Internet of Things – noch ist vieles offen

David Lämmler, Dipl. Ing. FH

Das Internet of Things wird der Hype, die Neverending Story der nächsten Jahre sein. Schätzungen gehen davon aus, dass alleine in der Arbeitswelt bis ins Jahr 2022 über 14 Milliarden IoT-Geräte im Einsatz und vernetzt sein werden. Hinzu kommen IoT-Geräte im Heim-, Freizeit- und Gesundheitsbereich, die in der Cloud und auf den persönlichen Mobiles und Tablets eingebunden sind. Ist das sinnvoll, zuverlässig und vor allem: sicher?

> *Definition*
> *Das Internet der Dinge oder Internet of Things (IoT) bezeichnet reale, meist miniaturisierte Objekte, die den Menschen bei seinen Tätigkeiten unbemerkt unterstützen. Ausgestattet mit Sensorik und verknüpft über Netzwerke, misst und präsentiert das Internet of Things eine Vielfalt von Daten und steuert Vorgänge mit einer eigenen Intelligenz, ohne aufzufallen. Es ist einfach da und unglaublich praktisch.*

Das Internet der Dinge wird die Wirtschaft und unser Leben verändern. Verbunden mit einer enormen Datenmenge, die mit intelligenten Algorithmen ausgewertet werden, wird die Sensorik der IoT-Devices Zustände und Verhalten bis ins kleinste Detail vorhersagen und steuern können. Der Einsatzbereich ist fast unbegrenzt: Automobilindustrie, intelligente Fertigung, Wearables, Medizintechnik, Gebäude- und Heimautomatisierung, Smart Cities und vieles mehr.

Grosser zu erwartender Nutzen

Das IoT entlastet uns von der Informationsflut. Es denkt an Dinge, die wir vergessen oder noch gar nicht in Betracht gezogen haben. Es erleichtert uns die Arbeit und den Alltag. Ältere Menschen können länger zu Hause wohnen, Krankheiten werden frühzeitig erkannt und Kinder sicher in die Schule begleitet. Dieser Nutzen hat aber auch seine Kehrseite: Das Ausliefern persönlicher Daten jeglicher Art. Nutzniesser sind letztlich nicht nur das Individuum selbst, sondern auch der Staat und die Wirtschaft. Der Missbrauch von IoT ist nicht auszuschliessen; in Anbetracht der Datenmenge und der Anzahl IoT-Beteiligter sogar sehr wahrscheinlich.

IoT bringt unserer digitalisierten Welt ein weiteres Element zur subtilen Beeinflussung des Menschen und seines Verhaltens.

Keine Standards

Um komplexe Dinge zu vereinfachen und zuverlässig in Betrieb zu halten, sind technische Standards und definierte Architekturen unabdingbar. Als neue Technologie und aufgrund seines extrem breiten Anwendungsspektrums ist IoT aber noch weit entfernt von einer allgemein akzeptierten Standardisierung. Sie fehlt in der Kommunikation ebenso wie bei der Datenspeicherung und -auswertung und nicht zuletzt im Berechtigungswesen.

Etablierte Unternehmen wie Microsoft oder Intel versuchen, über Normengremien wie die Open Connectivity Foundation (OCF) Standards zu etablieren. In Wahrheit geht es ihnen allerdings eher darum, ihre beherrschende Marktstellung auszubauen. Nicht dabei sind nämlich die wirklichen Vorreiterfirmen wie Raspberry Pi Foundation oder der Chiphersteller ARM.

Die Vielfalt von Geräten und Anbietern und das Basteln an eigenen Standards werden somit weiterhin zunehmen – eine schlechte Ausgangslage für die Sicherheit und die Marktverbreitung. Zweckmässige und offene Standards bleiben eine der grössten Herausforderungen der IoT, und das wird sich wohl auch in Zukunft nicht ändern.

