



IoThink

Internet of Things für Kinder & Jugendliche

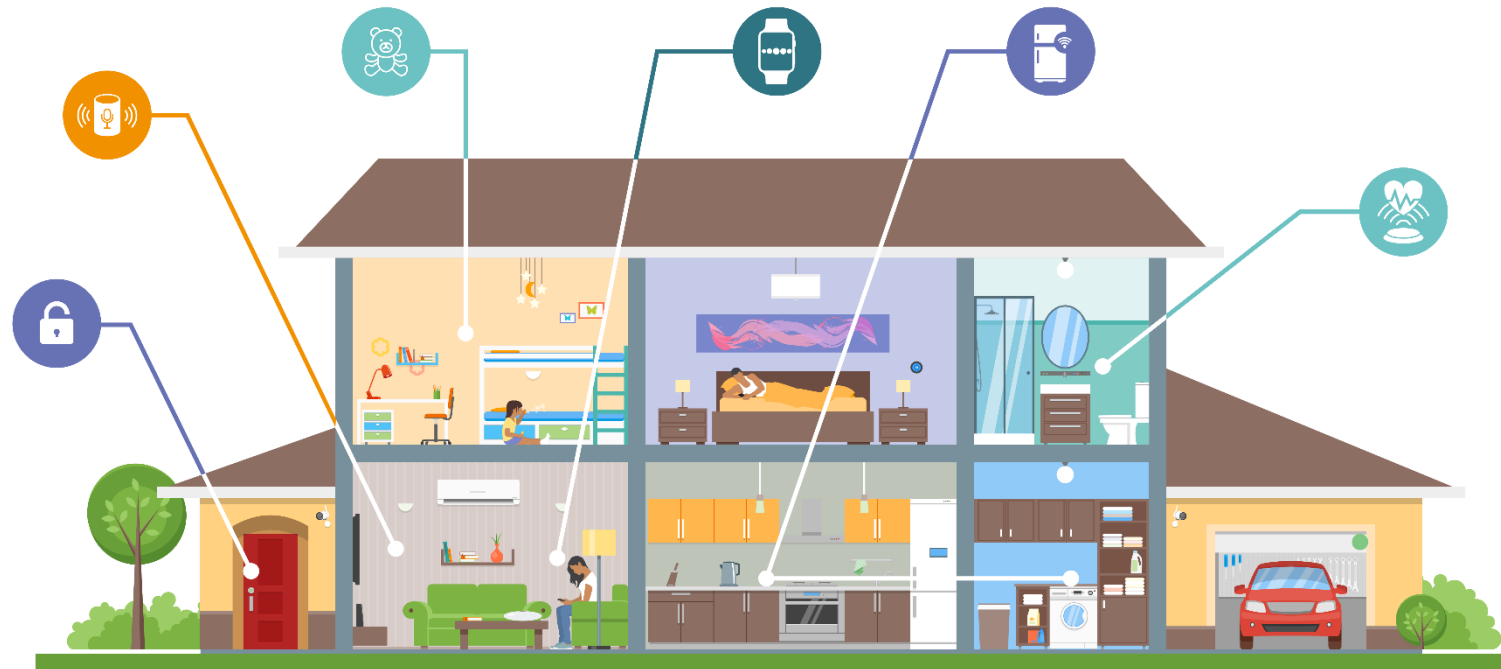


www.iothink.at

Was ist das Internet der Dinge?



Das Internet der Dinge vereint die physische mit der digitalen Welt



- Wir werden "offline" kaum noch von "online" unterscheiden können.
- Immer mehr Geräte sind mit dem Internet verknüpft und denken mit
- In Zukunft könnte das Auto auf dem Weg nach Hause mit deinem Haus sprechen um ihm mitzuteilen schon einmal die Heizung oder das Licht einzuschalten

„Dinge“ im Internet der Dinge





SMART-



Was macht diese Dinge so „smart“?

Bei IoT geht es in erster Linie nicht um Computer und Handys, sondern vor allem um Alltagsgegenstände wie Kühlschränke, Lampen, Schlösser, Spielzeuge und sogar Zahnbürsten. Das Gerät (oder das „Ding“) kann jedes Gerät sein, in das Elektronik, Software und Sensoren integriert sind.

