

Heinz Thielmann
Dieter Klumpp
Jörg Eberspächer

Herausgeber

Sicherheit und Datenschutz bei Smart Energy



MÜNCHNER KREIS

Übernationale Vereinigung für Kommunikationsforschung
Supranational Association for Communications Research

Das vorliegende Buch enthält Vorträge und Diskussionen der Fachkonferenz und des Berliner Gesprächs, die der Münchner Kreis zusammen mit der Alcatel-Stiftung für Kommunikationsforschung am 29. September 2011 durchgeführt hat.

Die vorliegende Produktion ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Die Verwendung der Texte, auch auszugsweise, ist ohne schriftliche Zustimmung des Münchner Kreises urheberrechtswidrig und daher strafbar. Dies gilt insbesondere für die Vervielfältigung, Übersetzung oder die Verwendung in elektronischen Systemen.

Herstellung: Knecht-Druck GmbH München

ISBN 987-3-9813733-4-9

Vorwort

Eines der drängenden Zukunftsthemen unserer Gesellschaft betrifft die nachhaltige Sicherstellung unserer Energie-Versorgung für die nachfolgenden Generationen bei gleichzeitiger Reduktion der Umweltbelastungen. Erneuerbare Energien müssen breitflächig nutzbar gemacht werden und der Energieverbrauch muss durch systematische Maßnahmen zum Energiesparen substantiell reduziert werden.

Das Energie-Management der Zukunft muss gezielt gesteuert und überwacht werden, um Angebot und Nachfrage in Einklang zu bringen und Lastspitzen zu vermeiden. Erforderlich ist ein komplexes IKT System, das in der Lage ist, die zur Steuerung und Abrechnung erforderlichen Daten zu erheben, über Kommunikationsnetze zu transportieren und mittels Energie-Managementsystemen zu verarbeiten. Voraussetzung dafür, dass ein solches komplexes IKT-System funktionsfähig ist und von den Verbrauchern akzeptiert wird, ist die systematische Integration von Sicherheits- und Datenschutzmaßnahmen. Nur wenn die Vertraulichkeit der ausgetauschten Daten und deren Korrektheit und Manipulationssicherheit gewährleistet werden kann, sind die gewünschten Effekte hinsichtlich Energieeinsparung und Umweltschutz erfüllbar. Die Schutzprofile für Smart Meter sind dafür ein wichtiger Ausgangspunkt.

In der Fachkonferenz und dem anschließenden Berliner Gespräch wurden die technischen, organisatorischen und rechtlichen Rahmenbedingungen eines sicheren, verlässlichen, datenschutz-orientierten Energie-Informationssystem beleuchtet, die Bedrohungslage analysiert und Handlungsbedarfe identifiziert. Der Münchner Kreis gemeinsam mit der Alcatel-Lucent Stiftung für Kommunikationsforschung haben damit den Dialog zwischen Politik, Wirtschaft und Wissenschaft unterstützt und eine neutrale Plattform für das Zusammenwirken der bisher getrennten Welten Energieerzeuger und –verteiler (EVU, Stadtwerke, etc.), Informations- und Kommunikationstechnik sowie Automobilwirtschaft und Verkehr geschaffen..

Die laufenden Förderprojekte des Bundesministeriums für Wirtschaft und Technologie zu „E-Energy“ und „IKT für Elektromobilität“ bildeten eine reale und konkrete Grundlage für eine nachhaltige Umsetzung, und damit für die Statements und die Diskussion.

Dieser Tagungsband enthält die Vorträge und durchgesehene und leicht gekürzte Mitschriften der Diskussionen sowie im Anhang Statements von Teilnehmern. Allen Referenten und Diskutanten sowie allen, die zum Gelingen der Konferenz und zur Erstellung dieses Buches beigetragen haben, gilt unser herzlicher Dank!

Heinz Thielmann

Dieter Klumpp

Jörg Eberspächer

Inhalt

1 Begrüßung und Einführung

Prof. Dr. Jörg Eberspächer, Münchner Kreis und TU München
Dr. Andreas Goerdeler, BMWi, Berlin
Prof. Dr. Wolf-Dieter Lukas, Alcatel-Lucent Stiftung und BMBF, Bonn
Prof. Dr. Ingo Wolff, ITG im VDE, Frankfurt

2 Risikowahrnehmung Energiesicherung International

Prof. Dr. Ortwin Renn, Universität Stuttgart

3 Sicherheit für das Energieinformationsnetz

Prof. Dr. Claudia Eckert, Fraunhofer Institut AISEC, München-Garching

4 Diskussion

Moderation: Prof. Dr. Jörg Eberspächer, Münchner Kreis und TU München

5 Prozessbezogener Datenschutz im Smart Grid

Dr. Oliver Raabe, Karlsruher Institut für Technologie

6 E-Energy und das Thema Sicherheit

Ludwig Karg und Michael Wedler, B.A.U.M. E-Energy-Begleitforschung, München

7 Semper Ident? Zur Notwendigkeit einer differenzierten grundrechtlichen Bewertung von Smart Metern

Prof. Dr. Gerrit Hornung, LL.M., Universität Passau

8 Sicherheit und Datenschutz im Smart Metering

Dr. Johann Kranz, Ludwig-Maximilians-Universität München

9 Sicherheit und Datenschutz im Smart Metering

Rolf Müller-Hermes, Detecon International GmbH, Bonn

10 Sicherheit und Datenschutz im Smart Metering

Martin Rost, Unabhängiges Landeszentrum für Datenschutz, Kiel

11 Diskussion

Moderation: Dirk Fox, Secorvo Security Consulting GmbH, Karlsruhe

12 System- und Architektur-Konzeptionen

Prof. Dr. Manfred Broy, Technische Universität München

13 Smart and Safe – intelligente Speichersysteme im Verteilnetz

Christian Müller-Elschner, Younicos AG, Berlin

14 Herausforderungen und Lösungen für die elektrischen Energieversorgungsnetze

Prof. Dr. Stefan Tenbohlen, Universität Stuttgart

-
- 15 Wirtschaftliche Aspekte, Ansätze für Geschäftsmodelle**
Prof. Dr. Arnold Picot, Ludwig-Maximilians-Universität München
- 16 Wirtschaftliche Aspekte, Ansätze für Geschäftsmodelle**
Prof. Dr. Helmut Krcmar, Technische Universität München
- 17 Das Programm der Bundesregierung zu Smart Energy**
Parlamentarischer Staatssekretär Hans-Joachim Otto, BMWi, Berlin
- 18 Smart Grid - Perspektiven der Energiewirtschaft**
Dr. Andreas Breuer, RWE Deutschland AG, Essen
- 19 Smart Grid – Perspektiven der IKT-Wirtschaft**
Herbert Merz, BITKOM, Berlin
- 20 Smart Grid – Perspektiven der IKT-Wirtschaft**
Prof. Dr. Ingo Wolff, Informationstechnische Gesellschaft im VDE (ITG), Frankfurt
- 21 Diskussion**
Moderation: Prof. Dr. Helmut Krcmar, Technische Universität München
Prof. Dr. Heinz Thielmann, Emphasys GmbH, Heroldsberg
- 22 Schlusswort**
Prof. Dr. Arnold Picot, Ludwig-Maximilians-Universität München

Anhang

Statement zu Aspekte und Handlungsbedarf bei Sicherheit, Datenschutz und Verbraucherschutz

Peter Büttgen, BfDI, Bonn

Statements der Marktteilnehmer / Internationale Aktivitäten

Stephan Gerhager, E.ON Energie AG, München

Steffen Heyde und Thomas Koelzer, secunet Security Networks AG

Andreas Kießling, MVV Energie AG, Mannheim

Dr. Christoph Mayer, OFFIS, Oldenburg

Kai Paulssen, Bundesnetzagentur, Bonn

Arne Rajchowski, BDEW, Berlin

Kerstin Straube, T-Systems International GmbH, München

Liste der Referenten und Moderatoren

1 Begrüßung und Einführung

Prof. Dr. Jörg Eberspächer, Münchner Kreis und TU München
Prof. Dr. Wolf-Dieter Lukas, Alcatel-Lucent Stiftung und BMBF, Bonn
Dr. Andreas Goerdeler, BMWi, Berlin
Prof. Dr. Ingo Wolff, ITG im VDE, Frankfurt

Prof. Dr. Jörg Eberspächer:

Guten Morgen, sehr geehrte Damen und Herren. Im Namen des Münchner Kreises möchte ich Sie herzlich zu unserer Konferenz „Sicherheit und Datenschutz bei Smart Energy“ begrüßen. Mein Dank gilt der Alcatel-Lucent-Stiftung, die diese gemeinsame Veranstaltung angeregt und tatkräftig unterstützt hat. Der Dank gilt außerdem auch den weiteren Unterstützern, den Firmen Detecon, Nokia Siemens Networks und RSA. Und nicht zuletzt gilt der Dank Herrn Kollegen Heinz Thielmann, der die Federführung bei der Vorbereitung des Programms hatte.

Meine Damen und Herren, alles scheint heutzutage „smart“ sein zu müssen, natürlich auch die Energie. Die Energie selbst kann natürlich nicht smart sein; aber Sie mögen uns den saloppen Titel der Konferenz verzeihen. Es geht natürlich um unser Energiesystem von der Erzeugung bis zur Verteilung. Sie wissen, dass es darum geht, mehr Dezentralität zu erreichen im Zuge des Aus- und Umbaus der Energieversorgung. Mehr Funktionalität, mehr „Intelligenz“ wird benötigt, um höhere Effizienz und damit auch geringere Kosten bei Nutzern und Betreibern zu erreichen. Eine weitere, nach meiner Meinung sehr wichtige Forderung ist die nach größerer Transparenz der Prozesse. Und alles soll selbstverständlich erreicht werden unter der Randbedingung einer mindestens so hohen Ausfallsicherheit wie bisher. Bei all dem soll der Benutzer mehr im Mittelpunkt stehen als bisher, sowohl was die Dienste als auch was seinen Schutz angeht.

Was folgt aus diesen Anforderungen? Da besteht wohl weitgehend Einigkeit: Man braucht neuartige Organisations- und Betriebsformen. Man braucht IT als Basis, massive Vernetzung, intelligente Benutzerführung, neue Geschäftsmodelle und natürlich auch wirksame Sicherheitskonzepte. Wenn wir künftig zwei oder sogar drei kritische Infrastrukturen, nämlich die Energiesysteme, die Telekommunikation und die Informationssysteme miteinander verknüpfen, haben wir davon nicht nur große Vorteile, sondern es drohen auch Risiken. Darum geht es heute in dieser Konferenz.

Ich freue mich, dass sich so viele Experten auf diesem Gebiet heute zusammengefunden haben. Wir wollen, wie das im Münchner Kreis und in der Alcatel-Lucent Stiftung Tradition ist, offen miteinander diskutieren, kritische Fragen stellen, aber natürlich auch möglichst Lösungsansätze und Handlungsempfehlungen formulieren. Wie Sie der Einladung und dem Programm entnommen haben, ist der Tag zweigeteilt. Der erste Teil konzentriert sich mehr auf die technisch-wissenschaftlichen Aspekte, während wir heute Abend die Tradition der Berliner Gespräche des Münchner Kreises fortsetzen, wo es dann auch in den Dialog mit der Politik gehen wird.

Ich wünsche uns allen eine ertragreiche Konferenz und darf das Wort an Herrn Kollegen Lukas vom BMBF übergeben. Herr Prof. Lukas ist Physiker, Leiter der Abteilung „Schlüsseltechnologien - Forschung für Innovationen“ im Bundesministerium für Bildung und Forschung (BMBF) und heute hier in seiner Funktion als Mitglied des Kuratoriums der Alcatel-Lucent Stiftung. Herr Lukas, darf ich Sie um Ihr Grußwort bitten!

Prof. Dr. Wolf-Dieter Lukas

Auch ich möchte Sie ganz herzlich willkommen heißen, nunmehr im Namen der Alcatel-Lucent-Stiftung, dem Mitveranstalter. IT-Sicherheit, aber auch Datenschutz, sind Themen, mit denen sich die Stiftung seit vielen Jahren nicht zuletzt im Stiftungs-Verbundkolleg „Recht und Sicherheit“ beschäftigt. Ein etwas jüngeres Thema der Stiftung ist die enge Verbindung von IT und Energie-Netzen, die uns nicht allein vor technische, sondern eben auch vor datenschutzrechtliche Herausforderungen stellt.

Das Stiftungs-Verbundkolleg „Energieinformationsnetz“ beschäftigt sich genau mit diesen Fragestellungen. Frau Prof. Eckert, die gleich hierzu vortragen wird, ist zusammen mit Herrn Prof. Rossnagel eine der maßgeblichen Ideengeber, das Bundesministerium für Wirtschaft und Technologie, heute durch Herrn Dr. Goerdeler hier vertreten, ein wichtiger Partner und verlässlicher Unterstützer. Beide möchte ich hier auch stellvertretend für all die anderen Mitstreiter ganz herzlich willkommen heißen.

Nun werde ich aber nicht weiter für die Stiftung sprechen, sondern - wie vom stets um Effizienz bemühten Programmkomitee gewünscht - meinen anderen Hut aufsetzen und aus Sicht des Bundesministeriums für Bildung und Forschung das Thema der Veranstaltung beleuchten.

Meine Damen und Herren, bei dem, was wir uns hinsichtlich des Umbaus unserer Energieversorgung und effizienteren Energienutzung vorgenommen haben, kommen wir bei den Energienetzen an intelligenteren Steuerungs-, Verteil- und Nutzungskonzepten nicht umhin. IKT muss und kann wieder einmal helfen, die Komplexität zu beherrschen. Damit ist Smart Energy- wie man heute sagt- ein Top-Thema, ein politisches Thema.

Smart Energy stellt uns auch vor neue Herausforderungen: So steigt die Gefahr möglicher Cyberattacken auf unsere Energieversorgung, wodurch den Themen Sicherheit und Datenschutz wichtige Rollen zukommen. Mehr denn je stehen diese Themen im Zentrum der öffentlichen Diskussion bei der Einführung neuer Technologien und der mit ihnen verbundenen Dienste.

Lassen Sie mich im Folgenden auf drei Aspekte eingehen, die mir in diesem Kontext besonders wichtig sind. Dies sind:

1. Die Sicherheit der neuen Smart-Energy-Technologien.
2. Die Privatsphäre seiner Nutzer.
3. Und letztendlich, auch als Resultat aus den ersten beiden Punkten, das Vertrauen der künftigen Nutzer.

Sicherheit neuer Technologien und Dienste

Die jüngsten Ereignisse haben gezeigt, dass vernetzte IT-Systeme und Informationen nur mit ganz erheblichem Aufwand zu schützen sind, sobald sie einmal in den Focus von Kriminellen geraten sind. Mit professionellen Methoden werden Industrieanlagen gezielt angegriffen und millionenfach die Kreditkartendaten von Kunden ausgespäht.

Die Motivation hinter den Angriffen ist von unterschiedlicher Natur, so dass nur schwer abzuschätzen ist, was eines besonderen Schutzes bedarf. Wir erleben es trotzdem oft, dass Produkte und Dienste mit gar keinen oder nur rudimentären Sicherheitsmechanismen auf dem Markt kommen. Wenn diese später nachgerüstet werden sollen, geschieht dies weder effektiv noch effizient. Ein solches Vorgehen können wir uns im Bereich der kritischen Infrastrukturen auf keinen Fall erlauben.

Meine Damen und Herren, wir sind uns vermutlich darüber einig, dass Sicherheit zu einem elementaren Faktor geworden ist, der von Beginn an bei der Konzeption eines Produktes oder eines Dienstes berücksichtigt werden muss. Security by Design ist hierbei eine zentrale Anforderung. Das Bundesministerium für Bildung und Forschung fördert daher drei Kompetenzzentren für die IT-Sicherheitsforschung. Das Kompetenzzentrum in Darmstadt wird sich genau diesem wichtigen Thema schwerpunktmäßig widmen.

Die Privatsphäre der Nutzer

In der Presse war kürzlich zu lesen, dass über sekundengenaue Messung des Stromverbrauches auf das aktuell geschautete Fernsehprogramm geschlossen werden kann oder ob die Hausfrau oder der Hausmann die Mikrowelle oder den Backofen benutzt. Auch wenn uns der eine oder andere konkrete Fall irrelevant erscheint, so zeigt dieses Beispiel doch ein Problem unserer Informationsgesellschaft. Mit Leichtigkeit lassen sich riesige Datenmengen erheben und automatisch Informationen über Nutzer generieren. Wie hier bei der Messung des Energieverbrauchs lassen sich also Zusammenhänge herstellen, die man zunächst nicht vermutet. Vermutlich würden die meisten Kunden bei einer direkten Befragung einer solchen Auswertung auch nicht zustimmen. Kunden wollen sicher sein, dass ihre Daten vertraulich behandelt werden. Privacy by Design ist hier das Stichwort. Auch dieses Thema wird in einem der drei Kompetenzzentren erforscht. Wir können deutlich beobachten, dass Vertrauen in die Sicherheit und der sorgsame Umgang mit Daten im Netz immer wichtiger wird, um neue Technologien wie Smart-Energy auch einsetzen zu können. Und damit komme ich zum letzten meiner drei Punkte.

Vertrauen der Nutzer

Einen Verlust von Vertrauen der Nutzer in die vielfältigen gesellschaftlichen und wirtschaftlichen Möglichkeiten, die uns das Internet bietet, können wir uns nicht leisten. Bereits heute fühlen sich viele Internetnutzer unsicher, und das zu Recht. Nutzer haben in der Praxis kaum Kontrolle darüber, was mit ihren Daten geschieht und von wem diese für welche Zwecke verwendet werden. Aber ohne den Erhalt des Vertrauens und die damit verbundene Akzeptanz wird das Internet nicht mehr die wichtige Basis sein können, die es für das Wachstum unseres Wirtschaftsstandorts Deutschland mittlerweile geworden ist. Hier ist nicht nur die Politik, sondern gleichermaßen die Wirtschaft und Wissenschaft gefordert, die Herausforderungen gemeinsam anzugehen und neue Lösungen zu erarbeiten.

Aufgabe der Politik

Letztendlich steht die Gesellschaft doch vor der entscheidenden Frage: Wie sollen die Datenetze der Zukunft aussehen? Hier werden wir aktiv gestalten. Bürgerinnen und Bürger, Wirtschaft und Politik werden gemeinsame Vorstellungen einer positiven Zukunft entwickeln und diese zusammen umsetzen.

Die Bundesregierung hat hierzu bereits zahlreiche konkrete Maßnahmen initiiert:

- Die Cybersicherheitsstrategie unter Federführung des BMI.
- Die Forschungsunion Wissenschaft-Wirtschaft - Zukunftsprojekt „Sichere Identitäten“.
- Die drei Kompetenzzentren IT-Sicherheitsforschung des BMBF.
- Das gemeinsame Arbeitsprogramm IT-Sicherheit von BMBF und BMI.
- Das Acatech-Projekt „Vertrauenkultur im Internet“.

Sie sehen also: Die Bundesregierung greift o.g. Fragestellungen auf und agiert. Der Schutz der Sicherheit und des Vertrauens im Netz werden zentraler Gegenstand zukünftiger Forschungsprojekte des Bundesministeriums für Bildung und Forschung sein. In diesem

Kontext möchte ich auch noch einmal auf die gute Arbeitssteilung mit dem Bundeswirtschaftsministerium hinweisen.

Dr. Andreas Goerdeler:

ich darf Sie auch von meiner Seite alle herzlich willkommen heißen. Ich freue mich über die Möglichkeit, heute einen übergreifenden Erfahrungsaustausch über das Thema Sicherheit und Datenschutz im Smart Energy mit Ihnen zu führen. Ich bin auch froh, dass wir die E-Energy-Modellregionen dabei haben. Es ist wichtig, dass wir uns einen Gesamtüberblick verschaffen und klären, wie weit wir bei den Themen sind und wo zukünftige Herausforderungen liegen.

Ich freue mich, dass die Alcatel-Stiftung und der Münchner Kreis diese Veranstaltung gemeinsam organisiert haben. Wir sind mit der Alcatel-Stiftung schon eine ganze Weile unterwegs. Nach dem IT Gipfel in Stuttgart gab es ein erstes Meeting. Es entstand u. a. das Projekt NEWISE, das die Stiftung unterstützt. NEWISE steht für nachhaltiges Energie-Informationssystem - und da geht es gerade auch um die Fragen von Wettbewerb, Information und Sicherheit in der Energieversorgung. Ich halte dies für ein wichtiges Diskursprojekt, das von Anfang an auch aufgelegt war, um die E-Energy Aktivitäten zu begleiten und das Augenmerk noch stärker auf gesellschaftspolitische Aspekte zu lenken. Folgerichtig hat man dann die zweite Konferenz konkret auf den Nutzerschutz bezogen, die am 17. Juni im letzten Jahr im BMWi stattfand. Viele Anregungen entstanden, die auch wiederum zu Folgeaktivitäten geführt haben. Auch aus dem Bereich der Sicherheitsforschung - Herr Professor Lukas hat gerade darüber berichtet - können wir zusätzliche Impulse aufnehmen. Insgesamt wird immer deutlicher, dass es umso dringlicher ist, dass wir neben dem Stromnetz eben auch ein Energieinformationsnetz brauchen, um das Smart Grid zu realisieren und dazu beizutragen, dass die Energiewende gelingt.

Wir haben bei der Energieerzeugung angesichts der großen Schwankungen sowohl bei Wind als auch bei Sonne große Volatilität. Aber auch die Dezentralisierung gehört ins Bild - in einzelnen E-Energy-Modellregionen wurden z. B. auch Blockheizkraftwerke einbezogen. All dieses führt dazu, dass wir sehr viel stärker ein Ausbalancieren zwischen Erzeugung und Nachfrage brauchen; Demand Side Management ist hier eine wichtige Herausforderung. Wir haben im Grunde einen Paradigmenwechsel, der durch den Übergang von der verbrauchsorientierten Erzeugung hin zu einem erzeugungsorientierten Verbrauch gekennzeichnet ist. Ohne IKT sind diese Entwicklungen nicht realisierbar. Und wir haben auch das Bild des Prosumers, das im Rahmen von E-Energy entstanden ist, also die Verbindung von Produzent und Konsument in einem Akteur, also z. B. Haushalte, die gleichzeitig selbst Energie erzeugen und sie auch verbrauchen. Insgesamt entsteht ein komplexes System, das die alte Welt der unidirektionalen am Verbrauch orientierten Erzeugung ablöst. Die neue Welt besteht aus vielen Akteuren und multidirektionalen Beziehungen.

Der Paradigmenwechsel bringt gleichzeitig neue Sicherheitsherausforderungen mit sich. Mit den E-Energy-Modellregionen haben wir eine Phase des Experimentierens eröffnet. Für die meisten war es von Anfang an klar, dass den Themen ‚Security by Design‘ und ‚Privacy by Design‘ eine wichtige Rolle zukommt. In der Begleitforschung wurden frühzeitig projektübergreifende Fachgruppen gebildet, um von Anfang an Aspekte wie Privacy vor die Klammer zu ziehen und so Generisches zu entwickeln. Und es ist bemerkenswert, was schon herausgekommen ist. Ich erinnere an das Papier „Anmerkungen und Anregungen zum Datenschutz in Smart Grids“, das zum Energy Jahreskongress Anfang des Jahres vorlag und wichtige Impulse gegeben hat. Das BSI spielt, insbesondere was die Beschreibung der Anfor-

derungen an Sicherheit anbelangt, eine zentrale Rolle. Ein Beispiel ist das Schutzprofil für den Smart Meter, der ein wichtiges Glied im Gesamtsystem darstellt. Allerdings sind die Anforderungen an die IT-Sicherheit im Smart Grid sehr viel weiter zu sehen. Wir brauchen hier eine Gesamtbetrachtung.

Wir haben im Deutschen den Begriff Sicherheit in verschiedener Bedeutung. Im englischen Sprachraum ist er differenzierter, indem zwischen Safety und Security unterschieden wird. Safety ist sehr stark verknüpft mit dem Begriff Ausfallsicherheit, mit der Versorgungssicherheit, um in der Begrifflichkeit der Energiepolitik zu bleiben. Das ist von Anfang an ein Anliegen gewesen. Wie kann ich z. B. durch Remoteanwendungen sicherstellen, dass das Gesamtsystem nicht zusammenbricht und es zu Blackouts kommt?

Das Thema Security betrifft demgegenüber Verlässlichkeit, Integrität und Verfügbarkeit der Daten. Und bei Datenschutz steht der Schutz von personenbezogenen Daten im Vordergrund. Schauen wir uns die einzelnen Modellregionen an. Die Sicherheitsansätze sind unterschiedlich ausgeprägt. Wir haben sechs Modellregionen insgesamt. Bei der Modellstadt Mannheim beispielsweise hat man sehr frühzeitig auf eine IBM Studie mit der Beschreibung der Bedrohungen aufgesetzt und daraus ein IT-Architektur-Konzept entwickelt. In der Modellregion MeRegio – die Region steht für Minimum Emission -, wurde ein White Paper mit Bedrohungen erarbeitet und dann konkret für eine Pilotphase angewandt. Bei Smart Watts, die Modellregion Aachens, geht von den dortigen Use Cases aus und versucht, die relevanten Sicherheitsaspekte aufzugreifen und zu bearbeiten. „eTelligence“, das Projekt im Norden, hat sich sehr stark nach dem BSI Katalog für Cyber Security ausgerichtet und daraufhin das Sicherheitskonzept abgeleitet. Für Edema, der Region im Ruhrgebiet, wurden verschiedene Studien zu den Risiken der Gesamtarchitektur gemacht. Hier wurde ein Sicherheitskonzept für ein Gateway im Haus erarbeitet.

Das sind alles erste einzelne Schritte und jetzt wird es darauf ankommen - und der heutige Tag bietet dazu eine sehr gute Gelegenheit - die Gesamtsicht wieder herzustellen. Wir haben Einzelsysteme, müssen aber ihre Verknüpfung betrachten. Und wir brauchen eine Absicherung sowohl in Bezug auf Hard- und Software als auch in dem Sinne, dass wir die gesamte Prozesskette ins Auge fassen müssen. In die Gesamtbetrachtung gehören die einzelnen Risiken, die man bewerten kann. Das sind Systemausfallrisiken, das sind aber auch Risiken, die sich aus der organisierten oder privaten Kriminalität ergeben. Und natürlich gehören auch die Gefahren des Cyberterrorismus, wie Denial of Service Attacks usw. dazu. Wichtig ist m. E. auch die Vielzahl der Akteure. Wir haben Produzenten. Wir haben Energienutzer. Wir haben Energienetzbetreiber. Wir haben Verteilnetzbetreiber. Wir haben Energielieferanten. Wir haben Energiehändler. Wir haben Messstellenbetreiber, Energiemarktbetreiber, Kommunikationsnetzbetreiber und Energiedienstleister. Das ist ein weites Spektrum, noch dazu mit Untergliederungen. Alle Akteure haben unterschiedliche Rollen mit ganz unterschiedlichen Schutzbedarfen, Rechten und Pflichten. Das muss man im Blick haben. Damit man nicht die Übersicht verliert, ist es wichtig, sich auf Use Cases zu konzentrieren, um die wesentlichen Aspekte, bei denen sicherheitsrelevante Fragen auftauchen, einzufangen. Beispiele sind die Abrechnung oder auch die Elektromobilität, die im Smart Grid als stationärer Speicher eine Rolle spielen werden.

Vielleicht noch ein Blick über den Tellerrand hinaus. Wir haben auch die Normungsroadmap zu berücksichtigen, die wir durch E-Energy mit auf den Weg gebracht haben. Hier ist auch das Thema Sicherheit in den einzelnen Schritten zur Normung mit angedacht. Man wird sich anschauen müssen, wo Normenstandards gesetzt werden müssen. Das spielt eine wichtige Rolle bei den Beteiligten in der DKE, die die Normungsroadmap stetig weiter entwickelt. Wir müssen auch die amerikanischen Anstrengungen im NIST-Kontext berücksichtigen. Wir haben im Übrigen in Europa im Rahmen des Projekts Future Internet einen auf das

Energiesystem bezogenen Teil, bei dem die Anforderungen aus dem Smart Grid für die IT bestimmt werden. Das ist ein großes Projekt, und auch hier ist es wichtig, die Sicherheitsfragen mit einzubeziehen.

Am Ende möchte ich noch einen Punkt hervorheben, der mir als Vertreter des Bundesministeriums für Wirtschaft und Technologie besonders am Herzen liegt. Wir dürfen die Chance für neue Geschäftsmodelle nicht aus den Augen verlieren. Wir dürfen nicht den Fehler machen, dass wir jetzt aus dem reinen Sicherheitsdenken solche Chancen zu sehr einengen. Es darf nicht passieren, dass wir Geschäftsentwicklungen zumauern. Insofern möchte ich am Ende als Appell loswerden: „So viel Geschäftsentwicklung wie möglich und so viel Sicherheit wie nötig“. Wenn wir das am Ende schaffen, liegen wir richtig.

Prof. Dr. Ingo Wolff:

Im Namen des Verbands der Elektrotechnik Elektronik und Informationstechnik (VDE) darf ich Sie ebenfalls ganz herzlich zu der heutigen Veranstaltung „Sicherheit und Datenschutz bei Smart Energy“ begrüßen. Der VDE ist seit nun nahezu 120 Jahren ein wirtschaftsneutraler, fachorientierter Verband, der in fünf Fachgesellschaften die Themenbereiche Informationstechnik, Energietechnik, Mikroelektronik, Automatisierungstechnik und Medizintechnik bearbeitet, systematisch aufbereitet und die Normung und Standardisierung über die DKE, die Deutsche Kommission Elektrotechnik, Elektronik und Informationstechnik, vorbereitet. Mit seinem Forum Netztechnik/Netzbetrieb im VDE (FNN), der der zuständige Ausschuss für die Erarbeitung von VDE-Anwendungsregeln und technischen Hinweisen für den sicheren und zuverlässigen Betrieb der Energieübertragungs- und -verteilungsnetze ist, ist der VDE der fachlich breit aufgestellte Fachverband, der die Problemstellungen des zukünftigen, intelligenten Energieversorgungssystems, Smart Grid, analysieren, bewerten und weiterentwickeln sowie die Bemühungen zur Standardisierung optimal unterstützen kann.

Der VDE hat die große Bedeutung des zukünftigen, intelligenten Energieversorgungssystems für die Entwicklung der deutschen Wirtschaft erkannt. Er hat deshalb im vergangenen Jahr eine breitbandig aufgestellte Arbeitsgruppe aus Wissenschaftlern und Industrievertretern aus den Bereichen der Energietechnik, der Informationstechnik und der Automatisierungstechnik zusammengestellt, die, unterteilt in drei Arbeitskreise Netzinformationstechnik, Netzautomatisierung und wirtschaftliche Geschäftsmodelle, das volle Spektrum des Smart Grid bearbeiten.

Mit der Entwicklung des Smart Grid werden neue Probleme und Aufgabenstellungen auf uns zu kommen. Der Begriff „Smart Grid“ umfasst die Vernetzung und Steuerung von intelligenten Energieerzeugern (im Sinne der Energieumwandler), Speichern, Verbrauchern und Netzbetriebsmitteln in Energieübertragungs- und -verteilungsnetzwerken mit Hilfe von Informations- und Kommunikationstechnik (IKT) sowie mit Hilfe der Automatisierungstechnik. Die IKT soll ein Hilfsmittel sein, um die aus der Komplexität resultierenden Probleme des Smart Grid zu lösen, sie spielt damit eine zentrale Rolle im Aufbau eines funktionierenden, dezentralisierten Energieversorgungssystems und stellt den Schlüssel zu dessen Erfolg dar. Sie ist allerdings nur Mittel zum Zweck, um eine möglichst optimierte Lösung im energiepolitischen Dreieck zwischen Umweltverträglichkeit, Versorgungssicherheit und Wirtschaftlichkeit zu erreichen. Die Herausforderung an die IKT besteht heute vor allem darin, rechtzeitig zu erkennen, welcher Bedarf an Informationsaustausch entsteht und wie dieser weitgehend standardisiert werden kann. Die Standardisierung spielt auf nationaler, europäischer und internationaler Ebene eine große Rolle. Hier kann die IKT mit ihren Erfah-

rungen aus der Standardisierung der Mobilfunksysteme viele Hilfestellungen leisten.

Welche Lösungen der IKT im Smart Grid letztlich zum Ziel führen, kann heute noch nicht vorhergesagt werden. Dies wird sich erst durch eine größere Anzahl von Piloten und exemplarischen Lösungen zeigen. Ob zusätzlich zu den heute bestehenden Kommunikationsmedien und -technologien weitere erforderlich sind oder ob bereits mit der bestehenden Infrastruktur weitgehend den kommenden Anforderungen begegnet werden kann, ist ebenfalls ungewiss. Ratsam ist jedoch, die bestehenden Lösungen auf ihre Tauglichkeit und ihre Sicherheitsaspekte hin zu untersuchen. Das soll heute hier in dieser Veranstaltung getan werden.

Meine Damen und Herren, nachdem ich mir das Programm des heutigen Tages angesehen habe, bin ich sicher, dass wir eine hochinteressante Veranstaltung vor uns haben. Ich wünsche Ihnen dazu viel Informationsgewinn und gute Diskussionen.

2 Risikowahrnehmung Energiesicherung International

Prof. Dr. Ortwin Renn, Universität Stuttgart

Zunächst einmal möchte ich mich ganz herzlich dafür bedanken, dass ich heute bei Ihnen zu Gast sein darf und Sie mir den Einführungsvortrag in diese wichtige Fachkonferenz anvertraut haben. Meine Aufgabe ist es, den technischen Horizont zu erweitern, um Sie auf die Sachverhalte hinzuweisen, die wir vor allem aus der Sicht der empirischen Sozialwissenschaften zu Fragen der Sicherheit der Energieversorgung und zu Themen wie Security, Safety, und Zuverlässigkeit beisteuern können.

Lassen Sie mich mit einem Zitat von Konrad Lorenz beginnen, das unsere Situation adäquat widerspiegelt. Er hat in seinem Buch „Die Gefährdung der Menschheit“ eine sehr prophetische Aussage getroffen. Er schreibt:“ Die Gefährdung der Menschheit besteht nicht in der mangelnden Verfügbarkeit zeitgerechter Problemlösungen sondern in dem Mangel an Koordination und sozialen Steuerungen, um die erforderlichen Lösungen zu erkennen und sie zeitnah umzusetzen.“ Wir haben in der Tat für alle Probleme, die im Verlauf dieser Tagung benannt werden, erfolgversprechende Lösungen, sowohl technische als auch soziale, organisatorische, rechtliche. Aber sie zu koordinieren und zeitgerecht einzusetzen und vor allem frühzeitig zu erkennen, wann was notwendig ist, ist die große Herausforderung, vor der wir alle angesichts der anvisierten Energiewende stehen.

Was bedeutet die Energiewende für Deutschland?

Fukushima hat in Deutschland die Karten neu gemischt und diese neue Mischung bedeutet, dass wir vor drei großen Veränderungen in der Gestaltung unseres Energiesystems stehen:

Beginnen wir mit Veränderung Nr.1, die auch schon vor Fukushima auf der Tagesordnung stand, aber jetzt noch einmal klarer geworden ist: Wir stehen weltweit - und in Deutschland ist es genauso - vor der Aufgabe, eine Reduktion der fossilen Energieversorgung von heute rund 80% auf unter 20% bis zum Jahre 2050 herbeizuführen. Das ist eine gewaltige Herausforderung, denn bislang stellt die fossile Energieversorgung die primäre Versorgung weltweit dar. Sie ist dies auch schon seit fast zwei Jahrhunderten. Innerhalb von 40-50 Jahren eine langfristig etablierte Versorgung von einem dominanten fossil getriebenem Antriebssystem auf ein neues System umzustellen, ist an sich schon eine enorme Herausforderung, die sehr viele technische, aber aber auch organisatorische Innovationen erfordert.

Die zweite Implikation der Energiewende ist, dass wir diese fossile Energie durch regenerative Energieträger ersetzen wollen, also nicht durch Kernenergie, auch nicht im nennenswerten Umfang durch Fusion. Im Klartext: Die volatilen und fluktuierenden Energieträger Sonne und Wind sollen die Hauptlast übernehmen, flankiert durch Wasserkraft und Geothermie, die ein Stück weit Grundlast bereitstellen können. Dazu kommt die Biomasse bis zu einem Maximalwert von 10 Prozent, wenn wir die Kriterien der Sozialverträglichkeit einhalten wollen. Vor allem sind es aber die Fluktuationen im erneuerbaren Energieangebot, die uns in Zukunft neue Systemlösungen abverlangen werden, Gerade hier sind sog. smarte und intelligente Lösungen gefragt.

Die dritte Implikation, die häufig vergessen wird, ist die erforderliche dramatische Verbesserung der Energieeffizienz. Bis zum Jahr 2050 müssen wir in Deutschland rund 40% des Primärenergieeinsatzes zusätzlich einsparen, um die Energieziele der Bundesregierung zu

erreichen. Das alles soll so geschehen, dass die Quantität und Qualität der nachgefragten Energiedienstleistungen nicht nennenswert in Mitleidenschaft gezogen werden.

Das sind die drei großen Herausforderungen, die natürlich mit Folgen verbunden sind, vor allem auch im Kontext von IT und Energie. Lassen Sie mich wieder einige wichtige Folgen aufzählen.

Gesellschaftliche Folgen der angestrebten Energiewende

Die erste wichtige Folge, die hier zu nennen ist, ist die systemische Vernetzung der Energieträger. In den Zeiten, in denen ich wie bisher auf Kohle- und Kernenergie im Strombereich und auf Öl und Gas im Wärmebereich setzen kann, ist die Vernetzung relativ einfach. Wir werden aber in Zukunft, wie eben schon Herr Lukas ausführte, sehr viel komplexere Systeme haben. Diese komplexeren Systeme bedeuten auch, und damit sind wir beim IT Einsatz, auf der einen Seite mehr Verwundbarkeiten und Risiken im Bereich der Security, aber eben auch sehr viel mehr neue Möglichkeiten der intelligenten Steuerung, die notwendig sein werden, um Spitzen und Täler auszugleichen und entsprechende Back-up Systeme bedarfsgerecht einzubinden. Das ist eine wichtige Herausforderung, die von IT Seite geleistet werden muss, damit dauerhaft Versorgungssicherheit gewährleistet ist.

Ein zweiter wichtiger Punkt ist die Integration. Wir sprechen heute über Energieversorgung. Wir werden in Zukunft über integrative Infrastrukturen von Dienstleistungen sprechen. Wasser, Energie, IT Information werden sehr viel stärker als heute miteinander verzahnt sein. Dies bringt die erhofften Synergieeffekte, aber eben auch Probleme, wenn sich das eine oder andere gegenseitig behindert. Eine Integration von Architektur, Design, Technologieentwicklung zur Bereitstellung unterschiedlicher Dienstleistungen wird das Rückgrat der künftigen Entwicklung sein. Hier wird deutlich, dass wir eben nicht nur Energietechniker oder Energiebereitsteller ansprechen müssen, sondern uns sehr viel breiter aufstellen müssen und bis heute getrennte Sektoren und Dienstleistungsanbieter interdisziplinär und über Branchen hinweg miteinander verzahnen müssen. Im Rahmen der Energieversorgung können etwa diejenigen, die in der Industrie Hochtemperatur bereitstellen und verbrauchen, Niedertemperaturen für andere Abnehmer abgeben. Diese Form der Integration über verschiedene Kaskadenformen hinweg wird weiter zunehmen, und dazu brauchen wir bessere und intelligentere Steuerungssysteme.

Die dritte Folge betrifft die Verbindung von zentral/dezentral. Ich würde davor warnen zu glauben, dass die gesamte Energieversorgung dezentral wird. Wenn wir uns die Stoffkreisläufe dezentraler Systeme vor Augen führen, sind sie sowohl was Materialverbrauch als auch Energieeffizienz und Flächenverbrauch betrifft keineswegs den zentralen Lösungen überlegen. Vor allem setzt ein Lastenausgleich zwischen Spitzen und Senken eine weiträumige Ausgleichsfunktion voraus. Wenn in einer Region weder Wind weht noch die Sonne scheint, müssen anderen Regionen mit ihrem Überschuss einspringen. Das bedeutet, wir müssen zentrale und dezentrale Versorgungsstrukturen miteinander kombinieren. Diese Mischung setzt wiederum eine intelligente Steuerung voraus. Das ist heute schon ein Problem und wird ein Riesenproblem werden, wenn wir im Rahmen regenerativer Energiesteuerung etwas mehr als 30% der Gesamtenergie über Wind und Sonne generieren. Dann wird es richtig spannend. Wie Sie wissen, war ich Mitglied der Ethikkommission der Bundesregierung „Künftige Energieversorgung“. Bei den Beratungen dort wurde uns schnell klar: 20% an Kernenergie einsparen ist nicht das Riesenproblem. Das bekommen wir noch mit relativ wenig Aufwand und Innovationen hin. Aber über 30% regenerativ Strom zu erzeugen, wird

ein Problem, wenn wir die Grundlast benötigende Industrie und die Ziele der Versorgungssicherheit im Auge behalten. Da werden wir wirklich neue Lösungen brauchen.

Die vierte Folge betrifft die Kooperation Verbraucher/Produzent. In Zukunft wird es neue, Betreibermodelle geben, also einen „Zwitter“ zwischen Konsum und Produktion. Heute ist es schon bei Photovoltaik Anlagen so, dass derjenige, der die Anlage auf dem Dach hat, gleichzeitig Produzent und Konsument (sog. Prosument) ist. Wir werden neue Contractor Modelle entwickeln müssen, die darauf abzielen, Menschen bestimmte Energiedienstleistungen zu einem mehr oder weniger festgelegten Preis anzubieten. Der Gewinn des Contractors besteht dann darin, diese Leistung zunehmend effizient bereit zu stellen. Die heute bereits praktizierten Contractor Modelle funktionieren nicht oder schlecht. Sie bringen nicht die Leistung, die man sich von ihnen versprochen hat. Sie sind aber für die Zukunft sehr wichtig. Wir benötigen effektive und effizient operierende Organisationsmodelle, um die erforderliche Effizienzrevolution zu verwirklichen.

Der letzte Punkt unter den Folgen, den ich noch aufgreifen möchte und bei dem auch IT eine große Rolle spielen wird, betrifft den gesamten Bereich der sozialen und politischen Akzeptanz. Man hat geglaubt, wenn man die Kernenergie auslaufen lässt, haben wir nichts mehr als eitlen Sonnenschein von der Bevölkerung zu erwarten. Dann würde die Akzeptanzproblematik wie von selbst dahinschwinden. Das ist weit gefehlt. Wir werden massive Akzeptanzprobleme bekommen, die vielleicht durchaus in ähnliche Richtung gehen wie das, was wir in der Kernenergie erlebt haben. Immer dann, wenn wir neue Netze verlegen wollen, wenn wir große Pumpspeicherkraftwerke bauen wollen, aber auch tatsächlich zu ganz neuen Smart Modellen aufbrechen, bei denen auch die Autonomie des Verbrauchers ein Stück weit eingeschränkt werden soll, können wir mit Widerständen der betroffenen Bevölkerung rechnen.

Das Institut für Demoskopie in Allensbach hat gerade eine Umfrage veröffentlicht, in dem 83% der befragten Deutschen Verständnis dafür äußern, dass sich die Anwohner von geplanten Stromnetzen gegen diese zur Wehr setzen. Der Anteil von 83% sinkt auf gerade mal 76%, wenn die Frage mit dem Zusatz versehen wird, dass über das Netz Ökostrom verteilt wird und dass die Mehrheit der Bewohner dieses Vorhaben befürwortet. Also hier sind weitere Proteste vorprogrammiert. In die gleiche Richtung zeigt eine Auswertung der Äußerungen, die Bürgerinnen und Bürger in den Energiedialog der Bundesregierung eingebracht haben. Etwa zwei Drittel derjenigen, die sich im Internet zu diesem neuen Energieprogramm gemeldet haben, finden die Energiewende wichtig und richtig. Dann gab es verschiedene Aussagen, denen man zustimmen und die man ablehnen konnte. Ein Aussage war: mit Hilfe der Sonnenenergie wird die Energieversorgung sicherer und billiger. Dazu gab es rund 70% Zustimmung.

