egal ob Eltern, Freunde oder Lehrer.

www.iothink.at




# Projekt Daten

**Dauer**
Jänner 2019 - Dezember 2019

**Referenz**
4070

**Koordinator**
SYNYO GmbH | www.synyo.com

**Programm**
Netidee

Das Projekt IoThink wird innerhalb des netidee call 13 (2018) durch die Internet Privat Stiftung Austria (IPA) gefördert.