IoT Geräte haben diese Eigenschaften:

- **Sensoren**, die permanent Daten aus ihrer Umgebung sammeln
- **Software**, um die gesammelten Sensordaten auszuwerten
- Eine **Internet Verbindung**, damit IoT-Geräte untereinander kommunizieren können



Spionieren uns IoT-Gegenstände aus?

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.



Prävention & Sofortmaßnahmen:

- ! Änderung des Standardpassworts
- ! Steigerung der Aufmerksamkeit beim Kauf von IoT-Geräten mit verbauter Kameras
- ! Verwendung technischer Präventivmaßnahmen (z.B. „Projekt Alias“)



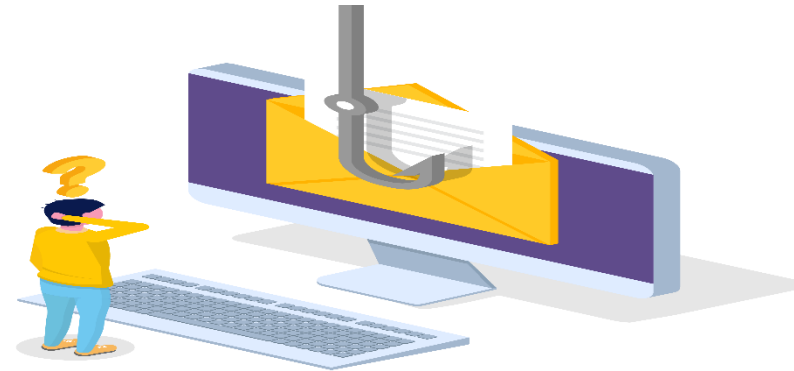
- **LG-Staubsaugerhack:** Eine Schwachstelle in der LG Smart ThinQ Smart Home-Anwendung ermöglicht es Hackern den Livestream von LG-Saugrobotern einzusehen. Die Mitarbeiter der IT-Sicherheitsfirma Check Point konnten dadurch mehrere fremde Kundenprofile kapern.
- **Puppe Cayla:** Die deutsche Bundesnetzagentur hat die interaktive Spielzeugpuppe "MyfriendCayla" als "verbotenes Spionagegerät" eingestuft. Wer die Puppe besitzt, aber nicht zerstört, wird mit bis zu 25.000 Euro bestraft



Fischen nach Passwörtern

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 Social Engineering Methoden, um als vertrauenswürdiger Kontakt zu erscheinen und so an wertvolle Informationen (wie z.B. Kontodaten) zu gelangen.



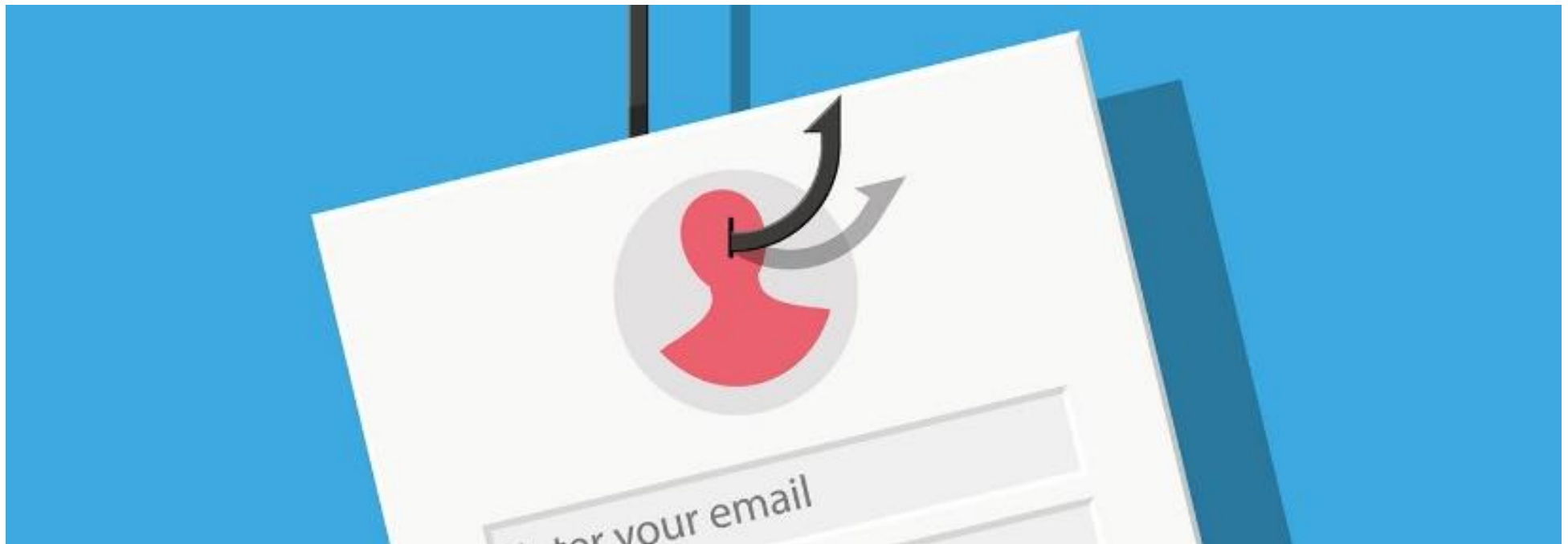
Prävention & Sofortmaßnahmen:

