



Bild: fotolia.com_Coloures-pic

Quo vadis erneuerbare Energien?

„Die Energiewende erfordert eine Kulturwende“

Die Energiewirtschaft ist im Umbruch. Erneuerbare Energien sind auf dem Vormarsch und decken laut jüngsten Schätzungen des Zentrums für Sonnenenergie- und Wasserstoff-Forschung Baden-Württemberg (ZSW) und des Bundesverbands der Energie- und Wasserwirtschaft (BDEW) „voraussichtlich 32 Prozent des Bruttostromverbrauchs in Deutschland“ im Jahr 2016 ab (siehe hierzu auch den Titelbeitrag, Anm. d. Red.). Hinzu kommen verstärkt neue technische Lösungen, um den Energieverbrauch zu senken. Digital und vernetzt heißt vielfach das Stichwort in der Energiebranche. Doch Vorsicht, denn neben neuen Chancen für die Energiewirtschaft der Zukunft lauern auch Gefahren, wie Sicherheitsexperte Herbert Saurugg in diesem Interview erklärt.

Autor: Andreas Eicher

Herr Saurugg, Sie sprachen jüngst in einem Beitrag bei Deutschlandradio davon, dass wir in Bezug auf die Stromversorgung derzeit nicht in der Lage wären, mehrere Tage Ausfälle zu bewältigen. Können Sie das etwas konkretisieren?

Die Stromversorgung ist die wichtigste Lebensader unserer modernen Gesellschaft. Sie verbindet fast alles miteinander, was unser Überleben sichert, ohne dass uns das wirklich bewusst wäre. Wenn die Stromversorgung großräumig und länger ausfällt, dann kann man das durchaus mit dem Blutkreislauf in unserem Körper vergleichen. Dadurch würde auch das Nerven- und Steuerungssystem ausfallen, nämlich die unterschiedlichen Telekommunikationskanäle, was dann in kürzester Zeit zum Multiorganversagen und Kollaps führt. Das Problem ist dabei nicht, dass so etwas passieren kann, da es nirgends eine hundertprozentige Sicherheit gibt, sondern dass wir das de facto ausschließen und so gut wie keine Rückfallebenen haben. Es beginnt bei den einzelnen Bürgern, von denen laut verschiedenen Studien nur eine Minderheit in der Lage ist, sich über mehrere Tage oder sogar Wochen selbst autark versorgen zu können. Und gerade nach einem europaweiten Strom- und Infrastrukturausfall, sprich Blackout, wie er leider immer wahrscheinlicher wird, wird es Tage, Wochen und in Teilen Monate dauern, bis sich die Logistik und Versorgung wieder normalisiert.

Daher kam auch die Studie „Gefährdung und Verletzbarkeit moderner Gesellschaften durch Stromausfall“ des Büros für Technikfolgenabschätzung beim Deutschen Bundestag bereits 2011 zum Schluss, dass bereits am Ende der ersten Woche eine unvorstellbare Katastrophe droht. Das hat sich in meiner langjährigen Auseinandersetzung mit diesem Szenario leider vielfach in der Praxis bestätigt. Grundsätzlich bedeutet das natürlich keinen Weltuntergang, aber wir werden in einer anderen Welt aufwachen.

Wir verharren hier in einem linearen Denken und projizieren dementsprechend lokale auch auf mögliche großflächige Ereignisse. Die schlecht vorbereitete Bevölkerung ist aber zugleich die Basis für die Wirtschaft, für Behörden und Organisationen mit Sicherheitsaufgaben, die dann anderen helfen sollten. Aber auch deren

Mitarbeitern und Familien sind erfahrungsgemäß oft nicht wesentlich besser als der Rest der Gesellschaft aufgestellt. Daher besteht hier durchaus die Gefahr eines disruptiven Ereignisses, das unser Leben, wie wir es jetzt gewohnt sind, wahrscheinlich eine Zeit lang auf den Kopf stellen würde. Was das für wirtschaftliche und gesellschaftliche Folgewirkungen haben könnte, können wir uns derzeit wohl nicht wirklich vorstellen.

