IT-Business

IOT – Smart Home

IOT und jetzt?

In den letzten Jahren hat sich das IoT (Internet of Things) zu einer der wegweisenden Technologien entwickelt. Da wir inzwischen Alltagsgegenstände z.B. Küchengeräte, Drucker, Autos etc. über eingebettete Geräte mit dem Internet verbinden können, ist eine nahtlose Kommunikation zwischen Personen, Prozessen und Dingen möglich. Das IoT bezieht sich auf eine Vielzahl von "Dingen", die mit dem Internet verbunden sind, damit sie Daten mit anderen Dingen austauschen können.

Mithilfe von Computing-Lösungen, der Cloud, Big Data und mobilen Technologien können physische Objekte Daten mit minimaler menschlicher Beteiligung teilen und sammeln. In dieser hochgradig vernetzten Welt können digitale Systeme jede Interaktion zwischen vernetzten Dingen aufzeichnen, überwachen und anpassen. Die physische Welt trifft auf die digitale Welt – und sie kooperieren.

Was ist das Industrial Internet of Things?

Industrial IoT (IIoT) bezieht sich auf die Anwendung von IoT-Technologien im industriellen Bereich, insbesondere im Zusammenhang mit der Instrumentation und Steuerung von Sensoren und Geräten, die auf Cloud-Technologien aufbauen. Neuerdings nutzen Branchen die Kommunikation von Maschine zu Maschine (M2M), um eine drahtlose Automatisierung und Steuerung zu erreichen. Aber mit der Entstehung der Cloud und verwandter Technologien (wie Analysen und Machine Learning) können Branchen eine neue Stufe der Automatisierung erreichen und so neue Umsatzmöglichkeiten erschließen und neue Geschäftsmodelle entwickeln. Das IIoT wird manchmal als die vierte Welle der industriellen Revolution oder Industrie 4.0 bezeichnet. Ein Anwendungsbereich des IOT ist das Smart Home, welches nachfolgend beleuchtet wird.

Was ist Smart Home?

In einem smarten Zuhause sind alle elektrischen Geräte über eine Zentrale verbunden und kommunizieren miteinander. Diese intelligenten Technologien ermöglichen automatisierte Abläufe von technischen Prozessen in Wohnräumen. Über die Zentrale können die einzelnen Installationen via App auf dem Smartphone, Tablet, Computer oder Laptop ferngesteuert werden. Unser Zuhause wird zunehmend intelligenter. Miteinander vernetzte und fernsteuerbare Lampen, Storen, die sich passend zu Licht und Wetter automatisch öffnen oder schliessen, Smart Speaker oder WLAN-Überwachungskameras sind inzwischen für viele erschwinglich. Allerdings haben einige Bedenken um Ihre Privatsphäre. Dies vor allem dann, wenn die neue Technologie zuhört oder zuschaut wie die smarten Lautsprecher oder Sicherheitskameras. Wie steht es mit dem Datenschutz in modernen Smart-Home-Systemen aus?

Datenschutz versus Smart Home

Laut Schweizer Bundesgesetz über den Datenschutz (DSG) sind Personendaten alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen». Jeder private oder staatliche Akteur, der solche Personendaten speichern, bearbeiten oder weitergeben will, darf dies nur aufgrund einer gesetzlichen Grundlage oder der Einwilligung der betroffenen Person. Der Eingriff in die Persönlichkeit der betroffenen Person muss nach Art. 4 DSG verhältnismässig und zweckmässig sein müssen. Zusätzlich müssen die bearbeiteten Daten richtig und sicher sein gemäss Art. 5 und 7 DSG.

Im Smart Home bekommen Geräte durch Funkchips und Prozessoren neue Fähigkeiten. Sie erhalten eine eigene Identität in einem Netzwerk und können Daten über den eigenen Zustand sowie ihre Umgebung an andere Geräte oder einen zentralen Server senden und empfangen. Da diese Daten im Haus oder in der Wohnung entstehen und Aufschluss über die Lebenssituation und das Verhalten der Bewohner geben, sind sie zumindest im weiteren Sinne personenbezogene Daten. Diese Daten können einerseits direkt Geräte im Haus ansteuern oder weiterverarbeitet werden, um komplexere Automatisierungsprozesse auszulösen.

Für fortgeschrittene Smart-Home-Funktionen sind zahlreiche personenbezogene Daten notwendig. Erst wenn das Smart Home das Nutzerverhalten regelmässig aufzeichnet und weiterverarbeitet, kann es z.B. eine Anwesenheitssimulation abspielen.

Es besteht ein erhöhtes Risiko, dass Daten der betroffenen Personen in Unmengen durch die Geräte im Haushalt aufgenommen werden und dann an die Server der Hersteller gesendet werden, die das Nutzverhalten der betroffenen Personen auswerten. Besonders schützenswert sind Videobilder, welche gewisse Geräte speichern können.

Hier müssen die Anbieter solcher Smart Home Geräten zur Verantwortung gezogen werden. Diese müssen sowohl technische als auch organisatorische Massnahmen ergreifen, welche die Datensicherheit der betroffenen Personen gewährleitstet. Die betroffenen Personen müssen zudem genau über den Zweck der Datensammlung und -verarbeitung informiert werden, ihre Zustimmung dazu explizit erteilen (und auch wieder entziehen können), Auskunft über die erfassten Daten verlangen sowie jederzeit die vollständige Löschung (bzw. Anonymisierung) ihrer personenbezogenen Daten fordern können.

Nutzer von Smart Home Geräten müssen die Tragweite möglicher Eingriffe in ihre Persönlichkeit abschätzen können, bevor sie das System installieren oder Parameter freigeben. Daher müssen die Nutzer aufgeklärt in die Smart Home Anwendungen einwilligen können, bevor solche Systeme installiert werden.

Fazit

Mit dem Begriff Internet of Things ist die zunehmende Vernetzung von Geräten gemeint, welche beginnen untereinander oder mit Menschen Informationen austauschen. Dies wird durch Software ermöglicht, welche in den Geräten enthalten ist.

Smart Home Anwendungen werden dem sogenannten Internet of Things zugeordnet. Grundsätzlich geht es dabei um einen Digitalisierungsprozess im privaten Bereich, indem alltägliche Funktionsbereiche quasi "online gehen" und so miteinander vernetzt werden, um zentral gesteuert zu werden.

Smart Home Geräte können personenbezogene Daten der Nutzer speichern und auswerten. Der Persönlichkeitsschutz der Nutzer wird tangiert und muss daher zweckgebunden geschützt werden.

Ursula Sury ist selbständige Rechtsanwältin in Luzern (CH) und Vizedirektorin an der Hochschule Luzern – Informatik. Sie ist zudem Dozentin für Informatikrecht in verschiedenen Nachdiplomstudien, welche am Institut für Wirtschaftsinformatik der Hochschule durchgeführt werden. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig.