

Alle Daten in die Cloud? IoT-Plattformen auf dem Vormarsch!



Wann stehen Sie morgens auf? Wann sind Sie normalerweise zu Hause? Sind Ihre Fenster verschlossen oder gekippt? Die Antworten dazu kennt Ihr Smart Home über Sensoren wie Bewegungsmelder oder Fensterkontakte.

So verrückt das im Moment klingen mag: In der Zukunft werden viele Nutzer diese Daten freiwillig „in die Cloud“ übertragen und zustimmen, dass weitere Dienstleister wie Versicherer, Sicherheitsdienste oder Paketzusteller darauf zugreifen.

Kundensicht: Smart Home „gerne“, aber möglichst günstig bzw. kostenlos!

Derzeit zeichnen sich in der Gesellschaft folgende parallele Trends ab:

Zum einen nimmt die Akzeptanz des „Smart Home“ zu. Hersteller von Smarthome-Komponenten bzw. Systemintegratoren verzeichnen eine zunehmende Nachfrage. Dabei hat der eigentliche Massenmarkt noch gar nicht begonnen. Eine Umfrage unter den Teilnehmern vom Smart Home Kongress vor wenigen Tagen in Nürnberg hat ergeben, dass der Durchbruch zum Massenmarkt von den meisten Teilnehmern im Jahr 2020 erwartet wird. Eine deutlich zunehmende Nachfrage steht also vor der Tür!

Andererseits sind Nutzer nicht bereit, für Software oder Dienste zu bezahlen. Während es Nutzer verstehen, dass man für „anfassbare“ Komponenten wie Controller/Gateway, Sensoren und Aktoren (also Taster, Präsenzmelder, Dimm- und Schaltaktoren, Stellventile für die Heizung etc.) Geld bezahlen muss, ist man in Bezug auf Apps, Dienste und Internetanbindung dahingehend verwöhnt, dass so etwas kostenlos ist. Nun ist aber die Hardware nur das Fundament und die Software der eigentliche Kern eines Smart Home. Und insbesondere die Software ist pflegeintensiv (Support, Weiterentwicklungen, Updates etc.) und erzeugt einen erheblichen Aufwand. Hierzu hieß es von einem Referenten auf dem erwähnten Kongress: Hardware ist der Revenue-Bringer; Software/Dienste sind Ressourcen-Killer.

Nun ändern sich im Internetzeitalter die Geschäftsmodelle. Die neue Währung heißt „Kundendaten“. Wenn ein Nutzer eines Smart Home bereit ist, Daten über sich bzw. sein Umfeld preis zu geben, gibt es zunehmend Dienstleister, die ihm dafür softwareseitige Funktionen kostenlos anbieten oder zumindest subventionieren.

Wenn ein Paketzusteller wüsste, wann jemand zu Hause ist, würde das helfen, Fehlfahrten zu vermeiden. Wenn Versicherer wüssten, ob bei Ihnen trotz Abwesenheit ein durchgängiger Wasserverbrauch vorliegt, könnte man teure Wasserrohrbruch-Folgeschäden vermeiden. Wenn ein Sicherheitsdienst aufgrund der Daten von Fensterkontakt und Präsenzmelder ableiten kann, dass ein Fenster von außen geöffnet wird, kann er Ihnen einen günstigen Einbruchs-Präventionsdienst anbieten.

Deshalb bilden sich derzeit cloudbasierte „IoT-Plattformen“ (IoT – Internet of Things). Diese Plattformen bieten an, möglichst viele Daten von Ihnen zunächst aufzunehmen und zu speichern. Zu diesen Daten dürfen Sie individuell entscheiden, welcher weitere Dienstleister diese Daten erhält. Dabei werden üblicherweise nicht die Rohdaten (d.h. tatsächlich der Fensterzustand), sondern nur das Ergebnis einer Verarbeitung (z.B. „Fenster muss von außen geöffnet worden sein, da vorher keine Präsenz im Raum erkannt wurde“) weitergegeben.

