Mittwoch, 11. Juli 2018, 10:00 Uhr
~5 Minuten Lesezeit

Alles wird intelligent

Das Internet der Dinge macht unsere Umgebung „intelligent“. Doch um welchen Preis?

von Wolfgang Romey
Foto: Billion Photos/Shutterstock.com

Wenn viele Dinge in meinem Haushalt nicht gleich „intelligent“ werden, so werden sie doch zumindest jetzt „smart“. Das ist das große Versprechen des Internets der Dinge oder – wie es im Werbeneusprech

heißen muss – des Internet of Things (IoT). Was ist von diesem Versprechen zu halten?

Früher hätte man das, was die Dinge im IoT machen, meistens als „Steuern“ oder „Regeln“ bezeichnet. Die Wassertemperatur meiner Dusche oder die Wärme in meiner Wohnung können schon lange geregelt werden, bei Dusche oder Heizung ist nicht die Spur von Intelligenz dazu nötig. Dass man heute in diesem Zusammenhang von Intelligenz spricht, zeigt, wie heruntergekommen die Verwendung dieses Begriffs mittlerweile ist. Aber ich will ja nicht kleinlich sein.

Schöne neue Welt

Seit einigen Wochen kann ich das Licht in meiner Duisburger Wohnung von Wolfsburg aus an- und ausschalten. Da die Lampen auch Kameras und Bewegungsmelder beinhalten, haben die Einbrecher keine Chance. Wenn ich aus dem Urlaub zurückkomme, stelle ich schon eine halbe Stunde, bevor ich da bin, die Heizung höher. Mein Kühlschrank und meine Kühltruhe wissen, wann Nachschub bestellt werden muss und erledigen das über das Internet. Mit einer Smartphone-App kann ich unterwegs nachprüfen, was vorhanden ist und ob etwas fehlt. Dankbar bin ich, dass mein neuer smarter Fernseher Sendungen oder Serien vorschlägt, die genau meinem Geschmack entsprechen, mein intelligenter Lautsprecher erledigt dasselbe für die Musik.

Ich war vollständig zufrieden.

Die neue Welt doch nicht so schön?

Einige Wochen lang lief auch alles wie gewünscht. Doch dann stellten sich merkwürdige Dinge ein: Mein Kühlschrank hatte 20 Dosen Hundefutter bestellt, obwohl ich doch eine Katze besitze. Die Heizung war heruntergeregelt, als ich nach Hause kam, obwohl ich die Temperatur wegen des frostigen Wetters ausdrücklich auf 22 Grad gestellt hatte.

Es wurde aber noch schlimmer: Die Tiefkühltruhe war abgetaut, obwohl die Kühlung einwandfrei arbeitete. Mein hochintelligenter Lautsprecher fing an, Volksmusik und Märsche zu spielen und machte sich über Gäste lustig. Dann wurde es extrem peinlich: Mein Fernseher spielte zu bester Kinderstunden-Sendezeit Pornos ab. Der Gipfel war erreicht, als ich vor wenigen Tagen von einem Besuch aus Mainz zurückkam und meine Wohnung verwüstet vorfand.

Wie kann das sein?

Das kann sein, *wenn Inkompetenz, Gleichgültigkeit oder Skrupellosigkeit bei den Herstellern und den Nutzern in beliebiger Kombination vorhanden sind.*

Jedem, der sich auch nur ein wenig mit dem Internet auseinandersetzt, muss bekannt sein: Alle Geräte, die mit dem Internet verbunden oder über Funk erreichbar sind, sind ständig vielfältigen Angriffen ausgesetzt. Eine ganze Reihe von Vorfällen ist bekannt geworden (1):

- Kraftfahrzeuge sind aus der Ferne geöffnet oder gesteuert worden.
- Sogenannte Bot-Netze, das heißt Netze, die aus einer Fülle von EDV-Geräten gebildet werden, sind enttarnt worden. Diese Netze werden zu umfangreichen Angriffen auf Rechenanlagen eingesetzt (2).
- Fernseher versenden hinter dem Rücken der Anwender in großem Umfang Daten zu den Sehgewohnheiten oder übertragen Bilder aus der Wohnung der Zuschauer. Es ist beispielsweise beobachtet worden, dass ein sogenannter Smart-TV sich während 15 Minuten Betriebszeit mit etwa 700 Adressen im Internet verbunden hat (3).
- Es ist bei einer drahtlosen Videokamera gelungen, über 200.000 Passwörter und die Adressen anderer Kameras desselben Herstellers auszuspähen, sich mit diesen Kameras zu verbinden und die von ihnen aufgenommenen Bilder und Töne abzugreifen (3).
- Ein „smarter“ Lausprecher hat ohne Wissen und Mitwirkung des Nutzers ein Gespräch mitgeschnitten und die Ton-Datei an eine E-Mail-Adresse versandt (4).
- Es könnte noch eine Vielzahl weiterer Fälle angeführt werden (5).