Meine Damen und Herren, die eierlegende Wollmilchsau werden wir weder in der Energieversorgung noch irgendwo anders bekommen. Irgendwo müssen wir mit den unvermeidbaren Zielkonflikten umgehen. Und wenn die Illusion in der Bevölkerung vorherrscht, dass wir weder zentrale Netze noch Pumpspeicherkraftwerke brauchen und die Sonnenenergie so billig wird, dass wir sie im Grunde genommen gar nicht mehr fördern müssen, dann laufen wir Gefahr, dass wir in eine Akzeptanzfalle hineinlaufen, die schwer zu überwinden ist. Denn sobald klar wird, dass auch bei erneuerbaren Energieträgern Belastungen auf den Einzelverbraucher zukommen werden, wird dieser sagen, dass er das alles nicht gewusst habe und jetzt nicht mehr zustimmen könne. Frühzeitig und schonungslos die Menschen an unvermeidbare Belastungen zu erinnern und sie darauf einzustellen, ist das A und O vorbeugender Akzeptanzpolitik. Das hinterher zu machen, läuft fast immer ins Leere. Da braucht man nur Stuttgart 21 zu erwähnen. Jetzt ist alles nur noch Stückwerk, wenn es um Kommu-

nikation und Beteiligung geht. Im Nachhinein ist man zwar meistens klüger, aber es hilft dann auch nichts mehr.

Bei diesen 5 Folgen möchte ich es belassen. Ich darf sie noch einmal kurz wiederholen: a) systemische Vernetzung der verschiedenen Angebote, b) die Integration von Design, Architektur, Dienstleistungen und Energieversorgung, c) die möglichst effiziente Vernetzung von dezentralen und zentralen Systemen in den Versorgungsstrukturen, d) die Kooperation zwischen Verbraucher und Produzent und deren quasi synoptische Verbindung und e) neue Akzeptanzfragen.

Zentraler Fokus: Risikowahrnehmung

Das Thema Akzeptanz führt mich zu dem Thema, das Herr Klumpp mir aufgetragen hat, nämlich auch die Wahrnehmung von Risiken mit zu thematisieren. Ich möchte Sie hier nicht mit allzuviel Theorie der Wahrnehmung langweilen. Das können Sie alles gut nachlesen, aber ich will die wichtigsten Punkte herausgreifen, bei denen wir nach Ergebnissen von empirischen Studien Probleme im Energiesektor erleben werden. Zunächst ist es wichtig zu erkennen, dass die Menschen das, was sie wahrnehmen, auch als wahr annehmen. Wir sind gesteuert von Wahrnehmungen, nicht von Fakten oder was wir als Fakten serviert bekommen. Das Wort Wahrnehmung trifft den Sachverhalt genau. Dahinter steckt: als wahr annehmen. Was wir wahrnehmen, ist unsere subjektive Wahrheit. Dann gibt es Wahrgeber. Das sind die Kollegen und Kolleginnen, die hier sitzen. Die geben Wahrheit vor in der Hoffnung, dass sie als Wahrheit angenommen wird. Das ist nicht immer der Fall. Dann gibt es die Wahrmacher. Das sind diejenigen, die Kraftwerke bauen und damit natürlich die Realität beeinflussen. Die schwierigste Gruppe sind die Wahrsager. Die haben zwar kein Wissen, aber sie wissen alles besser. Die Wahrnehmer müssen aus dieser Kakophonie der sehr verschiedenen Eindrücke eine für sie gültige Wahrnehmung konstruieren.

Was sind die empirischen Ergebnisse zur Wahrnehmung von Risiken? Ich möchte hier vor allem auf die Versorgungssicherheit eingehen. Dahinter verbergen sich Kriterien wie Zuverlässigkeit, Funktionalität, Effizienz, Resilienz und ausreichende Backup-Systeme. Wenn wir in der Bevölkerung fragen, wie wichtig dieses Kriterium ist, kommt Versorgungssicherheit zunehmend an vorderster Stelle. Vorher war eher Umweltqualität die Nummer 1 bei den Anliegen der Bevölkerung. Angesichts der vielen Verunsicherungen wollen die Menschen in Deutschland erst mal, dass ihre Versorgung sicher ist. Dahinter steckt natürlich die Sorge, dass wir mit all den Ausstiegen aus den fossilen und nuklearen Energiesystemen, die zusammen mehr als 80% der Energieversorgung bei uns ausmachen, den Einstieg in die neuen Energiestrukturen nicht zeitgerecht schaffen. Kann das überhaupt gut gehen?

Wirtschaft wie Politik haben hier den Auftrag aus der Bevölkerung, sicherzustellen, dass Versorgungssicherheit und Zuverlässigkeit nicht in Frage gestellt werden. Wir wissen, dass dies eine Herausforderung ist. Ich denke, das ist Grundvoraussetzung, ohne die man die Energiewende nicht politisch durchsetzen kann. Gibt es Zweifel an der Zuverlässigkeit der Energieversorgung, wird die Bevölkerungsmeinung sehr schnell umschlagen. Heute befürworten mehr als zwei Drittel der Bevölkerung die Energiewende. Je nach Fragestellung schwankt dieser Wert aber zwischen 38 und 92 Prozent. Darin zeigt sich die allgemeine Verunsicherung. Die Energiewende wird schnell zur Makulatur, wenn plötzlich die Ziele, die einem besonders lieb und wertvoll sind, nämlich die Sicherheit und Zuverlässigkeit, in Frage stehen.

Konsequenzen für die Synthese von Energie und IT

Was bedeuten diese Punkte für die Frage nach den gesellschaftlichen Konsequenzen des IT Einsatzes im Rahmen der Energieversorgung der Zukunft. Erstes Stichwort: Security. Security ist aus Sicht der Psychologie und der Wahrnehmungsforschung ein interessantes Thema. Es gehört zu der Klasse der „attentive topics“. Das sind Themen, die Menschen schnell und intensiv mobilisieren, wenn etwas schief läuft. Solange aber kein negatives Ereignis vorliegt, wird es weitgehend aus der Wahrnehmung und vor allem aber aus den Alltagshandlungen ausgeschlossen. Es ist dann nicht mehr präsent. Die überwiegende Anzahl der Aspekte im Bereich Security gehört in die Kategorie der attentive topics. Wenn wieder irgendwo ein Anschlag oder ein großer Cyber Attacke gemeldet wird, dann schreien alle, wieso so etwas passieren kann. Nach zwei, drei Wochen ist alles vergessen und Otto Normalverbraucher kauft bei Ebay wieder bedenkenlos ein, ohne die eigene Zahlung abzusichern. Security ist also ein Thema, das immer einem schlafenden Hund gleicht. Wenn der Hund geweckt wird, wird er richtig beißen.

Gerade im IT Bereich klaffen bei der Wahrnehmung von Security Einstellung und Verhalten auseinander. Ungefähr 80% halten etwa die Verschlüsselung der eigenen Daten für sehr wichtig, tun es aber nicht, weil es ihnen zu aufwändig erscheint. Hier tritt eine gewisse Brüchigkeit zwischen der Bequemlichkeit auf der einen Seite und einer sehr hohen Sensibilität, wenn etwas passiert, zu tage. Im Schadensfall erwartet man interessanterweise weniger die Lösung bei sich selbst als beim Staat. Da muss der Staat irgendetwas tun. Diese Kluft zwischen eigener Nachlässigkeit im privaten Bereich und einer Überanforderung an staatliche Regulierung bestimmt heute weitgehend das Spannungsverhältnis, in dem wir uns im Bereich Security bewegen.

Wenn Sie in diesem Zusammenhang an Smart Meter denken, können Sie sich schnell Szenarien vorstellen, beispielsweise, dass jemand über das Internet alle Kühlschränke und Gefrierschränke gleichzeitig zum Laufen bringt. Dann bricht das Netz zusammen. Das sind natürlich für Hacker außerordentlich interessante und attraktive Möglichkeiten. Diese Hacker sind in der Regel nicht wirklich politisch motiviert. Sie genießen es, einmal im Leben Macht ausüben zu können: etwas zu tun, was alle merken. Hacker sind nicht diejenigen, die den Kapitalismus zerstören oder Al Kaida unterstützen wollen, sondern es sind Leute, die häufig von Allmächtsphantasien motiviert Freude daran haben, Sand ins Getriebe zu streuen. Mit dem Smart Grid und seiner externen Steuerung durch Versorgungsunternehmen, bekomme ich als Hacker ein wunderbares Mittel an die Hand, die Energieversorgung so zu steuern, dass alle Waschmaschinen mitten in der Nacht angehen. Sofern technisch diese Möglichkeiten bestehen, sollte man vorab die Risiken abschätzen und möglichst ausschalten, denn ein Hackerangriff auf die deutschen Waschmaschinen hätte bei allem Schmunzeln, das diese Aussage gerade bei Ihnen auslöst, eine außerordentlich hohe Öffentlichkeitswirksamkeit, die eine Weiterverbreitung des Smart Grid infrage stellen könnte.

Zweites Stichwort: Autonomieverlust. Wenn wir tatsächlich in die Richtung Smart Meter gehen, wobei das Potenzial einer solchen Maßnahme ja durchaus umstritten ist, müssen wir einen Teil der Autonomie über die Steuerung der Elektrogeräte im Haushalt an eine zentrale Steuerungseinheit abgeben. Aus Umfragen wissen wir, dass Autonomieverluste in modernen Gesellschaften als äußerst heikel einzustufen sind. Man muss sich wirklich fragen, wie viel eine Außensteuerung des Stromverbrauchs bringt, um einerseits so viel Geld in die Infrastruktur zu investieren und andererseits ein enormes Potenzial an Vertrauensvorschuss zu fordern, dass Haushalte freiwillig auf einen Teil ihrer Autonomie verzichten. Ich habe in den Proceedings einer ihrer früheren Veranstaltungen gelesen, dass durch smart grid ein Gewinn von maximal 10 Prozent bei dem Ausgleich von Spitzenbelastungen zu erwarten wäre.

Kleinvieh macht auch Mist, aber vielleicht sollte man doch lieber erst mal in Großvieheinheiten investieren.

Granger Morgan von der Carnegie Mellon University hat für die USA ausgerechnet, was notwendig wäre, um die Batterien von E-Fahrzeuge als Speicher zu nutzen. Nach seinen Berechnungen ist das Potenzial von Autobatterien als Energiepuffer oder Speicher zu dienen, ohnehin relativ gering. Viel entscheidender ist aber der wirtschaftliche Aspekt. Damit das Geschäftsmodell funktioniert, kann man Autofahrer maximal 100 \$ pro Jahr anbieten. Wenn Sie 1 Million E-Fahrzeuge haben, ist das viel Geld, das Stromversorger für diese Speicherleistung ausgeben müssen. Wer wird aber für 100 \$ im Jahr auf die Autonomie verzichten, dann zu fahren, wann man will? Keiner, nicht einmal ein Hartz IV Empfänger. Daher müssen wir überlegen, ob es überhaupt sinnvoll ist, in die Nutzung von Autobatterien als Speicher zu investieren, wenn wir zum Schluss kommen, dass es finanziell überhaupt nicht attraktiv ist.

Die Frage des Autonomieverlustes ist noch zu wenig im Fokus der angewandten Forschung. Das kann man bei der Steuerung von PKWs gut illustrieren. Wir können heute im Prinzip Automobile durch Computer steuern lassen. Wenn man allerdings Autofahrer fragt, ob sie das wollen, stoßen wir auf einhellige Ablehnung. Sie wollen Assistenzsysteme, die sie ausschalten können. Autonomie ist ein wichtiges Gut, oft ein wichtigeres Gut als Bequemlichkeit oder Funktionalität. In einer Welt, in der wir immer enger verzahnt sind und in der immer mehr Menschen in anonymen Verhältnissen leben, ist das, was wir an Autonomie noch haben, hoch geschätzt. Viele fahren Auto, um diesen Autonomieeffekt zu erleben und nicht, um von A nach B zu kommen.

Letztes Stichwort: Privatsphäre und Datenschutz. Dazu gibt es viele Untersuchungen, gerade im Zusammenhang mit Energiesystemen. Auch hier erleben wir wieder die typischen Merkmale eines attentive topics. Das Thema kocht immer wieder hoch, wenn es einen Skandal gibt, und es verflüchtigt sich auch schnell, wenn längere Zeit nichts Aufregendes passiert. Wie sich das Thema weiter entwickeln wird, ist deshalb schwer vorhersehbar. Wenn es tatsächlich mehrere Ereignisse hintereinander geben würde, bliebe es hoch auf der Agenda. Wenn nicht, verbleibt es als „Schläferproblem“.

Gleichzeitig haben wir im Datenschutz eine ganze Reihe von organisierten Gruppierungen, die sehr darauf achten, dass Datenschutz bis auf den i-Punkt eingehalten wird. Die allgemeine Öffentlichkeit ist in diesem Punkt weit weniger sensibel als die organisierte Öffentlichkeit. Bei dem Thema des Autonomieverlustes ist es umgekehrt. Wir haben wenig organisierte Gruppen, die sich diesem Thema widmen. Es ist also wichtig, zwischen organisierter und nicht organisierter Öffentlichkeit je nach Thema zu differenzieren.

Als Fazit bleibt hier festzuhalten: Auf der Basis der neuen energiepolitischen Ausgangslage und der Wahrnehmung von Risiken müssen die drei Themen Security, Autonomieverlust und Datenschutz parallel gesehen und in ihrer Vernetzung betrachtet werden. Diese Probleme frühzeitig und konstruktiv unter Einbeziehung der organisierten und nicht organisierten Öffentlichkeit anzugehen, wird für die weitere Gestaltung der Technologien und den Ausbau der Netze von entscheidender Bedeutung sein.

Was ist zu tun?

Wohin führen diese Überlegungen? Was folgt aus dieser Diagnose für die Therapie. Ich denke, wir brauchen eine Art von Koevolution. Ich bin mir bewusst, dass sich ein Wort wie

Koevolution immer außerordentlich gelehrig anhört, ohne allzuviel auszusagen. Hier passt der Begriff aber wirklich und ist auch aussagekräftig. Gemeint ist damit, dass es sich um parallele Entwicklungen handelt, die sich gegenseitig beeinflussen und die sich auch gegenseitig befruchten müssen. Auf der einen Seite die sich herausbildenden neuen Energietechnologien und auf der anderen Seite die dazu angepassten Netz- und Infrastrukturen mit der entsprechenden IT-Unterstützung! All dies muss weiterhin abgestimmt sein mit den Verhaltensweisen und Präferenzen derjenigen, die später mit diesen Technologien leben müssen. Diese Art von Koevolution setzt eine wirklich intensive interdisziplinäre Zusammenarbeit zwischen den Technikern verschiedener Richtungen, Naturwissenschaftlern, Sozial- und Wirtschaftswissenschaftlern und auch Kulturwissenschaftlern voraus.

Die zweite Lehre, die eng mit der ersten zusammenhängt, betrifft die Forschung. Wir müssen mehr in die Erforschung der systemischen Struktur der Koevolution von Technik, Organisationsformen und menschlichen Verhaltensweisen investieren. Vor allem wenn wir in Zukunft mehr „Prosumenten“ haben werden, wenn tatsächlich mehr Dezentralität das System bestimmt und wenn neue Infrastrukturen auf Akzeptanz angewiesen sind, ist das Verhalten der Einzelnen systemrelevant. Ob ich mehr oder weniger Öl verbrauche, ist eine Frage des Geldbeutels. Wenn ich mich in einem integrierten System befinde, muss ich selbst entscheiden, wie viel Integration, wie viel Eigenproduktion und wie viel Systemakzeptanz ich möchte. Wenn man den gesamten Energiemarkt vor Augen hat und beispielsweise sein Eigenheim intelligent mit Strom und Wärme versorgt, stoßen wir auf ein großes Potenzial, das sich aber nur realisieren lässt, wenn die Bewohner dies bewusst ansteuern und auch entsprechend handhaben können.

Mein letzter Punkt betrifft das Thema Vertrauen. Alles, was an Informationen den Menschen zum Thema Energie, Energienachfrage, Energieangebot angeboten wird, ist im Prinzip etwas, was sie aus eigener persönlicher Erfahrung nicht nachprüfen können. Sie sind auf Erfahrungen Dritter angewiesen, und müssen deren Aussagen entweder mehr oder weniger blind vertrauen oder sie ablehnen. Vor 150 Jahren war etwa 70% unseres Wissens Primärwissen, das wir selber sinnlich erfahren haben. Heute sind es weniger als 10%. Die Risiken, denen wir heute ausgesetzt sind, sind fast alle kommunikativ vermittelt. Ob BSE gefährlich ist, kann keiner von uns überprüfen. Das hat uns jemand mitgeteilt. Ob es über uns ein Ozonloch gibt, kann niemand aus eigener Anschauung belegen, sondern wir vertrauen den Wissenschaftlern, die das mit komplizierten Messgeräten herausgefunden haben.

Das meiste, was wir auch über Energie erfahren, können wir ebenfalls nicht nachprüfen. Wir sind auf die Aussagen Dritter angewiesen. Dies führt zu der Schlüsselfrage: Vertraue ich den Institutionen, die mir dazu die notwendigen Informationen geben, ja oder nein? Wenn ich „nein“ sage, dann will ich Nullrisiko. Denn wenn ich bei der Bewertung solcher Risiken auf Informationen durch Dritte angewiesen bin, diesen Dritten aber nicht vertraue, dann lasse ich mich auf keine Kosten-Nutzen-Bilanz ein. Dann will ich Nullbelastung. In einer solchen Situation ist es durchaus verständlich, dass einer in einer Podiumsdiskussion zur Grünen Gentechnik darauf beharrt, dass er diese Technologie nicht will, egal wie hoch das Risiko auch sein möge. Und er hat links eine Zigarette, rechts ein Glas Bier und draußen einen Porsche stehen. Vertraue ich dagegen einer der Quellen, dann bin ich bereit, auf Basis der mir vertrauenswürdigen Informationen ein eigenes abgewogenes Urteil zu fällen.

Es gibt noch eine dritte Reaktionsweise: Wenn ich nicht weiß, wem ich trauen kann aber dennoch einem vertrauen will, dann werden periphere Merkmale entscheidend. Das sind Merkmale, die mit der Sache nichts zu tun haben. Sie sehen z.B., dass Herr Renn einen langweiligen Schlips trägt. Daraus kann man schließen, dass er offenkundig nicht in der Lage, die neuesten Daten für uns attraktiv aufzubereiten. Die Angewiesenheit auf periphere Merkmale als Indikatoren der Vertrauenswürdigkeit sind für Informationsträger sehr frust-

rierend. Zu den peripheren Merkmalen gehören vermutete Interessenabhängigkeit, Sprachführung, Argumentationsstil oder schlichtweg Kleidung und Auftreten. Interessanterweise ist Eloquenz oft kontraproduktiv, wenn es um periphere Merkmale geht. Viele fühlen sich dann an den Autohändler erinnert, bei dem sie ihr letztes Fahrzeug erstanden haben und das schon nach einigen Monaten den Geist aufgegeben hat. Wer Eloquenz zeigt, will einem etwas aufdrängen. So zumindest die landläufige Meinung!

Vertrauen als Schlüsselgröße für eine gelingende Energiewende

Wir kommen nicht daran vorbei, dass wir in der Energiewende Vertrauen brauchen. Dazu gehört auch, dass wir periphere Merkmale aufbauen, die vertrauenserweckend sind. Im Zentrum müssen aber Maßnahmen stehen, die eine Basis für die Zuschreibung von Vertrauenswürdigkeit bilden. Zunächst müssen wir deutlich machen, dass wir irgendwo zwischen absurden Illusionen und möglichen Entwicklungslinien eine klare Grenze ziehen. Schließlich gehört zur Vertrauensbildung auch die Ehrlichkeit und Aufrichtigkeit, unabhängig von unseren eigenen Wünschen und Präferenzen die Vor- und Nachteile einer jeden Alternative in der Energiepolitik ungeschminkt darzustellen. Schließlich sollten wir das auch selber beherzigen, was wir anderen predigen.



Für mich ist entscheidend, dass diejenigen, die Kraft ihres Amtes oder ihrer institutionellen Einbindung ein Stück weit Vertrauensvorschuss genießen, gemeinsame Anstrengungen unternehmen, um den betroffenen Menschen die Chancen und Risiken der Energiewende möglichst eindeutig und handlungsbezogen nahezubringen. Ob Regierung, Unternehmen oder Bürgerinitiative, in diesem Punkt gibt es bei aller Gegensätzlichkeit in Detailfragen einen großen Konsens. Wir alle wollen, dass die Energiewende gelingt. Deshalb möchte ich zum Schluss an alle hier im Saal die Bitte äußern, durch ihre Arbeit und ihre Aktivitäten auch kommunikativ an dem Gelingen der Energiewende mitzuwirken.

3 Sicherheit für das Energieinformationsnetz

Prof. Dr. Claudia Eckert, Fraunhofer Institut AISEC, München-Garching, TU München

Nach diesen wunderbaren Vorrednern ist es für mich schwer, einen neuen Anfang zu finden. Deshalb möchte ich zunächst direkt an meine Vorredner anknüpfen. Zunächst möchte ich ein Wort von Ihnen, Herr Renn, aufgreifen: die Sicherheit ist ein schlafender Hund. Das hat mir gut gefallen, ist aber vielleicht noch nicht ganz das, wie ich die Sicherheit sehen möchte. Auf die Schnelle ist mir keine geeignete Metapher eingefallen, aber wenn es denn schon ein Hund sein soll, dann doch bitte so etwas wie ein Blindenhund, der uns leitet, der uns führt, der uns hilft. Dann sind wir bei einer Bemerkung von Ihnen, Herr Goerdeler. Ich würde die Verbindung, die Sie zwischen Geschäftsmodellen, Geschäftsmöglichkeiten und Sicherheit aufgezeigt haben, gern ein bisschen anders betonen. Für mich ist Sicherheit der Enabler für neue Geschäftsmodelle. Das bedeutet, dass man nicht erst Geschäftsmodelle entwickeln sollte, um dann zu schauen, was man als Sicherheit noch braucht, sondern meine Bitte wäre, dass man ganz gezielt die Sicherheit von Anfang an mit bedenkt, in den Gesamtsystemansatz integriert und dadurch einen Mehrwert an Qualität schafft. Durch integrierte Sicherheit schaffen wir auch neue Möglichkeiten der IKT Nutzung und damit komme ich zu Ihnen, Herr Kollege Lukas: wir brauchen die Sicherheit im Future Internet, in den Energienetzen der Zukunft oder in den anderen Themen, um diese neuen Themen auch wirklich voranzubringen, so dass sie auch in der Bevölkerung auf Akzeptanz stoßen. Da bin ich natürlich voll bei Ihnen.

Überblick



1. Motivation
2. Bedrohungslage und Herausforderungen
3. Sicherheitskonzepte: Beispiele
4. Domänen-spezifische Sicherheitsreferenzarchitekturen
5. Zusammenfassung

Bild 1

Worüber möchte ich heute zu Ihnen sprechen? (Bild 1) Das Thema ist die Sicherheit in den Energie-Informationsnetzen der Zukunft, den Smart Grids. Ganz kurz möchte ich zunächst noch einmal motivieren, dass wir uns hier tatsächlich in einem hoch komplexen Feld bewegen.

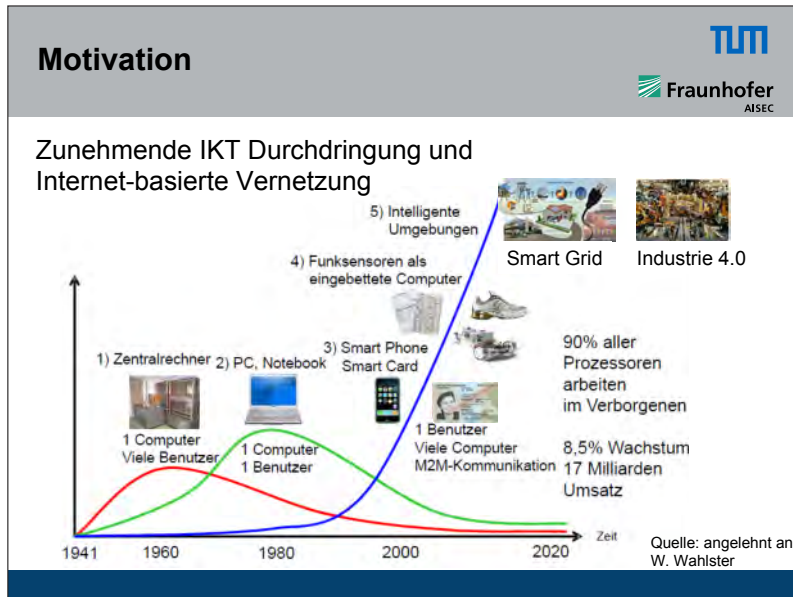


Bild 2

Die Energiesysteme und –netze der Zukunft sind natürlich sehr stark von IKT durchdrungen, sehr heterogen, hochgradig vernetzt und unterliegen einer hohen Dynamik (Bild 2). Die Sicherheit und Verlässlichkeit der IKT ist damit grundlegend, um die Stabilität und Sicherheit inklusive Versorgungssicherheit der zukünftigen Energiesysteme sicherzustellen. Ich werde deshalb in dem Vortrag auch noch einmal kurz auf die schon an mehreren Stellen erwähnte Bedrohungslage eingehen, um den Handlungsbedarf zu motivieren. Ich möchte einzelne Bedrohungen nicht im Detail durchspielen, sondern das Bewusstsein dafür schärfen, dass es im Bereich der Sicherheit in Energie-Informationsnetzen noch Einiges zu tun gibt. Meine Message heute ist aber gleichzeitig auch: Es ist nicht hoffungslos. Es gibt Probleme, aber wir arbeiten an vielen Stellen schon an sehr guten Lösungen. Diese Arbeiten müssen jedoch noch weiter systematisiert und zusammengeführt werden. An dieser Aufgabe arbeite ich in letzter Zeit mit der dankenswerten Unterstützung durch das NEWISE-Projekt der Alcatel-Lucent Stiftung. Unser Ziel hierbei ist es, einen systemischen Ansatz zu entwickeln und gleichzeitig die Komplexität zu reduzieren. Dazu betrachten wir so genannte Domänen innerhalb der Smart Grids, und entwickeln domänenspezifische Sicherheitsarchitekturen und Lösungskonzepte. Diese Domänen spiegeln die Anforderungen und Rollen von Teilnehmern in speziellen Bereichen, den Domänen wider. In einem nächsten Schritt sind dann die Domänen zu koppeln, indem Schnittstellen zwischen ihnen definiert und umgesetzt werden. Im heutigen Vortrag möchte ich Ihnen deshalb kurz den domänenbezogenen Ansatz, den wir weiter verfolgen werden, erläutern.

Motivation





Energie-Informationsnetze, Smart Grids

- Integration von **physischen Umgebungen, Prozessen und IKT**

Charakteristika

- Vielzahl **autonomer Geräte**
- **heterogene Netze**
- **Dezentrale** Verwaltung, Steuerung
- **Offener** Marktplatz



Herausforderung:

- **Steuerung und Überwachung** komplexer, vernetzter Systeme:
Anforderungen an Daten: **korrekt, vollständig, aktuell, ...**

Bild 3

Ich möchte beginnen mit Bild 3, das die Komplexität von SmartGrids verdeutlicht. Das Bild veranschaulicht ein Smart Grid als ein so genanntes Cyber-Physical System. Das sind Systeme, die durch das Zusammenführen physischer und IKT getriebener Systeme entstehen. Smart Grids sind eine wichtige Ausprägung von solchen Cyber-Physical Systems (CPS). Ein CPS ist durchdrungen von Hardware Komponenten und eingebetteter Software. Es sind sehr Software intensive Komponenten, die über heterogene Vernetzungstechnologie mit einander gekoppelt sind. Diese Komponenten sind in eine physische Umgebung eingebettet und es entstehen neue Betreibermodelle und Nutzungsszenarien für solche Systeme, wofür gleichzeitig neue Geschäftsmodelle erarbeitet und Dienste entwickelt werden. Hier sieht man auch die Verbindung zum Thema Cloud-Computing, da Cloud-basierte Bereitstellungsstrukturen auch im Smart Grid eine große Rolle spielen werden. Insgesamt sind die CPS durch eine sehr starke Heterogenität geprägt. Sie bestehen aus einer Vielzahl autonom agierender Komponenten, Sensoren, Aktoren. Sie sind durch ganz unterschiedliche Vernetzungstechnologie miteinander gekoppelt, wodurch sich dann auch Kaskadeneffekte aufgrund von Abhängigkeiten ergeben. Sie, Herr Renn, haben gesagt, dass wir nicht zu sehr in das Dezentrale gehen dürfen, sondern eine Mischung aus zentraler und dezentraler Organisation anstreben müssen. Das ist ganz richtig. Smart Grids werden aber auf jeden Fall dezentrale Managementanteile aufweisen, die es zu beherrschen gilt.

Zur Steuerung und Beherrschung der komplexen Systeme werden Informationen benötigt. Daten müssen rechtzeitig an den Stellen sein, wo sie benötigt werden. Sie müssen vollständig sein. Sie müssen korrekt sein und ggf. auch vertraulich verarbeitet werden. Damit ist ganz klar, dass wir die Sicherheit dieser Informationen gewährleisten müssen.

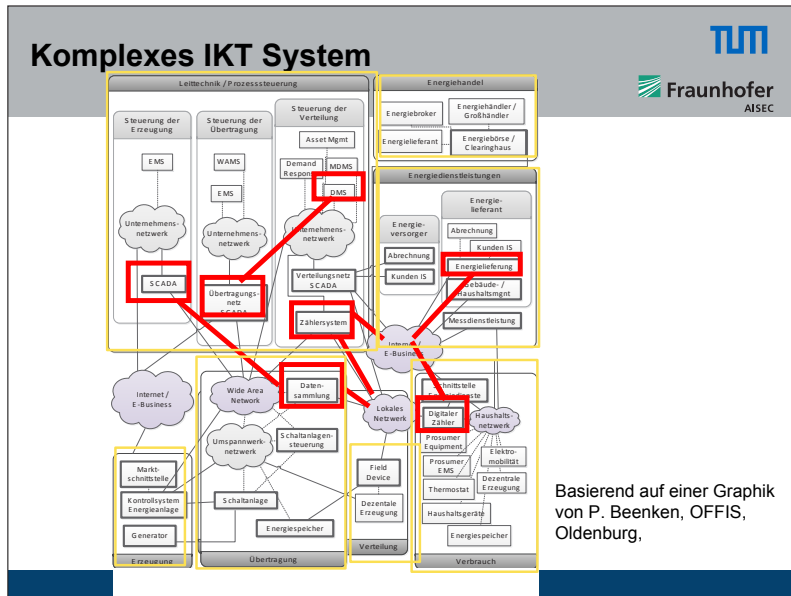


Bild 5

Bild 5 zeigt die NIST Referenzarchitektur für Smart Grids. Die deutsche Adaption stammt von Frau Dr. Behnken, vom OFFIS in Oldenburg, herzlichen Dank für die Bereitstellung der Grafik. Die Grafik veranschaulicht die wesentlichen Domänen (gelb umrandet) und die Akteure in einem Smart Grid. So kann man u.a. eine Privathaushaltsdomäne, eine Verteildomäne, eine energieerzeugende Domäne usw. identifizieren. Das sollten wir im Hinterkopf behalten, weil es uns gleich wieder begegnen wird. Ein Smart Grid als Gesamtsystem ist ein komplexes System, aber man kann auf der Basis von Domänen eine Struktur darüber legen. Sobald wir die Möglichkeit haben, ein System zu strukturieren, haben wir damit die Möglichkeit, Teilbereich zu isolieren, getrennt von anderen zu analysieren und auch Lösungen dafür losgelöst von anderen Bereichen zu integrieren. Kontrollpunkte können domänenspezifisch identifiziert und etabliert werden und wir sind in der Lage, die Systeme besser zu beherrschen.

Natürlich umfassen die einzelnen Domänen nach wie vor viele Komponenten, die einer Vielzahl von Bedrohungen ausgesetzt sind (rot eingerahmt). Einzelne Komponenten können unterwandert sein, es können unsichere Kommunikationsverbindungen etabliert sein, Schadsoftware kann verbreitet werden und auch die Komponenten innerhalb einer Domäne, können sich kaskadierend beeinträchtigen. Strukturierung allein löst natürlich keine Sicherheitsprobleme; es gilt die jeweiligen Bedrohungen zu identifizieren und mit zugeschnittenen Maßnahmen, die Risiken zu minimieren.

Bedrohungslage und Herausforderungen




Bedrohungen für Komponenten

- Ausspähen sensibler Daten,
- Einschleusen gefälschter Daten
- Gefälschte Steuerungssignale ...



z.B. Smart Meter

- Manipulation von Stromverbrauchsdaten
- Gefährdung der Versorgungssicherheit
- ...

Herausforderungen:


- Manipulationsresistente Hardware
- Sichere Komponenten-Identifikation (M2M)


Bild 6

Ich möchte deshalb im Folgenden ganz kurz auf wesentliche Problembereiche eingehen, ohne ins Detail zu gehen. Wir müssen uns um Bedrohungen auf unterschiedlichen Ebenen kümmern, wenn wir die Sicherheit vom Energieinformationssystem garantieren möchten. Ausgangspunkt muss die Hardware sein (Bild 6). Betrachten wir also zunächst die Hardware-Basis, zu der Smart Meter ebenso gehört wie Komponenten von SCADA Netzen, die u.a. zum Überwachen von Netzen, Anlagen, Infrastrukturen verwendet werden. Dann ist offensichtlich, dass eine Manipulation dieser Basis-Komponenten das gesamte System kompromittieren könnte. Wenn die Hardware-Komponenten schon nicht das tun, was sie eigentlich tun sollen oder wenn sie angreifbar sind, weil man z.B. physisch auf diese Komponenten direkt zugreifen kann und man sie manipulieren kann, ist bereits die Basis erschüttert. D.h. wenn wir hier schon angreifen können, ist es natürlich möglich, gefälschte Steuerungssignale auszusenden, gefälschte Daten einzuspeisen, Daten zurückzuhalten usw. Damit hätten wir das ganze System unterminiert. Dass dies durchaus möglich ist, haben wir anhand von handelsüblichen Smart Metern bei uns im AISEC- Test-Labor in München gezeigt. Das ist kein Hexenwerk. Man muss kein Spezialequipment haben, um tatsächlich einen handelsüblichen Smart Meter so zu manipulieren, dass man all dies machen kann, was auf der Folie steht: auslesen der Daten, die Daten ändern, zurückhalten, umlenken usw. Werden solche manipulierten Geräte ausgerollt und dann auf Knopfdruck dieses Fehlverhalten aktiviert, kann natürlich sogar die Versorgungssicherheit gefährdet sein. Das bedeutet, dass wir hier investieren müssen. Wir müssen Komponenten bauen, die manipulationsresistenter sind. Wir wissen, wie so etwas geht. Wir kennen geeignete Techniken und könnten diese in die Architekturen der Komponenten integrieren. Das erfordert eine Abkehr der üblichen Prozesse, dieser Weg muss beschritten werden. Die sichere Komponentenidentifikation ist ein weiteres großes Themenfeld, was auch schon angesprochen wurde. Wir haben im Smart Grid natürlich viele Komponenten im Einsatz, die miteinander kommunizieren, Daten austauschen. Da ist häufig kein Mensch mehr in der Loop, sondern alles läuft automatisiert und transparent ab. Wir brauchen deshalb gute, skalierende Ver-

fahren, die effizient und effektiv sind, natürlich auch kosteneffektiv, um beliebige Komponenten identifizieren zu können. Auch hier werden bereits seit einiger Zeit Techniken entwickelt, die dies leisten.

Bedrohungslage und Herausforderungen

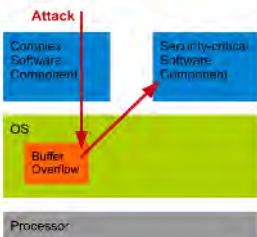




Bedrohungen für Software und Dienste

- Manipulierte Dienste/Systeme
- Daten stehlen, ausspähen, ändern, ...
- Störung sicherheitskritischer Prozesse

Beispiel: Life Hack Demo RSA Conf 2010



The diagram illustrates a security attack path. At the top, a red arrow labeled 'Attack' points to a blue box 'Complex Software Component'. A red arrow points from this box to a blue box 'Security-critical Software Component'. Below these, a green box labeled 'OS' contains a red box 'Buffer Overflow'. A red arrow points from the 'Buffer Overflow' box to the 'Security-critical Software Component' box. At the bottom, a grey box labeled 'Processor' is shown.

Einschleusen von Malware über Software-Lücke in Kernkraftwerk,


Herausforderungen:

- **Vertrauenswürdige Umgebungen**
- **Sicherheit als integrierter Service**
- **Durchgängiges Sicherheits-Health-Monitoring**

Bild 7

Was braucht man noch? Wo sind noch ganz wesentliche Bedrohungsfelder? Wenn man ein Stück weiter geht (Bild 7) von der Hardware der Komponenten oder der eingebauten Komponente in die Software, wissen wir alle, was da für eine Vielzahl von Problemen lauert. Ein SmartGrid umfasst neben den eingebetteten Komponenten auch Datenbanken, Webportale, Services etc.. Somit stehen wir der gesamten Problematik der Webdienste mit ihren vielen Verwundbarkeiten gegenüber. Dazu gehören Softwaresysteme, in die Schadcode eingebracht werden kann, die unautorisiert auf Daten zugreifen, diese lesen und manipulieren können. Eingebettete Systeme sind besonders gefährdet, weil sie nicht viele Sicherheitskonzepte zum Schutz vor derartigen Bedrohungen aufweisen. Dieses ist derzeit ein großer Problembereich. Benötigt werden neue Sicherheitsarchitekturen, die die erforderlichen Absicherungen im Design verankern, das Stichwort hier ist: Secure by Design. Was wir also benötigen, ist ein Schritt nach vorne auch bei der Softwareentwicklung. Wir brauchen betriebssystemnahe Software, die isolierte Umgebungen durchgehend unterstützt, so dass eine Schadensausbreitung minimiert wird. Wir benötigen zudem eine permanente Überwachung in den Systemen in Bezug auf den gewünschten Sicherheitszustand.

Bedrohungslage und Herausforderungen

Bedrohungen im Netz der Netze (u.a. GSM/LTE, WLAN, SCADA)

- Keine End2End Sicherheit
- Mangelhaftes Identitäts- und Schlüsselmanagement
- Kaskadierende Angriffe wg fehlender Isolation

Beispiel: Stuxnet 2010





Herausforderungen:

- Absicherung von drahtlosen Sensornetze, u.a. SCADA
- Abgestufte Sicherheitsdomänen

Bild 8

Der dritte Bereich ist die Vernetzung (Bild 8). Neben abgesicherten Komponenten benötigen wir sichere Kommunikationsverbindungen. Die Komponenten im Smart Grid interagieren über sehr unterschiedliche Vernetzungstechnologien, die jede für sich Sicherheitskonzepte beinhaltet, die aber nicht unbedingt aufeinander abgestimmt oder interoperabel sind. Im Zusammenspiel dieser verschiedenen Techniken gibt es Brüche, wenn sie auf einmal in diesen komplexen Szenarien zusammengekoppelt werden. Wir kennen diese Effekte, die zu kaskadierendem Ausbreiten von Schadcode führen können. All das müssen wir vor Augen haben, wenn wir solche Systeme zu einem Energieinformationsnetz der Zukunft verbinden. Wir müssen uns genauer anschauen, welche Systeme da eingebunden werden. Häufig handelt es sich um Systeme, die früher vollkommen isoliert betrieben wurden, z.B. die schon mehrfach genannten Sensornetze oder SCADA-Systeme. Deren Absicherung wird eine wesentliche Aufgabe im SmartGrid sein. Auch hierfür existieren bereits einige Lösungsansätze und -techniken, indem wir beispielsweise die Netze strukturieren und dadurch kontrollierbare und abgrenzbare Einheiten bilden.

Sicherheit im Smart Grid

Herausforderungen

Komponenten und System-Architekturen:

Secure by Design & Secure during Operation

Neue/erweiterte Sicherheitskonzepte und -verfahren

- Manipulationsresistente Hardware, z.B. Smart Meter
- Sichere Identität, M2M, z.B. Schlüsselmanagement, PKI
- Sichere Eingebettete Systeme, z.B. sichere Hypervisor
- Sicherheit als Service (u.a. in der Cloud), z.B. Sicherheits-Monitoring

Neue/erweiterte Sicherheitsarchitekturen!

Bild 9

Wir haben nun die verschiedensten Problemfelder vor Augen. Was wir brauchen (Bild 9), sind neue erweiterte Konzepte, Secure by Design. Wir müssen auch im laufenden Betrieb die Systeme durchgehend überwachen, kontrollieren, angleichen, nachjustieren. Wir müssen die Systeme in ihren Architekturen so vorbereiten, dass man dynamisch auf geänderte Sicherheitsanforderungen durch eine Rekonfiguration schnell und effektiv reagieren kann. Es sind Kontrollverfahren zu entwickeln und zu integrieren, so dass nach dem Prinzip des 'Secure during Operation', mittels dieser integrierten Tests kontinuierlich die Einhaltung von Sicherheitsvorgaben überwacht wird.

Wir brauchen also neue Konzepte, oder müssen bestehende Konzepte erweitern und benötigen dann zusätzlich noch, das ist ganz wesentlich, die systemische Sicht. Sichere Komponenten und Mechanismen zur Absicherung der Kommunikation sind wichtige einzelne Bausteine. Aber um ein Haus zu bauen, brauche ich einen Plan, eine Blaupause, wie sich das alles vernünftig zusammenfügen soll. Jede Komponente an sich kann toll sein, aber wenn ich sie an die falsche Stelle setze, ist sie nutzlos oder vielleicht kontraproduktiv.

Sicherheitskonzepte : Beispiele





Sicherer SmartMeter/Gateway

- AISEC-Prototyp eines Sicherer Smart Met
- Angepasstes [Hardware Security Modul](#)
- [effiziente \(kryptographische\) Protokolle](#)
- Erfüllt BSI [Protection Profile](#)



Sicheres Eingebettetes OS

- Hypervisor : [Isolierung, Sandboxes](#)
- VMI mit [Sicherheitsdiensten](#):
 - Erkennen von unsicheren Zustände
 - Reaktion. Schadensbegrenzung



10

Bild 10

Es gibt natürlich auch schon Lösungen (Bild 10). Wie ich vorhin schon sagte, haben wir in unserem Testlabor am AISEC handelsübliche Smart Meter gehackt und gezeigt, wie man sie manipulieren kann. Wir haben aber auch im Gegenzug einen sicheren Smart Meter Prototyp entwickelt, der das Protection Profile des BSI erfüllt. Damit wollten wir aufzeigen, wie eine sichere Lösung aussehen könnte und dass eine solche Lösung pragmatisch entwickelt werden könnte. Das Know How, das man hierfür benötigt, ist also da. Man weiß, wie man solche Probleme lösen kann. Auch in dem Bereich der sicheren Betriebssystemumgebung weiß man, wie man so etwas im Prinzip macht. Wir arbeiten am AISEC an solchen Lösungen, die die erforderlichen isolierten Umgebungen zur Verfügung stellen. Diese Beispiele sollen verdeutlichen, dass die Problemlage keineswegs hoffnungslos ist. Hier entstehen schon die verschiedensten Technologien, die geeignet sind für einen Einsatz im SmartGrid.

Sicherheitskonzepte : Beispiele

Sicherheitsmonitoring: z.B.

