



Wer nicht testen will, muss fühlen!

Manche Erfahrungen muss man selbst machen. Wir mussten alle mal an eine heiße Herdplatte greifen oder eine Treppe herunterfallen. Unsere Eltern hatten die gleichen Experimente schon gemacht und uns gewarnt. Aber das konnte uns nicht aufhalten. Denn manche Dinge lernt man nur, wenn es weh tut.

Hersteller von IoT-Geräten haben offenbar ein ähnliches Bedürfnis, schmerzliche Erfahrungen selbst zu machen. Im Internet der Dinge laufen miniaturisierte Computer mit PC-Technik von vor 20 Jahren. Die Veteranen aus der Frühzeit des Internet mahnen vor den Sicherheitslücken aus ihrer Jugend, aber die jungen IoT-Entwickler wollen selbst erfahren, wie schutzlos unverschlüsselte Funkprotokolle sind oder wie schnell Hacker Geheimnisse aus der Firmware pflücken.

Blöd nur, wenn den Schmerz zu den Fehlern nicht die Hersteller, sondern die Kunden zu spüren bekommen. Dann stellt sich nämlich kein Lerneffekt ein. Und ohne den verhalten sich die Hersteller wie Kinder: Sie wollen Saltos schlagen, bevor sie laufen können. Beispielsweise bauen sie Alarmanlagen, die nebenbei Thermostate steuern und Steckdosen schalten, dafür aber Einbrecher nicht fernhalten. Eine für Replay-Attacken anfällige Smart-Home-Alarmanlage ist wie die Erfindung des Elektromotors vor der des Rads: Ein potenziell cooles Ding, das so aber niemand braucht.

In Anbetracht so gravierender Fehler bei einer Branche, deren Geschäft die Sicherheit ist,

bekomme ich Angst vor den vielen "smarten" Geräten. Wie viele von denen werden WLAN können statt der Funktion, für die sie verkauft werden? Dass mit dem Internet auch die Hacker Einzug in Waschmaschine, Kühlschrank, Zahnbürste und Staubsauger halten, scheint unausweichlich. Ob meine Waschmaschine statt Buntwäsche dann stundenlange Kochwäsche macht, außer ich bezahle ein paar Bitcoins? Wird es eine Locky-Version geben, die meine Kühlschranktür verschließt? Möchte ich noch Zähne putzen, wenn auf der Bürste ein Trojaner läuft? Und welche Botschaft saugt der Saugroboter in den Staub, wenn seine Forderungen nicht erfüllt werden? Langweilig wird 2017 jedenfalls nicht.

Ein Ende dieser Misere gibt es nicht, solange die Kunden die Schmerzen für sich behalten. Nur wenn Hersteller und Entwickler für jede Sicherheitslücke eine kräftige Ohrfeige bekommen, haben sie eine Chance, aus ihren Fehlern zu lernen. Schreiben Sie den Herstellern doch mal eine wütende Mail, wenn die Firmware abstürzt. Oder posten Sie beim nächsten Virus eine Warnung in sozialen Medien. Im Idealfall machen die jungen IoT-Hersteller ihre Fehler dann immer nur einmal – so wie wir damals mit der Herdplatte und der Treppe.

*Johannes Merkert*

Johannes Merkert