- ! Vorsicht vor potentiellen Phishing E-Mails, die zur Aktualisierung von Kennwort oder anderen Anmeldeinformationen auffordern
- ! Verwendung von Multi-factor Authentifizierung
- ! Verwendung von Software gegen Phishing
- ! Strafrechtliches Vorgehen gegen Täter



Fallbeispiel

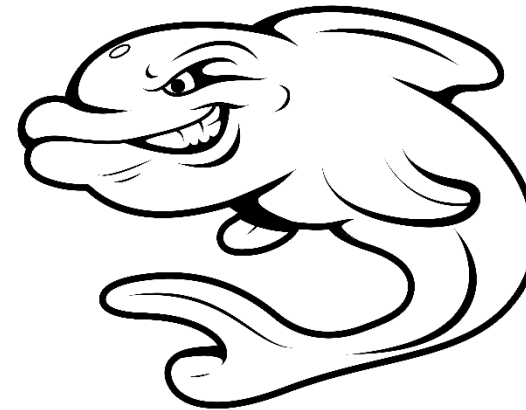
- Die Täter versenden eine Mail an das Opfer und geben sich als Hersteller eines Smarthome-Systems aus. Aufgrund einer Sicherheitsüberprüfung wäre eine Neueingabe der Zugangsdaten (inkl. Passwort) zum Smarthome-System erforderlich. Das Opfer wird so getäuscht und gibt seine Zugangsdaten preis, durch die die Täter Zugriff auf das Smarthome-System erhalten.



Stiller Angriff auf IoT-Geräte

Bei einer **Dolphin-Attacke** werden Ultraschall- oder Geräuschangriffe auf Smart Speaker verwendet – diese 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



Prävention & Sofortmaßnahmen:

- ! Absicherung von Sprachsystemen durch Klassifizierung der Audiodaten mithilfe einer Supported Vector Machine (SVM)



Fallbeispiel

- Forscher testeten Dolphin Attacken auf iPhone 4s auf iPhone 7 Plus, Apple Watch, Apple iPad Mini 4, Apple MacBook, LG Nexus 5X, Asus Nexus 7, Samsung Galaxy S6 Rand, Huawei Honor 7, Lenovo ThinkPad T440p, Amazon Echo und Audi Q3
- Sie verwendeten dafür eine externe Batterie, einen Verstärker und einen Ultraschallwandler.
- Die unhörbaren Sprachbefehle wurden auf allen getesteten Geräten von den Spracherkennungssystemen korrekt interpretiert.



Cryptocurrencies schürfen

Beim **Cryptojacking** findet ein Angreifer eine Möglichkeit, die Rechenleistung fremder IoT-Geräte 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.



Prävention & Sofortmaßnahmen:

- ! Opt-out option
- ! Ad-blocker, Blockieren von Java-Script
- ! Hardware-Lösungen (z.B. „Norton Core“)



Fallbeispiel

- Die Gruppe „Coinhive“ entwickelte 2017 ein Mining Modul, das auf fast jeder Website eingesetzt werden kann.
- Mit Anfang 2019 wurde Coinhive stillgelegt – Cryptomining zählt jedoch nach wie vor zu einer der größten Bedrohungen im Internet
- ‚Clipper‘ wurde erstmals auf dem Google Play Store gefunden



#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 Interaktionen 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.

#6 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.

#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 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.

#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.