- Domänenübergreifender Austausch von Informationen über Sicherheits-Vorfälle
- Frühzeitige Erkennung von Bedrohungen,
- anonyme Zertifikate,
- P2P-Overlay-netz,
- Secure Multiparty Protokoll,
- Anonymitäts-Wahrung

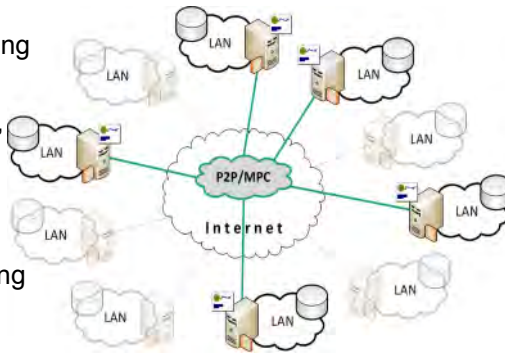


Bild 11

Als Beispiel (Bild 11) für den Netzwerkbereich möchte ich auf eine in der Entwicklung befindliche Lösung hinweisen, die derzeit im Rahmen des BMBF Projekts ASMONIA entsteht. Der Ansatz ermöglicht es, Sicherheitsvorfälle in einem komplexen Netzumfeld frühzeitig zu erkennen. Wir setzen dabei auf ganz klassische Technologien wie Peer-to-Peer Overlay Netze auf, um unter Nutzung spezieller Protokolle, die die Privatsphäre der Beteiligten wahren, ein IT-Frühwarnungssystem aufzubauen. Ein derartiges System kann man natürlich dann auch in ein Energieinformationssystem übertragen.

Sicherheits-Referenzarchitekturen

Domänen-spezifisch

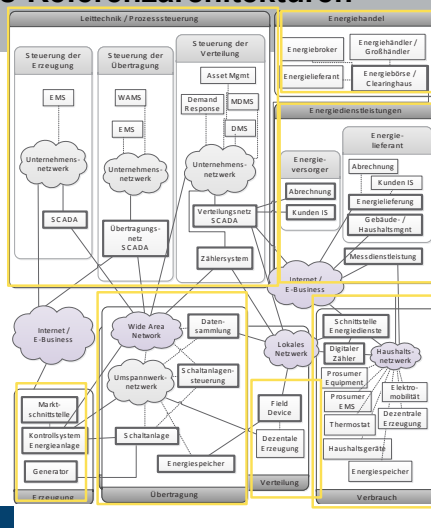


Bild 12

Die vorherigen Beispiele zeigen, dass es für einzelne Problembereiche sehr gute Lösungsansätze gibt. Es bleibt noch zu klären, wie diese Ansätze systematisch zu einer Lösungsarchitektur zusammen geführt werden können. Dazu betrachten wir erneut das Referenz-Modell (Bild 12). Unser Ansatz ist nicht, eine 'One fits all'-Lösung zu entwickeln. Die gibt es nicht. Vielmehr untersuchen wir, welche Strukturelemente wir identifizieren können - das sind diese gelben Bereiche in Bild 12. Diese Bereiche sind charakteristische Domänen. Auch die Player, die in der jeweiligen Domäne eine Rolle spielen, haben dedizierte Aufgaben für diese Domäne. Sie haben vielleicht in einer anderen Domäne eine ganz andere Aufgabe, eine ganz andere Rolle, und damit auch ganz andere Rechte und Pflichten, die dann auch andere Sicherheitskonzepte zur Umsetzung erfordern.

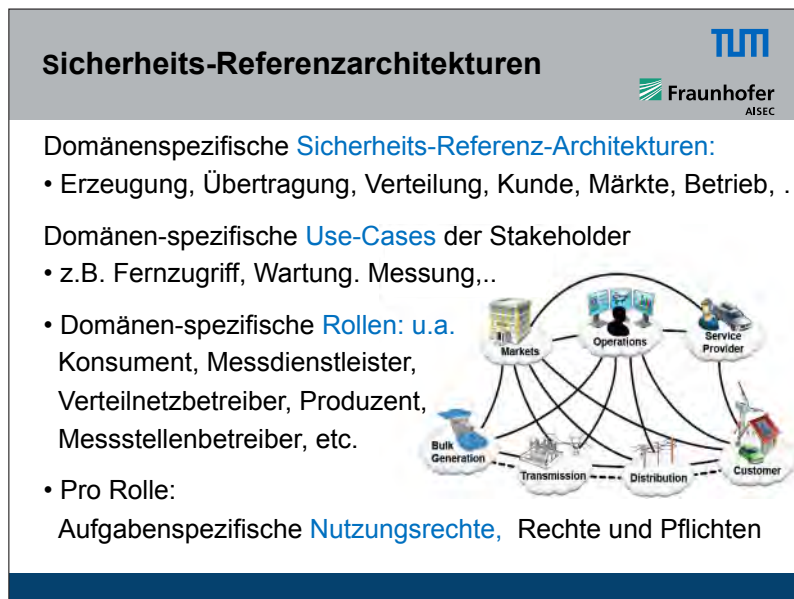


Bild 13

Deshalb untersuchen wir (Bild 13) die Sicherheitsanforderungen der verschiedenen Domänen und natürlich auch der Schnittstellen. Mittels Sicherheitsanalysen ermitteln wir die erforderlichen Rollen, deren Aufgaben, Rechte und Verpflichtungen, die sie in ihrer jeweiligen Domäne haben. Ich will hier nur andeuten, wie der von uns verfolgte Ansatz aussieht und freue mich dann auf die Diskussion mit Ihnen.

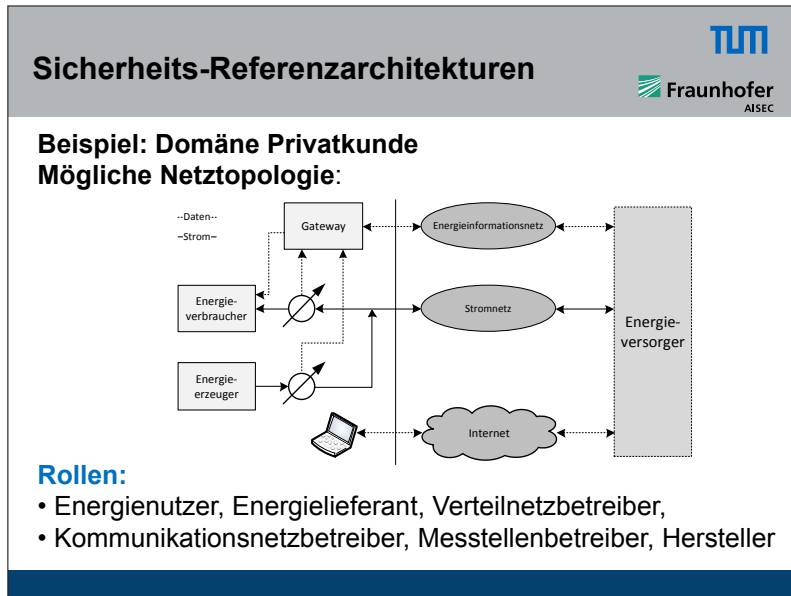


Bild 14

Betrachten wir deshalb hier nur als ein Beispiel die Domäne „Privatkunde“ (Bild 14). Das ist eine uns allen sehr naheliegende Domäne. Wie könnte das herunter gebrochen auf einen Privathaushalt aussehen? Das ganze komplexe Gebilde, was wir vorhin in Bild 12 gesehen haben, könnte sich vielleicht auf ein relativ einfaches Bild reduzieren lassen. Die Domäne umfasst Energieverbraucher. Das ist die schon mehrfach erwähnte Waschmaschine beispielsweise. Es kann natürlich auch etwas ganz anderes sein. Weiterhin umfasst sie Energieerzeuger, wie beispielsweise eine Photovoltaikanlage. Der Nutzer nimmt hierbei also die Rolle eines 'Prosumers' ein, als Verbraucher und Erzeuger von Energie. Daneben umfasst die Domäne eine Menge von Messgeräten, so dass die Domäne implizit auch denjenigen umfasst, der Messgeräte herstellt, bzw. diese betreibt. Desweiteren identifizieren wir Komponenten, die in Form von Gateways eine Interaktion mit dem Energieversorger ermöglichen. Ein Smart Meter ist entweder direkt integriert in das Gateway oder der Smart Meter ist selber die Sicherheitskomponente. Das will ich nicht weiter unterscheiden. Hinzu kommt die Interaktion über ein IKT Netz mit dem Energieverbraucher. Mit diesem skizzierten Vorgehen, könnte man bereits die Anzahl der für diese Domäne wesentlichen Stakeholder reduzieren, wenn wir uns auf eine gewisse Sicht der Dinge konzentrieren.

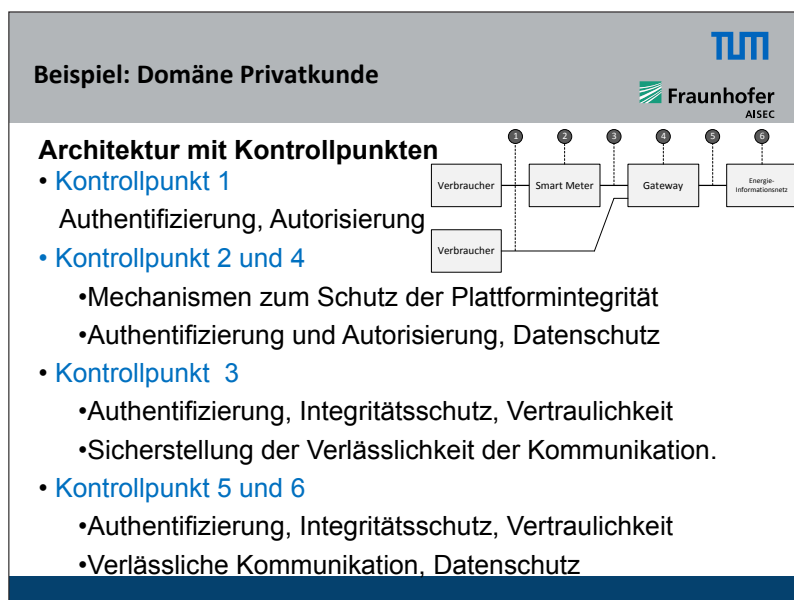


Bild 15

Wenn wir uns jetzt wieder auf die Sicherheit beziehen, kann man beispielsweise den Datenfluss zwischen den beteiligten Komponenten der Domäne beschreiben (Bild 15). Man sieht dabei, dass die Daten nicht nur von den erzeugenden bzw. verbrauchenden Komponenten zum Energieerzeuger fließen, sondern dass es durchaus auch ein bidirektionaler Weg sein kann, über den von Außen ggf. steuernd auf die Komponente im Haushalt zugegriffen werden kann. Diese bidirektionale Kommunikation sollte uns bewusst sein. Eine solche Möglichkeit für Fernzugriffe ist für verschiedene administrative Maßnahmen durchaus wünschenswert, aber eröffnet natürlich aus Sicherheitssicht einige Probleme.

In einem nächsten Schritt versucht man die Strukturen systematisch um Kontrollpunkte anzureichern. Diese zusätzlichen Kontrollen erfordern zusätzliche Sicherheitskonzepte.

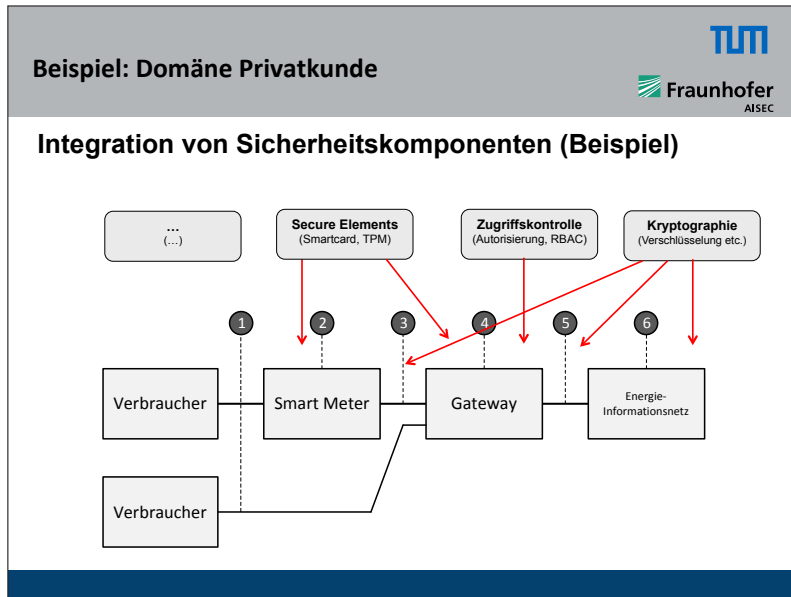


Bild 16

Wenn ich z.B. den Problemfall habe, dass auf einen Verbraucher wie die Waschmaschine von außen in irgendeiner Weise aktivierend oder deaktivierend zugegriffen werden kann, dann ist ganz klar, dass ein Mechanismus benötigt wird, um zu entscheiden, ob der Zugriff zulässig ist oder nicht (Bild 16, 17, 18). Dazu müssen die Zugreifer eindeutig identifiziert werden und eine Zugriffskontrolle muss an dem jeweiligen Kontrollpunkt durchgeführt werden. Das ist ein klassisches Vorgehen, was wir alle kennen. Ich will das nicht im Einzelnen weiter durchgehen. Sie sollen nur eine Idee mitbekommen, in welche Richtung wir diesen Ansatz ausarbeiten. Wir haben weitere Kontrollpunkte definiert. Beispielsweise benötigen wir Kontrollpunkte, um die Manipulationssicherheit von Smart Metern oder Gateways zu kontrollieren. Hierzu könnte man beispielsweise in die Architektur sogenannte Attestationsprotokolle integrieren. Ich hoffe, dass ich Ihnen im Groben eine Idee vermitteln konnte, wie wir bei der Problemlösung vorgehen.

Im nächsten Schritt würden wir die Punkte identifizieren, die eine Erweiterung um Sicherheitskonzepte erfordern. Dann können wir die erforderlichen Konzepte und Verfahren anpassen und integrieren. Wir müssen das natürlich differenziert machen, und die Differenzierung kommt dadurch, dass wir uns in der jeweiligen Domäne anschauen, welche Sicherheitsbedarfe die verschiedenen Player haben und welche Konzepte zur Erfüllung der Bedarfe angemessen sind. In der betrachteten Domäne gibt es beispielsweise den Privatkunden, der vielleicht sehr viel stärkere Datenschutzanforderungen hat als ein Messstellenbetreiber oder ein Energieversorger.

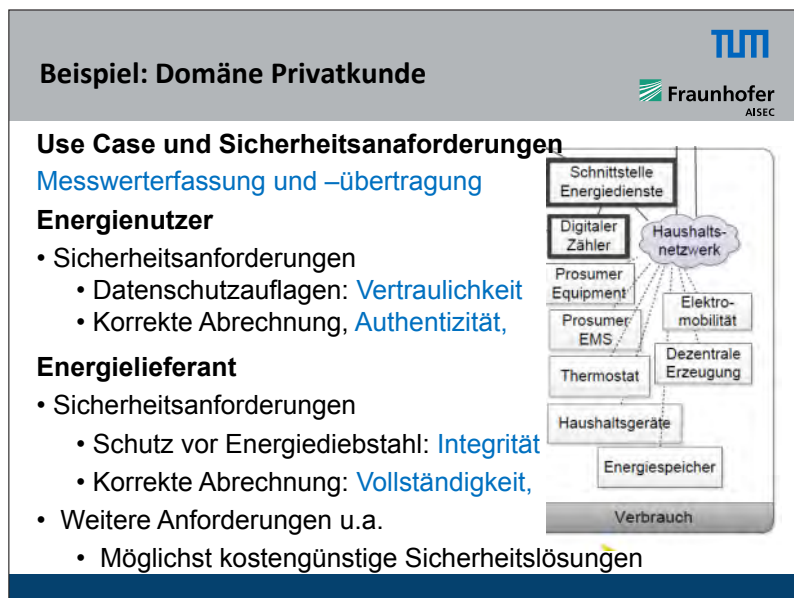


Bild 17

Der nächste Schritt besteht deshalb darin, Use Cases in den jeweiligen Domänen zu definieren. Was sind die wichtigen Anwendungsfälle, die Use Cases aus den verschiedenen Sichten der Teilnehmer?

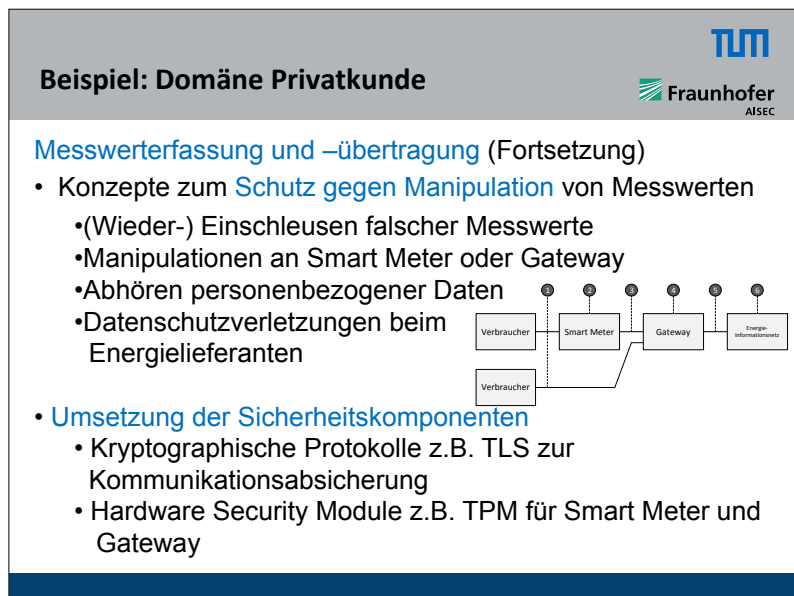


Bild 18

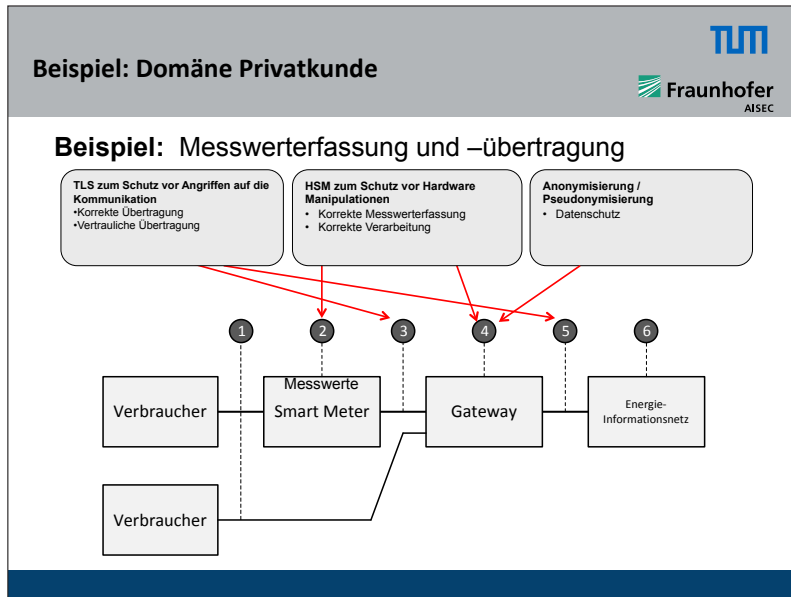


Bild 19

Was leiten wir daraus an Sicherheitsanforderungen ab (Bild 19), um dann konkret festzulegen, welche konkreten Sicherheitsmechanismen zu einer Sicherheitsarchitektur kombiniert werden müssen, um die differenzierten Sicherheitsanforderungen der Rollen zu erfüllen. Auf diese Weise lassen sich Blue-Prints von Sicherheitsarchitekturen entwickeln, die als Muster für ähnliche Anforderungsschemata genutzt werden können.

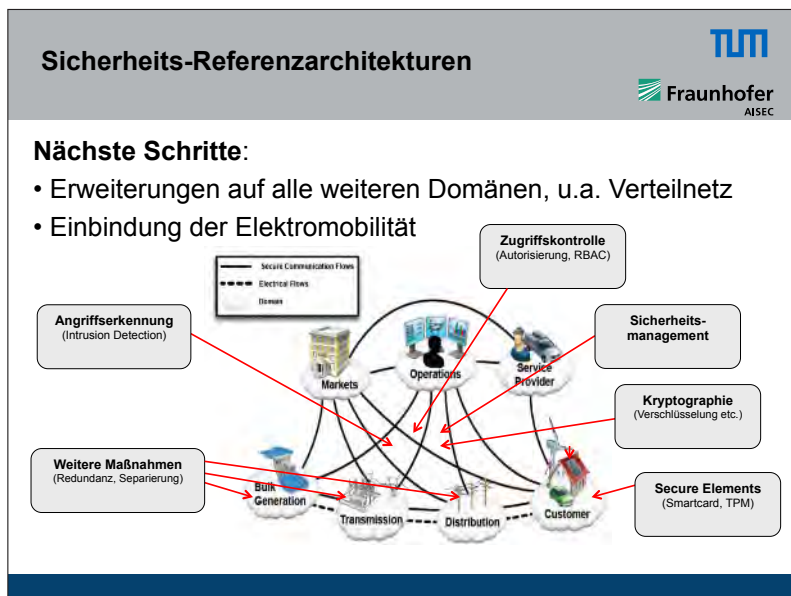


Bild 20

So etwas muss man dann für die wichtigen Domänen ausarbeiten, wie wir es in dem NEWISE Projekt derzeit angehen. Das Ziel ist es, (Bild 20), domänenspezifische Referenzarchitekturen für diese wichtigen Bereiche aufzubauen und zu identifizieren, welche fortgeschrittenen Sicherheitskomponenten noch benötigt werden, um die Anforderungen der Architekturen zu erfüllen, welche Standardkomponenten ggf. bereits ausreichend sind und welche völlig neuen Lösungen noch erforderlich sind.

Zusammenfassung





Smart Grid:

- **Konvergenz** von physischer und IKT-Domäne
- Sichere IKT ist für die **Steuerung und Kontrolle** unerlässlich

Situation heute: Wachsende Angriffsflächen durch

- unsichere eingebettete Komponenten
- fehlender Systemansatz



Herausforderung:

- neue/erweiterte **Sicherheitskonzepte &-Verfahren**
- Domänenspezifische **Sicherheits-Referenzarchitekturen:**
Secure by Design & during Operation: systematisch
- Kontinuierliches **Sicherheits-Monitoring**

Bild 21

Mein Ziel war es, Ihnen den Blick zu öffnen und zu verdeutlichen, dass Sicherheit für mich der Enabler für die Energieinformationsnetze der Zukunft ist (Bild 21). Es wird sich alles um die Sicherheit der Daten in diesen komplexen Netzen ranken. Wir müssen diese Netze steuern und kontrollieren können. Wir brauchen einen systemischen Ansatz, um dies in den Griff zu bekommen. Wir haben schon viele gute Einzellösungen entwickelt, die wir nun gezielt miteinander koppeln und in die entstehenden Architekturen integrieren müssen. Nachhaltig sichere Smart Grids erfordern sowohl systematisch integrierte Sicherheitskonzepte gemäß dem Prinzip des ‘Secure by Design’, als auch Überwachungs- und Kontrolldienste an dedizierten Kontroll- und Übergangspunkte, so dass gemäß des Prinzips des ‘Secure during Operation’ das erforderliche Sicherheitsniveau durchgehend aufrecht erhalten bleibt.

4 Diskussion

Moderation: Prof. Dr. Jörg Eberspächer, Münchner Kreis und TU München

Prof. Eberspächer:

Vielen Dank, Frau Eckert. Meine Damen und Herren, wir haben noch etwas Zeit für eine Diskussion über die Beiträge des Vormittags. Einige Themen werden natürlich heute Nachmittag noch vertieft. Ich stelle die erste Frage, die die beiden Beiträge von Herrn Renn und Frau Eckert verknüpft: Wenn wir jetzt die wohlstrukturierten und informatisch interessanten Bilder von Frau Eckert sehen, sieht man: Das Ganze ist recht komplex! Mich stört allerdings manchmal, dass wir Wissenschaftler oft umso begeisterter sind, je komplexer die Probleme sind, weil es dann natürlich auch eine größere Herausforderung ist, Lösungen dafür zu finden. Auf der anderen Seite, Herr Renn, haben Sie ganz deutlich gesagt, dass die Leute gern zu den Wahrsagern gehen, weil sie dort die einfachen Lösungen hören. Wie bringen wir das zusammen? Sehen Sie das auch als eine gewisse Herausforderung?

Prof. Renn:

Ich denke, die Herausforderungen und die Probleme sind komplex, auch die Lösungen müssen komplex sein. Das heißt, wir können nicht Dinge vereinfachen, die von Natur aus hohe Komplexität erfordern. Das muss aber nicht unbedingt ein Problem sein. Menschen können mit hochkomplexen Angelegenheiten umgehen, wenn man sie einfach handhaben kann. Denken Sie an Ihre HiFi Stereoanlage. Wichtig ist, dass man sie steuern kann. Was da im Inneren passiert, ist den meisten relativ egal, außer den Technikfreaks, die sich für die Funktionsweise besonders interessieren. Das wird auch in Zukunft bei Smart Grid und anderen komplexen Netzkonfigurationen nicht anders sein. Es gibt immer die 10 bis 15% Pioniere, die alle Dienstleistungen mit ihrem Computer nachbilden wollen. Die anderen 85% wollen einfach Strom oder Geld sparen oder sicher sein, dass ihre Dienstleistungen erfüllt sind und dies mit einem relativ hohen Komfort und – das möchte ich noch einmal betonen – mit einer gewissen Grad an Autonomie. Genauso wie ich die HiFi Anlage ein- und ausschalten und die Lautstärke regeln will, hasse ich es, wenn ein System mir vorschreibt, wann ich Mozart und wann ich die Beatles zu hören habe. Das wird nicht funktionieren. Von daher ist es gar nicht kritisch, dass die Systemsteuerung komplex ist. Entscheidend ist die Frage, wie ich Komplexität steuern kann und dass sie auch gegen Fehlbedienung resilient ist. Aber wir müssen sicher sein, dass das Interface zum Verbraucher benutzerfreundlich und simpel ist. Das ist die Herausforderung und, wenn uns das gelingt, ist es auch eine der tragfähigen Lösungen.

Prof. Eberspächer:

Jetzt gibt es einige Fragen im Auditorium. Bitte sehr!

Herr Cebulla, TÜV Informationstechnik:

Ein Aspekt, den ich sehr wichtig fand und unterstreichen möchte, ist, dass bei all diesen Entwicklungen die Lebensqualität der Menschen mit im Vordergrund stehen muss. Das hatten Sie auch angesprochen, Herr Renn. Aber das wird oft vergessen. Wir können als Bürger, als Verbraucher den Entwicklungen nur folgen, wenn sie unserer Lebensqualität nützen. Der andere Punkt ist - da in diesem Bereich vielfach nur das deutsche Datenschutzrecht betrachtet wird, wo der Verbraucher bzw. die natürliche Person im Vordergrund steht - dass meines Erachtens gerade der Bereich Smart Grid eine Möglichkeit bietet, im deutschen Datenschutzrecht die juristischen Personen stärker einzubeziehen. Die Problematik, dass ich als Bürger nicht will, dass jemand weiß, wie viel Strom ich in welcher Weise verbrauche, gilt auch für viele Unternehmen, für die es wichtige Informationen sind, die sie nicht nach außen

kundgeben wollen, wie viel Strom sie in welchen Lastprofilen verbrauchen. Daher müsste man den Schutzbereich zumindest hier auch auf die juristischen Personen ausweiten.

Prof. Eckert:

Das ist ein ganz wichtiger Aspekt, der aber auch schon aufgegriffen wird. In all diesen Diskussionen ist der Bundesdatenschutzbeauftragte mit dabei. Es ist in den Projekten der Alcatel-Lucent Stiftung der Kollege Rossnagel mit dabei, der genau diese Perspektive, die Sie ganz richtig hier noch einmal nach vorn gestellt haben, reinbringt, nicht im Sinne von bremsen sondern auch im Sinne von wie wir Technik gestalten müssen, damit wir diese Aspekte gleich von Anfang an bei der Gestaltung mit berücksichtigen.

Herr Rost, Unabhängiges Landeszentrum:

Es hat mir sehr gut gefallen, was Sie zur Steuerung gesagt haben. Das Entscheidende, als absoluter Ausdruck der Hoheit des Nutzers bestünde darin, dass er die Kommunikation mit dem EVU am Kommunikationsgateway ausschalten kann. Das ist leider bislang nicht vorgesehen. Ich versuche es gerade noch reinzubringen. Das wäre das Analogon der vertraglich abgesicherten Einwilligung auf technisch-operativer Ebene. D.h. es wird weiterhin der Energieverbrauch integer gemessen und gespeichert werden können, aber der Kunde kann sagen, dass er keine automatische Kommunikation darüber will, bis der Konflikt, der ihn treibt, gelöst ist.

Prof. Eberspächer:

Vielen Dank. Herr Thielmann hatte noch eine Wortmeldung.

Prof. Thielmann:

Herr Renn, Ihre Ausführungen haben mir sehr gut gefallen. Aber wir sind erst am Anfang dieser ganzen Thematik. Wir haben noch fünf bis zehn Jahre zu gehen. Was kommunizieren wir den Bürgern heute, damit das Vertrauen heute schon aufgebaut wird? Da fehlen mir noch konkrete Schritte und Maßnahmen.

Prof. Renn:

Das nehme ich gerne auf, und verbinde es mit der vorherigen Wortmeldung, was den Bürger eigentlich bewegt. Es gibt vier wesentlichen Motivatoren, die auf die eigene Person bezogen sind: Nr. 1 der Komfort, also die Qualität, die ich erwarte. Nr. 2 ist der Preis. Das sind die beiden wichtigsten. Nr. 3 ist Sicherheit, Risiko, Gefahrenvermeidung. Nr. 4 ist Anerkennung, Reputation. Dazu kommt ergänzend die Gemeinwohlorientierung. Auch die ist für viele bedeutsam. Nur darauf allein zu setzen, ist sehr problematisch. Allein aus Gemeinwohl machen die wenigsten Menschen etwas. Wenn das Gemeinwohl aber mit einem der vier persönlichen Motivatoren verknüpft werden kann, ist es häufig sehr wirksam – sozusagen als Verstärker. Bei Informations- und Kommunikationskampagnen muss ich auf diese vier Motivatoren eingehen. Ich kann also sagen: wenn ihr dieses tut, habt ihr mehr Komfort. Ich kann sagen: wenn ihr dieses tut, wird der Preis für Energiedienstleistungen preiswerter, denn ihr könnt dann lastabhängig den Strom oder andere Energie aufnehmen. Dabei kommt es auf alle Motivatoren an. Vor allem im Photovoltaikbereich merken wir, dass viele Menschen sich Photovoltaikanlagen auf das Dach holen, nicht weil sie besonders umweltfreundlich sind oder meinen Geld damit zu sparen, sondern weil sie ihrem Nachbarn zeigen können, dass sie ökologisch korrekt handeln wollen. Diese Art von sozialer Anerkennung ist vor allem in der hohen Mittelschicht ein wichtiges Motiv. Meine Grundbotschaft ist, dass ich an eines dieser vier Elemente in der Kommunikation andocken muss. Bei dem Sicherheitsaspekt ist noch zusätzlich von Bedeutung, dass es immer auf das Resultat ankommt und nicht auf die Art, wie es hergestellt wird. Der Nutzer will wissen, ob sich die Sicherheit erhöht, nicht ob wir uns alle darum bemüht haben.

Prof. Lukas:

Ich kann mich dem nur anschließen. Ich glaube, dass für IT-Systeme generell gilt – was auch für andere Systeme wie z.B. Verkehrssysteme gilt, nämlich dass wir immer berücksichtigen müssen, wo der individuelle Nutzen für den Bürger ist. Das muss nicht zwangsläufig ein materieller Nutzen sein. Das hat Herr Prof. Renn eben schon ausgeführt. Ich bin zudem der festen Überzeugung, dass dieser individuelle Nutzen auch als solcher vom Bürger wahrgenommen werden muss. Er darf nicht als mehr oder wenig verdeckter Zwang empfunden werden. Denn dann besteht die Gefahr, dass automatisch eine Gegenreaktion ausgelöst wird. Daher muss dieser individuelle Nutzen wirklich auf Grundlage einer freien Entscheidung bewertet werden – ein Beispiel ist die erfolgreiche Einführung der Payback-Karten. Viele Menschen geben mittlerweile beim Einkaufen private Daten preis, weil Sie das Gefühl haben, die Entscheidung über ihre Daten selbst zu fällen.

Prof. Wolff:

Ich kann da direkt anschließen. Es gibt eine ganze Reihe Untersuchungen zu dem doch etwas problematischen Smart Metering Markt. Wenn die Frage gestellt wird, was man den Leuten heute sagen kann, dann muss man schauen. In Untersuchungen ist festgestellt worden, dass die Energieeinsparung mit Smart Metern erstaunlicherweise von der Freiwilligkeit der Menschen, solch ein System einzuführen, abhängt. Woran hängt das? Das hängt daran, dass man den Nutzern eine interessante Einstiegsmöglichkeit gibt. Es sind im Augenblick diejenigen freiwillig daran interessiert, in dieses System einzusteigen, die sie mit anderen Technologien, im Smart Home zum Beispiel, verbinden, die gerne ihr Haus technisch ausrüsten möchten und dabei sehen, dass sie durch die Verbindung Smart Meter und Smart Home Technologien viel sparen können. Das geht von 5%, wenn Sie das über die Menge der Leute ohne Freiwilligkeit einführen bis zu 12% im Bereich derjenigen, die freiwillig die Systeme eingeführt haben, weil sie zusätzlich noch irgendetwas anderes getan haben. Das ist der Ansatzpunkt, interessante Einstiegsmöglichkeiten zu schaffen für die, die Interesse an dieser Technik haben.

Prof. Eberspächer:

Vielen Dank. Ich war gestern auf einem Workshop des Bundesinnenministeriums und von Fraunhofer FOKUS Berlin zum Thema „neuer Personalausweis“, der jetzt gerade ein Jahr alt ist. Da zeigte sich: wir haben etwa acht Millionen Menschen, die den nPA haben und davon haben etwa sechs Millionen die eID Funktion nicht aktivieren lassen. Das ist vom Gesetzgeber so vorgesehen – ich sage: leider -, dass man beim Aushändigen in der Behörde danach gefragt wird. Es kam bei diesem Workshop ganz klar heraus, dass wir mehr tun müssen, damit der Nutzen der eID Funktion, zusammen mit neuen Applikationen, deutlicher wird. Das ist hier ganz ähnlich. Man sieht eben immer wieder, was alles nötig ist, damit sich Innovationen durchsetzen!

Prof. Kühn, Uni Stuttgart:

Es wurde das Rollenmodell dargestellt, und die Stakeholder haben ja unterschiedliche Interessen. Die Frage ist hier, ob wir nicht eine stärkere Aufsicht brauchen, wie das in anderen Bereichen auch der Fall ist, um die verschiedenen Interessen zusammenzubringen? Wir haben z.B. schon vor 15 Jahren das Modell einer multilateralen Sicherheit entwickelt im Ladenburger Kreis der Gottlieb Daimler und Carl Benz - Stiftung in einem Diskurs, speziell für die Kommunikationstechnik. Hier haben wir noch mehr Stakeholder. Wir sehen an der Kommunikationstechnik und jetzt auch in der Energietechnik, dass ohne eine Aufsicht und Kontrolle es nicht möglich sein wird, weil die Geschäftsinteressen einfach zu unterschiedlich liegen. Wir wollen heute auch ein Signal an die Politik geben, d.h. hier ist auch die Politik gefragt, dass wir vielleicht Agenturen brauchen, die diese verschiedenen Anforderungen in Übereinstimmung bringen und auch kontrollieren. Denn wir sehen in der Kommunikations-

technik, dass der einzelne Benutzer heute etwas schwach vertreten ist mit seinen Sicherheitsanforderungen. Die starken, mächtigen Stakeholder setzen sich in der Regel durch. Könnten Sie dazu vielleicht noch eine Aussage machen?

Prof. Lukas:

Es ist schade, dass Herr Goerdeler gerade nicht anwesend ist, denn das Bundesministerium für Wirtschaft und Technologie ist das Ministerium, welches für diese Fragen zuständig ist. Deshalb wäre es mir ganz lieb, erst einmal von den anderen Teilnehmern eine Rückmeldung zu bekommen, ob Sie das für richtig halten, was gerade vorgeschlagen wurde. Wir haben auch heute schon eine Regulierung im Energiebereich. Ob sie allerdings noch zeitgemäß ist, wäre zu diskutieren. Wir werden diese Frage heute auch noch im Gesamtkontext der Tagung diskutieren. Mich würde jetzt aber interessieren, wie das die Experten hier am Tisch das sehen.

Prof. Eckert:

Ich möchte das gern noch einmal aufgreifen, Herr Kühn. Genau in diese Richtung wollten wir auch den Diskurs mit unseren Ausarbeitungen anstreben, dass man eben diesen konfliktären Bereich auch einmal klar auf dem Tisch hat, dass man sieht, wer gewisse Forderungen hat an das System, gewisse Wünsche. Das kann man mit Technik abbilden. Das kostet aber ggf. etwas, behindert vielleicht auch gewisse Dinge, so dass man einfach diese Dinge vor Augen hat. Wir können der Politik eigentlich nur sagen, dass das die Möglichkeiten sind, die wir uns alle so vorstellen können, auch zusammen mit den Industriepartnern. Wollt ihr das wirklich so? Und an den und den Stellen könnte man sich Regulierungsbedarf vorstellen. Jetzt haben Sie die anderen gefragt, ob wir das überhaupt wollen oder nicht. Von unserer Seite her sehen wir nur, dass wir das Feld präparieren und sagen: so sieht die Welt vielleicht aus und das könnten Bereiche sein, die es lohnt zu regulieren. Ich würde auch gern die Frage weitergeben, ob wir das überhaupt wollen. Das will ich jetzt hier nicht beantworten.

Prof. Eberspächer:

Vielen Dank. Ich möchte die Frage jetzt allerdings ungern weitergeben. Wir sind gehalten, die Mittagspause einzuhalten. Ich bedanke mich bei den Beitragenden, die den Tag sehr gut eröffnet haben und danke Ihnen für die Diskussionsbeiträge. Wir treffen uns um 13 Uhr hier wieder und da geht es dann um die Modellregionen E-Energy, die heute schon angesprochen wurden.

5 Prozessbezogener Datenschutz im Smart Grid

Dr. Oliver Raabe, Karlsruher Institut für Technologie

Mit der Einführung von Smart Metering ist ein erster Schritt zur informatorischen Vernetzung aller Komponenten und Akteure des Energiesystems in einem Smart Grid getan. Aus datenschutzrechtlicher Perspektive ist dabei zunächst bemerkenswert, dass damit erstmalig eine Pflicht zur Integration von IKT-Kommunikationsschnittstellen staatlich gesetzt wird. Hieraus ergibt sich ein erhöhter Schutzauftrag des Staates zur Sicherung der informationellen Selbstbestimmung der Anschlussnutzer. Auf der anderen Seite soll die Verwendung der Messdaten im Smart Grid einen Beitrag zu einem verbesserten Klimaschutz und zur Gewährleistung von Versorgungssicherheit leisten. Argumente, die im Sinne einer „praktischen Konkordanz“ eine Anpassung der Prämissen in datenschutzrechtlichen Abwägungsprozessen erfordern.

Datenschutzrechtliche Betrachtung von Modellszenarien

Datenschutzrechtliche Analyse von sieben Szenarien durch die Mitglieder der Fachgruppe Rechtsrahmen der E-Energy Begleitforschung anhand der sieben Grundprinzipien des Datenschutzes

- „Widerspiegeln“ und dynamischer Echtzeittarif mit Smart Metering
- Messstellenbetrieb und Messung durch den VNB
- Dynamische Tarifierung und Auftragsdatenverarbeitung
- Lastmanagement im Verteilnetz
- Regelung von KWK-Anlagen durch den VNB
- Elektromobilität mit untertäglichem Lieferantenwechsel
- Elektromobilität mit Roaming (ohne untertäglichem Lieferantenwechsel)





2 20.03.12
<http://compliance.zar.kit.edu>

Bild 1

Vor dem Hintergrund des bislang unverstandenen gesellschaftlichen Paradigmenwechsels beim Umgang mit Persönlichkeitsbildern im „Internet“ ist die vom Smart Meter Sensor ausgehende Gefahrenlage für die informationelle Selbstbestimmung schnell in den Fokus der Debatte geraten. Die kollidierenden gesamtgesellschaftlichen Interessenlagen nach Versorgungssicherheit und Klimaschutz hingegen werden häufig mit Verweis auf eine vermutete Unwirksamkeit der Maßnahmen diskreditiert. Dies erstaunt, da die Folgeszenarien wie die Integration von Elektromobilität in das Energienetz erst am Anfang der Erprobung stehen.

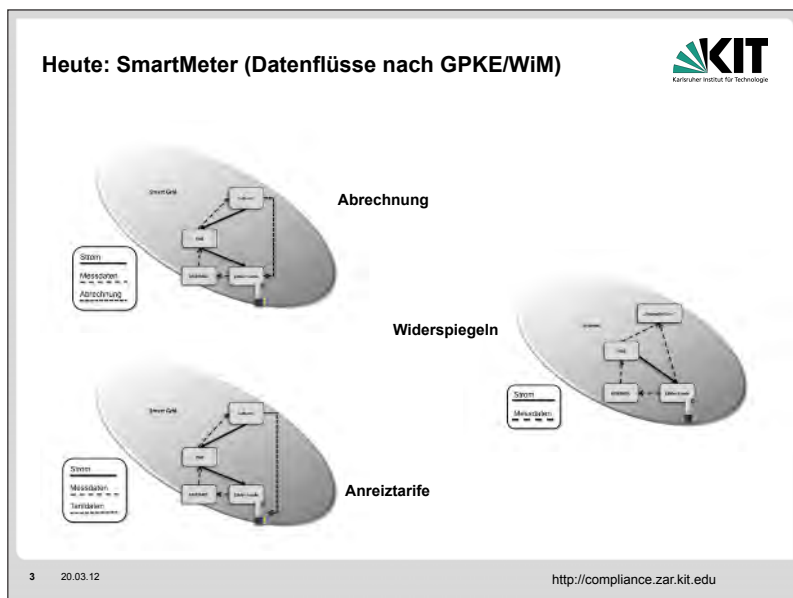


Bild 2

Aus dem sicheren Bestand datenschutzrechtlicher Erkenntnisse wird nun primär, da es sich beim Smart Grid ja vermeintlich um das „Internet der Energie“ handelt, das scheinbar einzige probate Mittel zur Abwehr datenschutzrelevanter Gefahranlagen im „Internet“ propagiert: „Datenhoheit“ im Sinne eines absoluten Beherrschungsrechtes des Einzelnen über seine Daten. Diese sollen, technisch gesichert, seine Sphäre ohne sein Einverständnis nicht verlassen dürfen. Für die Sachgestaltungen des klassischen „Internet“ muss die Perspektive, den Datenschutz maßgeblich auf den Nutzer-Clients zu realisieren als tragfähig gelten.