Das alles ist möglich, weil Sicherheit für die Hersteller meistens nur ein zusätzlicher Kostenfaktor ist. Da den allermeisten Käufern Sicherheit nicht wichtig ist oder ihnen mögliche Konsequenzen nicht bewusst sind, sparen sich die Hersteller die Ausgaben. Die in den Geräten arbeitende Software ist deshalb oftmals nachlässig programmiert oder sogar gezielt mit Sicherheitslücken versehen, was dem Missbrauch Tür und Tor öffnet.

Der Programmcode ist zudem in der Regel nicht einsehbar, sodass die Suche nach Fehlern und Sicherheitslücken sehr aufwendig ist. Werden sie gefunden, werden sie meist nicht von den Herstellern behoben oder sie sind nicht zu beheben, weil die Programme fest in die Hardware der Geräte eingeschrieben sind. Sollen die Kunden doch die neue Version des Gerätes kaufen; diese kommt dann allerdings in der Regel mit neuen Schwachstellen daher.

So entsteht im „smarten“ Home eine Infrastruktur, die die Ausforschung und Überwachung der dort lebenden Menschen erlaubt, durchsetzt mit Sicherheitslücken, die von Kriminellen genutzt werden können. Das Bedrückende daran ist, dass die Bürgerinnen und Bürger aus Gleichgültigkeit oder Unkenntnis am Aufbau aktiv mitwirken.

Ein weiterer Aspekt, der ebenfalls fast unbeachtet bleibt, sind die für Herstellung, Betrieb und Entsorgung der Geräte notwendigen Ressourcen. *Dass Milliarden dieser Geräte zukünftig genutzt werden sollen, wird wesentlicher Teil von Energievergeudung und Umweltzerstörung sein.*

Was tun?

Das Wichtigste ist, zunächst zu prüfen, was von den „smarten“ Eigenschaften wirklich notwendig oder wenigstens nützlich ist. Muss ich wirklich die Heizung aus der Ferne regeln oder das Licht an- und ausschalten? Brauche ich ein Türschloss, das mit dem Smartphone bedient werden kann? Ist es nicht schöner, selbst in den Kühlschrank zu schauen und zu überlegen, was ich einkaufen möchte? Brauche ich den durch Sprache steuerbaren digitalen Assistenten wirklich? Muss mein Fernseher unbedingt mit dem Internet verbunden sein? Sind es diese Eigenschaften wert, sich unter Umständen gefährliche Sicherheitslücken ins Haus zu holen?

In vielen Fällen wird die Antwort „nein“ sein; dies ist noch mehr der Fall, wenn man sich zusätzlich bewusst macht, dass man einen Beitrag zur Schonung der Umwelt leistet, wenn man sich diese Geräte nicht beschafft.

Quellen und Anmerkungen

(1) **https://www.schneier.com/blog/archives/2017/02/security_and_th.html** (https://www.schneier.com/blog/archives/2017/02/security_and_th.html)
(2) **https://www.heise.de/security/meldung/Neues-Botnetz-ueber-IoT-Geraete-3867237.html** (https://www.heise.de/security/meldung/Neues-Botnetz-ueber-IoT-Geraete-3867237.html)
(3) **https://www.privateinternetaccess.com/blog/2018/06/maybe-smart-devices-are-too-clever-they-know-all-about-your-facebook-friends-and-can-spy-on-you-and-your-family/** (https://www.privateinternetaccess.com/blog/2018/06/maybe-smart-devices-are-too-clever-they-know-all-about-your-facebook-friends-and-can-spy-on-you-and-your-family/)
(4) **https://www.theregister.co.uk/2018/05/24/alexa_recording_couple/** (https://www.theregister.co.uk/2018/05/24/alexa_recording_couple/)
(5) **https://freedom-to-tinker.com/2018/04/23/announcing-iot-inspector-a-tool-to-study-smart-home-iot-device-behavior/** (https://freedom-to-tinker.com/2018/04/23/announcing-iot-inspector-a-tool-to-study-smart-home-iot-device-behavior/)

Dieser Artikel erschien bereits auf www.rubikon.news.

Wolfgang Romey arbeitete nach dem Studium der Theoretischen Elektrotechnik als Lehrer für Mathematik, Elektrotechnik und Digitaltechnik im Berufsbildenden Bereich, später als Lehrerausbilder im Vorbereitungsdienst, dem Referendariat. Dann folgte ein Wechsel in die Bezirksregierung Düsseldorf als Dezernent für Lehrerausbildung und später auch -fortbildung. Er verfügt über etwa 20 Jahre Erfahrung darin, angehende Lehrerinnen und Lehrer auf die Bildungsarbeit mit Digitalen Medien vorzubereiten und deren Urteilskraft in diesem Feld zur Entfaltung zu verhelfen. Die kritische Auseinandersetzung mit den dramatischen Folgen der Digitaltechnik, die ihm extrem unterentwickelt scheint, ist bis heute sein Thema.

Dieses Werk ist unter einer **Creative Commons-Lizenz** (**Namensnennung - Nicht kommerziell - Keine Bearbeitungen 4.0 International** (https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de)) lizenziert. Unter Einhaltung der Lizenzbedingungen dürfen Sie es verbreiten und vervielfältigen.