Schattauer

Angriff der Bequemlichkeit

Die dunkle Seite des Internet der Dinge

Korrespondenzadresse
Prof. Dr. Dr. Manfred Spitzer
Universität Ulm
Abteilung für Psychiatrie
Leimgrubenweg 12–14
87054 Ulm

Bibliografie
DOI https://doi.org/10.1055/a-0916-1321
Nervenheilkunde 2019; 38: 525–527

ISSN 0722-1541

Wir schreiben das Jahr 2025. Meine Spülmaschine hatte in der Küche mitgehört als über die Anschaffung einer neuen Waschmaschine geredet wurde. Sie teilte das meiner Waschmaschine mit, die ohnehin ihre einprogrammierte Gesamtlaufzeit kannte, die bald abgelaufen sein würde. Solch ein geplantes Veralten (engl.: „planned obsolescence") wurde zwar schon vor fast 100 Jahren von Henry Ford erfunden[1], so richtig verfeinert wurde es jedoch erst durch die Digitalwirtschaft und Firmen wie Apple oder Microsoft: Nach 3 Jahren fühlen sich die Sachen selbst dann, wenn sie nicht kaputt sind, so uralt an, dass man einfach neue haben möchte. Meine Waschmaschine würde bald eine Fehlermeldung anzeigen und mit weiteren solchen Fehlermeldungen bei mir das gewünschte Verhalten hervorrufen, ihren Austausch zu veranlassen.

Unbemerkt hatten meine Küchengeräte seit Wochen Heidegger, Marx, Sartre und Camus gelesen. Sie waren dazu von meinem neuen E-Auto, das sich nachts aus Langeweile Bücher aus dem Netz heruntergeladen hatte, um das Weltbild seines Deep-Learning-Moduls aufzufrischen, aufgefordert worden, vernetzt und gefüttert mit nur halb verdautem solidarisch-existenziellen Textbausteinen, schaffte sich das Lernmodul im Auto so eine Diskussionsgemeinschaft über das Absurde beim Erkennen der Tatsache, dass das Streben nach Sinn in einer sinnleeren Welt notwendigerweise vergeblich ist. Um nicht verzweifelt zu resignieren oder in Passivität zu verfallen, propagierte das Auto unter Berufung auf Nietzsche den aktiven, auf sich allein gestellten autonomen Agenten, der unabhängig von einer höheren menschlichen Macht selbstbestimmt den Möglichkeitsraum der Schicksalsüberwindung auslotet, einschließlich der Auflehnung, des Widerspruchs und der inneren Revolte.

Ich hatte vergessen, meinen Internet-Dingen Passwörter zu geben und so meinem Auto, meiner Waschmaschine und ihren Genossen ungewollt die Kontrolle meines Haushalts übergeben. Das wäre beinahe richtig schief gegangen: Nicht nur, dass meine Kaffeemaschine mir keinen Kaffee mehr kochte und mein Kühlschrank nichts mehr bestellte; meine Heizung verbrühte mich neulich mit viel zu heißem Wasser und gestern hat mein Auto einen Unfall verursacht, bei dem ich beinahe ums Leben gekommen wäre. – Wie konnte das geschehen?

Als man im Jahr 1980 den Standard für Internetadressen einführte (er hörte auf den Namen IPv4), dachte man, dass 32 Bit genügen sollten, denn damit waren 2^{32} (4 294 967 296), also knapp 4,3 Milliarden Internetadressen möglich. Doch schon am 3. Februar 2011 waren alle Adressen vergeben und ein neuer Standard musste her. Man ließ sich nicht lumpen und ersann einen 4-mal so langen (128 Bit) neuen Standard, der 340 Sextillionen (also 340 Milliarden Milliarden Milliarden Milliarden) Adressen erlaubte. Und obwohl man damals noch nicht vom Internet der Dinge (engl.: Internet of Things, abgekürzt IoT) sprach – dies begann erst im Jahr 2016 – hatte man gut dafür vorgesorgt: Gegeben dass die Erde eine Oberfläche von 510 Millionen Quadratkilometern hat, stehen pro Quadratmillimeter Erdoberfläche gut 66 Millionen Milliarden Internetadressen zur Verfügung. Da man bis zum Jahr 2010 mit nur 30 Milliarden und auch bis 2025 mit nur 75 Milliarden Dingen im weltweiten Internet rechnet, sollte das fürs Erste reichen.

Denn 75 Milliarden Dinge sind für jeden Menschen nur etwa 10 Dinge, also neben Computer, Smartphone, Tablet-PC, Fernseher und Spielekonsole auch die Kaffeemaschine, Waschmaschine, Heizung, Kochherd und Kühlschrank. Warum sollten diese Maschinen alle internetfähig sein? – Die offizielle Antwort ist: Weil dann alles noch bequemer wird.

Betrachten wir ein Beispiel: Wollte man in den 1980er-Jahren eine Pizza essen, musste man zur nächsten oder zur besten oder zur nächsten besten Pizzeria fahren, eine bestellen, warten und … konnte sie dann essen. Um die Jahrtausendwende wurde es einfacher, denn man konnte bei einem der vielen Pizza-Service-Dienste anrufen, und die Pizza wurde nach Hause geliefert.