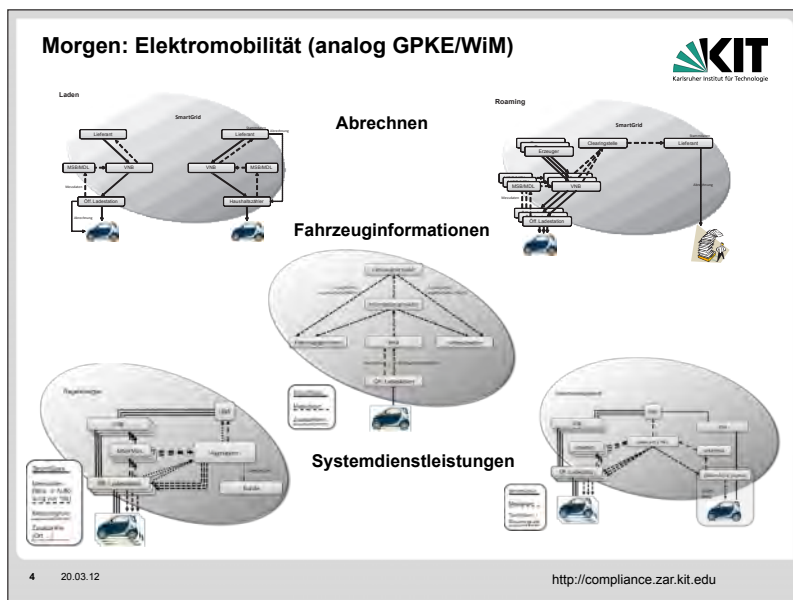


Bild 3

Für die Situation im künftigen Smart Grid gilt das aber nicht: Das historische Datenschutzrecht ist in seiner Systematik prozessorientiert. Dies hat seinen guten Grund in seinem historischen Herkommen aus dem Bereich der öffentlichen Verwaltung, wo die Förmlichkeit des Verfahrens jeden Verwendungsschritt strukturiert und für den Gesetzgeber vorhersehbar macht. Bei der Nutzung des „Internet“ gibt es dieses vorstrukturierende Wissen beim staatlichen Souverän zunehmend nicht. Damit geht einher, dass der Gesetzgeber sich auf Partialregelungen zur Technikgestaltung zurückzieht und die Entscheidung über sinnvolle und notwendige Datenverwendungen, aber auch das Prognoserisiko über tatsächlich zu erwartende Systemprozesse dem Einzelnen überlässt. Die Einwilligung als Legitimationsgrundlage der Datenverwendung wird zur Regel, die gesetzliche Vorabstrukturierung erwünschter Effekte und des Interessenausgleichs zur Ausnahme.

Herausforderungen - Überblick

- Einheitliche Modellbildung (Zwecke, Prozesse)
- Wie ist eine datenschutzfreundliche Echtdatenbilanzierung möglich
- Auswirkungen der EnWG-Novelle auf Modellszenarien
- Analyse europäischen Harmonisierungsbedarfs für die grenzüberschreitende Elektromobilität
- Datenschutzrechtliche Analyse der Integration von Elektromobilität in Systemdienstleistungsmärkte
- Analyse des Spannungsverhältnisses von möglichen Nachweispflichten und Datenschutz in Systemdienstleistungsmärkten

5 20.03.12

<http://compliance.zar.kit.edu>

Bild 4

Entgegen der verbreiteten Grundannahme, dass die Messsensorik zukünftig ein Teil des offenen „Internet“ sein müsse, besteht hierzu sowohl aus der motivierenden europäisch regulierenden Perspektive als auch sachlich im Hinblick auf die Erreichung der Effizienzziele keine Notwendigkeit. Vielmehr sollte der Energiekernmarkt in kommunikativer Hinsicht aus Gründen des informatorisch freien Marktzuganges, der notwendigen Interoperabilität, des Unbundling und der Rechtssicherheit bei den Marktakteuren auch in Zukunft durch das moderne und innovationsoffen gestaltete Instrument der Prozessfestlegung durch die BNetzA (oder ggf. eines europäischen Pendant) strukturiert werden.

Auf Basis dieses strukturierenden Verfahrens, das auch Transparenz über notwendige Datenverwendungen schafft, greift aber wieder das Paradigma des klassischen prozessorientierten Datenschutzes. Notwendige technische Mechanismen des Datenschutzes („Privacy by Design“) sollten dann sinnvoller Weise bei den sachkundigen Akteuren entlang dieser Prozesskette ansetzen. Damit können insbesondere die „vergessenen“ Datenschutzprinzipien, wie zum Beispiel Nutzerkontrolle, Transparenz über tatsächliche Verwendungsschritte, gesetzliche Löscho- und Sperrpflichten und nicht zuletzt die hoheitliche Datenschutzaufsicht deutlich effektiviert werden, ohne dem Nutzer regelmäßig Wissen um mögliche Datenverwendungen in komplexen Systemen abzuverlangen, zu deren prognostischer Bewertung der Staat besser in der Lage ist.

6 E-Energy und das Thema Sicherheit

Ludwig Karg und Michael Wedler, B.A.U.M. Consult, München

Die sechs Modellprojekte des E-Energy Programms (siehe www.e-energy.de) legen die Grundlagen für ein Internet der Energie. Aktuell befinden sie sich in der Phase der Feldtests. Ca. 5.000 Haushalte und Betriebe testen bis Ende 2012 die IKT-Lösungen, die von Unternehmen der Energie- und IKT-Wirtschaft in Zusammenarbeit mit Wissenschaftsinstituten entwickelt wurden. Die E-Energy Modellprojekte leisten damit entscheidende Beiträge zum Gelingen einer Energiewende in Deutschland. Und sie helfen Deutschland als Vorreiter eines intelligenten Energiesystems der Zukunft zu positionieren.

Das zukünftige Energieversorgungssystem wird dezentraler, volatiler und liberaler sein. Es muss ebenso wie das jetzige die Versorgungssicherheit bei gleichzeitiger Berücksichtigung der Wirtschaftlichkeit und der Anforderungen des Klimaschutzes gewährleisten. Es wird aber zusätzliche Marktrollen geben und eine Vielzahl neuer Dienste – nicht nur für die Stromverbraucher sondern auch für Energieerzeuger und Betreiber von Infrastrukturen. Das gesamte System wird geprägt sein von komplexen, in der Mehrzahl verteilten Informations- und Kommunikationssystemen. Das bietet Chancen in punkto Fehlertoleranz, Effizienz und Nachhaltigkeit. Es birgt aber auch Risiken: Geraten wir in eine Komplexitätsfalle? Lässt sich der notwendige Schutz der Privatsphäre sicherstellen? Wie lässt sich die Angreifbarkeit des Gesamtsystems und seiner Schlüsselemente minimieren?

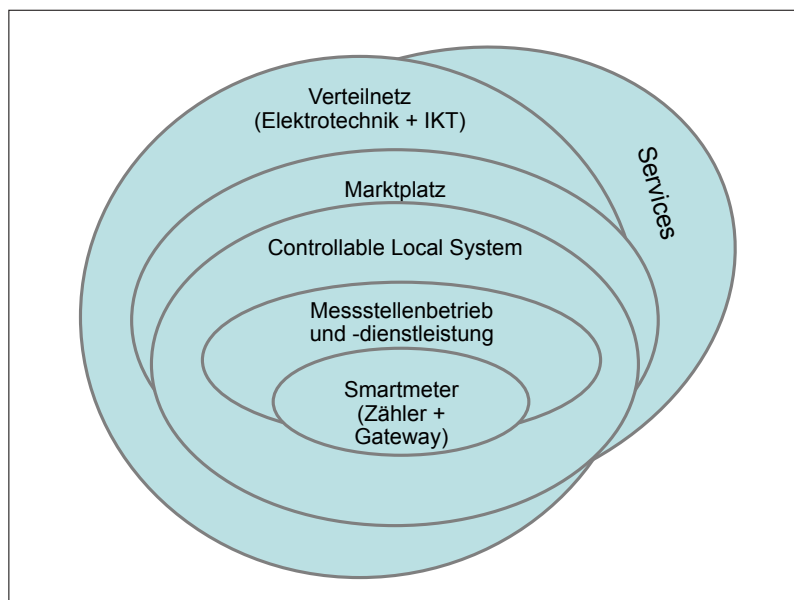


Bild 1

Für die Diskussion im Themenfeld „IT-Security im Smartgrid“ wurde von der E-Energy Fachgruppe Systemarchitektur ein Schalenmodell skizziert, das den Scope und die Beziehung der verschiedenen Untersuchungsfelder darstellt (Bild 1). Es verdeutlicht, dass die Sicherheitsfragen im Zusammenhang mit dem Smartmeter, einem wesentlichen Element in den meisten Smartgrid-Lösungen, geklärt sein müssen. Sodann gilt es auch alle anderen Bereiche systematisch zu analysieren sowie die Aufgaben und einen Arbeitsprozess zur

fundierte und zeitnahe Bewältigung der Anforderung zu strukturieren. Die E-Energy Modellregionen haben viele der Herausforderung bereits erkannt und benannt. Im Rahmen der laufenden Projekte können sie nicht alle bearbeiten. Die Begleitforschung hat deshalb die Modellprojekte und zahlreiche einschlägige Akteure im sogenannten „Kasselprozess“ zusammengeführt. Die Akteure haben dabei ihre Absicht erklärt, im Sinne des nebenstehend skizzierten Vorgehens (Bild 2) eng zusammen zu arbeiten und als erstes Ergebnis eine belastbare Situations- und Aufgabenbeschreibung zu erstellen. Dies soll im engen Kontakt mit weiteren Aktivitäten wie z. B. im Rahmen der Netzplattform des BMWi, des DKE Kompetenzzentrums E-Energy und internationaler Ansätze erfolgen.

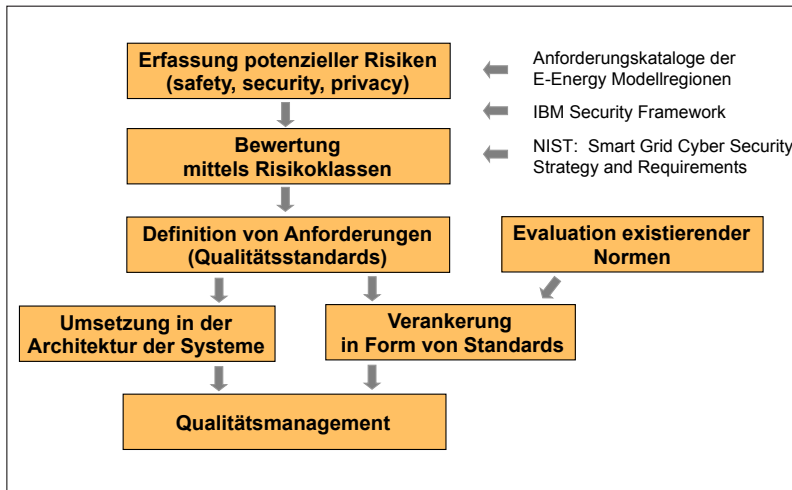


Bild 2

7 Semper Ident? Zur Notwendigkeit einer differenzierten grundrechtlichen Bewertung von Smart Metern

Prof. Dr. Gerrit Hornung, LL.M. , Universität Passau

Die Diskussion um die Auswirkungen des Einsatzes von Smart Metern auf die Persönlichkeitsrechte der Letztverbraucher hat – zu Recht – zunächst das Grundrecht auf informationelle Selbstbestimmung in den Blick genommen. Die Grundrechtsprobleme sind damit jedoch nicht ausgeschöpft: Zwar sind ohne technische Schutzmechanismen alle Letztverbraucher identifizierbar – das bedeutet aber nicht, dass alle Fälle grundrechtlich gleich sind und mit dem Grundrecht auf informationelle Selbstbestimmung hinreichend erfasst werden können.

Hintergrund

Aus verfassungsrechtlicher Sicht weist die Idee eines nachhaltigen Energieinformationsnetzes grundsätzliche Spannungsfelder auf. Einerseits verfolgt der Staat das Allgemeininteresse des Schutzes der natürlichen Lebensgrundlagen, das in Art. 20a GG als Staatsziel verankert ist. Andererseits wird die Nutzung personenbezogener Daten der Letztverbraucher teils erlaubt, teils vorgeschrieben, sodass deren grundrechtlich geschützte Persönlichkeitsrechte zu wahren sind. Anbieter und Betreiber von Netzen und Messgeräten werden durch die Berufsfreiheit geschützt. Wenn der Gesetzgeber mit den in § 21d EnWG legaldefinierten „Messsystemen“ (Smart Meter) Bausteine vorgibt, die dazu geeignet sind, allein oder in der Vernetzung mit Haushaltsgeräten in erheblichem Maße Informationen über die Privatsphäre der Letztverbraucher zu erheben und zu übermitteln, treffen den Staat grundrechtliche Schutzpflichten, deren Reichweite von den jeweils tangierten Grundrechten abhängt.

Betroffene Grundrechte

In der bisherigen Diskussion ist ausführlich herausgearbeitet worden, dass in praktisch allen Konstellationen einfachgesetzlich die Regeln des Datenschutzrechts und auf verfassungsrechtlicher Ebene das Grundrecht auf informationelle Selbstbestimmung einschlägig sind. Personenbezogene Daten fallen im Energieinformationsnetz in vielfältiger Weise an (Zahl der verbrauchten Kilowattstunden, Verbrauchszeitraum, Status einzelner Geräte und deren aktuelle Verbrauchswerte etc.). Ihre Schutzbedürftigkeit ist unterschiedlich, insgesamt ist aber deutlich, dass potentiell eine besondere Eingriffstiefe vorliegen kann, die durch den Umfang der Datenerhebung, die Vielzahl der betroffenen Lebensbereiche, die erhöhte Aussagekraft der Daten, die steigende Anzahl der datenverarbeitenden Stellen (vor allem durch die neue Rolle des Messstellenbetreibers nach § 3 Nr. 26a EnWG) und das erhöhte Interesse Dritter an den erhobenen Daten verursacht wird.

Aus dem verfassungsrechtlichen Schutzprogramm der informationellen Selbstbestimmung lassen sich Anforderungen an eine rechtliche Regelung des Energieinformationsnetzes und an seine technische Gestaltung ableiten. Der Gesetzgeber ist inzwischen aktiv geworden und hat mit dem Gesetz zur Neuregelung energiewirtschaftsrechtlicher Vorschriften (EnWRNRG) mit Wirkung vom 4.8.2011 Regelungen für die Erhebung und Verwendung personenbezogener Daten im Smart Grid geschaffen. Diese sehen auch Vorgaben für die Zertifizierung der Messsysteme anhand eines Schutzprofils nach Common Criteria vor (§ 21e Abs. 2 und 4 EnWG) vor.

Die grundrechtliche Dimension des Energieinformationsnetzes erschöpft sich jedoch nicht mit der informationellen Selbstbestimmung – die Letztverbraucher sind im Smart Grid zwar regelmäßig identifizierbar, aber nicht stets gleich zu behandeln. Dies soll im Folgenden anhand von drei Beispielen gezeigt werden.

Art. 13 GG: Unverletzlichkeit der Wohnung

Art. 13 GG verbürgt dem Einzelnen einen elementaren Lebensraum und gewährleistet das Recht, in ihm in Ruhe gelassen zu werden. Das Grundrecht schützt unter anderem gegen eine Überwachung mit technischen Hilfsmitteln von außerhalb der Wohnung, weil auch hierin eine Beeinträchtigung des räumlich-gegenständlichen Bereichs der Privatsphäre liegt, die durch eine anschließende Speicherung und Verwendung der gewonnenen Informationen oder eine Übermittlung an andere Stellen weiter fortgesetzt wird.

Die durch Smart Meter gewonnenen Daten stammen vielfach aus diesem Bereich der räumlichen Privatsphäre. Ihr Einsatz ermöglicht im Falle einer entsprechend hohen zeitlichen Auflösung die Erstellung eines präzisen Lastprofils, aus dem sich detaillierte Informationen über die Nutzung einzelner Geräte und damit über die jeweiligen Haushaltsmitglieder und ihre Verhaltensweisen und Gewohnheiten gewinnen lassen, die sonst nicht ohne herkömmliche Eingriffe in Art. 13 GG ermittelbar wären. Zweifel kann man an der Anwendbarkeit des Grundrechts höchstens deshalb, weil die Aussagekraft gegenüber einer direkten optischen oder akustischen Beobachtung herabgesetzt sein kann: Die anhand eines Lastprofils gewonnene Information, dass ein Fernsehgerät eingeschaltet ist, gibt zunächst noch keine Auskunft darüber, welches Programm ausgewählt wurde. Es gibt jedoch erste Forschungsergebnisse, die anhand des Stromverbrauchs auch den konsumierten Inhalt bestimmen. Auch ohne diese Möglichkeit wäre Art. 13 GG aber betroffen: Ob der Schutzbereich eines Grundrechts einschlägig ist, hängt grundsätzlich nicht davon ab, in welcher Intensität in diesen eingegriffen wird, und ob der Eingriff seiner Art nach mit bisher üblichen Eingriffen vergleichbar ist.

Schließlich greift auch das denkbare Argument nicht, das Bundesverfassungsgericht habe in dem vergleichbaren Fall der Online-Durchsuchung einen entsprechenden Eingriff abgelehnt. Dort wurde entscheidend damit argumentiert, der Eingriff könne unabhängig vom Standort des Betroffenen erfolgen, der den Behörden oftmals noch nicht einmal bekannt sei, sodass die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt bleibe. Dies ist hier anders: Der Standort der Smart Meter liegt regelmäßig ebenso in dieser Sphäre wie die elektronischen Geräte, durch deren Verbrauchsmessung die Informationen über Verhaltensweisen innerhalb der Wohnung erhoben werden.

Soweit Art. 13 GG nach diesen Kriterien anwendbar ist, wird das Grundrecht auf informationelle Selbstbestimmung verdrängt. Da Art. 13 Abs. 3 GG zur Aufklärung von Straftaten nur technische Mittel „zur akustischen Überwachung“ zulässt, ist ein externer hoheitlicher Zugriff auf die Daten zu diesem Zweck unzulässig. Denkbar wären zum einen eine Datenerhebung im Rahmen einer Durchsuchung (Art. 13 Abs. 2 GG), zum anderen ein Zugriff auf die Daten bei Betreibern von Messstellen oder Netzen. Im präventiven Bereich lässt Art. 13 Abs. 4 GG demgegenüber (unter weiteren Voraussetzungen) allgemein „technische Mittel zur Überwachung von Wohnungen“ zu. Dieser Begriff ist entwicklungs offen und würde einen externen Zugriff zur Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, zumindest prinzipiell ermöglichen.

Hinsichtlich der Rechtsverhältnisse zwischen Letztverbrauchern, Messstellen- und Netzbetreibern sowie Energieversorgungsunternehmen verstärkt Art. 13 GG die aus dem Grundrecht auf informationelle Selbstbestimmung abgeleiteten Schutzpflichten hinsichtlich der räumlichen Privatsphäre. Das betrifft insbesondere Maßnahmen der IT-Sicherheit gegen Angriffe, mit denen der Zugriff auf die Daten oder die Manipulation häuslicher Systeme (etwa deren missbräuchliche Steuerung von außen) bezweckt wird.

Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Smart Meter und eine Vielzahl elektronischer Haushaltsgeräte, deren Verbrauch sie aufzeichnen, sind IT-Systeme. Um von dem neuen „IT-Grundrecht“ erfasst zu sein, müssen sie allerdings „allein oder in ihrer technischen Vernetzung personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff [...] es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten“. Dies hängt von der technischen Gestaltung der Smart Meter und ihrer Vernetzung mit IT-Systemen im Haushalt ab. In der reinen Information über den Stromverbrauch wird man eher eine punktuelle Aussage über einen bestimmten Lebensbereich sehen müssen. Die oben beschriebenen detaillierten Aussagen über das Verhalten der Bewohner erreichen aber bereits eine andere Qualität. Wenn Smart Meter künftig mit weitreichender Steuerungstechnik in der Wohnung verbunden sein sollten, ist das Grundrecht jedenfalls betroffen.

Damit eine „grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung“ besteht, verlangt das Bundesverfassungsgericht überdies, dass der Betroffene das System „als eigenes“ nutzt. Dies kann bei Smart Metern zweifelhaft sein, ist zumindest bei der eigenen Haustechnik aber der Fall und erfasst beispielsweise den in § 14a EnWG ausdrücklich vorgesehenen Fall, dass Betreibern von Elektrizitätsverteilernetzen „die Steuerung von vollständig unterbrechbaren Verbrauchseinrichtungen“ der Letztverbraucher gestattet wird. Soweit der Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme reicht, müssen hoheitliche Eingriffe im präventiven Bereich den Anforderungen genügen, die das Bundesverfassungsgericht in der Entscheidung zur Online-Durchsuchung aufgestellt hat: vor allem Gefahr für ein überragend wichtiges Rechtsgut, Richtervorbehalt und Schutz des Kernbereichs privater Lebensgestaltung. Für den Bereich der Strafverfolgung fehlen dagegen bislang Leitlinien des Gerichts. Ebenso wie beim Grundrecht auf informationelle Selbstbestimmung und bei Art. 13 GG bestehen aber Auswirkungen auf das Privatrecht, die sich insbesondere in staatlichen Schutzpflichten niederschlagen. Damit gewinnt der Schutz der Integrität der Smart Meter und der mit ihnen vernetzten IT-Systeme der Letztverbraucher eine besondere Bedeutung. Dem ist präventiv auf der Verordnungsstufe (§ 21i EnWG), sowie auf technischer Ebene im Rahmen des gesetzlich geforderten „jeweiligen Stands der Technik“ (§ 21e Abs. 3 Satz 1 EnWG) durch erhöhte Anforderungen Rechnung zu tragen.

Kommerzialisierung der Verbrauchsdaten?

Eine letzte grundrechtliche Frage wird durch den besonderen Charakter der erhobenen Daten aufgeworfen, die nicht nur den neuen Funktionalitäten des Energieinformationsnetzes dienen, sondern auch Grundlage für neue Abrechnungsmodelle und andere wirtschaftlich relevante Tätigkeiten sind. Dies kommt besonders deutlich in der § 14a Satz 1 EnWG zugrunde-

liegenden Wertung zum Ausdruck: Im Gegenzug für das Überlassen der externen Steuerung wird die Berechnung eines reduzierten Netzentgelts explizit vorgeschrieben. Der Sache nach steht dies auch insgesamt hinter der Idee der Smart Meter: Die Effizienzsteigerung und Verbesserung der Auslastung wird durch die Erhebung der Verbrauchsdaten und (noch effektiver) durch die anbieterseitige Steuerung von Verbrauchseinrichtungen verbessert. Beide Mittel stammen aus der Sphäre der Letztverbraucher oder greifen in sie ein – deshalb sollen die Letztverbraucher hiervon auch profitieren.

Hierin liegt eine interessante Perspektive sowohl auf die raumbezogen geschützte Privatsphäre (Art. 13 GG und Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme), als auch auf das Grundrecht auf informationelle Selbstbestimmung, das losgelöst von solchen Räumen die Persönlichkeitsrechte schützt: „Gehören“ die Verbrauchsdaten den Bewohnern der Häuser und Wohnungen? Können sie im Grundsatz frei entscheiden, ob sie diese an Betreiber von Netzen und Messstellen „verkaufen“, und im Gegenzug Rabatte erhalten? Und muss der Staat, wenn er im übergeordneten Interesse den Einbau – und perspektivisch die Nutzung? – von Smart Metern vorgibt, neben Vorschriften zum Schutz der Persönlichkeitsrechte auch solche zu reduzierten Entgelten wie in § 14a Satz 1 EnWG machen?

Trotz des Bezugs zur räumlichen Wohnungssphäre, der Nutzung der im Eigentum der Letztverbraucher stehenden Elektrogeräte und der individuellen Lebensführung, die die Basis für die erhobenen Verbrauchsdaten bildet, kann man nicht soweit gehen, diese Position der grundrechtlichen Eigentumsgarantie zuzuordnen. Dennoch ist der wirtschaftliche Wert dieser Daten grundrechtlich nicht belanglos. Er wirft nämlich die grundsätzliche Frage auf, ob die erörterten Persönlichkeitsrechte (auch) eigentumsähnlich strukturiert sind. In Deutschland wird das für das Grundrecht auf informationelle Selbstbestimmung überwiegend abgelehnt, während man in anderen Ländern offen für diese Perspektive ist. Auch in Deutschland ist aber ein Trend zur Kommerzialisierung personenbezogener Daten erkennbar, der sich in ihrem wirtschaftlichen Wert niederschlägt und beispielsweise dazu führt, dass sehr viele Internetanwendungen entgeltfrei angeboten werden und sich über die werbeorientierte Nutzung der Nutzerdaten refinanzieren. Auch die Daten des Smart Grid werden nach der gesetzlichen und wirtschaftlichen Konzeption jenseits der Letztverbrauchersphäre kommerzialisieren und so zum Wirtschaftsgut. Dies spricht dafür, diese Dimension als Verstärkung des Schutzes der Letztverbraucher zu begreifen, deren Besonderheiten im Rahmen grundrechtlich begründeter Schutzprogramme zur berücksichtigen sind.

Fazit: Gestaltungsziele für Sicherheit und Nutzerschutz

Im Ergebnis haben alle drei Bereiche verfassungsrechtliche Auswirkungen für Sicherheit und Nutzerschutz im Energieinformationsnetz. Am deutlichsten sind diese für das Handeln staatlicher Stellen, weil Art. 13 GG und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme höhere Anforderungen an die Rechtfertigung von Eingriffen beinhalten. Der besondere Charakter der Daten ist, soweit der Schutzbereich der beiden Grundrechte betroffen ist, zumindest auf der Verhältnismäßigkeits-ebene auch dann zu berücksichtigen, wenn die Daten nicht beim Letztverbraucher, sondern bei Netz- und Messstellenbetreibern durch staatliche Stellen erhoben werden. Für den Bereich der Umsetzung zwischen privaten Betreibern und Letztverbrauchern ergeben sich ebenfalls höhere Anforderungen. Dementsprechend sind bei der Verabschiedung der Rechtsverordnung nach § 21i EnWG und bei der Erarbeitung der Vorgaben für die technische Umsetzung durch Schutzprofile hohe Anforderungen an den Persönlichkeitsschutz der Letztverbraucher vorzusehen, die überdies den besonderen Strukturen der zusätzlichen einschlägigen Grundrechte Rechnung tragen müssen.

Weiterführende Literatur

Artikel-29-Datenschutzgruppe, Stellungnahme 12/2011 zur intelligenten Verbrauchsmessung („Smart Metering“), abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_de.pdf, 2011.

Eckert, Sicherheit im Smart Grid. Eckpunkte für ein Energieinformationsnetz, Alcatel-Lucent-Stiftung, SR Nr. 90, 2011.

Göge/Boers, Gläserne Kunden durch Smart Metering? Datenschutzrechtliche Aspekte des neuen Zähl- und Messwesens, ZNER 2009, 368.

Greveler/Justus/Löhr, Hintergrund und experimentelle Ergebnisse zum Thema „Smart Meter und Datenschutz“, abrufbar unter http://www.its.fh-muenster.de/greveler/pubs/smartmeter_sep11_v06.pdf, 2011.

Heckmann, Staatliche Schutz- und Förderpflichten zur Gewährleistung von IT-Sicherheit. Erste Folgerungen aus dem Urteil des Bundesverfassungsgerichts zur „Online-Durchsuchung“, in: Rüßmann (Hrsg.), Festschrift für Gerhard Käfer 2009, 129.

Karg, Datenschutzrechtliche Rahmenbedingungen beim Einsatz intelligenter Zähler, DuD 2010, 365.

Müller, Gewinnung von Verhaltensprofilen am intelligenten Stromzähler, DuD 2010, 359.

Raabe, Datenschutz im SmartGrid. Anpassungsbedarf des Rechts und des Systemdatenschutzes, DuD 2010, 379.

Raabe/Pallas/Weis/Lorenz/Boesche, Datenschutz in Smart Grids, 2011.

Roßnagel/Jandt, Datenschutzfragen eines Energieinformationsnetzes. Alcatel-Lucent-Stiftung, SR Nr. 88, 2010.

Roßnagel/Jandt, Datenschutzkonformes Energieinformationsnetz. Risiken und Gestaltungsvorschläge, DuD 2010, 373.

Roßnagel/Schnabel, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, 3534.

8 Sicherheit und Datenschutz im Smart Metering

Dr. Johann Kranz, Ludwig-Maximilians-Universität München

Nachdem wir gehört haben, dass Juristen und Informatiker vor allem Probleme aufwerfen, bin ich nun als Wirtschaftsinformatiker dazu da, Lösungsoptionen für die Probleme aufzuzeigen. Bitte entschuldigen Sie den billigen Populismus, aber als ich heute Morgen die Schlagzeile „Skandal bei Facebook – Student deckt auf, was wirklich mit den Daten passiert“ in der Bild entdeckt habe, musste ich gleich daran denken, was wohl die Folgen wären, wenn man hier „Facebook“ durch „Smart Metering“ ersetzt? Dies wäre fatal und muss durch effektive Mechanismen und Richtlinien verhindert werden.

Wie die meisten von Ihnen wissen, ist man bei Facebook gezwungen, gewisse Daten preiszugeben. Doch dem Großteil der Nutzer ist nicht klar, was mit diesen Daten passiert, und oftmals hat man das Gefühl, dass diese Daten nur gesammelt werden, damit Facebook personalisierte Werbung und Kundenprofile an die Industrie verkaufen kann. Dies führt dazu, dass zumindest die deutschen oder europäischen Nutzer, die in datenschutzrechtlichen Fragen vielleicht etwas sensibler sind als die Amerikaner, Bedenken haben, was mit ihren Daten passiert. Diese Art Bedenken müssen beim Thema Smart Metering unbedingt vermieden werden. Wie wichtig das Thema ist, zeigen Umfragen wie beispielsweise die der Forsa, die im Auftrag des Bundesverbandes der Verbraucherzentrale erhoben wurden.

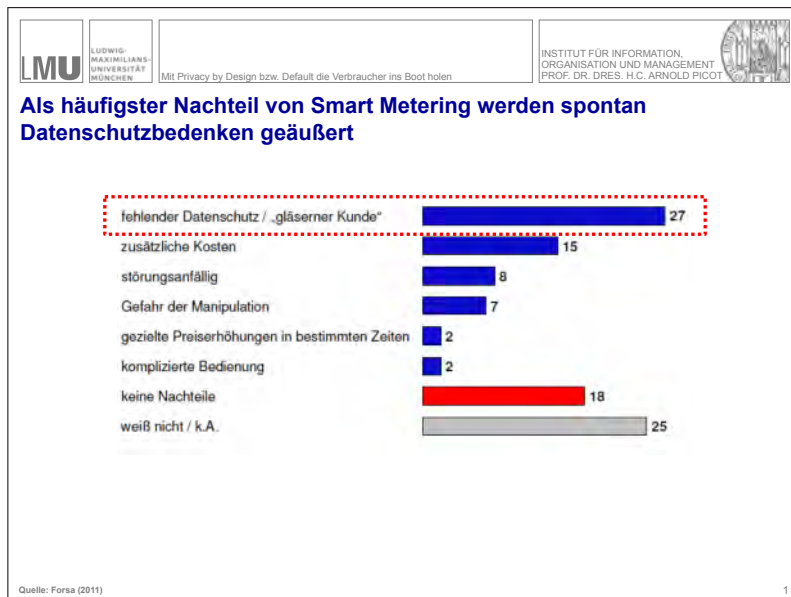


Bild 1

Zu den Nachteilen der Smart Metering Technologie befragt, antworten die meisten Verbraucher, dass ihnen der in ihren Augen fehlende Datenschutz und die Angst davor ein „gläserner Kunde“ zu sein, Sorgen bereitet (Bild 1). Dieses Ergebnis zeigt also, dass das Thema auf Verbraucherseite als Problem wahrgenommen wird, auch wenn, wie Herr Renn schon gesagt hat, da auch viel Unwissenheit mit dabei ist. Aber nichts desto trotz ist es für die Akzeptanz der neuen Zählertechnologie enorm wichtig, dass dieses Unbehagen von allen beteiligten Akteuren ernst genommen und adressiert wird.

Die Ergebnisse der Forsa-Befragung bestätigt auch eine Studie, die in Zusammenarbeit mit Herrn Prof. Picot entstand. Ich möchte Ihre Aufmerksamkeit speziell auf drei Fragen lenken (Bild 2): Die erste Frage beschäftigt sich damit, ob Verbraucher glauben, dass Netz- bzw. Messstellenbetreiber darum bemüht sind, unautorisierte Zugriffe auf persönliche Daten zu verhindern. Wie Sie sehen, ist weniger als die Hälfte davon überzeugt.

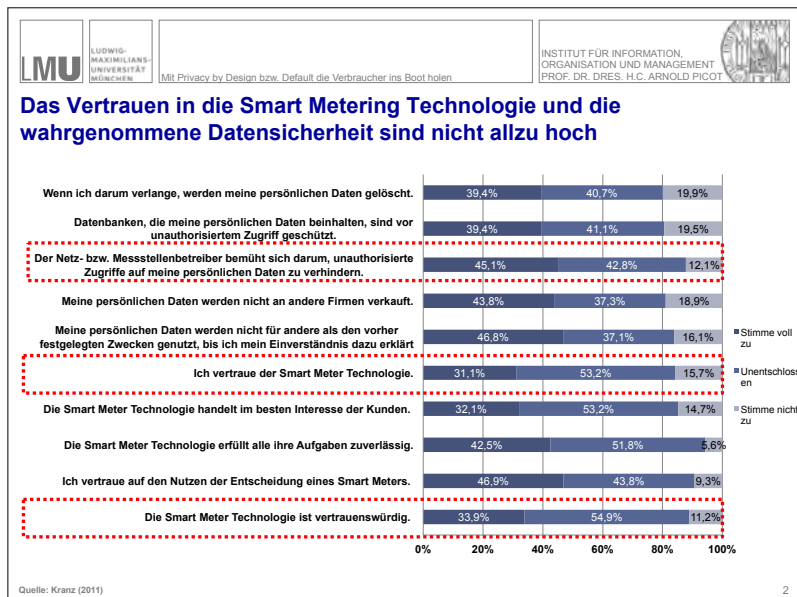


Bild 2

Auch die Frage nach dem Vertrauen, das der Smart Metering Technologie entgegengebracht wird, zeigt, dass nur rund ein Drittel der Befragten der Technologie vertrauen. Dies ist bei einer Technologie, die in 40 Millionen Haushalten ausgerollt werden soll, doch ein sehr bedenklich niedriger Wert.

Eine ähnliche empirische Evidenz zeigt sich auch bei der Frage, ob die Smart Meter Technologie vertrauenswürdig ist. Hier ist ebenfalls nur ein Drittel voll und ganz der Meinung, dass dies für die Technologie zutrifft.

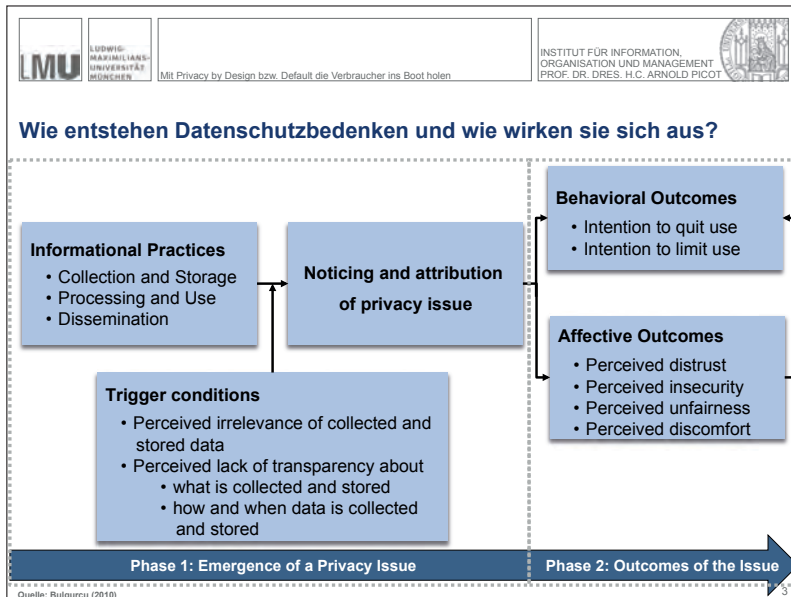


Bild 3

Kommen wir nun zur grundsätzlichen Frage, wie Datenschutzbedenken entstehen und welche Auswirkungen diese auf das Verbraucherverhalten haben (Bild 3). Das Verständnis darüber, wie Datenschutzbedenken ausgelöst werden ist sehr bedeutend. Wissenschaftler haben am Beispiel Facebook herausgefunden, dass Intransparenz und Irrelevanz der Datenerhebung die zwei entscheidenden Auslöser für Datenschutzbedenken sind. Wenn diese dann erst einmal wahrgenommen und dem Produkt zugeordnet werden, führt dies zu affektiven Reaktionen wie Misstrauen, Unbehagen, Unsicherheit und Unfairness. Diese Emotionen wirken sich dann wiederum auf das Verhalten aus. Für Smart Metering würde das bedeuten, dass die Verbraucher sich schlichtweg weigern Smart Meter zu benutzen oder assoziierte Dienstleistungen, bei denen ein Vertrauensdefizit herrscht, nachzufragen.

LMU	LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN	Mit Privacy by Design bzw. Default die Verbraucher ins Boot holen	INSTITUT FÜR INFORMATION, ORGANISATION UND MANAGEMENT PROF. DR. DRES. H.C. ARNOLD PICOT
<p>Bei konsequenter Anwendung der Prinzipien Privacy by Design bzw. Default werden große Datenschutzbedenken gar nicht erst entstehen</p>			
<p>Privacy by Design = technischer Datenschutz</p>		<p>Privacy by Default = „datenschutzfreundliche“ Produkte & Dienstleistungen</p>	
<ul style="list-style-type: none"> • Verbindliche <i>funktionelle</i> Vorgaben für die Systemgestaltung (siehe BSI Schutzprofil) • Vermeidung der Schwächen des organisatorischen Datenschutzes • Ausgleich zwischen Schutzinteresse der Verbraucher und Interessen der datenverarbeitenden Stellen 		<ul style="list-style-type: none"> • „Opt-In“ anstatt „Opt-Out“ • Entspricht den Prinzipien des §3a BDSG (Datenvermeidung und Datensparsamkeit) • Anonymisierung und Pseudonymisierung wann immer möglich 	
<p>Der Kundennutzen von Smart Metering und entsprechenden Diensten und Produkten sollte so hoch sein, dass die Verbraucher, die hierfür notwendigen Daten aus eigenem Antrieb zur Verfügung stellen.</p>			
4			

Bild 4

Deshalb die Empfehlung die beiden häufig diskutierten Schlagwörter „Privacy by Design“ und „Privacy by Default“ in die Praxis umzusetzen (Bild 4). Privacy by Design ist im Endeffekt das, was durch das BSI-Schutzprofil schon angedacht wird. So wichtig es auch ist, den Datenschutz von Anfang an in die technische Entwicklung mit einfließen zu lassen, ist mein Appell an das BSI in diesem Zusammenhang, eher von der Funktion her zu denken als von der Technik. Die Industrie muss bei aller notwendigen Regulierung genügend Spielraum für technische Innovationen haben. Dabei gilt es auch, stets einen tragfähigen Kompromiss zwischen dem berechtigten Schutzinteresse der Verbraucher und den Interessen der datenverarbeitenden Akteure zu finden. Das ist natürlich ein Spannungsfeld, bei dem es gilt, die Trade-Offs genau abzuwägen. Aber in Summe sollte innovativen Firmen genug Raum dazu gegeben werden, die Daten auch nutzen zu können, um neue Geschäftsmodelle zu entwickeln. Denn für mehr Innovation und Wettbewerb im Energiemarkt ist es enorm wichtig, dass innovative Player angelockt werden, die dann die Geschäftsmodelle bringen, von denen immer gesprochen wird.

Das andere Prinzip „Privacy by Default“ ist das, was Facebook vielleicht hätte auch machen sollen, um solche Schlagzeilen, wie gerade gezeigt, zu verhindern. Von Anfang an datenschutzfreundlich konfigurierte Produkte und Dienstleistungen anbieten, die dem Verbraucher die Kontrolle über die Daten geben. Der Verbraucher kann dann selbst entscheiden, welchen Akteuren, welche Daten anvertraut werden. Dies wäre die beste Lösung. Dazu muss aber der Kundennutzen durch auf Smart Meter-aufbauende Dienstleistungen und Produkte so hoch sein, dass die Kunden damit einverstanden sind; also ein Opt-In statt eines Opt-Out Verfahrens. Ich bin zuversichtlich, dass durch die Umsetzung der beiden Prinzipien die Akzeptanz von Smart Metering gesteigert werden kann und insgesamt ein Umfeld geschaffen wird, in dem die ersehnten Energie-Innovationen wie Pilze aus dem Boden sprießen.

9 Sicherheit und Datenschutz im Smart Metering

Rolf Müller-Hermes, Detecon International GmbH, Bonn

Wenn wir schon über Facebook sprechen: ein kleines Beispiel für Utilities und Social Media. Wir machen uns Gedanken darum, wie Social Media Plattformen für Utilities genutzt werden können. Die Nutzung von XING als technische Kontaktplattform, oder ein Firmen-eigenes Twitter Netzwerk sind schon in der Praxis vorhanden. Neu könnte es sein, bei Facebook sein Energieprofil auszutauschen und zu publizieren: Bei einer Partnersuche wüssten die Interessenten sofort, woran sie bei dem / der anderen sind: ein Langschläfer oder ein Frühaufsteher, jemand der nachts noch den Backofen benutzt. Daraus lassen sich interessante Kombinationen konstruieren. Natürlich sind das nur Gedankenspiele ohne jeglichen praktischen Mehrwert, oder etwa doch nicht?

Ich bin über 25 Jahre in der Energiebranche als CIO / CEO oder Berater unterwegs und kenne die Branche daher in- und auswendig. Anhand dieses Vortrages möchte ich meine Praxiserfahrung gegen die derzeitige Situation widerspiegeln, um uns auf den Boden der Tatsachen zu holen und zu zeigen, wo eigentlich aus Praxissicht die Probleme auf uns zu kommen. Gibt es da evtl. etwas, woran wir vielleicht noch nicht gedacht haben?

Ich freue mich, dass ich nicht der Älteste in dieser Runde bin. Sehr viele von Ihnen sind auch im letzten Jahrhundert groß geworden bzw. aufgewachsen. Smart Meter gibt es schon seit den 90er Jahren des letzten Jahrhunderts und ist im Grunde genommen eine alte Technologie. Damals haben wir mit den Vorgängern der heutigen Smart Meter die Verbräuche von Sondervertragskunden per Datenfernübertragung ausgelesen. Das waren damals Zähler mit V24-Schnittstellen, die dann über serielle Modems / Peer-to-Peer Verbindungen ausgelesen wurden. Wir haben Daten analysiert, Lastspitzen ermittelt, Tages-/Wochen-/ Monatsverbrauchscurven generiert. Die Lastprofile von heute sind also nichts Neues. Diese Daten hätten auch früher in falsche Hände fallen können. Aber da diese Verfahren noch nicht die breite Masse betrafen, war es damals auch nicht so populär, sich als Hacker hier zu betätigen.