#1 Es gibt weltweit mehr IoT-Geräte als Menschen

Die Anzahl der mit dem Internet verbundenen Geräte war im Jahr 2008 erstmals höher als jene der Menschen auf unseren Planeten. Bis zum Jahr 2020 soll diese Zahl sogar auf 50 Milliarden Geräte ansteigen.

#2 Das erste IoT-Gerät wurde in den 1980ern entwickelt

Das Internet der Dinge findet seinen Ursprung im Jahr 1981, als zum ersten Mal ein IoT-Gerät mit dem Internet verknüpft wurde. Dies geschah sogar vor dem Start des ersten Internet - Browsers.

#3 Das Internet der Dinge ist für viele noch ein neuer Begriff

Trotz der neuen vierten digitalen Revolution, dem Internet of Things, sind einer Studie zufolge 87% der Befragten mit dem Begriff *Internet of Things* nicht vertraut und haben diesen auch noch nicht gehört.

#4 Autos werden zunehmend Teil des Internet der Dinge

Es wird prognostiziert, dass 75% der neuen Autos bis 2020 Teil des Internet of Things sein werden. Autos werden miteinander und auch mit anderen IoT-Geräten wie Smart Homes kommunizieren können.

#5 City 4.0: Das IoT verbreitet sich rasant in Städten

IoT-Technologien verbreiten sich rasant in intelligenten Städten, sogenannten „Smart Cities“. Auch in den Bereichen Industrie und Gesundheitsvorsorge findet das Internet der Dinge weit Verbreitung.

#6 IoT-Geräte sind anfällig für Hacking

Ungefähr 70 Prozent der Geräte sind für Hacking anfällig – etwa können Sicherheitssysteme in Smart Homes außer Kraft gesetzt oder Zugriff auf Webcams erlangt werden. Viele Unternehmen erarbeiten Lösungen hierfür.

#7 IoT-Sicherheit gewinnt an Bedeutung

Einhergehend mit den Gefahren durch Hacking, gibt es immer mehr Lösungen, die die Sicherheit neuer IoT-Geräte garantieren. In Zukunft werden sich daher viele Berufe und Ausbildungen damit auseinandersetzen.

#8 IoT Vernetzung steigt rasant an

Im Jahr 2015 gab es weltweit rund 15 Milliarden Geräte, die mit dem Internet verbunden waren. Es wird angenommen, dass diese Zahl bis 2020 auf 75 Milliarden steigen wird.

#9 Mit IoT kann Geld & Energie gespart werden

IoT-Geräte können uns helfen, Geld und Energie zu sparen. Ein Beispiel ist die Stadt Barcelona, die jährliche reduzierte Erlöse von 37 Millionen Dollar durch ein innovatives Smart-Lighting-System verbuchen kann.

#10 Das Internet der Dinge ist auf Überholspur

Das Internet der Dinge (IoT) hat im Jahr 2018 die mobile Welt der Telefone als größte Kategorie im Bereich verbundener Geräte überholt.

#11 Immer mehr Menschen tragen „Wearables“

Immer mehr Menschen werden in den nächsten Jahren tragbare Computersysteme (zum Beispiel Smartwatches, Fitness-Tracker) sogenannte „Wearables“ am Körper tragen.

#12 Menschen besitzen zahlreiche IoT-Geräte

Bis Ende 2020 wird es weltweit rund 75 Milliarden IoT-Geräte geben. Ein Mensch wird im Durchschnitt rund 7 IoT-Geräte besitzen.

#13 Das Internet der Dinge bereichert die Arbeitswelt

Laut Experten aus dem Bereich IoT werden durch das Internet der Dinge in Zukunft Millionen von Jobmöglichkeiten entstehen.

#14 Das IoT verursacht 22-mal mehr Datenverkehr

Bis zum Jahr 2020 wird das Internet of Things 22-mal mehr Datenverkehr verursachen. 40% aller gesammelten Daten werden überdies von verbundenen Sensoren stammen.

#15 Künstliche Intelligenz treibt smarte IoT-Lösungen voran

Mithilfe der Verwertung von Daten werden Haushaltsgegenstände immer intelligenter. Somit lernen beispielsweise Staubsauger nach kurzer Zeit eigenständig, wann welche Räume zu reinigen sind.