Solche Ereignisse gibt es auf der ganzen Welt immer wieder. Aber nirgends ist man so von den Infrastrukturen abhängig und wohl nirgends auch so wenig vorbereitet, wie bei uns. Das nennt man auch Sicherheits- oder Verletzlichkeitsparadox. Auf der einen Seite eine sehr hohe Sicherheit und auf der anderen eine sehr hohe Unsicherheit und Verwundbarkeit, sollte doch einmal etwas größer fehlschlagen.

Das heißt, wir stehen permanent am Abgrund zu einem möglichen Blackout?

Aus meiner Sicht ja. Die Netzbetreiber machen einen hervorragenden Job, um das zu verhindern, was auch ziemlich viel kostet und zunehmend aufwendiger wird. Ein System, das jedoch unter Dauerstress steht, wird anfälliger für Störungen. Auch hier kann man eine Analogie zum Menschen beziehungsweise zur Burn-out-Gefahr ziehen. Grundsätzlich wird ein Blackout nicht durch ein Einzelereignis ausgelöst, sondern durch die Kumulation von an und für sich beherrschbaren Einzelereignissen zum falschen Zeitpunkt. So wie 2006 eine planmäßige Leitungsabschaltung in Norddeutschland 19 Sekunden später auch in Spanien die Lichter ausgehen lies. Damals hatten wir großes Glück und es kam nicht zum Blackout. Unter den heutigen Rahmenbedingungen geht jedoch niemand mehr davon aus, dass das nochmals so glücklich enden könnte. Auch wenn inzwischen sehr viel unternommen wurde, um so etwas zu verhindern. Ganz abgesehen davon, dass wir nicht wissen, was sonst noch den Dominoeffekt auslösen könnte, wie etwa ein zerstörerisches Erdbeben, ein Cyberzwischenfall oder ein Terrorangriff. Vielleicht auch eine Pandemie. Die Folge könnte sein, dass nicht mehr genug Fachpersonal zur Verfügung steht, um den hochoptimierten Normalbetrieb aufrechtzuerhalten.

Wenn Sie aus Ihrer Erfahrung auf die Energieversorger blicken: Wo sehen Sie den größten Handlungsbedarf in puncto Sicherheitslücken und -lösungen und warum?

Das jetzige System wurde für einfach berechenbare und steuerbare Großkraftwerke errichtet und auch sehr erfolgreich betrieben. Aber hier sehen wir gerade mit der Energiewende eine fundamentale Änderung hin zu mehr und mehr dezentralen Erzeugungsanlagen mit komplett anderen Charakteristiken. Die Energiewende wird derzeit einfach viel zu kurz gedacht und auf die dezentrale Erzeugung reduziert, was eine Sackgasse und ein großer Irrtum ist. Das Thema Energiebevorratung, ich nenne nur den Speicher als kleinen Teilaspekt, ist ja mittlerweile auch angekommen. Viele Netzausbaupläne zielen aber nach wie vor auf das großtechnische System ab. Wir haben ja gerade durch die aktuelle Kältewelle gesehen, dass auch Leitungen nichts nützen, wenn kein Wind geht und daher nichts produziert wird. Andererseits hat die jetzige Vernetzung wohl auch Schlimmeres verhindert, indem doch noch ein Stromaustausch innerhalb der europäischen Länder möglich war. Daher darf man die Dinge nie nur mit Entweder-oder betrachten. Es gibt immer ein Sowohl-als-auch.

Leider fällt es uns sehr schwer, die bisher durchaus erfolgreiche zweiwertige Logik abzulegen. Für die vor uns stehenden Herausforderungen brauchen wir aber eine mehrwertige Logik, die nur durch vernetztes und kooperatives Denken und Handeln zum Erfolg führen kann.

Dazu gehört etwa auch, dass wir nicht nur nach Sicherheitslücken suchen, die immer nur für spezifische Szenarien Gültigkeit haben. Wir benötigen vielmehr ein robustes Systemdesign, das gegen jegliche Störungen, auch jene, die wir heute noch gar nicht kennen, die Überlebensfähigkeit des Systems sichert. Da können wir viel von der Natur mit dem zellulären Systemdesign lernen. Und gerade die Energiewende, der Klimawandel oder die zunehmenden Herausforderungen aus dem Cyberraum werden dazu führen müssen, dass wir ein Energiezellensystem gestalten. Also ein System, in dem sich Störungen nicht fast uneingeschränkt auf das gesamte System ausbreiten können.