Hacker gab es damals auch schon. Ich erinnere an den Hamburger Chaos Computer Club, der sich in irgendwelche Systeme gehackt hat, um Schwachstellen aufzuzeigen. Ein Hack, an den ich mich erinnere, war das Knacken einer VideoText Plattform, bei der der Hacker eine Pixelgrafik manipulierte, um ein Ufo über den Bildschirm fliegen zu lassen. Das war damals meist nur Unfug oder aber ein versteckter Fingerzeig auf Schwachstellen in IT-Systemen, wie es sie damals wie heute gab bzw. gibt. Damals war es ein elitärer Kreis von Hackern, die meist nur über ihre Spitznamen wie 4711, 0815, Lonestar, Hackmeister, etc. bekannt waren. Das Wissen wurde in Studentenbuden weitergegeben. Zigaretten rauchend, eine Flasche Bier trinkend, einen Akustikkoppler oder ein V24-Modem mit nervtötendem Pfeifen und Zwitschern wurde vorgeführt, Wissen kommuniziert, eben halt ordentlich gehackt. Wenn man sein Modem an die Telefonanlage des Hotels anschließen wollte, hatte man Prüfspitzen dabei, um den Telefonhörer auseinanderzubauen und sich zum Telefonieren direkt an die Kabeleingänge im Telefon einzuklinken. Das haben viele von Ihnen wahrscheinlich auch mitgemacht. Insofern ist Hacking kein neues Problem. Herausforderungen stellten damals die Großrechner-Systeme dar, die als sicher galten und es war ein Sport, eben genau dies zu widerlegen. Es ging also i.d.R. nicht um zerstören oder eine Beschaffung persönlicher Vorteile, sondern nur um den Nachweis, etwas unmögliches geschafft zu haben. SCADA Systeme, als Systeme in der Prozess-Leittechnik waren früher grundsätzlich gekapselte, also proprietäre Systeme. Es war sehr schwer, in diese SCADA Systeme reinzukommen. Als Leiter der dezentralen IT der Stadtwerke Lübeck hatte ich damals kein Verständnis,

dass die SCADA Systeme sich gekapselt haben. Ich bin in der Client- /Server-Welt groß geworden und habe propagiert, Daten auf PCs nutzbar und auswertbar zu machen. Die Daten der SCADA Welt hatten den Reiz, Echtzeit-Status zu haben und waren hervorragend geeignet, Schalt- und Betriebs-Zustände online graphisch anzuzeigen, und wären so der statischen Dokumentation weit überlegen, die nur statische Zustände anzeigen.

Heutzutage bin ich mir nicht mehr ganz sicher, ob das damals der richtige Ansatz war und wirklich alle Daten immer und überall zur Verfügung gestellt werden sollten; damals war der Grund, weshalb Leittechnik-Daten nicht online zur Verfügung gestellt werden die Befürchtung, dies könne die Echtzeit-Prozess-Leittechnik z.B. durch Datenübertragung, etc. negativ beeinflussen. Schaltungen, die mit Erreichen bestimmter Grenzwerte in Milli-Sekunden ausgelöst werden müssen, könnten durch eine System-Öffnung behindert / verzögert werden und somit zu katastrophalen Schäden in den Netzen führen.

Darüber hinaus wurde der PC im Laufe der Zeit von einem High-Tech-Gerät (mit 5 MB Festplatte und 320 kB RAM) zu einem Spielzeug, das sich bereits schnell in Kinderzimmern wiederfand. Viele Kollegen hatten plötzlich ein Wissen über PC, das - weil zu Hause verfügbar - in der Firma genauso funktionieren musste wie zu Hause. Es wurden Programme und Daten privat kopiert, eigene Anwendungen aufgespielt und zwangen uns IT-Menschen, Sicherheitskonzepte zu entwerfen, IT-Governance-Konzepte zu entwickeln und die Rechte der Mitarbeiter einzuschränken. Das war ungefähr vor 15 – 20 Jahren.

Als ich jetzt bei einem großen Konzern wieder auf die gute alte 3270-Terminalemulation gestoßen bin, wie sie in der 90er Jahren Standard für PC-Anwendungen war, sagte ich mir, ganz so falsch lag man damals vielleicht doch nicht. Um als Hacker in ein System per Terminalemulation reinzukommen, stellt schon eine etwas gehobene Herausforderung dar. Wenn Passworte bekannt sind - sie stehen meistens unter der Tastatur oder in der rechten Schreibtischschublade, lauten häufig „QWERTZ“ oder „geheim“- ist natürlich auch ein derartiges System leicht attackierbar. Da dies aber nicht der Regelfall ist, ist ein System mit Terminalemulation wesentlich angenehmer zu administrieren, als in einem System mit 1.000 PCs mit unterschiedlichen Berechtigungen und Hierarchien und an internationalen Standorten. Dass die Anwender hier sich nicht frei entfalten und ein Maximum aus ihrem Arbeitsplatz-PC rausholen können, steht außer Frage. Aber ist dies in der heutigen Zeit speziell im Konzerngeschäft denn überhaupt noch zulässig ? Ist dieser Individualismus des Users in der Datenverarbeitung überhaupt noch gewollt oder wurde er durch Standards / CI nicht längst ad acta gelegt ? Ein Mitarbeiter darf in Word so ziemlich alles schreiben, aber wenn er anfängt, eigene Zeichensätze zu entwerfen und die Geschäftsbriefe entsprechend zu individualisieren, ist dies sicher nicht im Sinne des Unternehmens.

Aber zurück zum Thema, der Sicherheit und Datenschutz bei Smart Metering. Wie sieht es denn heute aus? Heute haben wir eine 100%ige Abhängigkeit von der Elektrizitätsversorgung. Wie dramatisch das ist, soll Ihnen die kleine Grafik (Bild 1) unten links zeigen.

Tag der offenen Tür im Smart Grid

Die Internationalisierung der Energieversorgung mit permanent wachsender Komplexität führt zu neuen Anforderungen.

Aktuelle Lage

- Vorläufer der SmartMeter sind im Rahmen der ZfA (Zählerfernauslesung) schon seit ca. 1995 bekannt.
- Proprietäre Prozessleitsysteme wickeln die MSR-Technik im Netz ab. (MSR = Messen, Steuern, Regeln)
- Fehler wg. Menschlichen Versagens möglich.

Europäische Netzstörung am 4. November 2006

Um 21:30 wurden 2130 Substationen einer 400kV-Leitung im Nord-West-Französischen NetZ abgeschaltet, um einen großen Schritt die Durchsicht auf der Erde zu ermöglichen

Gegen 22:18 war ganz Europa betroffen und UCTE in drei Systeme segment

Quelle: UCTE - Final Report 2007-01-30

- Diese Störung wurde auf „menschliches Versagen“ zurückgeführt. Eine Leitung (n+1) war geplant abgeschaltet; eine zweite Leitung (n) wurde ohne Rücksicherung vom Netz genommen.

Wo geht die Reise hin ?

- Commodity und Automatisierung sind die Schlüssel zum Kunden. Bei unsachgemäßer Anwendung kommt es zu massiven Sicherheits-Problemen.

Das Smart Grid geht TCP-IP !

- 2 -

Consulting
DETECON
© Detcon

Bild 1

Vielleicht erinnern Sie sich: ein Kreuzfahrtschiff ist in der Meyer-Werft gebaut worden, sollte auf dem Weser-Ems-Kanal auf die Nordsee ausgeschifft werden. Man hat eine Leitung abgeschaltet, um dieses Kreuzfahrtschiff darunter durchlaufen zu lassen. Eine andere Leitung war wegen Wartungsarbeiten ohne Strom. Zwei Leitungen wurden abgeschaltet, und das hat sich in ganz Europa ausgewirkt. Wir hatten Flächen / Länder mit Überspannungs-Problemen, dann andere Länder mit Unterspannungs-Problemen, Schwingungen im Netz, kurzum: die Energieversorgung in ganz Europa hing von 2 Leitungen ab und hat verrückt gespielt. Da sieht man im Grunde genommen, wie abhängig wir von der Elektrizität sind und wie leicht es ist, an einem strategischen Knoten Unfug anzurichten, um dadurch europaweit ein Problem auszulösen.

Gehen Sie heute in YouTube und geben ein: „Wie hacke ich einen Computer?“ Sie bekommen Hunderte von Beispielen angezeigt, die das Wissen entweder per Video erläutert oder á la CBT (Computer Based Training) das Wissen in Form einer Schulung vermitteln. Einige der „Wie hacke ich einen Computer?“-Beispiele haben einen Aufruf von über einer Million Interessenten. Wenn Sie heutzutage einen Jugendlichen fragen, was er später einmal werden will, ist Hacker ein häufiger Berufswunsch. Die Kiddies von heute wissen ganz genau: wenn sie spektakuläre Hacks machen und dadurch berühmt / bekannt werden, bekommen sie in den nächsten Jahren eventuell eine Jugendstrafe; wenn es zu einer Geldstrafe kommt, finden sich erst mal die Reporter der Regenbogenpresse, die das Thema gewinnbringend für beide Seiten ausschlichten. Irgendwann aber bekommen diese Kiddies einen Beratervertrag, der fantastische Konditionen hat. Es hat sich bewahrheitet: die Hacker von gestern sind heute die von der Industrie am höchsten dotierten Berater in Sicherheitsfragen.

Heute sind bereits einige Millionen Smart Meter im Einsatz. Italien und Schweden beispielsweise machen uns vor, wie man z.B. mit Power Line Communication Messdaten im M2M austauschen kann. Es gibt zig Pilotprojekte. Ob Sie es glauben oder nicht, man kann wirklich ein Smart Meter auslesen und die Daten auf einem Rechner darstellen. Ich oute mich. Auch ich habe einen Smart Meter zuhause, und er funktioniert tatsächlich. Meine Verbrauchsdaten

sind über ein Web-Portal auslesbar, mein Verbrauch ist transparent, man sieht, dass ich kein Nachtmensch bin, aber einen sehr hohen privaten Stromverbrauch habe; nebenbei bemerkt: 5 Personen mit 5 Laptops mit separaten Flachbildschirmen plus 2 Server verbrauchen mehr Strom, als wenn ich eine Klimaanlage durchlaufen lassen würde. Der Stromspareffekt, den wir Erwachsene mit Energie-Sparfunktionen und Abschalten statt Stand-By-Betrieb erzielen, wird durch die eigenen Kinder, bei denen der Rechner mindestens 12 h am Tag läuft, wieder vernichtet. Von den LAN-Parties will ich an dieser Stelle lieber nichts erzählen.

Aber was kommt morgen? Morgen kommt auf uns zu, dass die Smart Meter auch in E-Mobilen eingesetzt werden. Wir haben es jetzt nicht mehr mit stationären Zählern, sondern mit mobilen Zählern zu tun. Smart Meter werden verstärkt in Photovoltaik-Anlagen eingesetzt, um diese Anlagen zu steuern, zu regeln, zu begrenzen und auch durchzumessen. Morgen haben wir eine noch ausgeklügeltere Plug and Play Technik als heute. Commodity ist das Stichwort; alles geht einfacher; man hat ein verfügbares Wissen, auf das man von überall aus zugreifen kann. Überall geht es in Richtung TCP/IP, inklusive der Prozessleittechnik. Weil diese Entwicklung immer schneller abläuft – sie sicher auch wichtig ist – aber von der Welt der proprietären Systeme mit ihren Peer-to-Peer Verbindungen immer weiter abrückt, öffnen sich immer mehr ungeschützte IP Adressen, also mehr Angriffsflächen. Also den Tag der offenen Tür ist im Grunde genommen einleitet. Vielleicht kommunizieren die Hacker von morgen über die ungeschützte IP-Adresse des Kühlschranks mit der Netzleitwarte des lokalen Stromversorgers, um die Leitung über den Weser-Ems-Kanal abzuschalten.

IP-schaltbare Knoten können auch Smart Meter sein. Viele dieser Geräte sind mit Remote-Steuerfunktionen ausgelegt. Mit einem Befehl lässt sich also ein kompletter Haushalt abschalten. Nicht die Tatsache, dass meine Verbrauchsdaten an die Öffentlichkeit geraten können, verursacht mir Unbehagen, vielmehr die Tatsache, an einigen Stellen der Versorgung gezielt oder ungezielt Schaltmassnahmen durchzuführen, bereitet mir Angst.



Bild 2

Stellen Sie sich einen großen Wohnblock in Berlin Kreuzberg mit 2.000 Wohneinheiten vor (Bild 2). Es ist Dezember, kalt, eine sternklare Nacht, alle Fenster des Wohnblocks sind erleuchtet. Draussen sitzen 2 Hacker, ein Junge und ein Mädchen. Der Junge zeigt seiner

Freudin, wie sehr er sie liebt, indem er gezielt Wohnungen vom Netz abschaltet, bis über die übrig gebliebenen erleuchteten Fenster „I LOVE U“ zu lesen ist. Das „U“ ist der Kälte geschuldet und eine Abkürzung für „you“.

Morgen wird Cyber Kriminalität im Internet unter einem ganz anderen Kontext zu betrachten sein. Schauen wir uns z. B. die Gaslieferungen von Russland durch die Ukraine oder Weißrussland an, Stromlieferungen in Südafrika, die Stromversorgung in südamerikanischen Ballungszentren an. Wenn da dem Strom der Schalter oder dem Gas der Hahn abgedreht wird, zieht dies heftigste politische und volkswirtschaftliche / betriebswirtschaftliche Konsequenzen nach sich. Die Erpressbarkeit der Länder steigt. Dies haben die Geheimdienste erkannt und Cyberkrieg in der Energieversorgung ist längst keine Utopie mehr. Wenn wir uns das eben aufgezeigte Beispiel mit dem Stromausfall wegen des Kreuzfahrtschiffes vor Augen führen, zeigt dies unsere Verwundbarkeit. Es kommen schwierige Zeiten auf uns zu.

In der heutigen Welt nimmt mobile Kommunikation einen immer größeren Raum ein. Diverse Teilnehmer dieses Kongresses haben ihre PCs auf dem Tisch, diverse haben Ihre Handys oder die Blackberries in permanentem Einsatz, um Mails zu lesen. Das Angebot und die Nachfrage nach überall verfügbaren Informationen und der Beeinflussung von Steuerungsvorgängen wird sich in Zukunft noch weiter verstärken. Das Handy als Kontrollzentrum zum Home-Office ist längst schon keine Utopie mehr. Übrigens haben 20 von Ihnen ihre Bluetooths eingeschaltet und von diesen 20 Bluetooth sind „0000“ oder „1234“ die Standardzugangscodes, um die Kommunikation zum Bluetooth Gerät zu schalten. Selbst wir als Datenschutz- und –sicherheits-Experten gehen häufig zu sorglos mit Security um. Und über Handys lassen sich Smart Meter / Smart Homes genauso schalten wie über PC, drahtlos und einfach.

Was kommt noch auf uns zu? Häufig wird von einem bevorstehenden Daten-Tsunami durch Smart Meter gewarnt. Ein kleines Rechenbeispiel: 100.000 Smart Meter pro Jahr produzieren pro Tag 96 mal 15 Minuten Messwerte. Das sind 2 Milliarden Datensätze pro Jahr pro 100.000 Zähler. Wir reden über 54 Millionen Haushalte in Deutschland. Wir reden über Online Plattformen, wo auf diese Verbrauchswerte zugegriffen werden soll, um Verbräuche zu analysieren. Diese Datenzunahme kommt auf uns zu. Die einzigen heute verfügbaren Datenbanksystem, die in der Lage sind, derartig viele Datensätze zu verwalten, in Online-Plattformen zur Verfügung zu stellen bzw. in halbwegs vernünftiger Zeit Ergebnisse aus Abfragen zu liefern, werden in der Telekommunikations-Branche eingesetzt, wo über jedes Handy-Gespräch die Netze, die Dauer, etc. festgehalten und in endlicher Zeit abgerechnet werden müssen. Das ist übrigens aus meiner Sicht der Punkt, in dem sich die Telekommunikationsbranche und die Utilitiesbranche am ähnlichsten sind: Massendaten in regulierten Märkten zu verwalten und abzurechnen und parallel dazu einen Netzbetrieb zu gewährleisten.

Fazit: Wenn wir schon Smart Meter ausgerollt haben - und davon gibt es Hunderte, Tausende, Zehntausende, Hunderttausende, allein in Deutschland – und wir ändern irgendetwas an der Technologie oder an der Sicherheit, ist es unmöglich, Sicherheitseinstellungen manuell am Endgerät auszuüben. Die damit verbundenen Kosten wären immens. Insofern müssen die Vorgaben und auch die praktische Umsetzung von Sicherheitsvorgaben bei Smart Metern aus der IKT-Welt kommen, wodurch die Berührung zwischen Telekommunikation und Utilities noch weiter wächst.

Smart Meter: Wir diskutieren auf dieser Veranstaltung das Schutzprofil des Smart Meter Gateways. Wir werden es mit neuen Rollen zu tun haben, es kommt der Gateway Operator, der Gateway-Administrator auf uns zu. Wir reden von einer Kommunikation vom Smart

Meter bis in die Datenbank, haben aber noch eine Rollen-Definition, wie sie von der Bundesnetzagentur dargestellt wird, mit einem Messstellenbetreiber, der u.a. für die Qualitätssicherung der Daten zuständig ist. Dazu müsste der Messstellenbetreiber nach Einführung des Schutzprofils diesen Datenstrom zwischen Smart Meter und Datenbank des EVU auflösen, um seiner Qualitätssicherungs-Verpflichtung nachzukommen. Das bedeutet, dass wir in den Prozessen Änderungen haben werden. Wir werden neue Techniken, wie z.B. das Gateway Schutzprofil, und eventuell neue Standards einführen müssen. Hier trifft Theorie auf Praxis, wenn Prozesse und Rollen diskutiert werden, dann müssen die Ergebnisse ganzheitlich erarbeitet und zeitnah veröffentlicht werden.

Wie oben erwähnt, habe ich zu Hause einen Smart Meter. Ich gehöre somit zu der Anzahl an Kunden, die in zig Pilotprojekten getestet wurde: Einfamilienhaus, ein SmartMeter im Keller, über eine kleine Powerline Kommunikations-Strecke geht es hoch zum Gateway und von dort gehen die Daten in die weite Welt (Bild 3). Das alles liegt in meinem privaten Zuständigkeitsbereich und kann von mir administriert werden, somit kann ich auch den Zugang zum Gateway kontrollieren. Immer wenn der Gateway abgeschaltet wird, was häufig beim Staubsaugen passiert, wenn also der falsche Stecker gezogen wird, fällt der Gateway aus und der Smart Meter bekommt, sobald der Strom wieder da ist, dynamisch eine neue IP-Adresse zugewiesen. Das zwingt mich dazu, die Hotline meines Versorgers anzurufen, und mir die neue IP-Adresse des Zählers mitzuteilen, damit ich meinen Verbrauch wieder online sehen kann. Keiner außer mir und meiner Familie hat Einblick in diesen Kommunikationsstrom / Datenverkehr.

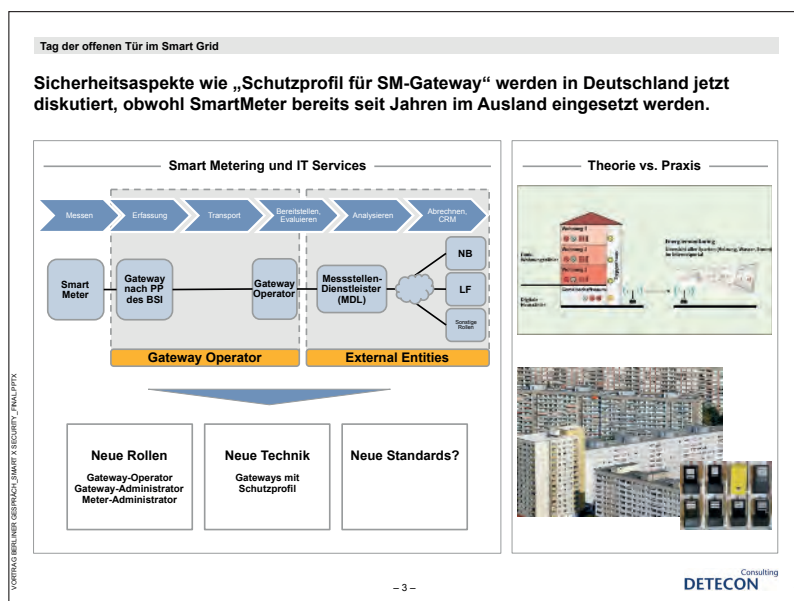


Bild 3

Stellen Sie sich jetzt den vorhin erwähnten Wohnblock vor mit 2.000 Wohneinheiten. Die Stromversorgungsleitungen, die in diesen Gebäuden verlegt sind, werden für PLC Kommunikation genutzt, um die Smart Meter auf einen Konzentrator zu schalten. Sie haben 2.000 Zähler dahinter, mit Sicherheit mehr als nur einen Stromlieferanten, die alle für sich beanspruchen, PLC auf diesen Leitungen zu ihrem Konzentrator zu betreiben. Die Bundesnetzagentur wird vermutlich – das ist meine persönliche Einschätzung - Powerline Communication auf der Last Mile regulieren, damit die Leitungs-/Kommunikationsnetze für jeden

Stromlieferanten / Messstellenbetreiber / etc. zugänglich sein. Dann beginnen wir wieder, neue Standards zu definieren, Kommunikationsnetze und Leitungsnetze zu trennen usw.

Wie weit Hacker bereits in die Versorgungswirtschaft eingedrungen sind, sehen Sie an den folgenden Zeitungsausschnitten, die nur aus dem Jahr 2011 sind (Bild 4).

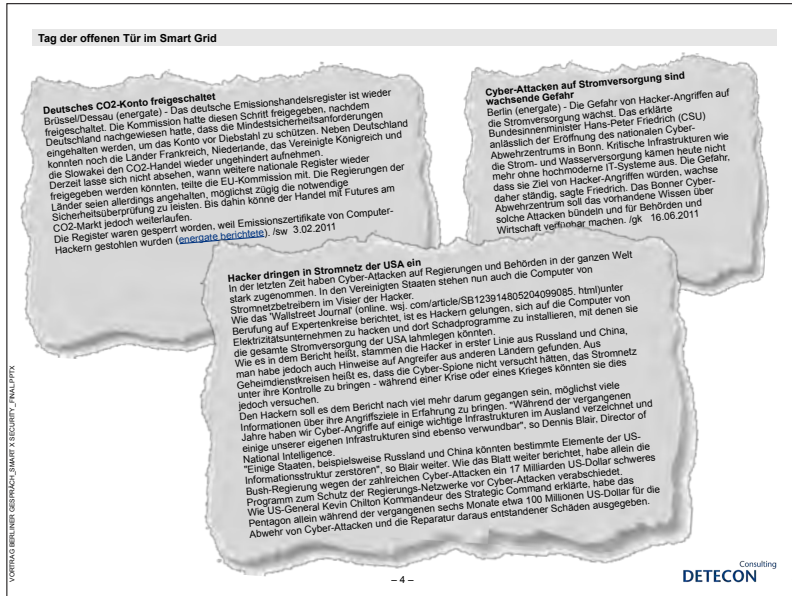


Bild 4

Beschrieben werden Cyberattacks gegen das CO₂-Konto des deutschen Emissionsregisters, wo Daten ausgelesen wurden. In einem anderen Fall haben sich Hacker in den USA in ein SCADA-System eingehackt. Derartige Hackerangriffe werden also demnächst State of the Art sein.

Die Empfehlung von unserer Seite:

Wenn wir schon wissen, dass wir im Bereich der Kommunikation die Sicherheit ins Netz legen müssen, nutzen Sie die Standards, die wir aufbauen / die wir in der Telekommunikation nutzen (Bild 5)!

Nehmen Sie die NISTIR 7628 Guidelines for Smart Grid Cyber Security; bauen Sie ein Informationssicherheitsmanagementsystem (ISMS) nach ISO 2700X auf. Machen Sie Risikoanalysen, wenn Sie in einer entsprechenden Größenordnung oder in einem entsprechenden Umfeld mit Smart Metern zu tun haben! Machen Sie eine Top-Down-Analyse, wo die Reise in Ihrem Unternehmen in Sachen Smart Meter hingehen soll, selbst das System betreiben oder auf einer bestehenden Plattform aufsetzen! Oder arbeiten Sie einfach mit Ihrem Kommunikationsunternehmen zusammen und verpflichten Sie diese Fachleute, die Sicherheit im Kommunikationsnetz zu gewährleisten. Dann können Sie sich auf Ihr Kerngeschäft als Versorger konzentrieren und brauchen nicht jeden Kommunikations- und Sicherheits-Trend mitzuführen und nachzumachen.

Tag der offenen Tür im Smart Grid

Aufgrund steigender Risiken im Smart Grid müssen EVUs zusammen mit Ihren Vendors normierte Cyber Security Strategien entwickeln.

Organisatorische Sicherheitsmaßnahmen

- Einführen eines Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001
- Spezifizieren der ISO 27002 Kontrollmechanismen für die Anforderungen einer der IP-basierten IT im EVU-Umfeld
 - Anpassung der ISO 27002 Mechanismen analog der geplanten Rollen im Smart Grid Umfeld
 - Berücksichtigung der regulatorischen Anforderungen

Sicherheits-Ansatz

```

graph TD
    RA[Risiko Analyse] --> SA[Sicherheits-anforderungen  
(z.B. ISO27002)]
    TDA[Top-down Analyse] --> SA
    BUA[Bottom-up Analyse] --> SA
    DSA[Datenschutz-anforderungen  
(BDSG)] --> SA
    SA --> SA_A[Sicherheits-architektur]
    SA --> SA_B[Bewertung von Smart Grid Standards]
    SA_A --> KB[Konformitäts-bewertung]
    SA_B --> KB
    
```

Technische Sicherheitsmaßnahmen

- Threat Modelling
- Vulnerability Management
- Verschlüsselung (PKI)
- Firewalls
- Authentication
- Penetration testing
- ...

Quelle: NISTIR 7628 Guidelines for Smart Grid Cyber Security

DETECON Consulting

- 5 -

Bild 5

Das war mein Vortrag. Meinen Dank an Sven Garrels, mit dem ich den Vortrag zusammen aufgebaut habe und der mich begleitet hat. Vielen Dank, Sven. Es war wie immer eine Super-zusammenarbeit.

10 Sicherheit und Datenschutz im Smart Metering

Martin Rost, Unabhängiges Landeszentrum für Datenschutz, Kiel

Ich denke ich muss kurz sagen, was Datenschutz ist. Denn ich habe den Eindruck, dass die wenigsten von Ihnen eine Vorstellung davon haben, was Datenschutz ist. Sie reden hier vielfach von Sicherheit und Datenschutz. Ich glaube, dass man noch viel tun muss, damit es überhaupt ein klares Verständnis von Datenschutz gibt, warum man Datenschutz beispielsweise nicht in Datensicherheit auflösen kann, dass Datenschutz gegenüber Datensicherheit eine eigene Dimension ist. Aber es ist auch eine Bringschuld der Datenschützer, diesen Unterschied zu markieren, die die Datenschützer bislang nicht eingelöst haben. Deshalb nun zum Einstieg die Bestimmung des Objektbereichs, dem Datenschutz sich widmet.

ULD www.datenschutzzentrum.de **Objektbereich des Datenschutzes**

Datenschutz beobachtet die organisierte Informationsverarbeitung und Kommunikation in der *asymmetrischen Machtbeziehung* zwischen Organisationen und Personen. Konkret umfasst das vor allem die Beziehung zwischen:

- öffentlicher Verwaltung und deren externen **Bürgern**;
- privaten Unternehmen und deren **Kunden**;
- Praxen / Instituten / Gemeinschaften und deren **Patienten, Mandanten, Klienten**;
- Wissenschaftsorganisationen und deren Forschungsobjekten **Individuen, Subjekte, Menschen**;
- IT- und Energie-Infrastruktur-Providern und deren **Nutzern** (bspw. Access-, Suchmaschinen-, Mail-, Socialnetwork-Betreiber – Energie-Unternehmen, Messstellen- und Leitungsbetreiber);
- Institutionen und deren **Mitarbeitern oder Mitgliedern**.

29.09.2011 - Berlin, Sicherheit und Datenschutz bei Smart Energy Folie 2

Bild 1

Datenschutz beobachtet die asymmetrische Machtbeziehung zwischen Organisationen und deren Personen (Bild 1). Im Außenverhältnis zwischen Organisationen und Personen sind die Organisationen dabei in der Regel ungleich mächtiger, sie verfügen über sehr viel mehr IT-Power und spezielle Expertisen. Es stehen sich in dieser Vorstellung klassisch generische Institutionen und Rollenkonzepte gegenüber: die Verwaltung und der Bürger, das Unternehmen und der Kunde, die verschiedenen Praxen der Dienstleistungen von Hochschulabsolventen und deren Patienten, Mandanten, Klienten. In diesen generischen Rollenkonzepten vom Bürger, Kunden und Patienten sind Freiheitsversprechen der Moderne enthalten. Datenschutz beobachtet nun, wie diese Versprechen in der Praxis tatsächlich eingelöst werden. Dieses asymmetrische Machtverhältnis muss dabei auf beiden Seiten, auf der Seite der Organisation und auf der Seite der Person, in seinen Auswirkungen jeweils gesondert betrachtet werden. Das alles lässt sich auf jeden Fall nicht mit den Mitteln der Datensicherheit allein auflösen. Oder um es schärfer zu formulieren: Eine auf Datensicherheit zielende Betrachtung übernehme untergründig allein die Macht- bzw. Sicherheitsinteressen der Organisationen.

Unser Thema hier ist die Konditionierbarkeit der Relation zwischen den IT-, Energie- und Access-Providern und deren Nutzer. Auch hier gibt es ein spezifisch zu betrachtendes Machtverhältnis. Und im Innenverhältnis zwischen Organisationen und Personen haben wir den Mitarbeiterdatenschutz zu beachten. Hier kann wiederum durchaus eine einzelne Person, ein Mitarbeiter, wenn sie auf einer hohen Ebene der Entscheidungsgewalt angesiedelt ist, eine Organisation zerstören. Die größten Risiken gehen sowohl vom Management als auch von der IT-Administration aus. Das ist aber eine andere Geschichte, die ich jetzt nicht weiter verfolgen möchte.

Datenschutz beobachtet also die reale Ausgestaltung dieser asymmetrischen Machtverhältnisse. Man hat es demnach mit einem Spannungsverhältnis zu tun. Aus der Sicht des Datenschutzes ist dabei jede Organisation ein Angreifer (Bild 2). Grundsätzlich ist keine Organisation vertrauenswürdig, keine Verwaltung, kein Unternehmen, keine Praxis. Zumal diese strukturell dazu gezwungen sind, bestimmten Funktionsimperativen, wie dem nach der Aufrechterhaltung der gegebenen öffentlichen Sicherheit, der Optimierung der Kapitalverzinsung oder der absoluten Diskurshoheit in der Interpretation von Ausschnitten der Welt, nachzugehen. Das sind einfach strukturell eingebaute Monopolisierungstendenzen. Sie haben heute jedoch schon viel von Hackern und Cyberkrieg gehört. Das ist eine ganz andere Perspektive. Aus dieser Perspektive sind es die Personen, die nicht vertrauenswürdig sind. Neben Hackern sind es vor allem betrügerische Kunden und (ehemalige) Mitarbeiter, denen nicht zu trauen ist. Vor diesen Schutz zu gewähren ist nun diejenige der Datensicherheitsperspektive. Die Datensicherheit sorgt dafür, dass die Integrität der Prozesse von Organisationen gesichert ist, ebenso wie deren Verfügbarkeit und die Vertraulichkeit des wesentlichen Kerns des Produktionsprozesses. Gesellschaftlich ist die Umsetzung auch dieser Anforderungen unerlässlich.


www.datenschutzzentrum.de

Zum Verhältnis
 von Datenschutz und Datensicherheit

- Datensicherheit nimmt primär die Organisation, Datenschutz nimmt primär die Person(en) in den Fokus, die von den Tätigkeiten der Organisationen sind.
- Datenschutz setzt funktionierende Datensicherheit einerseits voraus und steht zugleich dazu in einem im strukturellen **Spannungsverhältnis**.
 - **Datenschutz: Die Organisation ist der Angreifer!**
 Folge? Die Organisation muss (jederzeit) prüffähig nachweisen (können), dass sie kein Angreifer ist, sich an die Regeln hält und bei all dem ihre Verfahren und Prozesse beherrscht.
 (Grauzone: Hat auch die Einzelperson als datenverarbeitende Stelle zu gelten? Rechtlich noch offen, bislang von DS-Gesetzen nicht erfasst...)
 - **Datensicherheit: Die Person ist der Angreifer!**
 Folge? Die Person muss nachweisen, dass sie kein Angreifer ist und dass sie ggfs. mit einem Zugriff auf ihre Person rechnen muss. Klassischer Schutz vor Personen: Authentisierung, Autorisierung der Person, Protokollierung, Intrusion-Detection.)

29.09.2011 - Berlin, Sicherheit und Datenschutz bei Smart Energy
Folie 3

Bild 2

Dieses Auseinanderziehen von Datenschutz und Datensicherheit bedeutet beispielsweise, dass Sie erst einmal noch gar nichts für den Datenschutz tun, wenn Sie in ihrem System ganz viel für Datensicherheit machen, indem Sie beispielsweise mit SSL Verschlüsselungs- und Authentisierungsvorgänge in den Interaktionen zwischen Client und Server absichern.

Gleichwohl ist Datenschutz auf Datensicherheit angewiesen. Ohne eine IT, die datensicher gefahren wird, kann kein Datenschutz sichergestellt werden. Insofern ist das Verhältnis von Datenschutz und Datensicherheit kompliziert, weil in bestimmten Aspekten komplementär und in anderen widersprüchlich.

Auf dieser Grafik (Bild 3) sehen Sie das big picture, das heute moderne Datenschützer vor Augen haben, wenn Sie ihre Aktivitäten planen. Ich möchte diese Grafik nun nicht näher im Detail erläutern. Nur so viel: Wir gehen von den geltenden Normen aus und wollen Organisationen daran hindern, mit Personen als Objekte beliebig umzuspringen. Dazu müssen Organisationen über ein Datenschutzmanagement verfügen, das über spezifische Schutzziele reguliert ist bzw. gesteuert wird.

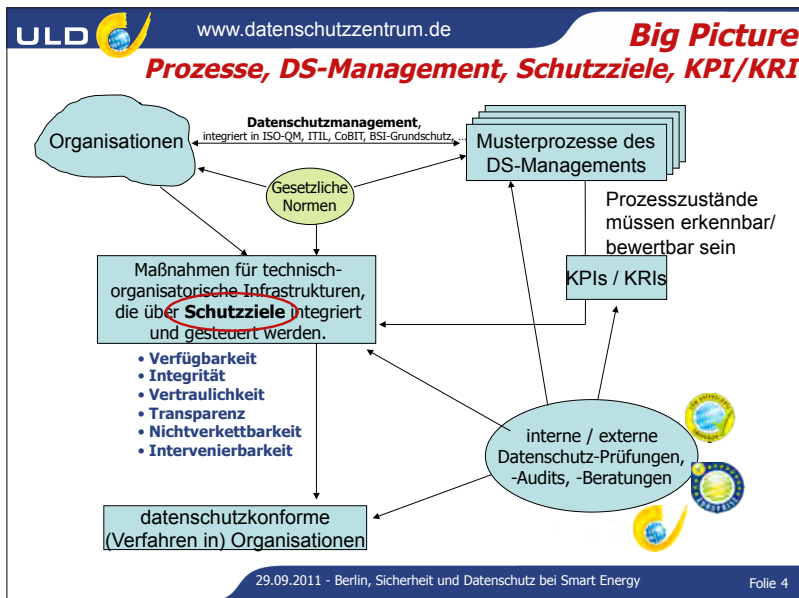


Bild 3

Es wäre dabei unerlässlich, dass auch die Prozesse des Datenschutzmanagements per key performance indicators, oder noch besser durch key risk indicators, wie sie im CoBIT-Paradigma vor gut zwei Jahren entwickelt wurden, kontrolliert würden. Damit der Nachweis geführt werden kann, dass Datenschutz umzusetzen tatsächlich zur Mehrwertschöpfung einer Organisation beiträgt. Und nicht nur kostet. Im Zentrum der Steuerung der Datenschutzprozesse stehen dabei, ganz konventionell gedacht, Schutzziele, zu deren inneren Systematik ich komme und die ich etwas näher im Detail nachfolgend ausleuchten möchte.

ULD  www.datenschutzzentrum.de **Die Systematik der Neuen Schutzziele**

Die elementaren Schutzziele:

Integrität Nichtverkeetbarkeit

Verfügbarkeit Vertraulichkeit

Transparenz Intervenierbarkeit



Rost, Martin; Pfitzmann, Andreas, 2009: Datenschutz-Schutzziele - revisited; in: DuD - Datenschutz und Datensicherheit, 33. Jahrgang, Heft 6: 353-358

29.09.2011 - Berlin, Sicherheit und Datenschutz bei Smart Energy Folie 5

Bild 4

Wenn Sie sich Schutzziele speziell der Datensicherheit angucken, so kennen Sie die drei Standard-Schutzziele CIA, nämlich die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit (Bild 4). Diese wurden beispielsweise besonders prominent 1995 vom Department of Defense ausgeführt. Zur Systematik der Schutzziele hatte Prof. Andreas Pfitzmann, Inhaber des Lehrstuhls für Datensicherheit und Datenschutz an der TU-Dresden, in 2001 einen Aufsatz geschrieben. Danach kam der wissenschaftliche Diskurs in dieser Hinsicht etwas zur Ruhe. Gleichwohl stellte in einem 2008 verfassten internen Arbeitspapier Herr Pfitzmann dann aber überraschend fest, dass Verfügbarkeit und auch Vertraulichkeit sowohl komplementär zueinander - man muss immer beides zugleich von sicheren IT-Architekturen fordern – als auch widersprüchlich sind. Ein Datum, das verfügbar sei, sei nicht mehr vertraulich und gleiches gilt umgekehrt. Diese strukturell gegebene innere Widersprüchlichkeit hatte Herrn Pfitzmann einige Jahre lang beunruhigt. Ich dagegen hatte, wenn ich als Prüfer oder Berater für IT-Systeme agierte, damals schlicht immer beide Schutzziele zugleich hochtreiben wollen, einfach weil ich den inneren Widerspruch zwischen den beiden Schutzziele nicht gesehen hatte. Und als Praktiker darauf vertraute, dass die Verhältnisse zwischen den Schutzziele theoretisch schon irgendwo geklärt sein dürften und man diese Schutzziele, und deren Schutzmaßnahmen einfach anwenden kann. Mir war nicht klar, dass man Schutzziele erst gegenseitig abwägen muss. Aber welche müssen es dann sein und warum? Ausgegangen waren wir damals von den drei, einfach unbestritten geltenden drei Standardschutzziele der Datensicherheit.

Jetzt frage ich Sie einmal pädagogisch hier in die Runde, wenn wir uns das Schutzziele Integrität vornehmen: Gibt es ein weiteres Schutzziele, das in einer gleichen Art wie zwischen Verfügbarkeit und Vertraulichkeit sowohl komplementär als auch widersprüchlich zur Integrität steht? Pfitzmann nennt diese Eigenschaft einer Relation ein Dual. Also erneut gefragt: Fällt Ihnen ein Dual zur Integrität ein? Das war die Fragestellung, mit der uns Pfitzmann 2008 in seinem internen Arbeitspapier konfrontierte.

Die Antwort lautet: Intervenierbarkeit! Das soll heißen, dass in einen integer laufenden Prozess, idealer Weise also ein perfekter Automat, eingegriffen werden kann. Ein Eingriff

macht die Perfektion dieses Automaten zunichte. Die Möglichkeit zum Eingriff bedeutet Angreifbarkeit der Integrität eines Prozesses. Aber man muss, wenn man ein System betreibt, in dieses eben auch eingreifen können, um dieses zu beherrschen. „Always be able to change a running system.“ Als Datenschützer ordne ich unter dieses Schutzziel dann zunächst einmal die Umsetzung der Betroffenenrechte auf Seiten einer Organisation ein. Wie kommt der Bürger, Kunde, Patient an die Daten heran, die eine Organisation von ihm speichert und verarbeitet? Und wenn ich eine Organisation dann tiefer gehend prüfe, dann verlange ich entsprechend der Zielvorgabe Intervenierbarkeit sicherzustellen, dass die Organisation sowohl über ein funktionierendes Projektmanagement als auch ein gesteuertes Configuration-, Patch-, Incident-, Problem- und vor allem Changemanagement verfügt.

Wir bewegen uns allerdings jetzt überwiegend noch im Bereich der Schutzziele, die primär zur Erreichung von Datensicherheit für Organisationen sind. Wie kommt nun der Datenschutz in den Gesamtaufritt? Wenn Sie in das Bundesdatenschutzgesetz hineinsehen oder in die Landesdatenschutzgesetze, dann finden Sie dort Vorgaben bzgl. der Kontrollierbarkeit von Prozessen, etwa was den Zugriff auf Systeme oder auf Applikationen angeht. Voraussetzung für Kontrollierbarkeit ist insofern Transparenz. Organisationen, die personenbezogene Daten verarbeiten, müssen prüffähig nachweisen, dass sie ihre Prozesse beherrschen. Sie müssen dazu Transparenz herstellen können - für sich selber als Organisation, prüffähig aber auch für die Personen, deren Daten eine Organisation verarbeitet und prüffähig für externe Aufsichtsinstanzen, mit denen nicht nur Rechnungshöfe oder Wirtschaftsprüfer, sondern auch die Datenschutz-Institutionen gemeint sind. Transparenz ist somit zweifelsfrei als ein eigenes herauszuhebendes Schutzziel für IT-Infrastrukturen gesetzt. Somit stelle ich erneut pädagogisch die Frage: Was ist das Dual zu Transparenz?

Antwort: Nichtverkettbarkeit! Nichtverkettbarkeit bedeutet, dass Dinge nicht in Beziehung gesetzt werden, obwohl ihre Verkettbarkeit naheläge, also Objekte und Eigenschaften in Beziehung gesetzt werden könnten. Nichtverkettbarkeit ist, als Negation zur Transparenz, die Herstellung von gesicherter Intransparenz. Funktional betrachtet bietet Nichtverkettbarkeit den Vorteil, dass ein Fehler, der in einem System an einer Stelle entsteht, sich nicht trivial fortpflanzen kann, weil eine Grenze, etwa im Sinne einer Brandmauer, vorhanden ist bzw. gezogen wurde. Man muss eine solche Verkettungs-Grenze eigens konstruktiv aus einer übergeordneten strukturellen Logik heraus einziehen, gerade weil sie aus einer anderen Erwägung heraus nicht auf der Hand liegt und unter Umständen die operativen Kosten erhöht. Damit sind wir am Kern der Funktionalität, der Dienstleistung, die der Datenschutz für die Gesellschaft leistet. Nämlich dafür zu sorgen, dass die Verarbeitung personenbezogener Daten durch Organisationen zugespitzt zweckgebunden geschieht. Ohne eine solche Grenze würde das Risiko bestehen, dass über diese Daten die parallel bestehenden Strukturierungsprinzipien der Gewaltenteilung, des Marktes und der freien Diskurse sozusagen einseitig von der Exekutive auf nur ein Ziel hin durchorganisiert werden.

Man muss beim Entwurf von IT-Systemen immer zumindest diese sechs elementaren Schutzziele gemeinsam betrachten und gegeneinander abwägen. Man kann, wenn man weitere Regeln zulässt, aus diesen sechs elementaren Schutzzielen zu insgesamt 14 weiteren Schutzzielen kommen. Darauf möchte ich jetzt und hier nicht weiter eingehen, sondern statt dessen fragen, was man nun davon hat, wenn man im Bereich der Smart Energy mit dem Konzept der Schutzziele arbeitet.

ULD  www.datenschutzzentrum.de

Zum Verhältnis von technisch-organisatorischen Maßnahmen nach Datenschutz und BSI-Grundschutz


Übernahme der BSI-Methodik plus Datenschutzmanagement in Anlehnung an ISO27001 bei Ausweis datenschutzspezifischer Ziele. Das heißt bspw. konkret:

- Leitlinien-, Schutzziele- und Maßnahmen-Orientierung
- Erstellung von Risikoanalysen und Risikobearbeitungsstrategien
- Schutzbedarfstellungen
- datenbankgestützte Modellierung von Systemen/IT-Verbänden
- **Ausweis datenschutzspezifischer Schutzziele**
- **gegenseitige Profilierung** der Schutzziele der Datensicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) und des Datenschutzes (Transparenz, Nichtverkettbarkeit, Intervenierbarkeit)
- und Integration von Datenschutzmanagementprozessen in Standard-Prozesssuiten wie ITIL, CoBIT, St. Gallerer Modell sowie ISO27001

29.09.2011 - Berlin, Sicherheit und Datenschutz bei Smart Energy Folie 6

Bild 5

Die Antwort liegt auf der Hand und zielt auf die innere Systematik und die Methodik ab (Bild 5). Man kann sich nämlich des bestehenden Methoden-Kanons etwa nach BSI-Grundschutz oder, speziell für das Datenschutzmanagement, der ISO 27001 bedienen, die nur um zusätzliche, gesondert zu betrachtende Schutzziele, zu erweitern sind und für die es dann Listen mit Maßnahmen gibt, mit denen die spezifischen Schutzziele des Datenschutzes auch für die Steuerung von Energieflüssen umsetzbar sind. Das Zusammenspiel der Steuerung der Energieversorgung und Datenschutz ist in einem ersten Ansatz im Energiewirtschaftsgesetz geregelt. Für den Datenschutz ist insbesondere der §21g EnWG heranzuziehen, der zwar noch sehr viele ganz wesentliche Fragen der Regelung offen lässt, aber aus dem immerhin deutlich wird, mit welchen Daten und Rollen bei Smart Metering und Smart Grid nun auf jeden Fall zu rechnen ist (Bild 6).

