# Was ist IoT?

Das Internet der Dinge ist ein Begriff für die Technologien, welche jegliche Gegenstände in Zukunft durch Informations- und Kommunikationstechniken verbinden werden. Es ist also ein System von miteinander verbunden Geräten, mechanischen und digitalen Maschinen, Objekten, Menschen oder Tieren, die mithilfe einer eindeutigen Kennung zur Identifikation über ein offenes Netzwerk Daten auszutauschen. Alles dies geschieht ohne jegliche Mensch zu Mensch oder Mensch zu Maschine Interaktion.

In diesem Sinne erweitert das Internet der Dinge den Teilnehmerkreis an Geräten mit einer Verbindung zum Internet von Desktop-Computern, Laptops, Smartphones und Tablets auf jedes von Menschen geschaffene oder natürliche Objekt, das Sie sich vorstellen können. Was heute schon das smarte Heizungsthermostat oder der intelligente Kühlschrank ist, kann morgen Ihre Schuheinlage, eine Zahnpastatube oder der Kugelschreiber sein.

Durch die drahtlose Kommunikation, der Mikrosystemtechnik und dem Internet wurden die Grundlage für das IoT geschaffen.

## Aufgabenbereiche IoT

Bereits heute werden immer mehr IoT fähige Geräte verkauft.

Autos kommunizieren direkt mit dem Hersteller, um diesen über den aktuellen Fahrzeugzustand zu informieren. Durch die Vernetzung der Fahrzeuge untereinander kann ebenfalls eine verbesserte Navigation erfolgen, da diese Staus und Verzögerungen erkennen und vermeiden kann. Bei Fahrzeugen besteht jedoch das Problem, dass viele Features erst in den nächsten 5-10 Jahren umgesetzt werden, da diese aktuell noch nicht zum Verkehr zugelassen sind.

Bei vielen Unternehmen wird eine Flottenverwaltung verwendet um die Wartungs- und Reparaturkosten gering zu halten und planbar zu machen. Dies wird durch die Auswertung von Nutzung und Zustand der Fahrzeuge vollautomatisch erledigt.

Im Jahr 2009 wurde beschlossen, dass jeder Haushalt mit SmartMetern ausgestattet werden muss. Diese intelligenten Stromzähler zeichnen den Stromverbrauch auf und senden ihn an den Stromanbieter, die Abrechnung sollte hierdurch erleichtert werden.

SmartGrids sind ein Zusammenschluss mehrerer SmartMeter, diese sollten in Zukunft eine Auswertung über den Stromverbrauch einzelner Regionen ermöglichen. Der Netzanbieter kann dadurch erkennen, in welchen Regionen ein zusätzlicher Netzausbau erforderlich ist. Weiters wäre es möglich den Strom, welcher auf Ihrem Dach durch zum Beispiel eine Photovoltaikanlage erzeugt wird, direkt an Ihren Nachbarn zu verkaufen. Sie bekommen für den Strom mehr, als bei direkter Einspeisung ins Netz, ihr Nachbar zahlt weniger für den Strom, als würde dieser vom Netz bezogen werden und der Energielieferant profitiert ebenfalls, da für diesen keine weitern Kosten für den Netzausbau auftreten. Die gesamte Abrechnung kann mithilfe der SmartMeter erfolgen, da diese dauerhaft online sind und deshalb genau dokumentieren können „welcher“ Strom benützt wird.

Ärzte können mithilfe von IoT den Zustand ihrer Patienten in Echtzeit verfolgen oder bei Über/Unterschreiten von Schwellenwerten benachrichtigt werden. Die Kosten für die Behandlung, aber auch die gesundheitliche Entwicklung kann dadurch verbessert werden.

# IoT Sicherheit

Durch die schnelle Entwicklung der Informationstechnologie können die Sicherheitsaspekte nicht mehr schritthalten und große Sicherheitslücken sind die Folge. Viele Hersteller wollen diese aber auch gar nicht schließen, da dies die Entwicklungskosten des Produktes steigern würde und der Gewinn gedrückt würde. Viele der IoT Devices besitzen und sammeln jedoch durchaus private Daten, wollen Sie, dass jeder jederzeit sehen kann welches Programm ihr Fernseher gerade anzeigt? Oder ihre smarte Waage auf Facebook postet „Juhu ich habe 2 Kilo abgenommen, wiege nun nur mehr 250kg“?

Manchmal ist das Auslesen der Daten jedoch nicht das größte Problem, smarte Thermostate bei ihrem Heizkörper sind zwar sehr praktisch, was jedoch, wenn ein Angreifer im Winter ihre Heizkörper lahmlegt? Viele IoT Devices werden aber auch Mitglieder in Botnetzen, welche die Rechenpower verbinden um Passwörter zu knacken oder DoS Attacken durchzuführen.

Die Hersteller wollen ihre Produkte so schnell wie möglich auf den Markt bringen, weshalb Security nicht ins Design Pattern passt. Viele Entwickler haben jedoch auch keine Ahnung davon, was es bedeutet Sicherheit für ein Gerät, welches frei im Netz erreichbar ist, einzurichten. Viele Hersteller kommen aus dem Embedded-System-Bereich, wo die Geräte in isolierten IP-Netzen angebunden

waren.

Eine neue Update-Politik müsste ebenfalls eingeführt werden, da IoT Devices häufig ein „installieren und aus dem Sinn“ Produkt sind. Keiner macht sich Gedanken, ob der Kühlschrank ein neues Update braucht.

Des Weiteren müssen neue Standards definiert werden, denn nur so garantiert man sichere IoT Geräte. Aktuell wird der Markt nur halbherzig reguliert, da es für Security und Sicherheit aktuell eigentlich keine Standards gibt.

Bis es neue Standards gibt sollten IoT Geräte mindestens folgende Punkte erfüllen

* Verwendung sicherer Entwicklungspraktiken

z.B.: starke Authentifizierung, sichere Webschnittstellen

* Schutz der Daten
* Offenlegung wie private Daten behandelt werden
* Verschlüsselung **Überall und immer**

# Funktionsweise

Da viele der IoT Devices in einem privaten Netzwerk angemeldet sind, sind diese nicht von außen erreichbar. Der Endbenützer müsste hohes technisches Wissen aufweisen, um Portforwarding und ähnliches zu konfigurieren. Um diese Hürde zu umgehen werden sogenannte Broker verwendet, das Gerät holt und sendet Daten an diesen. Sollte der Broker jedoch böswillig sein, so kann dieser bevor die Daten an den Hersteller weitergesendet werden diese ebenfalls speichern und verkaufen. Außerdem wäre eine Manipulation aller Daten möglich.