Herbert Saurugg

Herbert Saurugg ist Experte für die Vorbereitung auf den Ausfall lebenswichtiger Infrastrukturen. Er war 15 Jahre Berufsoffizier des Österreichischen Bundesheers, zuletzt im Bereich IKT-/ Cyber-Sicherheit. Seit 2012 beschäftigt er sich mit den möglichen Folgen der steigenden Vernetzung und Komplexität, insbesondere mit dem europäischen Stromversorgungssystem sowie einem europaweiten Strom- und Infrastrukturausfall („Blackout“). Er betreibt dazu einen umfangreichen Fachblog (www.saurugg.net).



Bild: Josef Bollwein

Das Thema der erneuerbaren Energien nimmt einen immer größer werdenden Stellenwert ein. Und das nicht nur in Deutschland. Wie beurteilen Sie die Gefährdung der Anbieter erneuerbarer Energien durch Hackerangriffe oder Sabotage, auch mit einem Blick auf die zunehmende Digitalisierung und Vernetzung im Energiesektor?

Obwohl unser zentralisiertes Stromversorgungssystem zu den verlässlichsten der Welt zählt, muss man auch dazusagen, dass es massive Verwundbarkeiten aufweist. Daher wäre es falsch zu behaupten, dass nun alles unsicherer wird. Natürlich wird es nicht einfacher, wenn immer mehr Player mitspielen und damit auch mehr potenzielle Fehler- und Angriffsstellen entstehen.

Das Hauptproblem sehe ich darin, dass wir noch nicht verstanden haben, dass Vernetzung zu mehr Komplexität führt und diese nicht mit unserer bisherigen Logik beherrschbar ist. Das erleben wir ja gerade in vielen Bereichen. Daher fürchte ich, dass der derzeitige und überhastete Digitalisierungshype noch zu einigen blutigen Nasen führen wird. Wohlgemerkt, im besten Fall. Denn wenn wir im Infrastruktursektor so weitermachen wie bisher, dann wird es wohl viel schmerzhafter werden. Nicht nur für Einzelne, sondern für die gesamte Gesellschaft.

Daher ist dieser Zellenansatz ja so faszinierend und gleichzeitig auch einfach, dass es schon wieder verwundert, warum wir nicht endlich damit anfangen. Das hängt

hauptsächlich mit unserem hochoptimierten Wirtschafts- und Wachstumsdenken zusammen, das nicht mehr mit einem lebensfähigen Systemdesign zusammenpasst, das auch Robustheit und Redundanzen vorsieht. Auch das können wir in vielen Bereichen beobachten. Immer schneller, immer höher, immer weiter; das verträgt jedoch auf Dauer kein System.

Die Dezentralisierung der Energieerzeugung erfordert daher auch ein dezentralisiertes Energiezellensystem, das noch dazu gegen jegliche Störungen robuster ist und gestaltet werden kann. Besonders erfreulich ist dabei, dass man diese Strukturen im laufenden Betrieb in das bestehende zentralisierte System integrieren kann. Das bedeutet, „Bottom-up“ die Robustheit des Gesamtsystems zu erhöhen. Dazu gibt es etwa bei der amerikanischen Armee schon erfolgreiche Umsetzungen.

Welche Rolle messen Sie den Geoinformationen im Gesamtkonstrukt von Energieversorgern, den Anbietern sogenannter smarterer Lösungen und dem Endanwender bei?

Wir werden auf jeden Fall technische Lösungen zur Umsetzung der Energiewende beziehungsweise auch des Energiezellensystems benötigen. Derzeit dreht sich aber fast alles nur um die Technik. Und das greift viel zu kurz. Die Energiewende erfordert eine Kulturwende, daher müssen wir auch die Menschen mitnehmen und zu aktiven Energienutzern machen. Denn wenn sie ihre eigene Rolle in ihrer Energie-

zelle sehen und erleben, werden sie auch anders mit Energie umgehen, als das heute der Fall ist.