ULD  www.datenschutzzentrum.de **EnWG §21g**
Erhebung, Verarbeitung und Nutzung personenbezogener Daten aus dem Messsystem

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten aus dem Messsystem oder mit Hilfe des Messsystems darf ausschließlich durch zum Datenumgang berechtigte Personen und auf Grund dieses Gesetzes nur, soweit dies erforderlich ist, für die folgenden Zwecke geschehen:

1. das Messen des Energieverbrauchs und die Belieferung mit Energie einschließlich des Einspeisen von Energie einschließlich der Steuerung von unterbrechbaren Verbrauchern im Niederspannung im Sinne von § 14 Abs. 1 Nr. 1;
2. das Messen des Energieverbrauchs und die Belieferung mit Energie einschließlich des Einspeisen von Energie einschließlich der Steuerung von unterbrechbaren Verbrauchern im Niederspannung im Sinne von § 14 Abs. 1 Nr. 1;
3. die Belieferung mit Energie einschließlich des Einspeisen von Energie einschließlich der Steuerung von unterbrechbaren Verbrauchern im Niederspannung im Sinne von § 14 Abs. 1 Nr. 1;
4. das Einspeisen von Energie einschließlich der Steuerung von unterbrechbaren Verbrauchern im Niederspannung im Sinne von § 14 Abs. 1 Nr. 1;
5. die Steuerung von unterbrechbaren Verbrauchern im Niederspannung im Sinne von § 14 Abs. 1 Nr. 1;
6. die Umsetzung variabler Tarife im Sinne von Absatz 5 einschließlich der Verarbeitung von Preis- und Tarifdaten für Verbrauchseinrichtungen und Speichereinrichtungen sowie der Veranschaulichung des Energieverbrauchs und der Einspeiseleistung eigener Erzeugungsanlagen;
7. die Ermittlung des Netzzustandes in begründeten und dokumentierten Fällen;
8. das Aufklären oder Unterbinden von Leistungerschleichungen nach Maßgabe von Absatz 3.

29.09.2011 - Berlin, Sicherheit und Datenschutz bei Smart Energy Folie 7

Bild 6

Bevor ich Ihnen das Modell, das wir mit diesen Angaben entwickelt haben, vorstelle, möchte ich drei einfache Fragen stellen, die bislang nirgends beantwortet werden: 1: Wem gehört das Gateway, das ehemals als MUC bezeichnet wurde? Man darf vermuten: Es gehört demjenigen, der das Gateway bezahlt. Ist die Option, dass der Kunde das Gateway bezahlt, in den Konzepten vorgesehen? Falls ja, dann wäre das operative Analogon zur Einwilligung in die Datenverarbeitung und Kommunikation zwischen Kunde und Organisation ein Ein/Aus-Knopf. Unabhängig von der Frage, wem das Gateway gehört muss es aus unserer Sicht in jedem Falle spätestens dann einen Ein/Aus-Knopf geben, wenn das Gateway bidirektionale und Fernwirkungs-Smart-Grid-Funktionalitäten beinhalten wird. Denn wenn ein Kunde beispielsweise mit seiner Lithium-Ionen-Batterie seines E-Mobiles selber zur kleinen EVU wird, dann haben wir es mit einer Rechtsbeziehung auf Augenhöhe zwischen dem Prosumer und der EVU zu tun. Wenn der eine von beiden Ein- oder Ausschalten können will, etwa wenn ein EVU säumige Kunden fernabschalten können möchte, dann muss es der andere grundsätzlich auch können, um als Energieproduzent eine unfair agierende, etwa falsch abrechnende, EVU stoppen zu können. Sie sehen, dass ich hier entsprechend der Anforderung argumentiere, die sich aus der Berücksichtigung des Schutzziels Intervenierbarkeit ergibt.

Kommen wir nun zu unserem Modell, in dem das gesamte System der Energiesteuerung auf einer gleichmäßigen Granularität dargestellt ist, mit der sowohl Techniker als auch Juristen als auch Betriebswirte etwas anfangen können sollen. Dieses Modell ist eine Arbeitsgrundlage, mit der wir das Protection Profile des BSI analysiert haben und mit dem wir bis zum Ende dieses Jahres noch Usecases entwickeln werden, um mit deren Hilfe klären zu können, welche Daten dabei zu welchem Zweck von wem wohin fließen müssen (Bild 7).

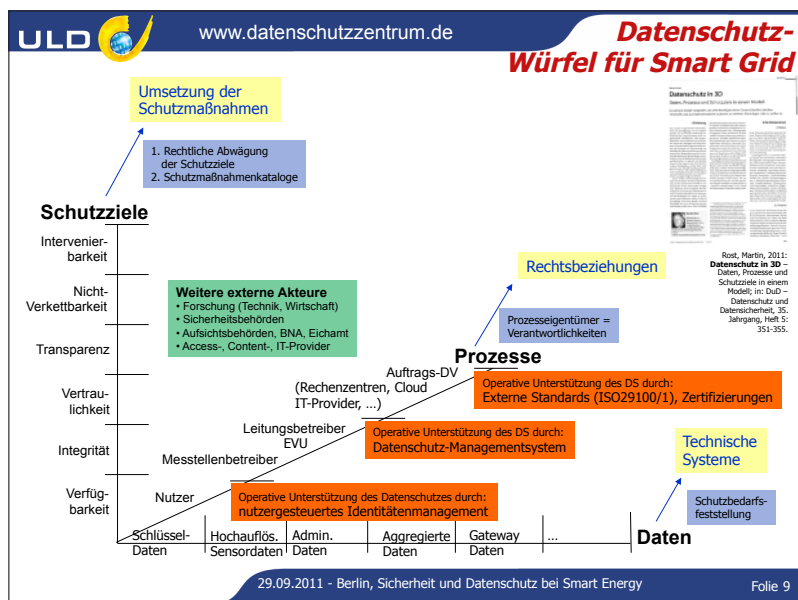


Bild 7

Wir haben in der Y-Achse die Schutzziele, die ich eben erläutert habe. Wir haben in der Z-Achse die Prozesse und Rollen abgebildet. Und wir haben in der X-Achse die Daten, die bei Smart-Metern prozessiert werden könnten, bei Smart-Grid kämen noch Steuerungsdaten zum Fernwirken hinzu, die per se einen mehr als nur hohen Schutzbedarf hätten.

Die Z-Achse der Prozess- und Rollendimension schlüsselt sich in drei Domänen auf: Es gibt den einzelnen Nutzer, also konkret den Haushalt. Dann haben wir als zweite Domäne die Leitungsbetreiber, die Messstellenbetreiber, die Energielieferanten. Und wir haben drittens die Dienstleister der Dienstleister. Man denke hier an Cloudbetreiber, Rechenzentren oder generell IT-Dienstleister (Hardware- und Software-Hersteller, IT-Wartungsarbeiten), die für die Organisation aus der zweiten Domäne, etwa im Rahmen einer Auftragsdatenverarbeitung agieren.

Auf der Y-Achse, also der Dimension der Daten, sind dann verschiedene Datentypen unterscheidbar. Ich habe hier versucht, die Daten von vermutlich sehr hohem Schutzbedarf zu normalem Schutzbedarf anzuordnen. Methodisch entscheidend ist nun, dass man entsprechend der BSI Grundschutzmethode den Schutzbedarf dieser Daten ermittelt und diesen Schutzbedarf der Daten dann vom dem gesamten technisch-organisatorischen System, mit dem diese Daten verarbeitet werden, geerbt wird. Wir müssen vermuten, dass wir stellenweise sehr hohen Schutzbedarf bei Smart Metering haben werden. Also: Dieser sehr hohe Schutzbedarf vererbt sich somit auf das gesamte System, also auch auf das gesamte Rechenzentrum in der dritten Domäne der Prozess-Dimension. Methodisch heißt es für den Entwurf einer Smart-Metering-Architektur, mit der Ermittlung der Daten und deren Schutzbedarf zu beginnen, um die IT-Komponenten entsprechend konzipieren zu können.

Auf der Z-Achse haben wir die Prozess-Eigentümer, können also Rechtsbeziehungen und Verantwortlichkeiten für Prozesse abbilden. Die Beteiligten bekommen ihre Rolle vor Augen geführt und können anhand der Daten, die sie erheben oder erzeugen bzw. verarbeiten,

weiterleiten, speichern, sowie den Schutzziele, die für sie von besonderer Bedeutung sind, ermitteln, was sie jetzt in ihrer Rolle konkret, aus Sicht der Datensicherheit und des Datenschutzes, tun müssen.

Die Schutzziele-Dimension unterliegt der Abwägung unter Einbeziehung insbesondere juristischer Intelligenz. Denn die Schutzziele haben generell die Funktion, rechtliche Anforderungen methodisch in technisch-organisatorische Maßnahmen transformierbar zu machen. Die Schutzziele sollen die Anforderungen des Datenschutzes in Deutschland operationalisieren. Zur Organisation des Zusammenspiels von Juristen, Technikern, Organisationsexperten und Betriebswirten benutzt man dann typischerweise eine „Gardner Spinne“, in der die Intensität der Umsetzungen der Schutzziele abgetragen und dann im Gesamtbild diskutiert wird. ob es ein bisschen mehr oder weniger Verfügbarkeit, Vertraulichkeit, Integrität, Intervenierbarkeit, Transparenz und Nichtverkettbarkeit sein darf. Entsprechend kann der Kaufmann dann anhand der von den Schutzziele dirigierten Schutzmaßnahmen mit dem Kalkulieren beginnen.

Denn letzteres ist das Entscheidende: Wenn die Schutzziele geklärt sind, und ebenso das Maß der Intensität, mit der ein Schutzziel umzusetzen ist, kennt man gemäß BSI Methodik auch die dazu gehörige Maßnahme(n). Die fallen nämlich aus der Tüte, sobald der Prozess des Abwägens beendet und eine Festlegung erfolgt ist. Man weiß, wie man die Integrität von Daten prüft, indem man Hashwerte vergleicht. Man weiß, wie man verschlüsselt, man weiß auch, wie Transparenz und Nichtverkettbarkeit zu sichern ist. Um ein Beispiel für eine Maßnahme für Nichtverkettbarkeit zu nennen: Mit anonymen Credentials lässt sich sozusagen direkt eine Berechtigung nachweisen, die beispielsweise mit der Volljährigkeit zu tun hat, ohne dass dafür das Geburtsdatum zu nennen ist und ohne dass verschiedene Akt des Nachweises untereinander noch in Beziehung gesetzt werden können. Letzteres ist der eigentliche Clou anonymer Credential, weil ein solches Credential nach jeder Nutzung seine Gestalt ändert. Diese Techniken bzw. deren Einsatzszenarien sind sicher noch ungewohnt. Es klingt kompliziert in der Anwendung, aber ist es nicht wirklich. Entsprechende Entwicklungen wie U-prove von Microsoft oder idemix von IBM stehen seit vielen Jahren zur Verfügung.

Es ist außerdem noch auf weitere externe Akteure hinzuweisen, auf die auch Herr Hornung bereits hinwies, die in der Prozess- und Rollen-Dimension hier bislang nicht auftauchen, aber eine latente Rolle spielen. So gilt es beispielsweise an Sicherheitsbehörden, die ebenfalls auf Smart-Meter Daten Zugriff haben wollen, zu denken. Zumindest dann, wenn wir einen Tick weiter in Richtung Smart Grid gehen: Kurz bevor eine Wohnung gestürmt wird, macht es vermutlich guten Sinn, diesem Haushalt den Strom zu entziehen. Eine Steuerprüfung könnte aus einem auffallenden Verbrauchsverhalten eines Haushalts Indikatoren gewinnen, dass ein Haushalt ein Profil wie ein Gewerbebetrieb aufweist. Ich halte es für durchaus legitim, dass solche Aktivitäten stattfinden. Was ich allerdings möchte ist, dass all diese Interessen an den Metering-Daten transparent gemacht und die Zugriffsmöglichkeiten unter Bedingungen gestellt werden. Um noch einen besonders heiklen Player zu nennen: Die Sozialforschung interessiert sich notorisch für diese Daten des Alltagslebens, zu vollkommen unbestimmten Zwecken. Letztlich wird all das, was facebook an Überwachung der Menschen bislang noch nicht gut zu fassen bekommt, dann von den Profilen des Smart Metering, der Home-Automation oder des Ambient Assistant Living erledigt. Am absehbaren Ende stünde der gläserne, voll vermessene Mensch, der sich in all seinen Aktivitäten, die nicht vollkommen auf den absehbaren Pfaden liegen, rechtfertigen muss.

Was man gegen diese Entwicklung zum Schutz der Menschen technisch machen könnte, dass in den drei Prozessdomänen datenschutzverbessernde Techniken eingesetzt würden.

Da wurde in Deutschland, mit Hilfe von EU-Geldern, bereits vieles entwickelt. Ich denke etwa an das nutzerkontrollierte Identitätenmanagement Typ 3, dessen wesentliche Funktionalität darin besteht, nichtverkettbare Pseudonyme und Credentials verschiedener Qualitäten zu erzeugen bzw. zu verwalten. Das Schöne am BSI-Protection-Profile für das Smart-Meter-Gateway besteht darin, dass man mit dem Gateway tatsächlich die für Identitätenmanagement relevanten Transaktionspseudonyme erzeugen kann. Das Gateway bietet allein für sich genommen noch nichts für einen wirksamen Datenschutz, es steht aber zumindest auch nicht im Wege. Das ist schon viel.

Das Wesentliche, was wir in der Domäne 2 auf Seiten der EVU brauchen, ist ein Datenschutzmanagement. Die Energielieferanten, Verteilnetz- und Messstellenbetreiber müssen nachweisen, dass sie ihre Prozesse der Datenverarbeitung geprüftermaßen beherrschen und dass sie an Fairness orientiert sind. Fairness heißt zunächst einmal nicht mehr, als dass sie sich einfach nur an Gesetze halten und das auch nachweisen können.

Wir brauchen natürlich operativ gewendete Datenschutzstandards sowie externe Datenschutz-Audits, gerade auch für die Industrie. Auf uns zukommen werden absehbar wohl die ISO29100 und 101, die ein international abgestimmtes privacy-framework bzw. privacy-controls bieten. Darauf wollte ich Sie am Ende jetzt nur hingewiesen haben. Entscheidend ist, dass diese drei Mechanismen, nämlich Identitätenmanagement, Datenschutzmanagement sowie externe Auditierungen implementiert und aufeinander abgestimmt werden, damit es nicht zum gläsernen Menschen kommt, der mehr oder weniger subtil, aber im Ergebnis doch eindeutig, von den großen Organisationen ferngelenkt werden.

11 Diskussion

Moderation: Dirk Fox, Secorvo Security Consulting GmbH, Karlsruhe

Herr Fox:

Ich will versuchen, die vier Statements ganz kurz mit einem Satz auf den wichtigsten Punkt zu bringen, so wie ich das verstanden habe, und damit die Diskussion eröffnen. Ich fange mit Herrn Rost an. Wir haben gesehen, dass wir, wenn wir Sicherheit und Datenschutz verstehen, mehr Schutzziele haben als Integrität und Vertraulichkeit. Wir haben von Herrn Müller-Hermes einige praktische Probleme kennengelernt, die sich ganz konkret im Doing stellen und die auch bestimmte Anforderungen an die Gestaltung der Geräte stellen. Wir haben von Herrn Dr. Kranz gelernt, dass bei ausreichendem Nutzen wir vielleicht unsere Grundrechte Grundrechte sein lassen und von Herrn Prof. Hornung gelernt, dass wenn wir grundrechtlich auf den Smart Meter schauen, wir vielleicht nicht nur die informationelle Selbstbestimmung im Kopf haben müssen sondern auch die Unverletzlichkeit der Wohnung. Damit schlage ich vor die Diskussion zu eröffnen. Sie haben das Wort. Da ist die erste Frage:

Herr Kießling, MVV Energie:

Eine Frage an Prof. Hornung. Als Physiker tue ich mich etwas schwer mit Rechtsfragen, aber Sie haben sinngemäß ausgedrückt, dass das Thema Daten nicht unter das Thema Eigentumsrechte eingeordnet werden kann. Das verstehe ich nicht so richtig, wenn man die heutigen Prozesse zur Abbildung der Realität in der virtuellen Welt betrachtet. Wenn man früher Bücher, Musik und Filme physikalisch besaß, digitalisiert man heute zunehmend diese Medien, kauft digitale Besitzrechte und besitzt dann auch ohne die physikalischen Originale trotzdem weiterhin virtuelle Bücher, Musikwerke und Filme. Warum sollten keine Eigentumsrechte auf Daten existieren. In früheren Prozessen wurde das Originalwerk in Form eines Buches oder einer Mastermusikaufnahme auf weitere physikalische Träger kopiert, um dann diese physikalischen Kopien zu verkaufen wobei der Käufer dann das Eigentumsrecht an der Kopie hatte. Warum kann man für das Weitergeben von eigenen Daten nicht auch Geld verlangen, also Daten als Eigentum zu betrachten?

Prof. Hornung:

Es gibt natürlich auch an nicht körperlichen Gegenständen Rechte: Wir haben natürlich Urheberrechte, vergleichbare Markenrechte und weitere Immaterialgüterrechte. Ich wollte auf die Konzeption der informationellen Selbstbestimmung hinaus, also nicht auf die Frage, ob ich ein Eigentum an CDs oder Musik habe. Aber informationelle Selbstbestimmung ist in der deutschen Konzeption wie es das Bundesverfassungsgericht im Volkszählungsurteil entwickelt hat etwas, das zum einen eine persönlichkeitsrechtliche, also eine auf Autonomie und Selbstbestimmung ausgerichtete Dimension und zum anderen eine gesellschaftsbezogene Dimension hat. Das Gericht sagt, dass Datenschutz nicht nur im Interesse des einzelnen gewährleistet ist sondern auch im Interesse einer demokratischen Gesellschaft, weil die nämlich nur dann funktioniert, wenn wir unbeobachtete Individuen sind, die im Grundsatz tun und lassen können was Sie wollen, ohne staatlicher Beobachtung ausgesetzt zu sein. Und freiheitliche Diskussionen und Gesellschaft funktionieren nur unter diesen Bedingungen. Insbesondere diese zweite Dimension steht dem entgegen, informationelle Selbstbestimmung zu konzipieren als ein Recht, das nur dem einzelnen und ihm absolut allein verfügbar ist, weil diese gesellschaftliche Dimension dann fehlt. Das schließt nicht aus, dass man unter den Bedingungen moderner Datenverarbeitung und Vernetzung, Web. 2.0 und Digitalisierung usw. natürlich auch im Bereich des Immaterialgüterrechts über neue Modelle nachdenkt. Insofern würde ich sagen, dass es dem nicht widerspricht, was Sie gerade gesagt haben.

Dr. Goerdeler:

Mich interessieren zwei Punkte. Einmal zum Smart Meter. Sind die vorhandenen Schutzprofile, wie sie jetzt durch das BSI vorliegen aus Ihrer Sicht ausreichend, um Datenschutz und IT-Sicherheit genügend abzubilden? Die zweite Frage ist, wie es mit dem Smart Grid aussieht: Was ist da noch zu tun oder welche neuen Fragen mit Blick auf IT-Sicherheit ergeben sich da? Wenn jetzt auf den Grundsatz der Unverletzlichkeit der Wohnung abgehoben wird, dann müssen wir diskutieren, ob oder inwieweit dieser auch bei der Steuerung im Smart Grid abgebildet und eingehalten wird. Da hätte ich gern noch eine Aussage.

Herr Fox:

Herr Rost wahrscheinlich noch einmal? Das Schutzprofil ist nicht im Weg. Das habe ich mitgenommen, aber...

Herr Rost:

Genau. Es gab einige Vorentscheidungen und Gerüchte über Vorentschiedenes, die nicht datenschutzfreundlich waren. Was ich jetzt jedoch mitbekommen habe, ist, dass das Schutzziel Transparenz sehr gut bedient wird, weniger durch die Möglichkeit eines Displays sondern vor allem durch eine PC-Schnittstelle. Das Schutzziel Intervenierbarkeit heißt, dass man auf Prozesse am Gateway Einfluss nehmen kann. Dabei ist noch nicht ganz klar, wie die Administration auf dem Gateway nun wirklich aussehen wird. Entscheidend: Der Ausschalter auch für den Kunden wurde sehr ernsthaft jetzt notiert. Auch ist die Möglichkeit gegeben, Transaktionspseudonyme nutzen zu können. Sicherheitsfragen, etwa dass man verschlüsseln kann, das integrierte Integrität-Checks durchgeführt werden können usw., sind sowieso umgesetzt. D.h. das ist gut geraten. Wir haben uns nun in einer ad hoc-Gruppe der Datenschützer vorgenommen, sozusagen in den höheren Layern nun Use Cases zu formulieren, um die ganzen Vertragsbeziehungen zu regeln und die gesamten möglichen Kommunikationen in den verschiedenen Rollen auf Seiten der Organisationen darüber in den Blick zu nehmen.

Das Gateway ist so wie es derzeit ausgebildet ist super flexibel. Wenn jetzt darüber datenschutzmäßig etwas passiert, was nicht gut ist, liegt es daran, dass wir nicht gut waren. Das Spiel ist jetzt offen. Wir haben noch einmal ein halbes Jahr, damit wir etwas für Datenschutz machen können. Die andere Seite ist allerdings sehr stark. Das kann ich von meiner Seite sagen.

Herr Fox:

Und eine offene Diskussion ist noch die des ‚Remote aus‘. Darf ich das Gateway Remote ausschalten? Das ist eine gewünschte Funktionalität, also nicht ein Problem des Schutzprofils im Kern. Aber es ist im Schutzprofil vorgesehen, aus Sicherheitsicht natürlich ggf. ein Problem. Wenn es gelingt, im großen Stil Remote auszuschalten, kann man natürlich Lichterspiele machen.

Herr Müller-Hermes:

In dem Moment, wo das Gateway abgeschaltet wird – Annahme: Sie arbeiten mit dynamischen IP-Adressen – kann der Zähler meistens nicht mehr angesteuert werden. Das war ein Problem von einem Energieversorger, der heute schon sehr viele Smart Meter ausgerollt hat. Das bedeutet, dass der Kunde auf seinem Kundenportal nicht angezeigt bekommt, wie sein Verbrauch ist und wie/ob sein Zähler momentan läuft. Der Energieversorger hat jetzt das Problem, dass in jedem Falle, wenn das Gateway abgeschaltet war, eine neue IP-Adresse vergeben worden ist. Die Servicebereiche des Versorgers werden dann mit unzähligen Anrufen bombardiert, dass ihr Zähler nicht mehr geht. Dann muss die Serviceabteilung sich auf den Gateway schalten, die IP-Adresse abfragen und in das System eingeben, damit die

Kommunikation zwischen Zähler und Kundenportal wieder aufgebaut werden kann. Auch in diesem Fall haben wir aus meiner Sicht momentan noch keine Erfahrungswerte, die aus der Praxis den praktischen Nutzen für alle Beteiligten und den Aufwand, der vom Energieversorger und anderen zukünftig alles geleistet werden müssen, belastbar darstellen.

Dr. Klumpp:

Die Feststellung, Herr Goerdeler, dass die Smart Meters, die heute in den Regalbrettern liegen, womöglich Elektronikschrott sind, haben wir erst für 2012 nach einigen Gutachten im nächsten Juni vorgesehen. Dass das Smart Grid eine völlig neue Architektur braucht, die nicht etwa einen Stoppknopf oder Rücksendeknopf aufweist und keine bidirektionale Übertragung direkt zulässt, ist auch noch ein bisschen früh. Das sollte man mit entsprechenden Werten belegen können. Auch das ist frühestens erst im nächsten Sommer möglich, wenn wir uns alle anstrengen. Nur diesen Hinweis, dass wir auch schrittweise ganz im Sinne von Prof. Renn reden.

Herr Cebulla, TÜV Informationstechnik:

Heute wurde mehrfach das Vertrauen angesprochen: Vertrauen in die neue Technik, in die Systeme, in die Verfahren oder auch in die Player. Dazu wurden auch Transparenz und Standards erwähnt. Noch nicht angesprochen worden ist, dass dieses Vertrauen natürlich auch dem Verbraucher vermittelt werden muss. Deswegen ist es sinnvoll und notwendig, nach Standards und Normen zu prüfen und dafür Gütesiegel und Audits zu entwickeln. Eine Möglichkeit wäre, dies an die gerade entstehende Stiftung Datenschutz zu adressieren. Sinnvoll wäre es aber vielleicht auch in diesem Kreis, im Münchner Kreis, im Rahmen einer Arbeitsgruppe zu überlegen, wie man für das Gesamtprojekt Smart Grid Gütesiegel entwickeln kann, die einen entsprechenden Status haben und vor allem auch von der Wirtschaft mitgetragen werden.

Dr. Kranz:

Ich kann dem nur zustimmen. Ich glaube, dass das Verbrauchervertrauen durch ein Zertifikat, z. B. von Ihrer Organisation oder auch anderen erheblich gesteigert werden kann. Wie wichtig solche Zertifikate sind, zeigen viele Studien. Also schaden wird es bestimmt nicht.

Herr Fox:

Verstehe ich Sie jetzt so, dass wenn wir den Nutzen nicht kommunizieren können, damit der Verbraucher das mit den Grundrechten nicht so wichtig findet, machen wir ein Zertifikat?

Dr. Kranz:

Da muss ich entschieden widersprechen. Es herrscht immer noch das Recht auf informationelle Selbstbestimmung. Wenn ein Kunde damit einverstanden ist, dass ein Serviceanbieter seine Daten zur Bereitstellung einer Dienstleistung nutzt, heißt das per se nicht, dass Grundrechte aufgegeben werden. Ganz im Gegenteil.

Herr Fox:

Wunderbar. Ganz herzlichen Dank.

12 System- und Architektur-Konzeptionen

Prof. Dr. Manfred Broy, Technische Universität München

Einleitung

Die Architektur der Energienetze wurde in den bisherigen Beiträgen dieser Veranstaltung bereits ausführlich dargestellt. Dieser Beitrag beschäftigt sich stärker mit dem IKT-Anteil im Smart Grid, der wesentlich zur Vernetzung zwischen den Teilsystemen beiträgt, Steuerungen im System ermöglicht und damit unterschiedlichste Regelungsfragestellungen adressiert. Ein weiteres wichtiges Thema dabei ist die dynamische Preisgestaltung und damit verbunden auch Fragestellungen wie sich das Energiesystem über ökonomische Prinzipien steuern lässt.

Ein zentraler Aspekt im Hinblick auf die Entwicklung des IKT-Systems ist die Gestaltung seiner Systemarchitektur. Die Systemarchitektur bestimmt aus IKT-Sicht direkt die Funktionalität des Systems und beeinflusst darüber hinaus maßgeblich dessen Qualität. Das Thema ist zentral, weil genau genommen zwei Architekturen eine wesentliche Rolle spielen und zu integrieren sind, einmal die Architektur des Energienetzes und zum anderen die Architektur des Informationsnetzes. Beide Netze unterliegen ihren eigenen Gesetzmäßigkeiten und Anforderungen, benötigen spezifische Modelle, die zu integrieren sind. Anders als bei dem Energienetz ist das Informationsnetz zwangsläufig ein offenes Netz, soweit eine offene Einbindung von Diensten angestrebt wird.

Zur IKT-Architektur des Smart Grid

Als Architektur wird die Gliederung eines Systems in Komponenten bezeichnet und die Art und Weise wie diese Komponenten interagieren und dabei bestimmte Rollen und Aufgaben im Rahmen der Architektur wahrnehmen. Eine gute Architektur hilft die Komplexität zu reduzieren und trägt entscheidend zur Entwicklung und Beherrschbarkeit verteilter Systeme mit umfangreicher Funktionalität bei. Zudem ermöglicht eine Architektur eine sinnvolle Strukturierung funktionaler und nicht-funktionaler Anforderungen und Eigenschaften. Die Architektur bestimmt dementsprechend maßgeblich die Qualität der Systeme.

Beispiele aus dem Automobilbereich zeigen, dass eine dreistufige Gliederung der Architektur in Abstraktionsebenen sinnvoll ist. Die Aufteilung erfolgt dabei in die Nutzungsebene (Funktionssicht, funktionale Architektur), logische Teilsystemarchitektur (Komponentensicht) und technische Architektur. Die Funktionssicht ist besonders wichtig für die Identifikation, Spezifikation und Strukturierung der Funktionalität eines Systems.

Die IKT-Architektur ist insbesondere für die Funktionalität des Smart Grid entscheidend. Zur Zeit ist nicht hinreichend geklärt, welche Funktionalität das Smart Grid umfassen soll und wie die IKT-Architektur diese am geschicktesten umsetzen soll. Allerdings kristallisieren sich in einigen Versuchsregionen bereits erste Anforderungen heraus. Für die langfristige Weiterentwicklung der Systeme müssen Änderungen oder neuartige Funktionalitäten jedoch jederzeit integrierbar sein. Aus diesem Grund muss eine Architektur erarbeitet werden, die mögliche Änderungen der Anforderungen und möglichst flexibel und kostengünstig die Integration neuer Funktionalität in das Gesamtsystem zulässt. Die funktionale Sicht dient somit einer abstrakten aber leicht verständlichen Beschreibung des Systems, bietet die Grundlage zur Diskussion und erlaubt durch die hohe Abstraktion Erweiterungen frühzeitig und systematisch zu berücksichtigen.

Steht die Funktionalität fest, so erfolgt im nächsten Schritt die Implementierung durch die Zerlegung des Systems in Teilsysteme, welche die Logik der Architektur bestimmt. Besonders bedeutsam ist hierbei die Verknüpfung des Energienetzes mit dem Informationsnetz und Methoden zur integrierten formalen Beschreibung beider Netze. Schließlich erfasst die technische Architektur die Umsetzung der Architektur auf technische Komponenten.

Rollen und Funktionen von Teilsystemen: Smart Meter

Ein derzeit stark diskutiertes Thema ist die technische Umsetzung der Smart Meter. Die ganzheitliche Betrachtung des Smart Meter als Teilsystem im Smart Grid benötigt für das Verständnis jedoch vor allem die Identifikation seiner Funktionalität und damit Schnittstelle sowie die mögliche Interaktion, die ein Smart Meter und ein Gateway zwischen öffentlichen Energienetz und Informationsnetz und den Verbraucher, Prosumer oder Micro Grid bieten sollen. Der Smart Meter und ein Gateway sind entscheidende Elemente, welches den Prosumer mit dem Smart Grid verknüpft. Daher muss zunächst geklärt werden welche Rolle der Prosumer im Smart Grid im Sinne der Architektur einnehmen soll. Obwohl Prosumer, die Energie erzeugen und verbrauchen, eine zentrale Rolle im Smart Grid einnehmen, wurde ihre Rolle bisher im Sinne der IKT-Architektur noch nicht hinreichend spezifiziert. Bereits jetzt ist abzusehen, dass sich Prosumer in professionelle Teilnehmer, also Betriebe, und private Prosumer unterscheiden lassen. Anforderungen an die Funktionalität und die dadurch geprägte Schnittstelle mit dazugehöriger Nutzenerwartung sind für die unterschiedlichen Gruppen noch zu identifizieren. Ein wichtiger Aspekt ist dabei die Kostentransparenz und Abrechnung. Vor allem die dynamische Preisgestaltung muss in der Abrechnung transparent und nachvollziehbar gestaltet werden.

Es ist abzusehen, dass der Markt im Smart Grid zusätzlich zum Stromgroßhandel für große zentrale Stromerzeuger und Versorgungsunternehmen weitere Funktionalität bieten soll. So sollte der Endkunde stärker in das Marktgeschehen eingebunden werden. Bisher konnte der private Kunde nur zwischen den Anbietern wählen, nicht aber direkt an der Volatilität des Strommarktes teilnehmen. Der IKT-Einsatz kann dies grundlegend ändern. Die dazu notwendige Funktionalität kann im Rahmen einer umfassenden Architektur identifiziert und spezifiziert werden. Weitere zentrale Aufgaben, wie Energieerzeugung, Energieverteilung, Energienutzungen, Steuerung des Netzes, Markt- und Preisgestaltung, sind ebenfalls in der Smart-Grid-Architektur zu erfassen.

Was soll durch IKT erreicht werden?

Eine wichtige Aufgabe der IKT ist eine Optimierung der Energieversorgung. Wichtige Optimierungskriterien sind dabei die Versorgungssicherheit, Energiekosten, Ökologieaspekte (Emissionsreduzierung), Energiemanagement (global vs. lokal) und Kosten für die Infrastruktur. Für die Optimierung muss dabei klar spezifiziert werden, wie die Steuerung von Teilsystemen aussieht und welche Effekte im System entstehen und wie sie bewältigt werden können. Die einzelnen Strukturierungskonzepte, wie Prosumer, Micro Grids oder virtuelle Kraftwerke, unterliegen dabei unterschiedlichen Steuerungsmechanismen und können damit unterschiedlichen Effekte im System dienen, je nachdem wie die einzelnen Komponenten untereinander vernetzt sind, wie organisiert sie in der Hierarchie nach oben wirken und ob klassische regelungstechnische Ansätze genutzt werden können.

Die dargestellten Aspekte sind Teil der Anforderungserhebung, die die folgenden Fragenstellungen beantworten muss: Welche konkrete Aufgaben muss ein „Internet der Energie“ erfüllen? Wie kann eine hohe Anzahl verteilter und volatiler Energieerzeuger mit den Energieverbrauchern interagieren und dabei die Stabilität im Energienetz gewährleisten?

Wie können dezentrale Speicher in das System integriert werden?

Die anspruchsvolle Steuerungsaufgabe eines optimierten Energiemanagements bedarf aufwändiger verteilter Regelungstechnik im Smart Grid, die sich durchaus deutlich von den Verfahren unterscheiden muss, die bisher eingesetzt worden sind. Bei der Integration neuartiger, verteilter Steuerung muss geprüft werden, wie zentrale mit dezentralen Steuerungsverfahren interagieren und kooperieren aber auch, ob sie sich negativ beeinflussen können.

Ferner müssen auch nicht stationäre Verbraucher, wie zum Beispiel E-Fahrzeuge, in die Gestaltung der Architektur einfließen. Hierbei muss sichergestellt werden, dass ein E-Fahrzeug einerseits als flexibler Speicher bzw. Verbraucher im System auftreten kann, andererseits muss auch die Markttransparenz hinsichtlich der Abrechnung jederzeit gewährleistet werden. Diese erweiterte Abrechnungsfunktionalität könnte in Anlehnung zu den heute üblichen Verfahren zur Vergebührung bei den Kommunikationsnetzen gestaltet werden.

Zur Nutzung der vielfältigen Informationen des Smart Grids werden Plattformen für Applikationen benötigt. Eine zentrale Frage ist hierbei, welchen Mehrwert neuartige Apps zur energietechnischen Verwaltung und welche Aufgaben die wahrnehmen können und wie lokale Energieverbände damit unterstützt werden können.

Es ist demnach eine Vielzahl von Aufgaben zu lösen. Für eine systematische Vorgehensweise hat es sich als sinnvoll erwiesen, die Fragestellungen in Teilfunktionalitäten herunter zu brechen und sie hierarchisch zu gruppieren, etwa in die Sicherstellung der Versorgungssicherheit, den Verteilnetzbetrieb, die Planung der Netzlast und die Prognose von Engpässen. Im Hinblick auf die Wirtschaftlichkeit sind dabei Prognosen zum kurzfristigen Energiebedarf besonders interessant, vor allem wenn es um Fragen der Wartung der Netze, Fehlerbehebung, den weiteren Ausbau und den vernünftigen Einsatz von Batterien und Speicherkapazität geht. Dabei sollten die Energienetze und die Steuerung mittels IKT unbedingt gemeinsam betrachtet werden, denn IKT hat in den letzten Jahren gezeigt, wie stark verschiedene Bereiche zusammenwachsen.

Funktionale Anforderungen an die IKT-Anteile des Smart Grid

Das Teilsystem Prosumer nimmt eine zentrale Rolle im Smart Grid ein. Es ist dabei wichtig zu verstehen, welche funktionalen Anforderungen dieses Teilsystem erfüllen soll. Erste Erkenntnisse zeigen, dass der reine Datenschutz des Smart Meters und die Ankopplung privater Netze über Gateways an die öffentlichen Netze in Zukunft voraussichtlich gelöst werden kann. Eine zentrale Frage aus der Systemsicht ist dabei, welche Schnittstellen dabei geschaffen werden, um das Netzmanagement des privaten Bereichs auf die Besonderheiten des öffentlichen Netzes auszurichten.

Ein Prosumer möchte am Marktgeschehen teilnehmen aber voraussichtlich nicht täglich aktiv Stromtrading betreiben. Daher müssen bestimmte Automatisierungen und Dienstleistungen dazu vorgesehen werden. So könnte ein Trader derartige Leistungen anbieten, die ein Prosumer vom Markt flexibel beziehen kann. Die täglichen Auktionen würden somit aggregiert von einem Dienstleister durchgeführt werden. Eine offene Frage ist dabei, wie sich das organisieren lässt und ob nicht soziale Netze hierbei eine Rolle spielen könnten. Weiterhin möchten Prosumer nicht täglich aktiv dafür sorgen müssen, dass ihre Elektrofahrzeuge morgens auf einen bestimmten Ladezustand gebracht wird. Naheliegender ist es das Fahrzeug mit dem Terminkalender des Nutzers zu vernetzen, sodass das Fahrzeug automatisch darauf eingeteilt ist, welchen Energiebedarf der Fahrer benötigt. Verbunden ist damit auch die Frage, ob ein lokaler Markt mit „Minitrading“ Möglichkeiten für die Steuerung des gesamten

Systems sinnvoll ist und welche Funktionalitäten damit verbunden wären.

Diese Beispiele zeigen, wie stark verschiedene IKT-Teilfunktionen in Zukunft miteinander vernetzt werden müssen und welche automatisierten Vorgänge stattfinden können und müssen. Schnittstellen sind dabei ein zentrales Thema, welches unbedingt im Gesamtkontext stärker beleuchtet werden muss. Damit verbunden muss auch untersucht werden, welche Sicherheitsfragen Rechte- und Authentifizierungssysteme benötigen.

Derzeit wird im Rahmen von acatech ein Projekt zum Thema Cyber-Physical Systems (CPS) durchgeführt. Ein zentraler Aspekt ist dabei, dass die physikalische Welt, bestehend aus physikalischen und eingebetteten Systemen (Cyber Space) und die Nutzerwelt über entsprechende Mensch-Maschine-Interaktionen über bestimmte Schnittstellen interagieren. Wesentliche Fragen sind dabei, welche Informationen dem CPS zur Verfügung stehen, wie diese Informationen mit Medien wie dem Internet vernetzt werden und welche neuen Funktionalitäten dies ermöglicht. Hier gibt es eine Reihe von interessanten Vorstellungen, zum Teil sehr ambitioniert. Unabhängig zu den technischen Visionen sollten stets die Fragestellungen passend zu den Zielen, die langfristig erreicht werden sollen, im Zentrum stehen. Das Smart Grid, das als Cyber-Physical System par excellence gesehen werden kann, spielt dabei eine prominente Rolle.

Nichtfunktionale Anforderungen

Neben den funktionalen Anforderungen existiert auch ganze Reihe nichtfunktionaler Anforderungen für das Smart Grid und seine IKT-Anteile. Das Thema Security, wie bereits im Vorfeld umfassend dargestellt, ist eine wichtige nichtfunktionale Anforderung, aber es gibt noch eine Vielzahl weiterer Anforderungen, die beachtet werden müssen. Dazu gehört zum einen die Interoperabilität, die Fähigkeit die Funktionalitäten von Teilsystemen mit anderen Teilsystemen zu vernetzen. Außerdem sind Aspekte wie Zuverlässigkeit, Effizienz, Betriebssicherheit, angemessene Betriebskosten, Performanz, Evolution – die Fähigkeit das System weiter zu entwickeln, Skalierbarkeit, Langlebigkeit, Versorgungssicherheit, Robustheit und eine dynamische Anpassung bei Störfällen weitere nichtfunktionale Anforderungen. Ferner ist die Benutzerfreundlichkeit und Benutzerakzeptanz eine der wichtigsten Anforderungen für den Nutzer, wozu auch die Transparenz und die Nachvollziehbarkeit von Prozessen gehören. Nur wenn der Nutzer versteht, was die angebotenen Aktionen und Funktionen bewirken, wird er das erforderliche Vertrauen haben um am Smart Grid aktiv teilzunehmen.

Herausforderungen

Die identifizierten Anforderungen ermöglichen die Entwicklung einer Architekturbeschreibung für die einzelnen IKT-Teilsysteme. Die Systeme sollten die Funktionalitäten von verschiedenen Stakeholdern, wie Betreiber der Netze, Betreiber der Erzeuger, Großverbraucher, Endkunden sowie Trader und andere Dienstleister abbilden. Es muss dabei unbedingt berücksichtigt werden, dass die Stakeholder über eine lange Zeit mit den Netzen leben müssen und ihre Geräte und Anschlüsse nicht einheitlich auf dem neuesten Stand der Technik sind. Daher muss die IKT-Architektur des Smart Grid mit existierenden Altgeräten kompatibel sein und die genutzten Protokolle müssen unterschiedliche Stufen der Intelligenz unterstützen. Eine Architekturbeschreibung muss dies unbedingt gewährleisten.

Eine Möglichkeit einer derartigen Lösung bieten serviceorientierte Architekturen, die die Hierarchie der Dienststrukturen der IKT-Netze gut abbilden können. Derzeit existieren jedoch viele unterschiedliche Vorstellungen, was die Architektur und Architekturbeschrei-

bung betrifft. Das zeigen die Untersuchungen aus den Versuchsregionen des E-Energy Projekts genauso wie internationale Bestrebungen zur Smart Grid IKT-Architektur. Die bislang entwickelten Lösungen und Vorstellungen weisen derzeit noch (zu) viele Unterschiede auf. Eine große Herausforderung besteht also darin, wie die Vielfalt der Funktionalitäten erhalten werden kann und gleichzeitig genug Einheitlichkeit und Interoperabilität entsteht, um die Ansätze einheitlich zu beschreiben.

Fazit

Die Tagungsbeiträge zeigen, wie vielfältig die Herausforderungen in der Smart Grid Entwicklung sind und wie umfangreich die Anforderungen. Eine tragende Rolle wird daher insbesondere für die IKT-Anteile voraussichtlich die Koevolution einnehmen, die kooperative Evolution der Systeme und ihrer Funktionalität. Es erscheint derzeit unwahrscheinlich einen großen Entwurf für die Architektur zu erstellen, der Bestand für die nächsten Dekaden hat. Die IKT-Technik ist hierfür zu dynamisch, zu volatil und unvorhersehbar, um sie schon heute für die nächsten Jahrzehnte im Detail fixieren zu können. Daher wird eine Netzarchitektur benötigt, die eine Evolution zulässt und offen genug ist, um auch Themenbereiche einzubinden und Lernkurven von Nutzern in der Akzeptanz zuzulassen.