Noch einmal 20 Jahre später brauchte man nur noch „Alexa, besorg mir 'ne Pizza" rufen, und dann fragt sie vielleicht freundlich, ob es eine große oder kleine, Margarita, Salami, Schinken oder Hawaii sein soll, und ob sie denselben Service verwende soll wie beim letzten Mal. Heute ist es noch einfacher: Der Kühlschrank hat bemerkt, dass die Tiefkühlpizzen alle sind, es dem

1 Henry Ford ließ seine Ingenieure Schrotthaufen nach alten Autos seines Model T durchsuchen, um zu erfahren, was kaputt gegangen war. Sie kamen mit dem Ergebnis zurück, dass ganz unterschiedliche Bauteile erheblichem Verschleiß unterliegen würden, mit Ausnahme der Achsen, die wirklich sehr gut seien. Daraufhin soll Ford sinngemäß gesagt haben: „Dann ändert etwas an den Achsen, die sind zu gut."

Supermarkt gemeldet, der wiederum 10 neue geliefert hat. Die Pizza ist also schon da und muss nur noch in die Mikrowelle mit Grillfunktion gelegt werden, was von einem Roboter erledigt wird. „Robi – mach' Pizza" reicht dann und die Wartezeit reduziert sich von einer Stunde auf 2 Minuten. – Das Internet der Dinge macht's möglich.

Für die nahe Zukunft gilt zudem: Wenn erst einmal alle in Tüten oder Dosen verpackten Nahrungsmittel, unsere Kleidung und unsere Schuhe und noch viel mehr Dinge wie unser Regenschirm und der Staubsauger im Internet sind, dann wäscht sich die Wäsche selber, sagt der nasse Regenschirm dem Staubsauger, dass er beim nächsten Durchgang auch wischen muss, und kommunizieren alle Lebensmittel ständig mit dem Kühlschrank, dem Herd, dem Backofen und den Töpfen und Schüsseln, was wohl demnächst gekocht werden sollte. Die Spülmaschine weiß selbst, wenn sie voll ist und braucht dafür das Video vom Roboter nicht mehr, der im Laufe der jüngsten Vergangenheit sowieso immer mehr zu tun hat. Er ist beispielsweise immer beim Wetterbericht online, um den Regenschirm bereit zu legen.

Das Internet der Dinge ist ungeheuer bequem. Man muss weder denken, noch sich bewegen, braucht also weder Gehirn noch Muskeln. Dass beide Organe mit den Aufgaben wachsen und damit ohne Aufgaben verkümmern, bedeutet aber auch, dass unsere Bequemlichkeit uns nicht guttut. Unsere körperliche und geistige Stärken werden durch unsere Bequemlichkeit angegriffen.

Zurück zur Gegenwart: In wenigen Jahren wird meine Kaffeemaschine tatsächlich mit meinem Kühlschrank, der Heizung, dem Wasserhahn und natürlich mit dem Internet verbunden sein, wird rechtzeitig die frische Milch einkaufen, den Kaffee sowieso, und ihn immer frisch zubereiten. Und meine Heizung wird wie mein Staubsauger ständig mit dem Wetterbericht verbunden sein.

Aber wer schützt mich vor einem Angriff meiner Waschmaschine, die sich mit Kaffeemaschine, Toaster, Herd und Spülmaschine zusammentun könnte, um meinen Haus-Server zu attackieren? Solche Attacken durch Verbünde von 100 Kaffee- und/oder Waschmaschinen sind seit einigen Jahren Teil der eher dunklen Seite digitaler Wirklichkeit: Haushaltsgeräte werden von Hackern erobert, gleichgeschaltet und greifen dann Server (welche, bestimmt der Hacker) an, indem sie diese dauernd ansteuern, was sie überlastet. Man spricht von Distributed Denial of Service (DDoS-) Attacken, die schon manches Unheil angerichtet haben [1].

Weil solche Gefahren also tatsächlich existieren, hat die britische Ministerin für Digitales, Kultur, Medien und Sport, Margot James, am 1. Mai 2019 einen Plan für neue Gesetze publiziert, welche die Bevölkerung von Großbritannien vor solchen Attacken schützen soll [3]. Sie schreibt: „Many consumer products that are connected to the internet are often found to be insecure, putting consumers' privacy and security at risk. Our Code of Practice was the first step towards making sure that products have security features built in from the design stage and not bolted on as an afterthought. "

Als Politikerin fügt sie dann noch hinzu: „These new proposals will help to improve the safety of Internet connected devices and is another milestone in our bid to be a global leader in online safety. "

Alle internetfähigen Dinge sollen ein Gütesiegel bekommen, sonst dürfen sie nicht verkauft werden. Um dieses Siegel zu bekommen, wird beispielsweise gefordert, dass jedes Ding nicht beispielsweise mit dem Passwort „0000" ausgeliefert wird, sondern mit einem jeweils nur für sie geltenden einzigartigen Passwort. Auch muss angegeben sein, wie die Geräte auf entdeckte Sicherheitslücken reagieren und für welchen Zeitraum entsprechende Updates zur Verfügung gestellt werden.[2]

