Jeder ist angreifbar

Essay Über Hacker und die brüchigen Fundamente der Industrie 4.0

Von Frank Rieger

Die Säulen der Welt im anbrechenden Digitalzeitalter sind bröckelig. Die Technologien, auf denen die Vernetzung des Alltags und die Informationsströme der Wirtschaft beruhen, ähneln eher provisorischen Holzgestellen als soliden Stahlkonstruktionen. Meistens funktioniert alles – solange niemand an den Brettern rüttelt oder einen Balken durchsägt.

Nun sind aber auch Spione, Militärs und Kriminelle aller Art in der digitalen Sphäre angekommen. Und rütteln und sägen. Spätestens seit den Snowden-Enthüllungen darf es als Standardinstrument staatlicher und privater Spitzel gelten, Sicherheitslücken systematisch auszunutzen – oder sie sogar heimlich zu erzeugen. Wöchentlich gibt es neue Schlagzeilen über kriminelle Einbrüche in Onlineshops, Datingportale und Zahlungssysteme. Sie sind zur Normalität geworden. Doch was genau schiefgeht, welche Schwächen ausgenutzt und weshalb immer neue Sicherheitslücken aufgedeckt werden, dafür interessiert sich kaum jemand – weder in der Politik noch in der Wirtschaft.

Es herrscht ein Desinteresse an den Details der digitalen Welt, das fatal ist. Natürlich sind die Einzelheiten kompliziert. Das sind sie immer. Aber es geht in diesem Fall nicht nur um ein paar Schrauben, sondern um die Fundamente der modernen Wirtschaftswelt.

Hacker treibt eine tief sitzende Neugier an, alles über diese Details wissen zu wollen. Deshalb erforschen sie die wackeligen Technologiekonstruktionen. Deshalb wollen sie die Schwachstellen präzise kennen. Und so erwerben sie die Fähigkeiten, mit denen sie sich die technologischen Systeme untertan machen können.

Eine der wichtigsten Erkenntnisse von Hackern in den letzten Jahren ist dabei: Die Abwehr ist in der digitalen Welt die langfristig sinnvollere Strategie als der Angriff, auch wenn Letzterer meist viel einfacher ist.

Vor allem in Offensivmethoden zu investieren, wie es etwa Bundesverteidigungsministerin Ursula von der Leyen jüngst wieder propagierte, bringt letztlich nichts. Denn was hat man davon, über Mittel zur elektronischen Ausschaltung eines Gegners zu verfügen, wenn die eigene Infrastruktur verwundbar ist?

Eine Strategie der Abschreckung funktioniert im digitalen Raum auch deshalb nicht, weil es fast nie möglich ist festzustellen, von wem man gerade angegriffen wird. Ob hinter einer Attacke, die von einem chinesischen Server ausgeführt wird, der chinesische, der russische oder der amerikanische Geheimdienst steckt oder ob nur schnöde Onlinekriminelle am Werk sind – und ob diese vielleicht von einem ganz anderen Geheimdienst kontrolliert werden: Dazu sind verbindliche Aussagen kaum möglich. Folglich kann man auch niemandem sinnvoll mit Vergeltung drohen. Die „Cyberwaffen“ zielen ins Leere.

Wenn aber jeder ein Ziel und jeder verwundbar ist, dann ist der Zustand der digitalen Welt grundsätzlich ein unsicherer. Dann ist Abwehr die beste Verteidigung. Und aus dieser Erkenntnis heraus verbreitet sich in der Hackercommunity ein Gedanke immer weiter: die Lage endlich grundlegend zu verbessern.

Die Angreifbarkeit digitaler Systeme ist kein Naturgesetz. Sie beruht ganz einfach auf schlecht geschriebener Software. Wer programmiert, macht Fehler. Es ist kein Hexenwerk, diese Fehler zu verhindern oder Schwachstellen, die durch sie verursacht wurden. Es ist nur teuer und aufwendig.

Um eine grundlegende Änderung zu erreichen, ist eine umfassende Erneuerung nötig. Die Fundamente der Informationsgesellschaft müssen langfristig neu gebaut werden. Und möglich wäre das. Technologien, die von vornherein verhindern, dass sicherheitsrelevante Programmierfehler gemacht werden, sind in der Forschung weit entwickelt. Zudem gibt es sichere Programmiersprachen, automatische Methoden zur Softwareprüfung und Bausteine für sichere Betriebssysteme. Sie müssen nur in der Fläche den Weg in die Praxis finden – und das ist teuer.