Man braucht nicht viel Fantasie, um zu erkennen, dass diese Daten ausgesprochen interessant für den kriminellen Missbrauch sind. Für Einbruchsbanden wäre es extrem hilfreich zu wissen, wann und wie

lange Personen abwesend sind und ob zeitlich sogar ein Fenster offen oder zumindest gekippt ist. Diese Missbrauchsgefahr wirkt sicher bremsend, aber wird den erwähnten Trend nicht komplett verhindern. Dass Nutzer bereit sind, Daten über sich preiszugeben – obwohl man regelmäßig von Datenklau und –missbrauch liest – sieht man an den zunehmenden Nutzerzahlen von Facebook, Google, Amazon Echo („Alexa“) & Co.. Man kann nur hoffen und appellieren, dass die Betreiber der cloudbasierten IoT-Plattformen vertrauenswürdig sind und ausreichende IT-Schutzmaßnahmen ergreifen.

Dass der beschriebene Trend keine Utopie ist, zeigen folgende, nicht vollständige, Beispiele:

- Beispiel für die Weitergabe von Daten an einen Versicherer/Sicherheitsdienstleister: Der Versicherer ERGO bietet in Kooperation mit der Deutschen Telekom einen Schutzbrief gegen Einbruch-/Wasserschäden
- Beispiel für eine Online-Plattform, die von Firmen nutzbar ist: Microsoft Azure
- Beispiel für Software, mit der eine eigene Online-Plattform betrieben werden kann: Software „Niagara“ der Firma Tridium
- Beispiel für eine lokales Gateway: Amazon Echo („Alexa“)

Systemarchitektur

Abbildung 1 zeigt die dazu nötige Systemarchitektur. Im Gebäude wird ein Controller oder womöglich auch nur ein Gateway benötigt. Über dieses Gerät können alle Sensoren und Aktoren im Gebäude (also Fensterkontakte, Präsenzmelder etc. aber auch Aktoren) mit der im Internet positionierten IoT-Plattform kommunizieren. Die Anbindung der Sensoren/Aktoren an Controller/Gateway erfolgt zunehmend über funkbasierte Systeme – alternativ ist auch eine kabelbasierte Anbindung denkbar.