Wir müssen daher einmal die Zielsetzungen klar definieren. In erster Linie geht es um unser Überleben – und das ohne Übertreibung. Denn wie eingangs dargestellt ist hier der Spielraum sehr gering. Und dann sollten wir überlegen, wie wir die Robustheit dieser Lebensgrundlage bestmöglich technisch unterstützen und verbessern können.

Danach kann man auch noch über den Markt nachdenken. Wobei wiederum das eine das andere nicht ausschließt. Aber derzeit dreht sich so gut wie fast alles nur um den Markt und die Rentabilisierung. Das ist einfach die falsche Reihenfolge, auch wenn immer betont wird, wie wichtig die Versorgungssicherheit ist.

Daher sehe ich hier durchaus auch Einsatzmöglichkeiten für Geoinformationen. Denn um die Energiezellen gestalten zu können, müssen wir einmal erfassen, was wir derzeit überhaupt verfügbar haben, und wie wir das bestmöglich für die Zielerreichung nutzen können. Zum anderen können diese Daten sicher auch für eine vorausschauende Wartung, Stichwort Predictive Maintenance, von hohem Nutzen sein.

Seit Juli 2015 ist nun das IT-Sicherheitsgesetz in Kraft, das dazu beitragen soll, kritische Infrastrukturen, beispielsweise im Energiesektor, besser zu schützen. Das Gesetz wurde mit viel Getöse von

der Politik verkündet. Kritiker sehen es indes mehr als Papiertiger. Was ist Ihre Meinung hierzu?

Wieder, Sowohl-als-auch und das fehlt mir hier, wie auch in vielen anderen Bereichen. Schutz ist zwar wichtig, aber wir müssen auch wissen, wie wir damit umgehen, wenn dieser nicht mehr funktioniert.

Und das ist derzeit so gut wie überall der Fall und das führt uns wieder zur eingangs dargestellten Achillesferse unserer Gesellschaft. Eigentlich zäumen wir damit das Pferd von hinten auf. Und gerade in einem sehr dynamischen und komplexer werdenden Umfeld ist es umso wichtiger, sich nicht zu sehr auf die Vergangenheit zu konzentrieren, sondern auf die Verwundbarkeiten. Und da wiederum nicht nur auf die technischen Aspekte zu schauen, sondern vielmehr auf unsere Abhängigkeiten und wie diese reduziert und kompensiert werden können. Die im vergangenen Sommer vom deutschen Innenminister und jetzt im Januar vom Schweizer Verteidigungsminister empfohlene Notbevorratung ist etwa eine solche Maßnahme zur Reduktion der Abhängigkeiten und zur Erhöhung der gesellschaftlichen Resilienz. Also die Fähigkeit, auch mit Störungen umgehen zu können. Daher sind Maßnahmen wie das IT-Sicherheitsgesetz ein Puzzlestein, welche häufig als die Allheilslösung verkauft werden, was sie aber nicht bieten können. Zum anderen fehlen gesamtheitliche Betrachtungen und etwa die Darstellung des Links zwischen dem IT-Sicherheitsgesetz und des Zivilverteidigungskonzepts mit der Aufforderung zur Notbevorratung. Wahrscheinlich ist dieser Link auch vielen Entscheidungsträgern nicht so richtig bewusst.

Bestehen Unterschiede im europäischen und internationalen Vergleich in puncto Sicherheit von Energieunternehmen? Wenn ja, von welchem Land, welchem Unternehmen, können Unternehmenslenker aus Ihrer Sicht etwas lernen?

Unterschiede gibt es definitiv, wobei ich die einzelnen nicht im Detail kenne. Aber auch hier ist es egal, wer das schwächste Glied in der Gesamtkette ist. Wenn dieses Glied groß oder systemwichtig genug ist, kann es das Restsystem zum Fall bringen, auch wenn ich gleichzeitig selbst top aufgestellt bin. Daher ist es so wichtig, das Gesamtsystem zu kennen und zu betrach-

ten. Denn sonst betreibt man möglicherweise dort, wo man sich gut auskennt, viel Aufwand für nichts. In Österreich wird gerade ein Energie-CERT, Computer Emergency Response Team, aufgestellt, um besser mit Cybervorfällen im Energiesektor umgehen zu können. Ich denke, solche Vernetzungsmaßnahmen, nicht nur technischer Art, sind wichtig und nachahmenswert. Wir hinken leider in vielen Bereichen der technischen Vernetzung hinterher. Und gerade für vernetztes Denken und Handeln und den Umgang mit Komplexität brauchen wir viele Blickwinkel.