Das Problem ist jedoch, dass die Digitalbranche nach wie vor auf ein möglichst hohes Innovationstempo bei gleichzeitiger Kostenreduktion setzt. Und der schnellste Weg, ein Produkt auf den Markt zu bringen, ist: ohne große Rücksicht auf mögliche Sicherheitsprobleme zu arbeiten. Und so schwanken alle weiter auf denselben wackeligen Holzgestellen und hoffen, dass diese nicht einstürzen.

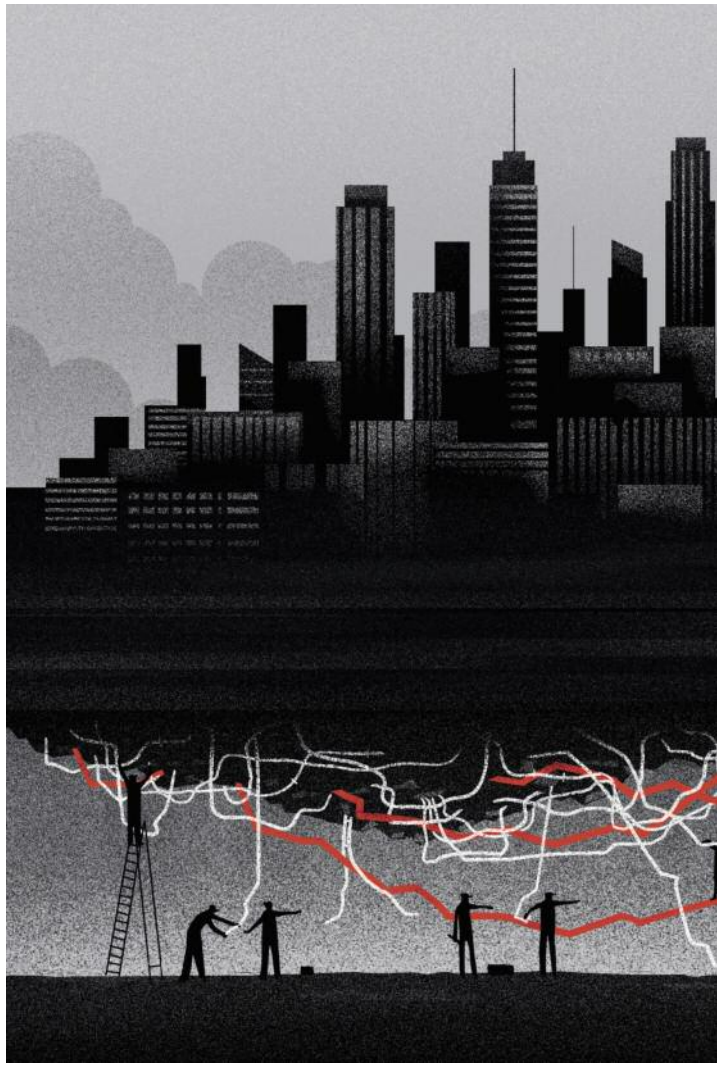

FOTO: DANIEL STOLLE

Die Aufgabe wird nicht kleiner. Im Vergleich zu dem, was wir heute kennen, wird schon in naher Zukunft die Abhängigkeit von digitalen Systemen exponentiell wachsen. Das Schlagwort vom Internet der Dinge bedeutet vor allem eines: Die Fallhöhe steigt dramatisch. Die IT-Zukunft wird nicht aus mindernützlichen Kuriositäten wie „intelligenten“ Kühlschränken bestehen. Sie wird vielmehr aus selbst fahrenden Autos, Altenpflegerobotern, mobiltelefonbasierten Bezahlsystemen, vernetzten Heizungen und Stromspeichern errichtet und aus Sensoren, die uns sagen, wie voll das Fitnessstudio und das Bürgeramt gerade sind. Alles was irgendwie vernetzt werden kann, wird vernetzt werden.

Industrie 4.0 bedeutet, dass Produktionsprozesse und Geräte, die bisher zwar computerisiert, aber weitgehend offline waren, ans Netz kommen. Aus der Sicht eines Hackers sind sie damit vor allem direkt angreifbar. Die bisherige Strategie der Konzerne lautet: Wir bauen erst einmal das Produkt, und dann können im besten Falle von uns bestellte Hacker schauen, wo die Schwachstellen sind.

Doch wenn heute etwa in einer Autofabrik eine neue Produktionsstraße überprüft wird, haben diese vom Unternehmen bestellten Angreifer meist leichtes Spiel. Die Werksingenieure sind häufig schon froh, wenn sie die komplexe Anlage überhaupt rechtzeitig zum reibungslosen Funktionieren bringen. Ihre Emotionen wechseln dann von staunendem Unglauben zu resignierender Verzweiflung, wenn die professionellen Hacker als sichtbaren Beweis ihres Erfolgs ein kleines Roboterballett ablaufen lassen oder die Antriebsmotoren plötzlich den Imperialen Marsch aus „Star Wars“ summen.