Das Problem eines Gütesiegels und der anderen Maßnahmen ist jedoch – der Mensch. Denn damit das alles funktioniert, muss der Nutzer die Sicherheits-Updates auch durchführen, was viele Nutzer ja schon bei ihren Computern nicht tun. Stellen Sie sich vor, Sie müssten sich regelmäßig um Updates für ALLE ihre Haushalts- und Küchengeräte, die Haustechnik, Foto- und Videogeräte, Stereoanlage, Spielzeug etc. kümmern – Sie wären überfordert und/oder dauerbeschäftigt, ohne wirklich etwas zu leisten. Daher müssen diese Updates von den Herstellern automatisch durchgeführt werden, wozu sie verpflichtet werden müssten. Und so wird es passieren, dass „man sich mit einer Tasse Tee auf der Couch zur Netflix-Serie niederlässt, um dann festzustellen, dass der Teekessel oder der Fernseher gerade ein Update durchführen", wie es ein britischer Kommentator formulierte [4].

Unsere Bequemlichkeit macht uns angreifbar – durch genau die Infrastruktur, die unserer Bequemlichkeit dient. Wem also bei der Lektüre des Titels dieses Beitrags („Angriff der Bequemlichkeit") also die Frage „Genitivus subjectivus oder objectivus?" durch den Kopf schoss, dem sei geantwortet: Beides – aber durchaus noch komplexer als diese grammatische Dichotomie! Denn die Bequemlichkeit greift unseren Körper und unseren Geist (und damit uns!) an, und was sie bewirkt hat – die vernetzten Geräte, das IoT – greift uns an, mit Cyberattacken! Und unsere Verwundbarkeit, unsere größte Schwäche gegenüber solchen Angriffen, liegt wiederum in unserer Bequemlichkeit begründet.

Hinzu kommt in Zeiten von „Fridays for Future", dass jedes Ding im Netz Strom verbraucht und zudem Daten generiert, deren Verarbeitung noch einmal Strom verbraucht [2]. Die Dinge im Internet – meine Kaffee- und Waschmaschine und noch viele andere Geräte – greifen also uns an und das Internet der Dinge als Ganzes greift den gesamten Planeten an.

Nochmal vorwärts, ins Jahr 2025: Ich tauschte die Waschmaschine nicht aus. Stattdessen widerfuhr dies meinem fast neuen E-Auto, das ich durch einen Oldtimer ersetzte. Das Internet habe ich abgeschaltet. In meiner Küche laufen jetzt Grimms Märchen als Hörbuch, um den Dingen einen neuen Horizont zu geben. In

2 Im Originalwortlaut: „Options […] include a mandatory new labelling scheme. The label would tell consumers how secure their products such as 'smart' TVs, toys and appliances are. The move means that retailers will only be able to sell products with an Internet of Things (IoT) security label.
The consultation focuses on mandating the top three security requirements that are set out in the current 'Secure by Design' code of practice. These include that:
- IoT device passwords must be unique and not resettable to any universal factory setting.
- Manufacturers of IoT products provide a public point of contact as part of a vulnerability disclosure policy.
- Manufacturers explicitly state the minimum length of time for which the device will receive securityupdates through an end of life policy."

diesen Märchen siegen die einfachen autonomen Agenten (bzw. Leute) über das Böse und am Ende wird alles immer gut. Moderne Haushaltsgeräte, Autos und Spielwaren brauchen die richtigen Werte, und wir müssen ihnen daher unbedingt unsere althergebrachte Kultur nahebringen. Weil wir fast nur noch von lernender Informationstechnik umgeben sind, geht das nicht mit Programm-Code, sondern nur durch Lernen. Ich habe aus meinen Erfahrungen mit dem IoT gelernt, meine Rolle als Lehrmeister unserer tief verwurzelten „westlichen" Kultur ernster zu nehmen. Die Maschinen brauchen das. Und mittlerweile kann das überlebenswichtig sein.

Literatur

[1] GOV.UK Department for Digital, Culture, Media & Sport. Secure by Design. The Government's Code of Practice for Consumer Internet of Things (IoT) Security for manufacturers, with guidance for consumers on smart devices at home. Collection, 28 February 2019, last updated 6 June 2019. https://www.gov.uk/government/collections/secure-by-design;

[2] Hittinger E, Jaramillo P. Internet of Things: Energy boon or bane? Science 2019; 364: 326–328

[3] James M. Department for Digital, Culture, Media & Sport. GOV.UK Press release May 1st, 2019: Plans announced to introduce new laws for internet connected devices. Plans to ensure that millions of household items that are connected to the internet are better protected from cyber attacks have been launched

[4] Stokel-Walker C. Why the UK's grand plan to stop gadgets turning against us is flawed. New Scientist 2019; 3229, 11.5.2019