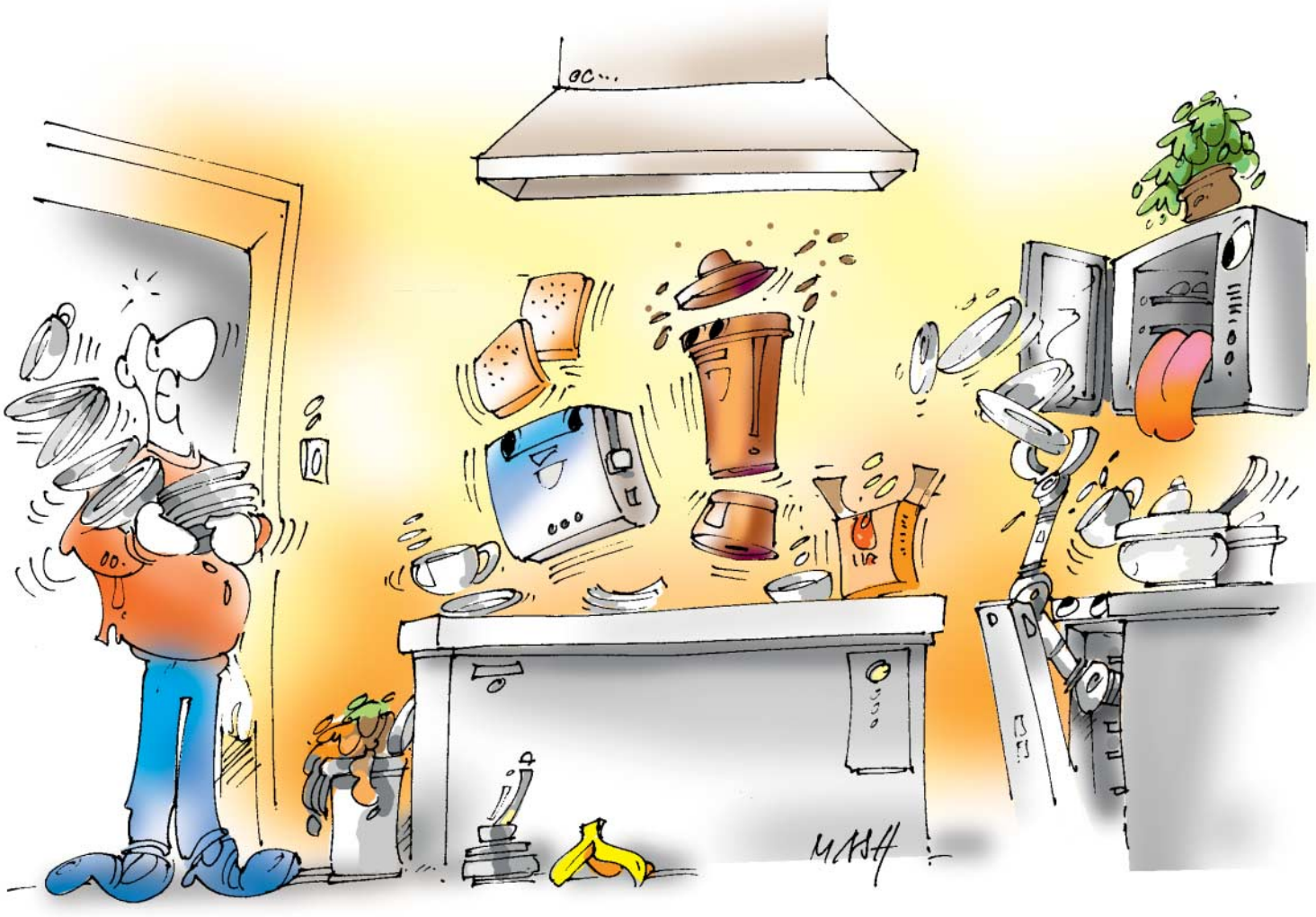

Dinge, denen wir vertrauen können

VW-Diesel stoßen auf dem Prüfstand weniger Schadstoffe aus und Samsung-Fernseher spielen Testfilme besonders energiesparend ab. In beiden Fällen steuert ausgefeilte Software den Betrug – und zwar nicht irgendwelche Software, sondern Closed Source Software. Denn erst die Tatsache, dass da keiner ohne Weiteres reinschauen konnte, gab den Herstellern die (letztlich doch trügerische) Sicherheit, es käme ihnen schon keiner auf die Schliche. Mit quelloffener Software hätten sie sich das gewiss nicht getraut.

Diese Fälle zeigen vor allem eines: Wir können uns nicht auf die Ehrlichkeit der Hersteller verlassen. Wie soll das erst werden, wenn das Internet der Dinge wirklich kommt? Wenn Ihr Stromzähler, Ihr Kühlschrank und Ihre Kaffeemaschine „intelligent“ werden? Wollen wir wirklich eine Zukunft, in der uns die Dinge um uns herum nach Strich und Faden verarschen?

Der einzige Weg, das noch zu verhindern, ist eine konsequente Offenlegung der Software, die auf diesen Dingen läuft. Zwar kann auch Open Source betrügen. Doch ist die Gefahr, dabei erwischt zu werden, so offensichtlich, dass sich die meisten Hersteller das wohl mindestens zweimal überlegen würden.

Nur mit Open Source bekämen wir die Möglichkeit, den Firmen bei dem, was sie tun, auf die Finger zu schauen. Und in einem Aufwasch gäbe es die Garantie, dass man auch ohne Mithilfe des Herstellers Updates entwickeln könnte, die beispielsweise Sicherheitslücken schließen.

Diese Transparenz ist eine essenzielle Grundvoraussetzung, damit ein allgegenwärtiges Internet der Dinge nicht zu einem Alptraum aus Beschiss und Spionage mutiert. Wir als Gesellschaft können uns Closed Source Software schlicht nicht mehr länger leisten.

Jürgen Schmidt