Im Lagebericht des Bundesamts für Sicherheit in der Informationstechnik wurde ein konkreter Schadensfall berichtet, der die Bedrohlichkeit deutlich aufzeigt: Ein Hochofen wurde von bösartigen Angreifern über das Netz so heruntergefahren, dass die Anlage schwer beschädigt wurde. Der Angriff könnte ein Menetekel für die digitale Zukunft der Industrie sein. Denn der Vernetzungsgrad der Industrieanlagen steigt schon heute rasch – auch ohne Industrie-4.0-Visionen. Und wenn beide Großprojekte – die Vernetzung der Industrie und des Alltags – auf dem heutigen erbärmlichen Niveau der IT-Sicherheit geschehen, dann werden die Meldungen über Sicherheitsschwankungen nicht länger bloß den Charakter eines irgendwie hinnehmbaren Grundrauschens haben.

Ein Vater der modernen Science-Fiction, Arthur C. Clarke, hat das Phänomen des allgemeinen Desinteresses an den Details der technisierten Welt mit den Worten beschrieben: „Jede hinreichend fortgeschrittene Technologie ist von Magie nicht zu unterscheiden.“

Es besteht die einmalige Chance, jetzt von Anfang an sichere, solidere Systeme zu bauen.

Noch vor zwei Jahrzehnten wäre uns das, was wir jeden Tag selbstverständlich benutzen, wie Magie erschienen. Wir haben große Teile des Wissens der Menschheit auf einem Gerät abrufbar, das in die Hosentasche passt. Mit ein paar Klicks kann man dafür sorgen, dass fast alles, was irgendwo in der Welt produziert wird, wenige Tage später an der Haustür erscheint. Wie das genau funktioniert, müssen wir nicht wissen. Die Magie wirkt schließlich fast immer.

In vielem ähnelt die Magie des Netzes damit einem anderen Wunder der modernen Zeit: den Trinkwasserleitungen. Wenn man den Hahn aufdreht, sprudelt, wie durch Zauberhand, Wasser heraus. In Gegenden mit guter Infrastruktur kann man es sogar direkt trinken. Der tatsächliche Zustand der digitalen Technologien entspricht aber eher dem des Wassernetzes einer Megametropole in der Dritten Welt mit schlecht gewarteten Rohren.

Es sieht übel aus in den Kellern des Netzes. Wenn wir uns die globale Informationsinfrastruktur als ein Gewirr von Druckwasserleitungen vorstellen, dann sind Techniker rund um die Uhr damit beschäftigt, sie zu flicken. Es spritzt an allen möglichen Stellen heraus, aber es gibt nur Heftpflaster für die Leckstellen. Die Heftpflaster sind das, was man heute als „IT-Sicherheitstechnologien“ angeboten bekommt. Und am Ende geht es den Verkäufern von Sicherheitssoftware nur darum, dass sie die Rohre wenigstens ein Weilchen halbwegs dicht halten – und mit möglichst innovativen Heftpflastern Geld verdienen.

Diese De-facto-Kapitulation der IT-Sicherheit ist für niemanden in der Branche ein Geheimnis. Die marktführende Antivirus-Firma Symantec gestand jüngst ein, dass Antivirus-Software weniger als die Hälfte aller Angriffe erfassen kann. Gegen Angreifer, die über Motivation und Ressourcen verfügen, gibt es angesichts der Vielzahl an Schwachstellen derzeit keine wirksame Verteidigung.

Die Unternehmen engagieren Hacker, um Lücken zu finden. Sie kaufen Versicherungspolicen, um sich gegen Cyber-Risiken abzusichern. Sie stolpern durch die Bedrohungsszenarien wie Getriebene. Ihre Strategie besteht letztlich vor allem darin zu hoffen, dass es ihren eigenen Laden nicht allzu heftig trifft.

Das Internet der Dinge und die Industrie 4.0 böten jetzt die einmalige Chance, den notwendigen grundlegenden Umbau der digitalen Technologien in Angriff zu nehmen und von Anfang an stabile, sichere Systeme zu bauen. Jetzt etwas langsamer, aber solider voranzuschreiten ist möglich, und es wäre langfristig der bessere Weg. Sonst werden wir in zehn Jahren konstatieren müssen, dass es zwar viele neue, magisch anmutende vernetzte Dinge gibt, dass sie aber leider unter den bunten Oberflächen stinkendschleimig sind, uns ausspionieren und nicht gehorchen.

Rieger, 43, ist einer der Sprecher des Chaos Computer Clubs.