Ein wichtiges Ziel ist dabei stets, für die IKT-Lösungen für das Smart Grid Legacy zu vermeiden. Wenn Systeme gebaut werden, die nicht weiter entwickelbar sind, müssen die Systeme früher oder später entsorgt werden, was mit unakzeptablen Kosten verbunden ist. Die Fragen muss somit lauten: Wie kann Legacy vermieden werden? Wie können zentrale und dezentrale Elemente im neuen System sinnvoll kombiniert werden? Wie können neue Funktionalitäten zugelassen, neue Mehrwerte ermöglicht und neuen Businessmodellen zugänglich gemacht und integriert werden? Wie wird sich die Benutzerakzeptanz hinsichtlich der Autonomie der Netze auswirken und wie viel Kontrolle brauchen die Nutzer? Erst wenn dazu all Anforderungen richtig verstanden sind, kann eine Architektur sinnvoll gestalten werden. Unbenommen ist dabei, dass eine Architektur, die auf eine langfristige Entwicklung des Smart Grids ausgerichtet ist, in der Lage sein muss, sehr schnell neue Anforderungen aufzunehmen und sich anzupassen.

13 Smart and Safe – intelligente Speichersysteme im Verteilnetz

Christian Müller-Elschner, Younicos AG, Berlin

Mit Freude sehe ich, dass die Themen Sicherheit und Datenschutz im Rahmen der Diskussion um Smart Metering und Smart Grid Konzepte mittlerweile den Stellenwert eingenommen haben, den sie verdienen. Gleiches gilt für das Verständnis, dass es sich im Zusammenhang mit Smart Metering vor allem auch um die Verarbeitung von Massendaten handelt. Dies war, insbesondere auf der Herstellerseite, nicht immer so. Vor ca. 5-6 Jahren, ich war zu dieser Zeit bei der T-Systems beschäftigt, haben Rolf Müller-Hermes und ich unter anderem die Grundlagen für die Energiestrategie für die Deutschen Telekom entwickelt und gemeinsam mit den Technischen Werken Friedrichshafen eines der ersten Smart Metering Projekte im Rahmen des T-City Projekts initiiert. Relativ früh haben wir auf Basis der Erfahrungen im Telekommunikationsmarkt die Themen Sicherheit und Datenschutz adressiert und zum Beispiel frühzeitig einen Datenschutzbeauftragten mit in das Projektteam geholt. Das nur als kleiner Ausflug.

Vielen Dank an meinen Vorredner, der eine sehr gute theoretische Einführung und Überleitung zum Thema Speicher gegeben hat. Ich werde Ihnen im Folgenden beispielhaft aufzeigen, wie Energiesysteme der Zukunft aussehen könnten. Wichtige Bausteine solcher Systeme sind neben regenerativen Energieerzeugungsanlagen Speichertechnologien und neue, dezentralere Steuerungssysteme. Vorweg ein paar Informationen zu Younicos. Younicos ist ein junges Unternehmen, welches sich seit nunmehr sechs Jahren mit speicherbasierten Energiesystemen auf Basis erneuerbarer Energien beschäftigt. Wir entwickeln und realisieren Produkte und Projekte vom Watt- bis zum Megawattbereich, von netzbasierten Energiesystemen für Haushalte und Energieversorger bis hin zu Systemen für ganze Inseln. Bis Anfang 2013 werden wir eine Azoreninsel - die Azoren gehören zu Portugal - mit ca. 4.500 Einwohnern und zwei Industrieunternehmen auf eine Energieversorgung basierend auf regenerativen Energien umstellen und wirtschaftlich betreiben. Zirka 75% der Energie werden ab dann aus Sonne und Wind gewonnen, Batterien mit einer Leistung von insgesamt 3 MW und einer Kapazität von 18 MWh machen die regenerativ gewonnene Energie planbar, die restlichen 25% sollen später aus Biodiesel erzeugt werden. Die Batterien sind bereits heute verfügbar. Die größte technologische Herausforderung lag in der Entwicklung des Inselsteuerungssystems. Warum? Im bestehenden Energiesystem hatten die Dieselgeneratoren bereits ab 15% Windanteil Schwierigkeiten, das Netz stabil zu halten. Aber dazu später mehr.

Smart und Safe – Speicherbasierte Energiesysteme im Verteilnetz

1. Die Energiemärkte werden sich fundamental verändern
2. Der geplante Ausbau erneuerbarer Energien bedingt Energiespeicher und neue Steuerungssysteme
3. Mix aus zentralen und dezentralen Speichern
4. Der Bedarf an dezentralen Steuerungselementen steigt
5. Intelligente Speichersysteme können einen Beitrag zu mehr Netzsicherheit leisten
6. Fazit - Vom Smart Grid zum Safe Grid



Younicos
Let the fossils rest in peace.

Seite 2

Bild 1

Nun zu den wesentlichen Aussagen meines Vortrags (Bild 1). Ich werde zeigen, dass der eingeschlagene Weg in Richtung mehr erneuerbare Energien zwei Dinge unabdingbar macht: Energiespeicher und neue Steuerungsmechanismen. Ich werde ihnen einen kurzen Überblick über aktuell verfügbare Speichertechnologien und aktuelle Anwendungsfelder geben. Danach werde ich ihnen aufzeigen, wie ein Steuerungssystem der Zukunft aussehen kann und ihnen anhand eines konkreten Beispiels aufzeigen, wie intelligente Speichersysteme einen Beitrag zu mehr Netzsicherheit leisten können, das heißt, wie wir von einem Smart Grid zu einem Safe Grid kommen.

Der Energiemarkt befindet sich im Wandel. Das wissen wir hier im Saal alle. Die Nachfrage nach plan- und steuerbarer Energie auf Basis erneuerbarer Energien wird steigen, die Energieversorgung wird dezentraler und neue, dezentralere Steuerungs- und Regelmechanismen werden notwendig. Auch die bestehenden Markt- und Versorgungsstrukturen müssen überprüft werden.

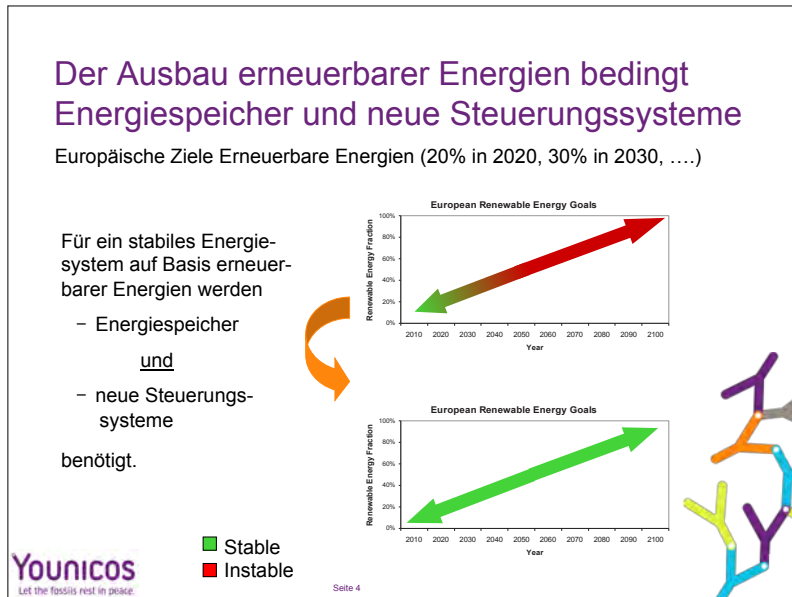


Bild 2

Wenn wir den Anteil regenerativer Energien wie politisch geplant steigern, ohne die Netzstrukturen zu verändern, werden wir schnell an technologische Grenzen stoßen. Wir haben in Deutschland mittlerweile ca. 20% regenerative Energien im Netz. Irgendwann werden wir, wie auf Graciosa, an eine Grenze kommen, ab der die bestehenden Steuerungssysteme nicht mehr in der Lage sein werden, die Netzstabilität zu gewährleisten (Bild 2). In Teilbereichen geschieht dies bereits heute. Die Folge, regenerative Erzeugungsanlagen insbesondere Windkraftanlagen werden zunehmend abgeschaltet; das Osterbeispiel wurde ja gerade beschrieben. Bisher nicht erwähnt wurde, dass Investoren, die in Windkraftanlagen investiert sind, um Investitionssicherheit zu erhalten, auch dann eine Vergütung erhalten, wenn eine Anlage aus Netzstabilitätsgründen vom Energieversorger abgeschaltet wird. Das heißt, wir als Endverbraucher zahlen in zunehmendem Maße dafür, dass regenerative Energie nicht erzeugt beziehungsweise eingespeist wird. Das ist doch absurd. Um dieses zu ändern, brauchen wir Speicher und neue dezentralere aber auch sichere Steuerungssysteme.

Zum Thema Energiespeicher: Von meinem Vorredner wurden 'Car to Grid' Systeme als Speichermöglichkeit aufgezeigt. Meines Erachtens werden diese im heutigen Nutzungsmodell nur ergänzende Bausteine in einer zukünftigen Speicher- und Energielandschaft darstellen. Ich werde ihnen Beispiele für stationäre Speichersysteme zeigen, die bereits heute eingesetzt werden können, langlebiger sind und die einfacher zu steuern und zu managen sein werden als zum Beispiel mobile 'Car to Grid' Systeme.

Wozu brauchen wir Speicher? Sonnen- und Windkraft fallen nicht immer dann an, wenn wir die Energie benötigen. Das heißt, wir brauchen Energiespeicher, um kurzfristige, tageszeitliche, wöchentliche und saisonale Schwankungen auszugleichen. Ähnlich einer Groß- und Einzelhandelsstruktur wird es zukünftig einen Mix aus großen, zentralen Speichern wie zum Beispiel Pumpspeichern, CO₂-Speichern oder „Power-to-Gas“ Anwendungen für den Ausgleich monatlicher und saisonaler Lastschwankungen, schnell reagierenden „Megawatt-Batteriespeichern“ zur Teilnahme am Primär- oder Sekundärregelenergiemarkt und dezentralen Batteriespeichern im Verteilnetz zum Ausgleich von Last- und Preisverteilungen im Tagesablauf geben.

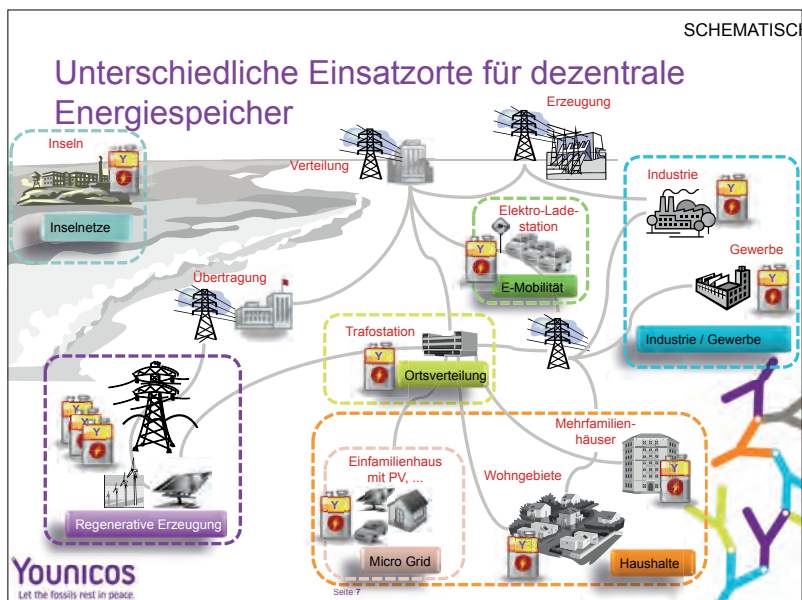


Bild 3

Ähnlich dem Supermarkt um die Ecke, dem Kühlschrank im Haus, dem Einkaufszentrum vor der Stadt wird es unterschiedliche Standorte, Anwendungsfelder und Geschäftsmodelle für Speicher geben. Dezentrale Speicher können Bausteine des Microgrids eines Hauses oder eines Wohngebiets sein, sie können helfen, Lastunterschiede eines Ortsnetzteils oder einer Region auszugleichen und ggf. sogar helfen, Netzausbaumaßnahmen zu verschieben (Bild 3). Im Übertragungsnetz können Speicher aktive Teilnehmer im Regelenenergiemarkt werden und in Kombination mit z.B. Gaskraftwerken flexibler als die Grundlastkraftwerke auf die fluktuierenden Erzeugungskurven regenerativer Erzeugungsanlagen reagieren.



Bild 4

Derzeit sind drei Batterietechnologien für den Einsatz in dezentralen Energiesystemen verfügbar (Bild 4).

Im Megawattstundenbereich sind dies Natrium-Schwefel Batterien. Sie werden in Japan bereits seit über 13 Jahren erfolgreich eingesetzt und betrieben, was unter anderem die Erstellung technologisch belastbarer Businesspläne für Großprojekte ermöglicht. Im Norden Japans wird zum Beispiel seit vielen Jahren ein 34 MW Speicherpark in unmittelbarer Nähe zu einem 51 MW Windpark betrieben. Die geographischen Gegebenheiten hatten es nicht erlaubt, die Stromtrassen aus dem windigen Norden in den Süden weiter auszubauen. Dort befinden sich unter anderem die Großstädte Tokio, Osaka und Nagoya. Wir nutzen Natrium Schwefel Batterien derzeit bei der Realisierung von Inseln und für Lösungen im Sekundärregelmarkt.

Eine weitere attraktive Batterietechnologie stellen Vanadium-Redox-Flow Batterien dar. Sie sind mittlerweile serienmäßig verfügbar, decken derzeit den „Kilowattstunden-Bereich“ ab und lassen sich natürlich auch zu größeren Batterieeinheiten zusammenstellen. Auf dem Chart sehen sie zwei Batterien unserer Tochtergesellschaft Cellstrom, den Cellcube 10/100 (100 kWh) und den Cellcube 200/400 (400 kWh). In der aktuellen Forschung wird versucht, diese Batterietechnologie noch weiter zu skalieren.

Im Bereich der Energiesysteme für Haushalte (Micro Grids) favorisieren wir derzeit Lithium-Titanat Batterien. Im Gegensatz zu den Lithium-Ionen Batterien, die derzeit in der Elektromobilität eingesetzt werden, kommt es bei stationären Speichersystemen vor allem auf die Langlebigkeit (> 7.000 Zyklen), Sicherheit und die einfache Integrierbarkeit in bestehende Systeme an. Baugröße, Spitzenleistung und das Verhalten bei niedrigen Temperaturen stehen bei stationären Batterien weniger im Fokus.

Für alle aufgezeigten Bereiche gilt, ein speicherbasiertes Energiesystem auf Basis erneuerbarer Energien muss sich irgendwann rechnen. Im internationalen Umfeld ist dies bereits

heute bei vielen Inseln der Fall. Speicherbasierte Energiesysteme auf Basis erneuerbarer Energien stellen über einen Betrachtungszeitraum von mehr als 10 Jahren bereits heute eine attraktive Alternative zu den bislang üblichen dieselbetriebenen Systemen dar.

Ähnliches gilt auch für den Einsatz von großen Speichern im Regelenergiemarkt. In Primär- und vermutlich bald auch im Sekundärregelenergiemarkt lassen sich unter bestimmten Rahmenbedingungen auch in Deutschland jetzt schon attraktive Business Cases und somit neue Einnahmequellen finden.

Für die folgenden Anwendungsbeispiele gilt: Noch sind die Speichertechnologien vergleichsweise teuer. Das waren die ersten Mobiltelefone des C-Netzes allerdings auch. Der Markt wird sich weiterentwickeln, die Speicherlösungen werden spezieller auf die einzelnen Anwendungen zugeschnitten, die Stückzahlen werden steigen und Anbieter mit innovativen Geschäftsmodellen werden auf den Markt kommen. Die Anwendungsfälle und die Bedürfnisse sind da; und die ersten Kunden setzen dezentrale Energiespeicher bereits ein. Denken sie nur an den Markt für mobile Datendienste; vor der Einführung des iPhones und heute, nur vier Jahre später.



Bild 5

Anwendungsfall Hausspeicher (Bild 5): Die Barwertbetrachtung der meisten für das nächste Frühjahr angekündigten Lithium-Ionen Hausspeicher lässt diese derzeit nicht attraktiv erscheinen. Betrachtet man allerdings das gesamte Energiesystem eines Haushalts inklusive Wärme und Elektromobilität, dann können sich ganz andere Businesspläne ergeben. Es gibt immer mehr Privatpersonen, die von den Energieversorgern unabhängiger werden wollen, Energieautonomie anstreben. Denken sie an den Pendler, der jeden Tag 15 bis 20 km fährt und zukünftig abends den gespeicherten Sonnenstrom tankt; es sei denn, er tankt tagsüber beim Arbeitgeber. Diese Szenarien werden kommen. Die Resonanz aus dem Markt ist da. Es gilt nun, die Systeme richtig zu dimensionieren und anwendungsbezogen auszugestalten. Als Kapazitätserweiterung von Hausspeichern ergeben sich dann möglicherweise auch attraktive Anwendungsfälle für Car-to-Grid Lösungen.

Parallel dazu muss natürlich alles getan werden, um die Kosten für Lithium-Ionen-Speicher weiter zu senken. Zum Beispiel auch durch die Verwendung von auf die spezifischen Anforderungen eines stationären Umfeldes zugeschnitten langlebigen und sichere Zellen mit den entsprechenden Funktionsgarantien der Zellhersteller.

ANWENDUNGSBEISPIEL

Beispiel Gewerbekunden – Haupteinsatzgebiet von Redox-Flow Batterien

- Peakabsenkung
- Planbare Energiekosten
- Erhöhung Eigenstromanteil von PV und Windanlagen
- „grünes Image“ z.B. CO2 freies Tanken
- Absicherung der Stromversorgung
- Spannungsstabilität

Younicos
Let the fossils rest in peace

Quelle: Cellstrom Referenzprojekte Seite 10

Bild 6

Beispiel Gewerbe- und Industriekunden (Bild 6): Die Firma Gildemeister hat sich Anfang letzten Jahres zu etwas mehr als 50% an unserer Tochtergesellschaft Cellstrom beteiligt. Warum? Gildemeister verkauft weltweit hochpräzise Werkzeugmaschinen. Schwanken die Frequenz oder die Spannung eines Stromnetzes oder fällt der Strom ungeplant aus hat dies Auswirkungen auf die Qualität des Werkstücks. Bei Bearbeitungszeiten von teilweise mehreren Stunden entstehen im Ausschussfall schnell auch einmal Kosten in fünfstelliger Höhe. Die Anschaffung von zum Beispiel Redox-Flow-Batterien rentiert sich in Ländern mit unsicherer Netzinfrastruktur dann sehr schnell.

Wie sieht es zukünftig in Deutschland aus? Uns besuchen immer häufiger Familienunternehmer, die sich Gedanken um die zukünftige Netzstabilität und steigende Energiekosten machen. Sie informieren sich über die Möglichkeiten und Geschäftsmodelle, die sich durch eine stärkere Nutzung von regenerativen Energien ergeben. Auf dem Chart sehen sie einige Anwendungsbeispiele der Vanadium-Redox-Flow-Batterie Cellcube 10/100.

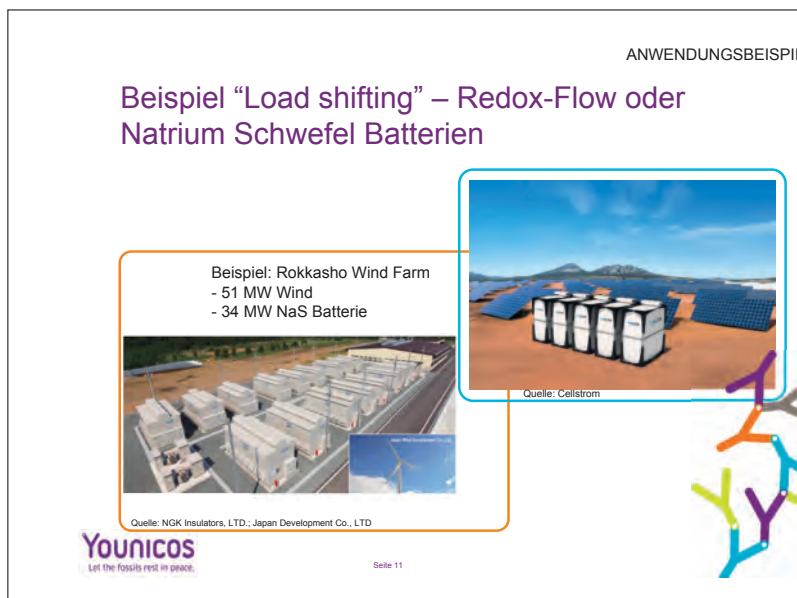


Bild 7

Ein weiteres Anwendungsfeld ist das „Loadshifting“ (Bild 7), die Glättung der Lastspitzen vor der Einspeisung ins Netz. Links sehen sie den Rokkasho Windpark in Japan mit der 34 MW Natrium-Schwefel-Batterie den ich eingangs erwähnt habe. Jeder Block hat eine Leistung von 2 MW und 12 MWh Energie.



Bild 8

Eine Elektrotankstelle (Bild 8) für CO₂-freies Tanken: Die Elektrotankstelle auf dem großen Bild steht auf dem Gelände der Gildemeister AG. Sie unterscheidet sich deutlich von den

bisherigen Lösungen. Sie wird von Gildemeister Energy Solutions als Komplettlösung inklusive Batterie, PV-Fläche und Windrad verkauft. Mehr als sechs solcher Tankstellen sind in diesem Jahr bereits verkauft worden, unter anderem auch an Automobilunternehmen.

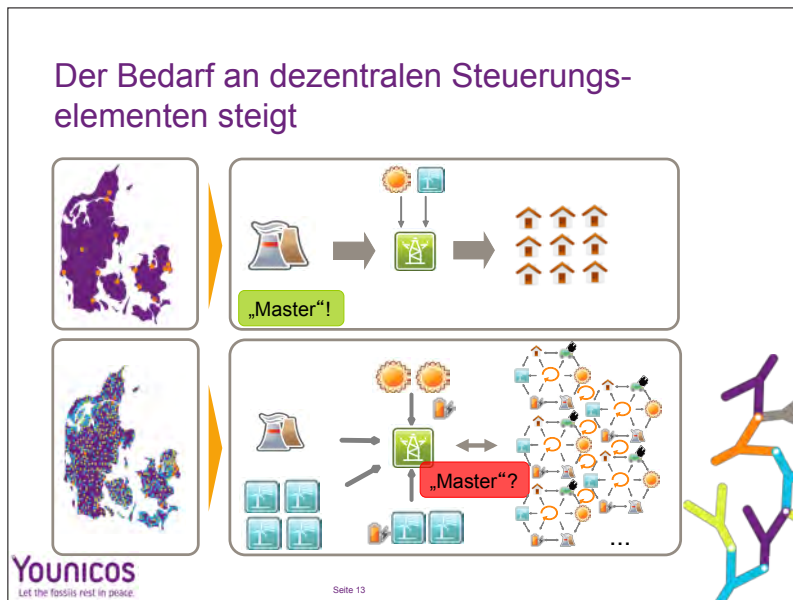


Bild 9

Nun zu den Steuerungsmechanismen (Bild 9). Vorhin wurde schon gesagt, dass die Grundstruktur unserer Energiesysteme bereits 100 Jahre alt ist: Auf der einen Seite stehen große, zentrale Energieerzeugungsanlagen auf der anderen Seite finden sich die „Abnehmer“. Die Abnahmemengen sind über die Jahre hinweg immer besser prognostizierbar und somit planbarer geworden. Der zentralisierte Kraftwerkspark war für die Netzstabilität verantwortlich. Es gab keine Notwendigkeit, im Verteilnetz „intelligente“ Kommunikationsinfrastrukturen aufzubauen.

Dies ändert sich gerade. Die Energieerzeugung wird immer dezentraler, Die Zahl der Energieerzeugungsanlagen steigt, Abnehmer werden zu „Prosumern“ und fragen immer weniger Energie aus dem Netz nach, die erzeugten Mengen richten sich nach klimatischen Bedingungen, nicht nach dem Bedarf. Die bisherigen Prognosemodelle reichen nicht mehr aus, die Nachfrage an „Intelligenz“ in den Verteilnetzen steigt. Aber wie steuert man ein solch immer komplexer werdendes System? Wer sichert die Stabilität und vergibt Prioritäten? Wer investiert in eine „intelligente“ ICT Infrastruktur? Wer verarbeitet das riesige, entstehende Datenaufkommen? Wie stellen wir die Sicherheit eines solchen Systems sicher? Wenn wir über neue Steuerungssysteme nachdenken, müssen wir diese beispielhaft genannten Fragen beantworten können.

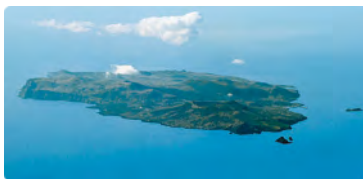
Am Beispiel unseres Inselprojektes möchte ich ihnen nun zeigen, wie wir diese Fragen auf der Insel Graciosa gelöst haben und wie vielleicht ein Steuerungssystem der Zukunft strukturiert sein könnte. Graciosa gehört zu den kleineren Azoren Inseln. Auf der Insel leben 4.500 Einwohnern, die derzeit durch große Dieseldgeneratoren mit Strom versorgt werden. Verbraucht werden ca. 4 Millionen Liter Diesel pro Jahr (Bild 10). Das bestehende, auf „drehenden Massen“ basierende Steuerungs- und Regelsystem stößt bei ca. 15% fluktuierender Windkraft im Netz an seine Grenzen.

Beispiel speicherbasiertes Inselfsystem auf Basis erneuerbarer Energien

Um zu beweisen, dass eine 100%ige Energieversorgung aus erneuerbaren Energien heute schon möglich ist, haben wir uns eine Insel gesucht

Graciosa

- die kleinste Azoreninsel
- 4.500 Einwohner
- Fläche ca. 67 km²
- kein Seekabel bzw. Anschluss an ein großes Netz
- Versorgung durch Dieselgeneratoren (ca. 4 Mio Liter Diesel pro Jahr)



Younicos
Let the fossils rest in peace.

Seite 14

Bild 10

Bis Anfang 2013 planen wir, ein speicherbasiertes Energiesystem auf Basis regenerativer Energien einzuführen und das System auf Basis eines PPA Agreements die nächsten 20 Jahre zu betreiben. Wir sind gerade dabei, die Finanzierung und die letzten Schritte vor der Realisierung abzuschließen. Bis dahin war es aber ein langer Weg. So haben wir in Berlin einen Inselteststand aufgebaut, der das gesamte Inselnetz im Maßstab 1:3 abbildet.

In diesem Teststand wurde zum Beispiel Deutschlands erste 1 MW NaS Batterie Europas installiert. Eine der wichtigsten Aufgaben des Inselteststands lag darin, dem lokalen Energieversorger EDA und der portugiesischen Regulierungsbehörde zu zeigen, dass wir in der Lage sind, ein System auf Basis erneuerbarer Energien stabil zu betreiben, auch im Falle von kritischen Situationen wie zum Beispiel einem Kurzschluss.

Um es vorweg zu nehmen. Wir haben den Beweis erbracht und dieses Jahr das „Go“ der EDA und der Regulierungsbehörde erhalten. Ich zeige ihnen nun den Verlauf einer ca. 10-15 Minuten dauernden Simulation, die wir in unserem Teststand mit dem dort installierten Energiesystem durchlaufen haben (Bild 11).

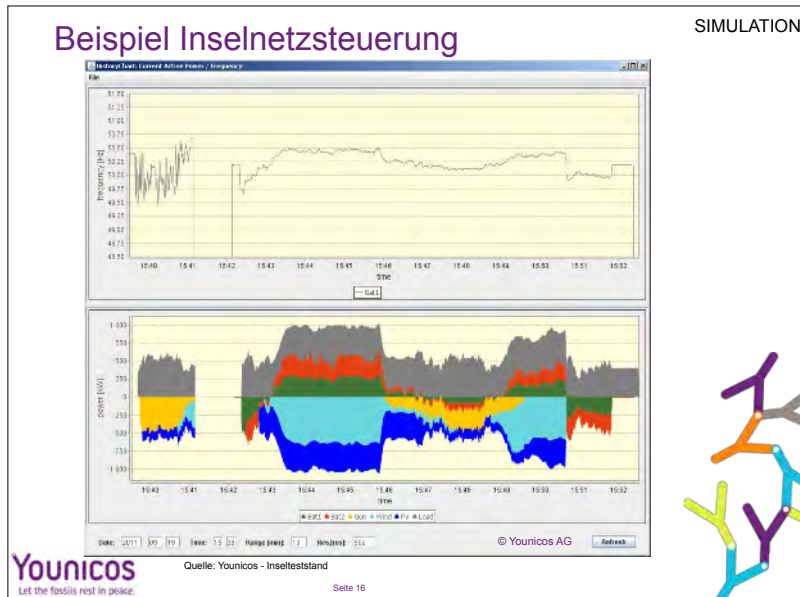


Bild 11

Auf der ganz linken Seite unten sehen Sie das herkömmliche System. Sie sehen die Last (grau), die Erzeugungskurve des Generators (gelb) und die eingespeiste Wind (hellblau) und PV Energie (blau). Am Anfang erzeugen der Generator und die PV-Anlage die benötigte Last von ca. 500 kW. Jetzt kommt Wind auf. Der Anteil von Wind und PV steigt signifikant an, das System kollabiert und fährt runter.

Nun bringen wir die Batterie ins Netz. Die grüne und die rote Fläche stellen die beiden synchron geschalteten 500 kW Blöcke der Batterie dar. Zunächst wird die Last von der Batterie bedient. Jetzt kommen Wind und Sonne auf (ca. 1 MW). Die benötigte Energie wird bereitgestellt, der Rest in die Batterie eingespeist. Der Wind geht zurück, der Generator fährt hoch (gelb), die Energie wird vom Generator, der Batterie und der Sonne bereitgestellt. Nun kommt wieder Wind auf, der Generator wird abgeschaltet. Jetzt kommt es zu einer kritischen Situation. Kurzschluss im Verteilnetz. Wind- und Sonnenenergie (1 MW) fallen aus. Die Batterie schaltet innerhalb von Millisekunden von Laden auf Entladen, das System bleibt stabil.

Wenn wir uns nun den Frequenzverlauf (oberes Bild) ansehen zeigt sich zum einen, dass die (zulässigen) Frequenzschwankungen im Netz in einem generatorgeführten System deutlich höher sind, als in dem System mit einer netzgebundenen Batterie, auch wenn der Generator im zweiten Durchlauf dazu geschaltet wird. Wir können aber noch etwas anderes aus dem Frequenzverlauf ablesen. Legen wir bei ca. 50,25 Hz eine Gerade über die Kurve, dann stellen wir fest, dass die Frequenz beim Laden der Batterie immer oberhalb der Geraden verläuft und beim Entladen unterhalb der Kurve. Die „Nulldurchgänge“ finden sich in den Punkten der „Zustandsumkehr“. Was heißt das? Wir sind in der Lage, mit unserm System Systemzustandsinformationen über die Frequenz zu übertragen.

BEISPIEL INSELSTEUERUNG

Intelligente Wechselrichtersteuerung übernimmt die Stabilisierungsfunktion

Batterie

Wechselrichter

Y-Inverter Controller

Intelligente Steuerung und schnelle Verarbeitung

=



Stabilisierungsfunktion einer rotierenden Masse

Copyright Younicos AG



Younicos
Let the fossils rest in peace.

Seite 17

Bild 12

BEISPIEL INSELSTEUERUNG

Spannung (U) und Frequenz (f) transportieren die Information

- Reliable means of transportation assured
- Control schemes of today's primary control can be applied

→ Integration with existing power plants possible

Distributed Units

Controllers and Interfaces (voltage & frequency control)

Battery interface & control

Wind farm interface

PV park interface

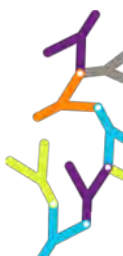
Diesel plant interface

U, f

15 kV Grid

10, Hz, 5

Communication via f and U



Younicos
Let the fossils rest in peace.

Seite 18

Bild 13

Wer etwas von Netzen versteht, weiß, dass dies ein Novum ist. Man hat es uns zuerst nicht geglaubt. Wir zeigen damit, dass die Steuerung, die wir dort implementiert haben, in der Lage ist, das Netz stabil zu halten, d.h. Batterie, Wechselrichter und unsere Steuerung sind in der Lage, die Stabilität des Netzes sicherzustellen (Bilder 12 und 13).

Der Generator übernimmt nur noch die Funktion einer weiteren Energiequelle. Die Leistungselektronik einer intelligenten Batterie ist in der Lage, die Stabilisierungsfunktion im

Netz zu übernehmen und die Führungsrolle der „rotierenden Massen“ abzulösen. Die intelligente Batterie funktioniert wie eine Synchronmaschine und die einzelnen Teilnehmer synchronisieren sich auf das Netz.

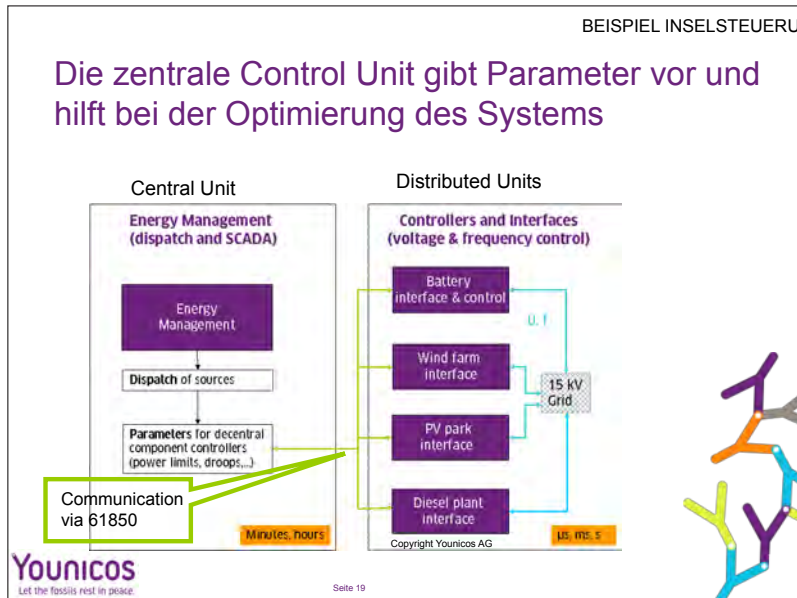


Bild 14

Was bedeutet das nun? Wir haben gesehen, dass die Grundfunktionalitäten eines „intelligenten“ Netzes auch bei einem Ausfall des IKT Systems sicher betrieben werden können. Kleinere dezentrale Einheiten könnten sich demnach selbst synchronisieren und stabilisieren, der dezentrale IKT Steuerungsaufwand könnte dadurch sinken, die IKT Systeme sich stärker auf übergeordnete Steuerungsaufgaben konzentrieren (Bild 14). Ähnlich dem menschlichen Körper, der im Falle von Reflexen, zum Beispiel bei einem Schlag aufs Knie, dezentral schnelle Entscheidungen trifft („Tritt“), ohne das Gehirn zu bemühen. Ein weiteres Beispiel ist das ESP-System eines Autos. Eine zentrale Kontrolleinheit definiert die allgemeinen Parameter und Verhaltensanweisungen zum Beispiel im Fall einer Vollbremsung. Die kontinuierlichen Entscheidungen im regulären Fahrbetrieb werden aber innerhalb kürzester Zeit dezentral in den Bremsen an den Fahrzeurädern getroffen.

Ob und wie das Ganze in einem stark vermaschten Verteilnetz funktioniert gilt es nun durch den Transfer der „Inselerfahrung“ gemeinsam mit lokal und regional agierenden Verteilnetzbetreibern oder Stadtwerken in geeigneten Pilotprojekten zu testen.

Mögliche Auswirkungen dezentralerer Strukturen auf Sicherheit und Datenschutz

Fragen / Hypothesen:

- Auswirkungen zusätzlicher, dezentraler „Eingangstore“ u.a. Energiemanagement, Schwarmsteuerung, ...
- Parametrisierung vs. Echtzeitsteuerung reduziert „Angriffsfläche“ im System; „Angriffe“ auf das SCADA System führen nicht zwangsläufig zu Ausfällen im gesamten Verteilnetz
- Aber: Beeinflussen sich eine Vielzahl von sich selbst synchronisierenden dezentralen Systemen gegenseitig?
- Durch eine autonome Selbstregelung entfällt die Notwendigkeit externer Steuersignale in Echtzeit
- Frequenzbasierte Steuerung reduziert Notwendigkeit einer Echtzeitsteuerung und das Kommunikationsaufkommen bzw. Datenvolumen im Verteilnetz
- Dezentrale speicherbasierte Energiesysteme können Basisfunktionalitäten im Verteilnetz aufrechterhalten
- ...

Datenschutz

Sicherheit gegenüber Angriffen

Betriebs-sicherheit

Younicos
Let the fossils rest in peace.

Seite 20

Bild 15

In diesem Zusammenhang müssen auch die Auswirkungen der neuen dezentraleren Strukturen auf die IKT Systeme sowie Sicherheit und Datenschutz frühzeitig betrachtet werden (Bild 15). Wie gezeigt, können intelligente speicherbasierte Energiesysteme frequenzgesteuert Teile der Netzsteuerungsfunktionen übernehmen und sind somit zum Beispiel weniger anfällig gegenüber externen „Angriffen“. Auch sind dezentralere Energiesysteme bestehend aus dezentralen Energieerzeugungsanlagen und Speichern deutlich weniger anfällig gegenüber Netzausfällen. Inwieweit sich eine Vielzahl sich selbst synchronisierender dezentraler Systeme beeinflusst und welche Auswirkungen dies auf die Gesamtnetzstabilität haben kann werden Pilot- und Forschungsprojekte zeigen müssen.

Auch auf die von Rolf Müller-Hermes vorhin gestellte Frage: Wer stellt im Falle eines Stromausfalls eigentlich den Strom für die IKT-Systeme im Verteilnetz und die Sicherheitssysteme im Smart Home bereit und ob wir dafür eine Backup Stromversorgungsinfrastruktur benötigen? muss beantwortet werden. Eine frequenzbasierte Steuerung reduziert auf jeden Fall das Datenaufkommen zwischen einer zentralen Steuereinheit und den dezentralen Einheiten. Eine Echtzeitsteuerung durch das zentrale SCADA System kann entfallen. Steuerungsparameter können in bestimmten vorgegebenen Zeitfenstern übermittelt werden, die Angriffsmöglichkeit dort anzugreifen wird geringer.

Ich komme zum Ende. Was ich zeigen wollte, ist, dass sich der Energiemarkt signifikant verändern wird und wir uns frühzeitig mit den möglichen Marktstrukturen auseinandersetzen müssen, um die richtigen Sicherheits- und Datenschutzkonzepte dafür zu entwickeln. Dies dürfen wir allerdings nicht nur durch die Brille eines Energieversorgers oder aus der Sicht eines IKT Providers, sondern wir müssen dies gemeinsam mit einer integrierten Sicht tun. Dann wird aus dem „Smart Grid“ auch ein „Safe Grid“ werden.

14 Herausforderungen und Lösungen für die elektrischen Energieversorgungsnetze

Prof. Dr.-Ing. Stefan Tenbohlen, Institut für Energieübertragung und Hochspannungstechnik, Universität Stuttgart

Die Rahmenbedingungen der Erzeugung und Verteilung elektrischer Energie und die dazugehörige Technologie befinden sich in einem stetigen Wandel. Während der letzten Dekaden des 19. Jahrhunderts stritten die beiden Amerikaner Thomas Alva Edison und George Westinghouse im sogenannten Stromkrieg um die Technologie der Netze. Edison bevorzugte die Gleichspannung und zog mit nicht gerade zimperlichen PR-Kampagnen gegen Westinghouse zu Felde. Tiere wurden mit Wechselspannung getötet, um die Gefahren dieser Technik zu belegen. Edison ersann eigens das Verb „to westinghouse“ dafür. Nachdem Oskar von Miller 1891 die Überlegenheit der Wechselspannung durch Übertragung einer Leistung von 70 kW von Lauffen am Neckar 176 km weit nach Frankfurt am Main gezeigt hatte, konnte auch Westinghouse mit Nikolai Teslas Hilfe den Stromkrieg für sich und die Wechselspannung entscheiden. Allerdings erlebt die Gleichspannungstechnik durch die technische Entwicklung der Leistungselektronik in den letzten Jahrzehnten wieder eine wachsende Verbreitung. Doch dazu später mehr.

Die Herausforderungen des 21. Jahrhunderts an die Energieversorgung sind seitdem ungleich größer geworden. Während die elektrische Energieversorgung zum ausgehenden 19. Jahrhundert noch eine Nischenanwendung war, ist sie heute umfassend und selbstverständlich. Große Veränderungen der Energieversorgungssysteme sind unumgänglich, wie wir im Folgenden noch sehen werden. Sie werden Investitionen in Milliardenhöhe erfordern.

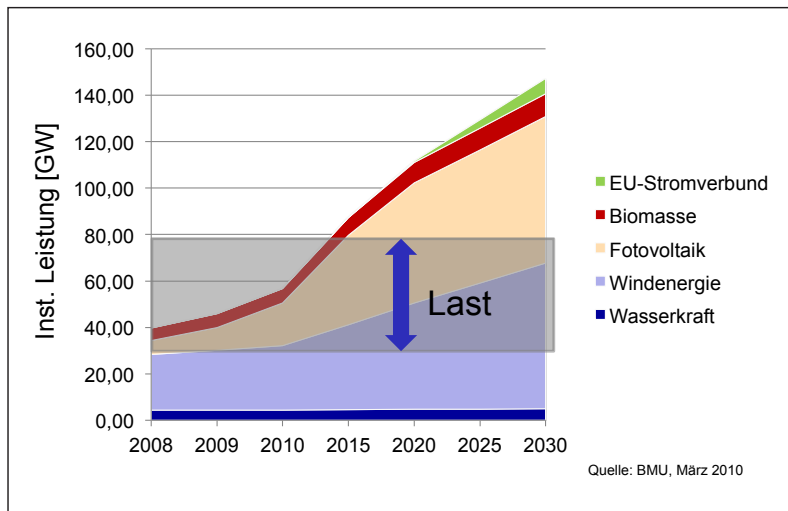


Bild 1: Installierte Leistung erneuerbarer Energiequellen in Deutschland [1].

Die wohl gewaltigsten Veränderungen ergeben sich aus der globalen Klimaerwärmung durch Verbrennung fossiler Energieträger. Um sie aufzuhalten oder zumindest den Temperaturanstieg abzumildern, ist eine signifikante Absenkung der CO_2 -Emissionen erforderlich. Um dieses Ziel zu erreichen, soll nach den Zielen der Bundesregierung 2020 der Anteil der erneuerbaren Energien am Strommix 30 % betragen. In Bild 1 ist die prognostizierte Entwicklung der installierten Leistung erneuerbarer Energiequellen in Deutschland dargestellt. Den Großteil wird hierbei die Windenergie bilden. Auch die Photovoltaik wird dank

Subventionen und fallender Kosten weiterhin zulegen. Bei der Wasserkraft ist nur noch ein geringer Zuwachs durch Modernisierungsmaßnahmen und Neubau zu erwarten, da ein Großteil der geeigneten Standorte bereits genutzt wird. Die Biomasse besitzt noch ein großes Potenzial, obgleich hier eine gewisse Konkurrenz zur Nahrungsmittelproduktion besteht. Schon 2014 könnte die Jahreshöchstlast Deutschlands (ca. 80 GW) durch erneuerbare Energien gedeckt werden. Allerdings muss natürlich beachtet werden, dass auf Grund der stochastischen Einspeisung nur ein geringer Anteil als gesichert angesehen werden kann. Daher ist konventionelle Kraftwerksleistung als Reserve bereit zu halten.