Hier erfährst du Genaueres über die Möglichkeiten aber auch Gefahren im Umgang mit dem Internet of Things

Safer Internet

Plattform, die Kinder, Jugendliche, Eltern und Lehrende beim sicheren, kompetenten und verantwortungsvollen Umgang mit digitalen Medien unterstützt

www.saferinternet.at

Watchlist Internet

Informiert über aktuelle Betrugsfälle im Internet und gibt Tipps, wie man sich vor gängigen Betrugsmaschen schützen kann

www.watchlist-internet.at

Jugendschutz.net

Das deutsche Kompetenzzentrum für Jugendliche im Internet arbeitet mit gesetzlichem Auftrag und Fokus auf Online Inhalte die Minderjährige gefährden, ängstigen oder in ihrer Entwicklung beeinträchtigen können

www.jugendschutz.net



Hier kannst du mit ExpertInnen und Experten direkt in Kontakt treten, die dir bei Problemen oder in Krisensituationen Rat und Hilfe bieten können.

147 Rat auf Draht

Die österreichische Notrufnummer „Rat auf Draht“ bietet Kindern und Jugendlichen anonym und kostenlos Unterstützung bei Problemen, Fragen sowie in Krisensituationen und befasst sich auch mit dem Thema Handy & Internet.

www.rataufdraht.at

Internet Ombudsmann

Bietet kostenlose Schlichtung und Beratung zu internetbezogenen Themen (Persönlichkeitsrechte, Datenschutz, Urheberrecht, etc.)

www.ombudsmann.at

Austria Cyber Security Challenge


Du interessierst dich für Cyber Security und möchtest dich den Herausforderungen in den Kategorien Web, Crypto, Reverse Engineering Exploitation und Forensik stellen? Dann ist die Austria Cyber Security Challenge genau das Richtige für dich!

- <https://www.verbotengut.at/>

ELVIS – Embedded Lab Vienna for IoT & Security

Das ELVIS IoT-Security Lab ermöglicht Beratung zu aktuellen IoT-Security Themen in Anspruch zu nehmen. Im Zuge der Arbeit des ELVIS Lab werden auch Workshops an Schulen angeboten, die das Thema IoT-Security erfahrbar machen.

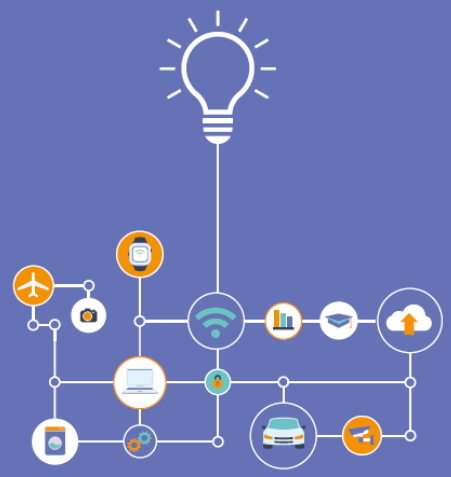
- <https://elvis.science>

IoThink 

Tipps & Tricks

für den sicheren Umgang mit dem IoT

iothink.at



ang

helfen, das en sicheren ichtern. Der ie von Geräten Smart Home, nmer.

mäßig ändern y sofort nach dem regelmäßigen rden. Ein sicheres iben, Symbole,

2. Achtung bei Smart Toys!
Smart Toys erkennen ihre Umgebung und reagieren auf Sprachbefehle oder andere Interaktionen 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.

12

IoThink 

Guide

für technikinteressierte Kinder und Jugendliche

iothink.at



en und Initiativen, in rf und Bau von IoT- ekte gliedern sich in i Robotern) sowie IoT- enen Eindringlingen).



RoboFit
Im Projekt RoboFIT werden SchülerInnen aller Schulstufen dazu angeregt, sich mit dem Thema Robotik vertieft und kritisch auseinanderzusetzen. Hier wurden zum Beispiel einige Workshop-Formate (Robina mit Scratch, Robo-Wunderkind und RoboRetter) und Materialien für den Unterricht entwickelt.

Quelle: <https://www.robokit.at/>

4



IoThink

Was ist das Internet der Dinge?



Microchips



Sensoren



Datenspeicher

IoThink



Christoph Steiner
Researcher
SYNYO GmbH

IoThink


Phishing

Wie beim echten Fischen gibt es einen Angler (Angreifer), einen Köder (Nachricht) und einen Fisch (Opfer).




IoThink


Smart Things




Smart Speaker




Smart Cameras




Smart Fridges



Smart Phones



Smart Watches



Smart Toys





Vielen Dank für die Aufmerksamkeit!

www.iothink.at