Viel Kommunikation

IoT-Geräte müssen untereinander, im internen Netzwerk und in der Cloud kommunizieren können. Zum Einsatz kommen nicht nur bekannte, standardisierte Kommunikationstechniken wie WLAN oder Bluetooth. Neu dazu kommen IoT-Systeme mit Funknetzen in jedem erlaubten Frequenzbereich und mit eigenen Verbindungsprotokollen. Um diese eigene Welt mit dem Internet zu verbinden, sind Gateways und Controller notwendig. Diese oft proprietären Devices verdienen leider vielfach das Prädikat: billiger Mist.

Die Qualität und Vielfalt der Kommunikation überfordert die Integratoren, sei dies auf Seiten der Benutzer oder seitens der IT-Dienstleister. Wer in den eigenen vier Wänden von der Audio-Anlage über die Lichtsteuerung bis zum Start der Waschmaschine ein durchgängiges System hat, darf sich glücklich schätzen. Wer für dessen Bedienung nur eine einzige App benötigt, ist ein seltener Glückspilz, und wer über eine bidirektionale Kommunikation sogar eine Rückmeldung über den Zustand des ausgeführten Befehls bekommt, ist endgültig im IoT-Paradies angekommen.

Mit dem Internet of Things hat sich eine Marktnische für professionelle Integratoren geöffnet, da die IoT-Anbieter ihre jeweils eigenen Apps einsetzten. Dies führt schnell zu vielen Apps, die auch noch unterschiedlich zu bedienen sind. Über eine Middleware greifen die Integratoren nun auf die unterschiedlichen Systeme, auf Gateways und sogar auf die Cloud zu. Sie sammeln die Informationen und bereiten diese zentral sowie benutzerspezifisch in Form nur einer App auf; ein wahrer Segen für die Benutzer und für die Usability.

Kaum Sicherheit

Viele IoT-Devices und -Implementationen erfüllen heute nicht einmal annähernd die Sicherheits-Standards einer Best Practice oder Good Privacy. Unsorgfältig auf die Schnelle programmiert und auf den Markt geworfen, sind sie die Einfallstore für Hacker. Die Firmware für das Stopfen von Sicherheitslücken muss praktisch ausnahmslos von den Benutzern eingespielt werden. Und von wem? Vom 13-jährigen Teenie oder dem 70-jährigen Grossvater? Das ist wohl beides illusorisch. Hinzu kommen Default-Passwörter auf den IoT-Geräten und Gateways, die der Benutzer nicht geändert hat. Diese Passwörter lassen sich praktisch ausnahmslos auf den Webseiten der Geräteanbieter im Internet finden und sind bei Hackern äusserst gefragt. Auf den Tausenden gehackten Devices lassen sich in der Folge BotNets aufbauen und schliesslich

andere Systeme wie Internetseiten in übelster Weise und weltweit kompromittieren. So geschehen im Oktober 2016, als der Hackerangriff Avalanche über eine BotNet-Struktur weltweit für Aufruhr sorgte.

Von vielen Unternehmen, die IoT-Produkte auf den Markt bringen, darf man heute eines sagen: Sie wissen nicht, was sie tun. Auch hier gilt die seit Jahrzehnten gültige Direktive im IT-Markt: Für eine sichere und stabile Implementation braucht es ein professionelles Systemdesign und viel Erfahrung. Die eigene IoT-Idee zu skizzieren und als programmierte App einzukaufen, reicht nicht. Gefragt sind das Verständnis für die Technologie, das Know-how für die Integration der IoT-Geräte und -Systeme und nicht zuletzt eine professionelle Implementation in die benutzerfreundliche App. Als Sicherheitsmassnahmen bieten sich standardisierte Architekturen wie Mutual Authentication mit Zertifikaten und Trustet Network Connect an. Die Firmware muss automatisch die Upgrades erhalten und Installationen ohne sichere Passwörter sind systemseitig zu unterbinden.

Als Benutzer wünsche ich mir eine IoT-Welt, die mich wie ein selbstfahrendes Auto von der ermüdenden Tätigkeit des Fahrens entlastet, die Gefahren vermeidet und Unfälle verhindert. Dies in einer Wohlfühl-Umgebung und in einer privaten Atmosphäre, weder überwacht noch bevormundet.

Ich lasse es offen, ob all das mit IoT gelingen wird. Bei den aktuell verfügbaren Produkten fahre ich aber noch lieber selber.