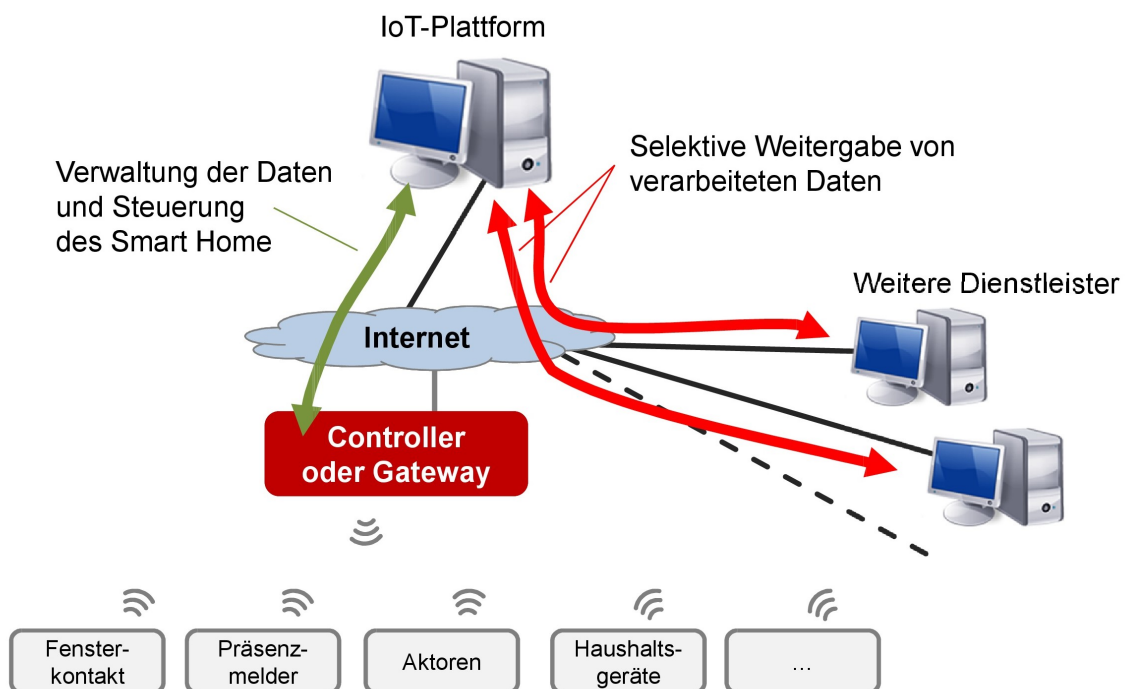


Abbildung 1: Systemarchitektur IoT-Plattform

Der Unterschied zwischen Controller und Gateway ist folgender: Ein Controller kann auch eigene Regeln/Funktionen ausführen (d.h. „Licht an“ bei Tastendruck) und ist die übliche Variante. Ein Gateway hingegen vermittelt nur die Kommunikation zwischen Sensoren/Aktoren und IoT-Plattform.

In Abbildung 1 ist im unteren Bereich bewusst ein Block für „Haushaltsgeräte“ aufgenommen worden. Nehmen wir als Beispiel den Herd: Wenn ein Online-Shop wüsste, wie oft bei Ihnen gekocht wird (bzw. auch was), könnte er viel gezielter Werbung für Rezeptbücher oder passende Lebensmittel/Gewürze etc. machen. Wer hier der Phantasie freien Lauf lässt, wird noch auf viele weitere „Geschäftsmodelle“ kommen. Dabei ist das nicht auf das private Gebäude beschränkt. Auch die Nutzungsdaten von Kaffeemaschinen in der Cafeteria oder dem Drucker/Scanner/Kopierer im Büro können wertvolle Daten liefern ...

Konsequenzen

Als konkreter Tipp gilt zunächst, sich dieser Entwicklung bewusst zu sein und entsprechende Marktentwicklungen und Produktangebote wahrzunehmen.

Womöglich macht es auch Sinn, bei zukünftigen Installationen zu berücksichtigen, dass eine spätere Anbindung an eine IoT-Plattform möglich sein muss (falls diese später benötigt wird). Entscheidend für eine Einbindung in eine IoT-Plattform wird sein, dass der Controller das entsprechende Protokoll spricht – sinnvoll wäre hier eine Unterstützung von MQTT und/oder RESTful services (http, JSON etc.).

Bei Interesse zu exemplarischen Aufbauten unterstützen wir (IGT - Institut für Gebäudetechnologie) Sie gerne. Sei es bei der exemplarischen Anbindung von lokalen Controllern/Gateways in eine existente cloudbasierte IoT-Plattform oder der exemplarische Aufbau einer eigenen IoT-Plattform. Kontaktieren Sie uns gerne unter: info@igt-institut.de

Über das Institut für Gebäudetechnologie

Das IGT (Institut für Gebäudetechnologie GmbH) ist ein unabhängiges Institut im Umfeld energieeffizienter Gebäude mit dem Fokus auf Gebäudeautomation und Energiemanagement. Der Schwerpunkt liegt darin, das Thema Gebäudeautomation über pragmatische Vorgehensweisen und Hilfsmittel für die Praxis anwendbar zu gestalten. Wir bieten hierzu Weiterbildungsveranstaltungen, Planung und Beratung, Gutachten und weitere Dienstleistungen an.

IGT - Institut für Gebäudetechnologie GmbH

Prof. Dr. Michael Krödel
Telefon: 089 / 66 59 19 73
Mail: info@igt-institut.de
Web: www.igt-institut.de