An welchen Stellschrauben müssen Energieversorger stärker drehen, um zu einer besseren Informationssicherheit in unseren digitalen Zeiten zu gelangen?

Ich denke, das ist ein ständiges Hase-und-Igel-Rennen, bei dem der Verteidiger immer das Nachsehen haben wird. Der Angreifer muss nur einmal erfolgreich sein, der Verteidiger immer. Und zum anderen möchte ich davor warnen, immer nur nach Angreifern Ausschau zu halten.

Das könnte zu bösen Überraschungen führen, wie wir das etwa 2013 mit einer Leittechnikstörung in Österreich erlebt haben. Ein fehlerkonfiguriertes Telegramm hätte beinahe in die Katastrophe geführt. Eine wesentliche Erkenntnis daraus war, neben der Sinnhaftigkeit eines E-CERT, das wir heute nicht mehr wissen, wie die Systeme wirklich aussehen und welche wechselseitigen Abhängigkeiten entstanden sind. Der Grund ist, dass diese Systeme unter ganz anderen Voraussetzungen eingerichtet wurden. Meiner Meinung nach können die zunehmend schärfer werden Regularien nicht mit der Geschwindigkeit der Entwicklungen mithalten und auch zur Lähmung führen. Wir sollten daher weniger an den Stellschrauben als vielmehr am Systemdesign arbeiten. Aber nochmals, Sowohl-als-auch.

Bringen wir uns durch die zunehmende Digitalisierung und Vernetzung nicht selbst immer stärker unter Zugzwang? Sprich: Auf jede neue technische Entwicklung muss in immer kürzeren Abständen mit Sicherheitslösungen reagiert werden.

Ja, wenn man nicht dazulernt, schon, was wir gerade beim sogenannten Internet der Dinge sehr drastisch sehen. Hier haben wir ein Sicherheitsniveau, das wir vor 20 Jahren in der IT auch hatten, nämlich

keines. Nur sind die Dinge heute alle vernetzt und sofort angreifbar. Aber solange uns nicht wirklich etwas ordentlich um die Ohren fliegt, werden wir wohl so weitermachen. Danach werden wir uns hoffentlich das Systemdesign neu überlegen. Das könnte man also auch billiger haben. Aber das geht jetzt nicht, weil wir ja wachsen müssen und es ja schon immer so gemacht haben.

Wenn Sie nach vorne blicken. Welche Chancen und Risiken ergeben sich Ihrer Meinung nach zukünftig durch den stärkeren Einsatz von Geoinformationen im erneuerbaren Energiebereich?

Ich denke, die generellen Risiken wurden bereits ausführlich aufgezeigt, wobei die Risiken von der Geoinformation eher überschaubar sein dürften. Die Chancen sehe ich vor allem im Energiezellensystem, wo sicher auch Geoinformationen eine Rolle spielen werden. Und das, obwohl zwar jede Zelle ein selbstreferenzielles Design aufweisen soll, dieses jedoch auf die lokalen und regionalen Voraussetzungen angepasst werden muss. Daher geht es wohl häufig einmal um die Datenerfassung, was heute überhaupt Sache ist, und dann um die Wartung und Instandhaltung. Übrigens ein wichtiger, aber oft vernachlässigter Baustein in der Informationssicherheit, was aber nicht zu einer Bürokratisierung führen soll. Daher geht es nicht darum, alte Prozesse elektronisch abzubilden, sondern neue zu schaffen, die erst durch die heutigen technischen Möglichkeiten umsetzbar sind und die vor allem zur Systemrobustheit und nicht nur zur Selbstverwaltung beitragen. Es gibt noch sehr viel zu tun. Nur werden wir halt mit den falschen Zielsetzungen nicht wirklich ans Ziel kommen. Daher mein Rat: Wenn du es eilig hast, gehe langsam.

**Herr Saurugg,
vielen Dank für das Gespräch!**

.....
Das Interview führte Andreas Eicher