Neue Zürcher Zeitung

Internet of Things und Privatsphäre

Kühlschrank verkauft Passwort

GASTKOMMENTAR / von Jean-Marc Hensch / 11.1.2017, 05:30 Uhr

Ein Kühlschrank, der selbst den Nachschub bestellt. «Smarte» Geräte sind ja eine feine Sache, aber was passiert mit den Daten, welche diese Geräte «en passant» über mich sammeln? Diese sagen über eine Person fast mehr aus als deren E-Mail-Verkehr.

Es ist ja durchaus komfortabel, wenn vor dem Wochenende mein Kühlschrank automatisch erkennt, dass mein Biervorrat bald zur Neige geht. Er bestellt gleich Nachschub. Vorher hat er in meinem Outlook-Kalender nachgeschaut, ob ich Gäste erwarte, und weiss, ob sie überhaupt Bier trinken und welche Biermarke sie bevorzugen. Vor der Party senkt der Kühlschrank die Temperatur um ein paar Grad, damit das Bier dann auch schön kalt ist.

Zugegeben, dies ist ein recht prosaisches Beispiel für die Möglichkeiten des Internet of Things (IoT). Aber es zeigt sehr anschaulich, worum es geht: Maschinen und sogar Dinge (wie Kühlschränke und Bierflaschen) kommunizieren autonom miteinander und lösen Handlungen aus, in unserem Fall die Bestellung oder die Kühlung. Dafür braucht es somit vier Komponenten: eine eindeutige Identifikation einzelner Objekte, Sensoren für die Erfassung der Aussenwelt, Aktuatoren für die Steuer- und Regeltechnik und eine Vernetzung aller Objekte untereinander über das Internet.

Pionier- und Experimentierphase

Werden wir bald nur noch von «smarten» und «intelligenten» Dingen umgeben sein, welche uns sämtliche Routinetätigkeiten abnehmen? Die Technologie ist da, aber unser Umgang damit ist noch bei weitem nicht klar. Wir befinden uns nach wie vor in einer Pionier- und Experimentierphase. Viele Produkte, die heute für den Markt lanciert werden, werden den Hype nicht überleben.

Dies hat insbesondere mit fehlenden Standards zu tun. In welcher Sprache kommunizieren die Geräte: mit «IOTDB», «RAML», «SENML» oder «LsDL»? Oder mit einer anderen Sprache? Dies wird die Industrie allerdings regeln, entweder durch Verdrängung oder Kooperation. Als viel wichtiger betrachte ich jedoch die Herausforderungen, die sich beim Datenschutz stellen. Hier sind zwei Ebenen zu unterscheiden:

Einerseits stellt sich die Frage, was mit den Daten passiert, welche diese Geräte «en passant» über mich sammeln. Diese sagen über mich und mein Leben fast mehr aus als mein E-Mail-Verkehr. Wer sich über die Vorratsdatenspeicherung empört, möchte nicht, dass solche Daten in unbefugte Hände gelangen und gegen ihn oder ohne seine Einwilligung verwendet werden. Es geht den Kühlschrankhersteller doch nichts an, wie oft und wie viel Bier ich trinke!

die Hersteller tun gut daran, sich intensiv der Standardisierung, dem Schutz der Privatsphäre und der Verhinderung von Hacking zu widmen.

Möchten die Hersteller aus der Nische der Technikfans ausbrechen und das breite Publikum erreichen, kommen sie nicht darum herum, hier stringente Regeln aufzustellen und entsprechende Garantien abzugeben. Privacy muss zum Verkaufsargument werden. Damit dies gelingt, braucht es aber auch mündige Konsumenten, welche genau dies einfordern.

Ein weiteres Problem besteht darin, dass der Masseneinsatz von IoT-Chips nur möglich ist, wenn die Anwendung und der Einsatz möglichst einfach und günstig sind. Die Chips werden in ganz unterschiedlichen Produkten verbaut, welche letztlich zum Konsumenten gelangen. Wer kümmert sich darum, dass bei einer neuen Technologiegeneration ein Update vorgenommen wird? Oder wenn das Kommunikationsprotokoll ändert?

Die Gefahr, gehackt zu werden, ist real

Und zuletzt gilt es zu beachten, dass IoT-Geräte eigentlich vollwertige Computer sind, welche über das Internet erreichbar sind. Die Gefahr, gehackt zu werden, ist nicht theoretisch: Kürzlich wurde nachgewiesen, dass ein Angriff auf ein System durch ein Bot-Netz durchgeführt wurde, das aus «intelligenten» Glühbirnen bestand, welche sich gegenseitig infiziert hatten. Und was passiert, wenn ich meine Heizung nur noch gegen ein Lösegeld in Bitcoins anwerfen kann?

Mir geht es nicht darum, auf Panik zu machen: IoT wird kommen und gewaltige Komfort- und Effizienzsteigerungen bringen. Aber die Hersteller tun gut daran, sich intensiv der Standardisierung, dem Schutz der Privatsphäre und der Verhinderung von Hacking zu widmen. Und den Konsumenten sei angeraten, in dieser Beziehung genau hinzuschauen, wenn sie sich mit «smarten» Geräten umgeben.

Jean-Marc Hensch ist Geschäftsführer des ICT-Anbieterverbands Swico.

Jahresrückblick
Dynamisch dem Ende entgegen
KOLUMNE / von Stefan Betschon / 20.12.2016, 05:30
Welches waren 2016 die wichtigsten Innovationen? Neben Berichten über elektrisierende Netzteile, irre gewordene Internet-Kameras und explodierende Smartphone-Batterien gab es auch gute Nachrichten.

Datenschutz und das «Persönliche»
Wo beginnt die Privatsphäre?
GASTKOMMENTAR / von Thomas Geiser und Ursula Uttinger / 1.11.2016, 16:30
Es gibt einen rechtlichen Anspruch auf Vergessen, dieser lässt sich aber nur noch sehr beschränkt durchsetzen, wenn Informationen einmal allgemein zugänglich sind.