Ausbau des Übertragungsnetzes

Das Übertragungsnetz transportiert die elektrische Energie von den Kraftwerken zu den Lastschwerpunkten. In Deutschland werden hierfür im Höchstspannungsnetz Wechselspannungen von 220 kV oder 380 kV genutzt. Der Ausbau der Offshore-Windenergie und die zunehmende Abkehr vom Prinzip der Erzeugung in der Nähe der Verbraucher erfordern auch einen Ausbau der Übertragungskapazität des Netzes. Schon heute müssen wegen Netzengpässen in Norddeutschland Windparks zeitweise abgeschaltet werden. Die Basis für die Netzausbauplanung zur Integration der Windenergie bilden zwei Netzstudien der Deutschen Energie-Agentur (DNA) aus den Jahren 2005 und 2010 [2, 3]. Laut der ersten Studie (DNA I) müssen bis 2010 zusätzlich 461 km und bis 2015 weitere 390 km neue Leitungstrassen gebaut und zusätzlich bestehende verstärkt werden. Die Kosten für diesen Netzausbau wurden auf 1,1 Mrd. Euro geschätzt. Nach DNA II müssen bei Einsatz etablierter 380-kV-Freileitungstechnik bis zum Jahr 2020 insgesamt 3600 km Höchstspannungstrassen neu gebaut werden. Die Kosten für diese Basisvariante betragen einschließlich des Anschlusses der Offshore-Windparks insgesamt 9,7 Milliarden Euro. Ohne diese Maßnahmen ist der wachsende Anteil Erneuerbarer Energien nicht vernünftig in das Netz einzubinden. Den Vorgaben der DNA-Studie hinkt die Realität aber weit hinterher. Die für das Genehmigungsverfahren erforderlichen Zeiten übersteigen die Zeit für den Trassenbau um den Faktor fünf. Selbst wenn die Bauanträge genehmigt sind, können Klagen von Anwohnern oder Grundstücksbesitzern die Projekte über Jahre verzögern.

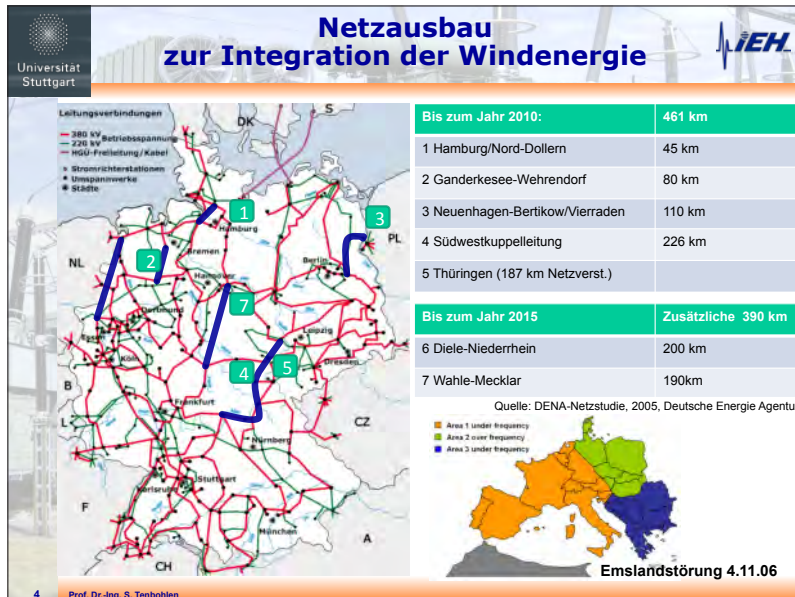


Bild 2: Übertragungsnetz und Ausbauempfehlungen zur Integration von Windenergie [2].

Systemdienstleistungen

Innerhalb eines elektrischen Energieübertragungsnetzes müssen zu jedem Zeitpunkt Erzeugung und Verbrauch elektrischer Energie im Gleichgewicht sein. Ist der Verbrauch niedriger als die Erzeugung, dann steigt die Netzfrequenz (Überfrequenz), weil die rotierenden Generatoren sich durch den Leistungsüberschuss schneller drehen. Übersteigt umgekehrt der Verbrauch die Erzeugung, dann sinkt die Netzfrequenz (Unterfrequenz), weil die Generatoren durch das Leistungsdefizit abgebremst werden. Ein plötzlicher Ausfall eines großen Kraftwerkblocks führt demnach zum sofortigen Absinken der Frequenz. Ohne Gegenmaßnahmen würde er zum automatischen Abschalten von Verbrauchern bis hin zum teilweisen oder kompletten Zusammenbruch der Stromversorgung, einem „Blackout“, führen. Letzterem Leistungsungleichgewicht kann man nur schnell entgegen wirken, indem man sofort „positive Regelleistung“ einsetzt. Die europäischen Netzbetreiber sind deshalb zur Vorhaltung einer sogenannten primären Regelleistung von 3000 MW verpflichtet, die innerhalb von 30 s aktiviert werden kann. Diese Primärregelleistung entspricht einem angenommenen Ausfall zweier Großkraftwerke mit je 1500 kW. Zur Aktivierung werden in den thermischen Kraftwerken, die in der Regel angedrosselt gefahren werden, die Einlassventile geöffnet, um mehr Dampf auf die Turbinenschaufeln zu bringen. Außerdem werden Speicher- und Pumpspeicherkraftwerke gestartet.

Der Großteil der Erneuerbaren nahm bisher nicht an dieser Leistungs-Frequenzregelung teil, denn ihr Anteil an der Stromerzeugung war lange zu gering. Zudem sind sie in der Regel entweder an das Mittelspannungsnetz angeschlossen, das die über das Übertragungsnetz ankommende elektrische Energie in den Städten und Kommunen verteilt, oder – wie die vielen kleinen Photovoltaik-Dachanlagen – sogar an das Niederspannungsnetz, das schließlich die einzelnen Gebäude versorgt. Viele Anlagen verfügen auch nicht über die notwendigen Regelungs- oder Kommunikationseinrichtungen, um an der Frequenzregelung teilzunehmen.

Inzwischen wächst der Anteil der Produzenten regenerativer Energie stetig und wegen ihrer Volatilität auch der entsprechende Bedarf an Regelleistung. Vor allem die dominierende Windenergie muss folglich in Zukunft auch sogenannte Systemdienstleistungen im Netz bereitstellen. Diese sind in der „Verordnung zu Systemdienstleistungen durch Windenergieanlagen“ für Neuanlagen ab dem 30. Juni 2010 festgeschrieben. Neben der Bereitstellung von Blindleistung ist auch die eingespeiste Wirkleistung ab 50,2 Hz abzusenken. Im Bereich von 51 Hz bis 51,5 Hz werden die Windkraftanlagen gestaffelt durch den Überfrequenzschutz vom Netz getrennt. Dies erfolgt dezentral an jeder einzelnen Windkraftanlage.

Generell können Windkraft und Photovoltaik bei zu hoher Frequenz die Einspeiseleistung absenken. Dabei geht jedoch die Energie, sofern sie nicht gespeichert wird, verloren. Eine gesteuerte Leistungssteigerung ist dagegen wegen der Wetterabhängigkeit allgemein nur möglich, wenn vorher ein gedrosselter Betrieb gefahren wurde. Dieser ist aber natürlich bei den regenerativen Einspeisern nicht gewollt. Die Biomasse ist hier im Vorteil, da sie zu den steuerbaren erneuerbaren Energien gehört. Ist im Netz ein Überangebot an Strom, kann das Biomasseheizkraftwerk seine Leistung herunterfahren und der Brennstoff, die Biomasse, wird eingespart. Bei sinkender Frequenz kann das Heizkraftwerk seine Leistung wieder hochfahren. Wie notwendig die Beteiligung der erneuerbaren Energien an der Netzregelung ist, zeigen die sommerlichen Osterfeiertage 2011. Zur Zeit der Mittagsspitze wurde die Netzlast von 41 GW zu etwa 25 % durch Photovoltaik gedeckt. „Glücklicherweise“ war zu diesem Zeitpunkt die Windkrafteinspeisung mit 2 GW nur sehr gering, denn nach dem Erneuerbare-Energie-Gesetz hat Strom aus regenerativen Quellen Vorfahrt im Netz. Damit war noch genügend konventionelle Kraftwerksleistung am Netz, um Lastschwankungen auszuregeln.

Integration der erneuerbaren Energien in das Verteilnetz

Die Verknüpfungspunkte des Übertragungsnetzes sind die Umspannwerke. In ihnen übernimmt das Verteilnetz die Verteilung der elektrischen Energie über zwei oder mehrere Spannungsebenen zu den Netzstationen. Diese versorgen das Niederspannungsnetz und die daran angeschlossenen Verbraucher mit 400-V-Drehstrom oder 230-V-Wechselstrom. Mit steigendem Anteil erneuerbarer Energie fällt dem Verteilnetz mit der Integration der von Photovoltaikanlagen und kleineren Windparks erzeugten elektrischen Energie eine neue Aufgabe zu. Gerade Photovoltaik- und Windkraftanlagen produzieren stark vom Wetter abhängig. Bild 3 zeigt die Schwankungsbreite der Windenergieeinspeisung durch die Viertelstundenwerte im November 2009. Innerhalb eines Tages schwankte diese um bis zu 12 GW. An mehreren Tagen gab es Zeiten, in denen die Windenergie zeitweise weniger als 1000 MW einspeiste. Das ist unter dem Gesichtspunkt der Versorgungssicherheit bedenklich, da in diese Jahreszeit auch die Jahreshöchstlast fällt. Diese muss die Kraftwerksleistung natürlich decken können.

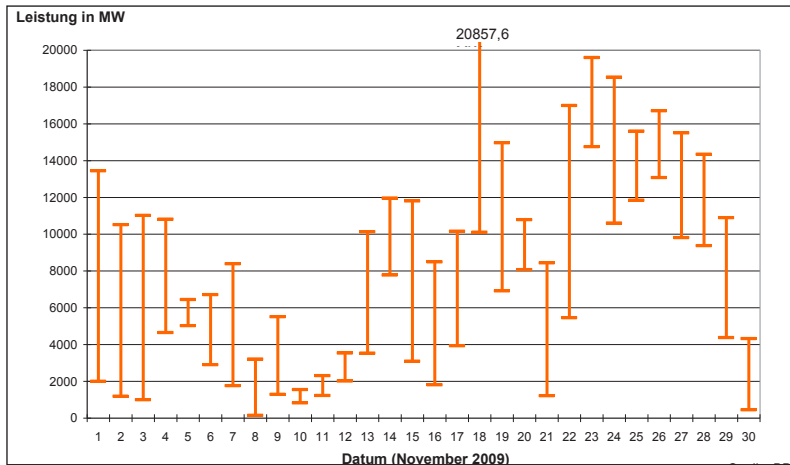


Bild 3: Volatilität der Stromerzeugung aus Windenergie: Tagesminima und Tagesmaxima der Viertelstunden-Leistungsprofile (Quelle: BDEW).

Virtuelle Kraftwerke

Das Erneuerbare Energien Gesetz (EEG) und das Gesetz zur Förderung der Kraft-Wärme-Kopplung schreibt den Netzbetreibern vor, sämtliche Energie aus solchen Quellen selbst bei einem Überangebot ins Netz einzuspeisen und nach festgesetzten Tarifen zu vergüten. Im Zweifelsfall müssen konventionelle Kraftwerke heruntergefahren werden, um dies auszugleichen. Nur wenn die Netzstabilität gefährdet ist, darf die aus erneuerbarer Energie eingespeiste Leistung reduziert werden.

Mit dem wachsenden Anteil des Stroms aus Windenergie- und Photovoltaikanlagen wächst nun auch die Herausforderung, ihre Fluktuationen mit Wetter und Klima auszugleichen. Die Übertragungsnetzbetreiber sind für die Vermarktung des Stroms aus erneuerbaren Energien verantwortlich. Sie verwenden hierfür spezielle Wind- und Photovoltaikprognosen. Die für den nächsten Tag erwartete Energiemenge wird Day-Ahead vermarktet. Abweichungen, die sich am folgenden Tag durch aktualisierte und damit genauere Prognosen zeigen, werden am Intra-Day-Markt gehandelt. Die verbleibenden Prognoseungenauigkeiten müssen dann durch Regenergie ausgeglichen werden. Die regionalen Schwankungen und Abweichungen durch Wetter und Klima kann man jedoch gut ausgleichen, indem man verschiedene Anlagen in einem „virtuellen Kraftwerk“ verbindet (Bild 4). Dieser Verbund sorgt dann für eine relativ konstante Leistung und eine Verfügbarkeit, die durchaus vergleichbar mit konventionellen Kraftwerken ist [5]. Eine Zusammenfassung etwa von Windenergie- und Solaranlagen in einer ausgedehnten Region erhöht die Versorgungssicherheit, weil sie die Standort- und Wetterabhängigkeit reduziert und zugleich die Prognostizierbarkeit erleichtert. Einzelne Wolken, die ein Solarpanel verdecken, sind schwerer vorherzusagen als Tiefdruckgebiete, die eine ganze Region bewölken. Allerdings müssen die Anlagen im virtuellen Kraftwerk miteinander kommunizieren können. So können zum Beispiel Biogasanlagen hochfahren, um eine größere Windflaute zu kompensieren. Bisher hatten die Anlagenbetreiber auf dem Gebiet erneuerbarer Energie allerdings wegen des EEG keinen Anreiz, ihre Erzeugung dem Verbrauch anzupassen. Kleinen Anlagen fehlen wie schon erwähnt auch noch die notwendigen, aber aufwendigen Kommunikationsschnittstellen. Erst die intelligente Regelung und Kommunikation zwischen den Erzeugungseinheiten und den Verbrauchern (Lasten) ermöglichen den stabilisierenden Verbund in einem intelligenten Netz (Smart Grid).

Das Einbeziehen von Wind-, Sonnen- und Lastprognosen in das System sowie die Verknüpfung von intelligenten Stromzählern und steuerbaren Verbrauchern eröffnet hier ein großes Optimierungspotential. Neue Technologien und sinkende Preise im Markt für Kommunikationstechnik haben einen deutlichen Entwicklungsschub ausgelöst. In diesem Bereich werden auch die größten Forschungsanstrengungen unternommen. Die Kommunikationsinfrastruktur muss schließlich hohe Anforderungen erfüllen, etwa Sicherheit gegen Missbrauch und ausreichende Reaktionsgeschwindigkeit. Bislang spielen Informations- und Kommunikationstechnologien in der Energieversorgung noch keine große Rolle. Ihre großen Optimierungspotenziale für den Energiebereich zu erschließen erfordert einen erheblichen technologiepolitischen Handlungsbedarf.

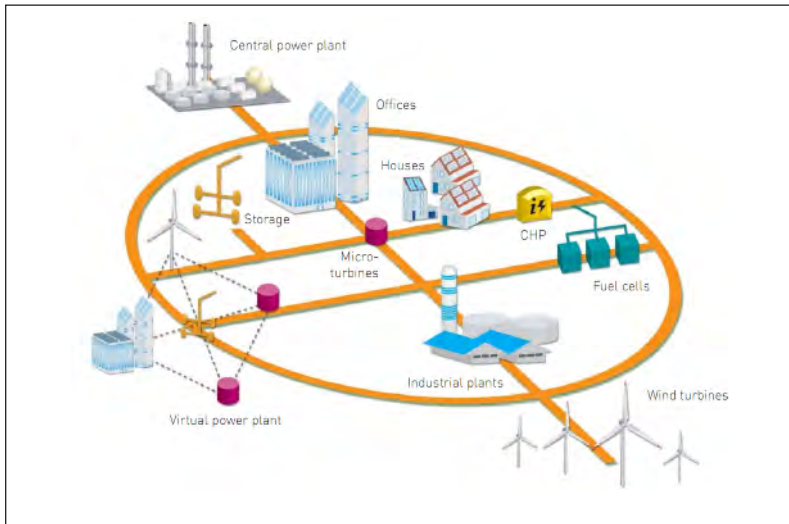


Bild 4: Virtuelle Kraftwerke im Smart Grid

Lastbeeinflussung durch intelligente Zähler

Auch auf Seiten der Verbraucher besteht Handlungsbedarf. Nach der Ölkrise wurde auf elektrische Nachtspeicherheizungen gesetzt, die mit günstigerem Nachtstrom geladen wurden. Mit Kohle- und Kernkraftwerken war man unabhängig vom Öl und hatte zudem die Möglichkeit, den nächtlichen Energieüberschuss der Grundlastkraftwerke nutzen zu können. Elektrische Nachtspeicherheizungen sind jedoch wegen der Klimaproblematik nicht sinnvoll, wenn der Strom aus Kohle gewonnen wird. Es ist ineffizient, diese im Kraftwerk zu verfeuern, aus der Wärmeenergie mit nur rund 40 % Wirkungsgrad dann elektrische Energie zu erzeugen, nur um diese wieder in Wärmeenergie umzuwandeln. Diese Betrachtung ändert sich allerdings schlagartig, wenn der Strom CO₂-frei aus erneuerbarer Energie gewonnen wird. Nachtspeicherheizungen bieten die Möglichkeit, die Last in großem Maßstab der Erzeugung anzupassen. Intelligente, kommunikationsfähige Stromzähler (Smart Meter) und flexible Tarife sind allerdings notwendig, um den Verbrauchern auch einen Anreiz zu geben, sich mit den verschiedenen Verbrauchern im Haushalt an der Lastregelung zu beteiligen. Der Netzanbieter kann dadurch das Lastprofil vorteilhaft beeinflussen, weil die Kunden bei großer Netzauslastung Strom sparen. So benötigt er weniger teure Regelenergie, um Lastspitzen zu kompensieren. Dies sollte mit Hilfe der intelligenten Zähler automatisiert werden. Dazu müssen die Haushaltsgeräte allerdings kommunikationsfähig werden. Somit könnten zum Beispiel Gefriertruhen oder Wärmepumpen immer dann laufen, wenn ein hohes Stromangebot herrscht.

Smart Meter sind somit ein Herzstück der Smart Grids. Seit dem 1. Januar 2010 ist bei Neubauten und Altbausanierung der Einbau von intelligenten Stromzählern verbindlich vorgeschrieben. Bis 2022 müssen in Deutschland 42 Millionen Stromzähler ausgetauscht werden. Allerdings stecken die automatisierte Verbrauchersteuerung und die zur Verbreitung der Zähler notwendigen Geschäftsmodelle noch in den Kinderschuhen.

Speichertechnologien

Ein weiteres wichtiges Element in einem intelligenten Netz der Zukunft sind Energiespeicher für Über- oder Unterkapazitäten. Die Speicherung von elektrischer Energie ist als Aufgabe so alt wie die Stromnetze selbst. Weil Strom in großem Maßstab nur schwer und mit großen Verlusten gespeichert werden kann, wird die Energieerzeugung dem Energieverbrauch nachgeführt, so dass hier ein Gleichgewicht herrscht. Um die benötigte zusätzliche Energie beispielsweise zur Mittagszeit zur Verfügung zu stellen, können Speicher verwendet werden. Diese werden zur Schwachlastzeit, also normalerweise nachts, geladen. Sie sind zudem unverzichtbar, um kurzfristige Lastspitzen auszugleichen. Als Energiespeicher haben sich seit Anfang des 20. Jahrhunderts Pumpspeicher-Wasserkraftwerke bewährt. Allerdings sind in Deutschland die geographischen Möglichkeiten für Wasserkraftwerke begrenzt. Deshalb sind alternative Speichertechnologien in Entwicklung. Dazu zählen Druckluftspeicher, die mit Turbinen Energie als Druckluft in unterirdischen Kavernen speichern. Für den weiteren Einsatz der erneuerbaren Energien in der Stromerzeugung sind Speicher unverzichtbar. Sie helfen, die Unsicherheiten in den Prognosen der Kapazitäten aus der Erneuerbaren Energie abzufangen.

Elektromobilität

Im Vergleich zu den bislang erwähnten Speichertechnologien haben Batterien einen hohen Wirkungsgrad – bei Lithiumionen-Akkumulatoren sind es bis über 95 %. Damit wird das Einbinden von Elektroautos als mobile Speicher ins Netz interessant. Noch ist dies teuer, und Elektroautos sind rar. Doch das könnte sich in Zukunft ändern, sofern Elektrofahrzeuge sich breit etablieren können [6]. Die Bundesregierung hat immerhin eine Million Elektrofahrzeuge bis 2020 in Deutschland zum Ziel [7].

Allerdings stellt sich die Frage, ob das derzeitige Stromnetz dieser Verbreitung gewachsen ist oder auch dafür ausgebaut werden muss. Viele Berufstätige werden ihr Auto abends Zuhause zum Laden anschließen. Zu dieser Zeit wird die Stromnachfrage rapide steigen. Auf der anderen Seite werden Elektroautos tagsüber die meiste Zeit ungenutzt auf einem Parkplatz stehen. Sie könnten also mit ihren Batterien als Speicher das Netz entlasten. Ist ihre Zahl groß, dann könnten sie nennenswert helfen, regenerative Energien im Verbund mit einem virtuellen Kraftwerk besser zu nutzen, indem sie zu Starklastzeiten Strom zurück ins Netz einspeisen. Zudem könnten die Fahrzeuge nur dann laden, wenn das Netz dafür gerade ausreichend Kapazitäten hat. Bild 5 stellt ein Lastmanagement dar, das die aktuelle Auslastung des Ortsnetztransformators einbezieht und danach entscheidet, welche Fahrzeuge wie stark geladen oder entladen werden. Für solche Konzepte ist bereits heute in dem normierten und standardisierten Mennekes-Ladestecker für E-Fahrzeuge ein Kommunikationskanal vorgesehen. Für Stromerzeuger und Netzbetreiber ist dieses Konzept interessant, da sie weniger Regelleistung bereithalten müssen und auch bei großen Speichern Kapazität sparen können. Für die Halter kann es ebenso interessant sein, ihr Auto für Regeldienste zur Verfügung zu stellen, die entsprechend entlohnt werden würden.

Heutzutage stehen diesem Vehicle-to-Grid-Konzept allerdings noch die hohen Kosten für die Energiespeicherung in der Lithium-Ionen-Batterie entgegen. Unter der realistischen Annahme, dass 2015 der Anschaffungspreis bei 200 €/kWh und die Lebensdauer bei 5000 Ladezyklen liegen werden, würde die Speicherung einer kWh etwa vier Cent kosten. Auf diesem Preisniveau wäre diese Technologieoption durchaus ökonomisch sinnvoll. Mit 5000 Vollzyklen kann ein durchschnittliches Elektroauto mit 150 km Reichweite zudem theoretisch 750 000 km fahren. Da die meisten Fahrzeuge im Lauf ihres Lebens nicht annähernd so weit kommen werden, würde diese zusätzliche Nutzung der Batterie für Netzdienstleistung die Halter kaum zusätzlich etwas kosten.

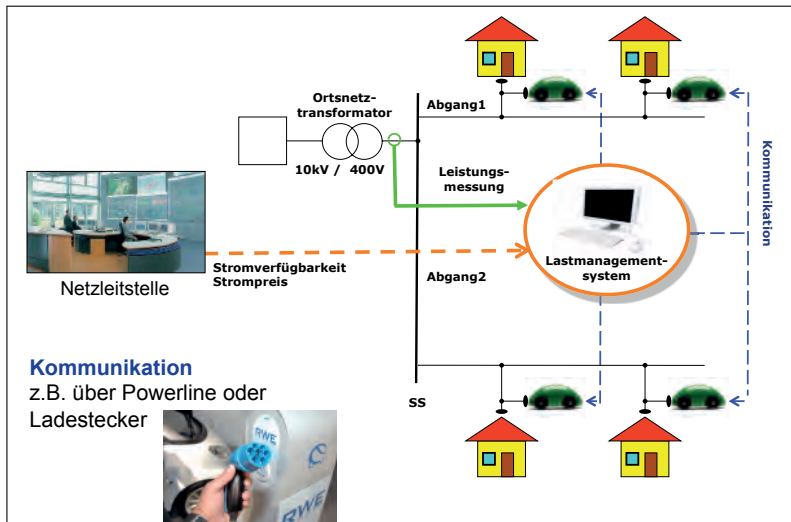


Bild 5: Konzept eines Lastmanagementsystems für Elektrofahrzeuge.

Literatur

- [1] Leitsstudie 2010: Langfristszenarien und Strategien für den Ausbau erneuerbarer Energien in Deutschland. Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, Dezember 2010. Download unter www.bmu.de/erneuerbare_energien/downloads/doc/46260.php.
- [2] DENA-Netzstudie: Energiewirtschaftliche Planung für die Netzintegration von Windenergie in Deutschland an Land und Offshore bis zum Jahr 2020, Deutsche Energie Agentur GmbH (dena), Köln 2005.
- [3] DENA-Netzstudie II: Integration erneuerbarer Energien in die deutsche Stromversorgung bis 2020, Deutsche Energie Agentur GmbH (dena), Köln 2010.
- [5] VDE-Studie: Smart Distribution 2020, Virtuelle Kraftwerke in Verteilungsnetzen – Technische, regulatorische und kommerzielle Rahmenbedingungen, Frankfurt am Main 2008.
- [6] VDE-Studie: Energiespeicher in Stromversorgungssystemen mit hohem Anteil erneuerbarer Energieträger – Bedeutung, Stand der Technik, Handlungsbedarf, Frankfurt am Main 2009.
- [7] Bundesregierung, Nationaler Entwicklungsplan Elektromobilität, Berlin 2009.

15 Wirtschaftliche Aspekte, Ansätze für Geschäftsmodelle

Prof. Dr. Arnold Picot, Ludwig-Maximilians-Universität München

Meine Damen und Herren, im Namen des Münchner Kreises begrüße ich Sie ganz herzlich zum zweiten Teil der heutigen Veranstaltung, dem sogenannten Berliner Gespräch, das schon eine gewisse Tradition hat. Der Münchner Kreis veranstaltet von Zeit zu Zeit zu aktuellen, der vertieften Diskussion und dem vertieften Verständnis bedürftigen Fragen sogenannte Berliner Gespräche mit Vertretern aus Politik, Verwaltung, Wirtschaft und Wissenschaft hier in Berlin. Ich freue mich, dass Sie so zahlreich heute Abend zu uns gekommen sind.

Herzlich Willkommen zu dem abendlichen Teil, vor allem auch denjenigen, die tagsüber noch nicht dabei waren. Ich danke zu Beginn der Alcatel-Lucent Stiftung, die als Kooperationspartner bei den Veranstaltungen heute hier mitwirkt und die die Veranstaltung auch mit unterstützt. Herr Dr. Klumpp als Geschäftsführer der Stiftung ist hier. Ich selbst bin auch im Kuratorium der Alcatel-Lucent Stiftung tätig, und insofern gibt es eine sehr schöne, bewährte Kooperation.

Meine Damen und Herren, der erste Teil steht unter der Überschrift „Wirtschaftliche Aspekte, Ansätze für Geschäftsmodelle“. Geschäftsmodelle sind in der Tat ein wichtiger Aspekt dieser enorm bedeutenden Transformation des Energiesystems. Die Thematik, mit der wir uns heute beschäftigen und die viele von Ihnen sehr gut kennen und die heute schon tagsüber intensiv erörtert wurde, spielt eine wichtige Rolle in der sogenannten Energiewende und in der Weiterentwicklung unseres Energiesystems. Sie alle wissen, dass es im Kern um die Bewältigung der Volatilität der Energieerzeugung und Energieeinspeisung und ihrer Abstimmung mit der Energienutzung hier geht. Wo kann man da Geschäftsmodelle ansetzen? Es sind Dinge wie neuartige oder zusätzliche Speichermöglichkeiten, beispielsweise Power to Gas, Demand Side Management und endkundenorientierte Effizienz- und Kostenvorteile, die man vielleicht auf der Basis geeigneter Geschäftsmodelle durch das Zusammenwirken von Energie- und IKT-Systemen generieren kann. Aber es gibt bei solchen Geschäftsmodellen eine Reihe von offenen Fragen. Dazu gehören nicht nur Schutz und Sicherheit, die heute ja auch im Zentrum stehen, sondern einige weitere Aspekte. Ich möchte nur ganz wenige anreißen und dann an meinen Kollegen Helmut Krcmar übergeben, der das weiter vertieft.

Ein erster Problemkreis: Wo kann sich Zahlungsbereitschaft für welche Art von Vorteilen entwickeln? Wer bietet attraktive Lösungen an? Sind das einzelne Akteure, sind das Verbände, Kooperationen von Akteuren? Wer sind in dem Zusammenhang die relevanten Akteure? Es treten ja viele und unterschiedliche Akteure auf: die Netzbetreiber, die Verbraucher selbst natürlich, die Händler, die neuen und alten Dienstleister, die Messstellenbetreiber, Telekommunikationsunternehmen, traditionelle Versorgungsunternehmen, Kommunen – also ein bunter Strauß von Akteuren, die in irgendeiner Weise zusammenwirken müssen. Wer trägt da die Fahne? Wer übernimmt da unter welchen Voraussetzungen die Initiative? Hier bestehen offene Fragen.

Ferner: Wie werden Vorteile, wenn sie denn generiert werden, unter den Beteiligten verteilt? Das Revenue Sharing ist mit Sicherheit ein sehr wichtiger, oftmals ungelöster Aspekt, von dessen Klärung die Verwirklichung neuer Märkte abhängen kann.

Ein weiterer Aspekt betrifft den Datenzugang. Viele neue Geschäftsmodelle, auch neue Unternehmer, die sich auf dem Feld betätigen wollen, sind auf Daten angewiesen, die nicht ohne weiteres mehrfach erhoben werden können (z.B. Verbrauchs-, Verlaufs-, Kapazitäts-,

Zustands-, Wetterdaten). Wem gehören diese Daten? Unter welchen Bedingungen kann man diese Daten tatsächlich nutzen und wer kümmert sich darum? Handelt es sich dabei um eine Wettbewerbsfrage, ein hoheitliches Problem, ein Problem der Gemeinschaftsgüter, der öffentlichen Güter? Unter welchen Bedingungen trifft welche Problemsicht zu und was folgt dann daraus?

Dies ist Reihe von Punkten, die es nicht einfach machen, auf dem Feld von E-Energy, Smart Grids und Smart Metering ein Geschäftsmodell aus dem Hut zu zaubern und umzusetzen. Andererseits stecken große wirtschaftliche und ökologische Perspektiven in diesen Ansätzen. Es gibt Untersuchungen, die darauf hinweisen, dass zweistellige Prozentbeträge des Energieverbrauchs eingespart werden könnten, wenn man die Ehe von Energiewirtschaft und IKT flächendeckend und perfekt installieren würde. Insofern besteht natürlich ein großes wirtschaftliches Potenzial, aus dem Geschäfte zu machen wären.

16 Wirtschaftliche Aspekte, Ansätze für Geschäftsmodelle

Prof. Dr. Helmut Krcmer, Technische Universität München

Nach der fokussierten Diskussion über Sicherheit und Datenschutz bei Smart Energie beginnen wir nun unter dem Titel „Wirtschaftlichen Aspekte und Ansätze für Geschäftsmodelle“ mit der einfachen Frage von Peter Drucker: Wer ist Kunde? Das könnte ein Verbraucher im Sinne des Consumers sein. Das könnte aber auch ein Unternehmen oder viele andere Akteure sein. Dieser einfache Frage folgen schnell weitere Überlegungen: Was ist der Wert dieser Dienstleistung für den Kunden? Was davon ist ein Serviceversprechen? Was davon ist ein Produkt? Was davon ist eine Potenzialeistung? Und wie will die Organisation – so hat man das 1960 einmal formuliert – Geld verdienen? Allein aus dieser Formulierung ‚die Organisation‘ entstehen heute weitere Themen, denn unter Geschäftsmodellen verstehen wir die Muster, wie die Flüsse von Produkten, von Informationen und Daten, wie der Fluss des Geldes und wie die Dienstleistungsflüsse und materiellen Austausche organisiert werden.

Wenn wir das aus einer Perspektive von außen nach innen betrachten, kann man mit Peter Keen, drei Fragen formulieren: Wie wird der Wert eigentlich kreiert? Wie wird der Wert, der kreiert und ausgedacht wurde, so zuverlässig geliefert, dass man sich darauf verlassen möchte? Und schließlich, wie kann man Value Appropriation oder Value Capture, also die Zahlungsbereitschaft erreichen? Diese hängt davon ab, dass im Ecosystem der Akteure ein Nutzen tatsächlich wahrgenommen wird. Wir haben gelernt, dass Zahlung nicht immer direkt erfolgen muss, sondern auch indirekt erfolgen kann. Wir erleben heute viele Geschäftsmodelle, die vom direkten Austauschen zu sehr viel indirekten, oftmals werbungsorientierten Modellen übergehen.

Bei solchen neuen Geschäftsmodellen oder eigentlich Verdien- oder Geschäftsmustern stellen sich einige Fragen. Die eine ist die Nachhaltigkeit des Geschäftsmodells. Dann die Frage, wie lang ein Geschäftsmuster „vernünftig“ ist und welche Investitionen es wann erfordert. Das andere ist, dass wir eine Bewegung von sehr stark Ein-Organisationsstrategien, ein Kunde, ein Lieferant hin zu plattformgetriebenen Ökosystemen von Firmen sehen. Ein plattformgetriebenes Ökosystem von Firmen ist als Zusammenarbeitsstruktur ein höchst komplexes Gebilde. Es ist normalerweise schon schwierig genug, wenn Sie in einer Industrie eine Plattform betreiben oder auf mehreren Plattformen in einer Branche dann Wettbewerb treiben. Wenn man aber, wie bei smart grid, mehrere Industrien miteinander verbindet, dann kommen deren Historien der Zusammenarbeit, deren Plattformen, deren Standardisierungsbemühungen zusammen. Nicht immer entsteht sofort eine Passung zwischen diesen Themen, Friktionen großen Ausmaßes sind eher zu erwarten als ein sofortiger Fit. Plattformgetriebene Ökosysteme sind etwas, was man heute gerne hat, aber wie sie genau funktionieren, was die erforderlichen Governance Mechanismen sind, wer den Wechsel von einem zum nächsten Standard verkündet, ist in solchen Ökosystemen schwierig.

Neben dieser Komplexität und den Möglichkeiten ihrer Governance gibt es auch die spannende Frage, wie wir damit umgehen, dass immer mehr Offenheit in der Innovation, in der Kundenintegration herrscht und solche Kunden immer mehr Einfluss nehmen wollen, welche Dienste ihnen tatsächlich geliefert werden. Open Innovation setzt auch voraus, dass ein gewisser Zugang zu den relevanten technischen und ökonomischen Themen gegeben wird. Wer will das schon immer tun?

Wir haben auch noch einen Wettbewerb unterschiedlicher Geschäftsmodelle. Es könnte ja sein, dass ganz unterschiedliche Muster von Geschäftsmodellen entstehen. Ein in der aktu-

ellen Diskussion vorgebrachtes Modell trägt den Namen „Freemium“, ich gebe in einem Kontext etwas für umsonst und mache woanders eine Premiumleistung daraus.

Wie kann ich das in diesen Bereich smart grid hineintragen?

Zunächst lassen sich noch mehr Fragen aufwerfen, die ja alle neuen Möglichkeitsräume umschreiben: Lassen sich andere Geschäftsmodelle bauen, wenn Micropayments, minimale Zahlungsflüsse, ökonomisch sinnvoll abwickelbar sind? Muss ich dann unbedingt noch Jahresabos anbieten oder kann ich da nicht einfach viel mehr Wettbewerb zulassen? Und was passiert, wenn Verbraucher sich sekundlich umentscheiden, woher sie etwas beziehen?

Was also passiert, wenn wir das in diesen Bereich der neuen Energiesysteme übertragen? Zum einen wird offensichtlich, dass wir ganz ernsthaft diskutierten, die klassische Kunden-Lieferanten-Beziehung ein Energie- oder Spannungslieferant und ein Abnehmer auf der Konsumentenebene aufzulösen in ein Akteursnetzwerk. Im Akteursnetzwerk wird im Moment aktiv die Schnittstelle oder Nahtstelle „Smart Meter“ diskutiert. Es werden aber weitere Akteure erforderlich sein. Dann wird begonnen, das Erzeugungssystem aufzuteilen in Erzeugung und Verteilung und vielleicht in noch ganz andere Dienstleistungen. Dann entstehen in diesem Akteursnetzwerk zum einen Interoperabilitätsfragenstellungen wie im eigentlichen Produktionsbereich, also in der Herstellung dessen, was der Kunde dann tatsächlich kauft. Aber auch Interoperabilität in dem, was an Koordinations- und Datenflüssen dazu gebraucht wird. Das Thema Interoperabilität bei Geldflüssen ist bei einheitlichen Währungen etwas einfacher. Es wird natürlich ein schwieriger, wenn Sie dort schwankende Wechselkurse dazu nehmen. In solchen Akteursnetzwerken, in denen nicht nur das Produzieren sondern auch das Informieren real time miteinander verknüpft sein müssen, entstehen höchst spannende Fragen aus dem Bereich des Zyklusmanagements. In welchen Geschwindigkeiten entwickelt sich bei jedem Akteur dessen Geschäftsmodell eigentlich weiter? Durchschnittsstandzeiten von Elektrogeräten in Haushalten, Durchschnittsstandzeiten von Messgeräten in Haushalten und Durchschnittsstandzeiten von Kraftwerken sind nicht identisch: diese verschiedenen Zeitzyklen müssen harmonisiert werden. Neben diesem langfristig angelegten Volatilitätsproblem geht es natürlich auch um das Zusammenbringen ganz unterschiedlicher Firmenkulturen.

Die zweite Herausforderung wird deutlich, wenn man sich smart grids als Cyber Physical Services Systems vorstellt. Warum Service Systems? Die Kunden wollen einen Wert haben. Wie die Lieferanten diesen Wert genau erzeugen, ist nicht jedem Kunden oder Nutzer besonders wichtig. Es muss eine Dienstleistung erbracht werden und diese wird auf der physikalischen und sensor-basierten Ebene wie auf der informationellen Ebene erstellt. Dabei werden die Komplexitäten zweier Welten miteinander vermählt. Wir addieren dazu die verschiedenen Zeitzyklen, in denen das passiert. Wir addieren die unterschiedlichen Sicherheitsverständnisse, die in diesen Welten herrschen. Und wir addieren, dass vielleicht auch die Kunden sich weiterentwickeln und unterschiedliche Ansprüche entwickeln. Es wird deutlich, dass ein derart aufgespannter Möglichkeitsraum auf diesem Weg vom Erzeuger über Infrastrukturen zur Verteilung, Koordination und Speicher über Smart Meter bis zu dem Verbraucher groß ist und vieler Entscheidungen bedarf, aber auch die Möglichkeiten für viele Irrwege bietet. Hier nun muss man beim Begriff des Verbrauchers differenzieren. Zunächst meine ich vorrangig nicht private Konsumenten sondern nur den Stromverbraucher, sei er ein privater Endkunde oder eine Firma. Es ist also zu klären, welche Endkunden tatsächlich gemeint sind. Machen wir uns Gedanken um den Schutz der Daten des privaten Endkunden? Da müsste man fragen, wieviel Prozent des Stromverbrauchs dort stattfindet. Und machen wir uns Gedanken zum Datenschutz der Maschinen, die wir möglicherweise in einer Handwerkerwerkstatt haben?

Die Wertfrage beim Kunden muss aber vor allem vom Ende her gedacht werden, zumindest von der Nutzung her. Wert ergibt sich dann als Konzeption x Implementierung und Umsetzung durch alle Akteure x Nutzung durch Kunden. Anders formuliert: wir können uns noch so viel Gedanken machen wie die Blaupausen aussehen und ob eine Blaupause auch nach Deutschland und Europa übertragbar sein darf. Wir müssen es auch umsetzen. Aber, wenn dann letztendlich die Nutzer, die Verbraucher nicht das Vertrauen haben, diese Infrastruktur tatsächlich zu verwenden, sich darauf zu verlassen, dass dies alles funktioniert, wäre dennoch alles verloren. Dann wäre das Resultat der eben genannten Gleichung die Gleichung: $1 \times 1 \times 0 = 0$. Wir müssen es also vom Endverbraucher her denken, und dieser Nutzer muss das bei einem derartig komplexen System notwendigerweise Vertrauen aufbringen wollen.

Er muss das Vertrauen aufbringen, dass selbst wenn er den Diskussionen über Schwierigkeiten und Komplexitäten hier zugehört hat, er sich traut, einem Smart Grid seine Energieversorgung anzuvertrauen. Und dass nicht plötzlich irgendetwas Schlimmes passiert, denn sonst dürfte er kein Geld aus dem Automaten verwenden, worauf Sie nach Jahren der Übung mittlerweile auch vertrauen, dass das tatsächlich funktioniert. Viele von Ihnen, die ich als Passagier der Luftverkehrsunternehmen kenne, beginnen ja auch langsam zu vertrauen, dass das eTicket tatsächlich auf dem Endgerät angezeigt wird.

Das war eine längere Zeit bis vom Karton über das ausgedruckte Blatt bis zur Anzeige im Smartphone das Vertrauen in eTickets entstanden ist. Und dieses Vertrauen ist nicht nur in die Frage der informationellen Selbstbestimmung. Neben der Sicherheit meiner Daten geht es aber vor allem um Versorgungssicherheit, also, dass das versprochene Produkt, die Leistung, tatsächlich zur Verfügung stehen wird und auch abrufbar ist. Dieses Vertrauen setzt in aller Regel voraus, dass wir denjenigen Systemen vertrauen, die das Risiko, das bei der Erzeugung und Verteilung immer besteht, managen sollen und auch eine Gefahrenabwehr gelingt. Wenn man sich dieses Risiko betrachtet, brauchen wir dafür die viel diskutierten Sicherheitskomponenten, die vielen anderen Verfahren, die uns davon ausgehen lassen, dass wir bei aller Komplexität, bei allem zu beherrschendem Risiko einem Smart Grid vertrauen können.

Damit ist klar geworden, warum wir uns heute so viele, ganz unterschiedliche Perspektiven anhören. Denn wer das Thema reduzieren würde auf nur die Frage Sicherheit, würde an der Frage vorbeigehen, ob es sich denn für den Verbraucher lohnt. Aber auch bei der Frage jeden Geschäftsmodells - und das ist bei Akteursnetzwerken die ganz kritische Frage - ist zu prüfen, ob alle Akteure in diesem Netzwerk zumindest die Hoffnung hegen können, dass sie das etwas verdienen können. Denn wenn Sie ein Netzwerk gebaut haben und auch nur einen Rollenträger darin haben, der keine Hoffnung hat, und diese Hoffnung auch nicht durch Querfinanzierung, Subvention oder sonst etwas aufrechterhalten kann, gehen solche Netzwerke meist und auch schnell auseinander, weil genau dieser Akteur wieder aussteigt. Nun werden wir uns also dem Thema über die unterschiedlichen Perspektiven der Akteure nähern.

Wir werden Smart Grid zunächst aus der Perspektive der Energiewirtschaft und der der IKT Wirtschaft sehen, sozusagen der beiden Partner, die zu einem Cyber Physical Service System vermählt werden sollen. Ich fände es höchst interessant, herauszufinden, wie denn dieser Ehevertrag aussehen soll.

Dann werden wir uns mit der Frage Sicherheit, Datenschutz und Verbraucherschutz beschäftigen. Dort geht es eben nicht nur darum, die Daten der Koordination zu schützen, sondern auch die Frage zu stellen, ob der Verbraucher in die Bereithaltung solcher Dienste auch vertrauen kann, welche Versorgungsverlässlichkeit er hat. Dann kommt die Vielfalt der weiteren Akteure, die gerne mitspielen wollen, im Netzwerk der Smart Grids. Immer wenn neue

Akteursnetzwerke, neue Geschäftsmodelle ausprobiert werden, ist das wie ein spannendes Rennen auf einen Gipfel. Alle vermuten, dass dort eine ganze Menge Gewinn zu holen wäre. Dummerweise liegt der Gipfel aber noch im Nebel. Wir wissen nicht so genau, wie hoch er wirklich ist, was alles zu erledigen ist. Aber wir sehen alle anderen rennen. Die spannende Frage ist, wer dann noch mit rennt, wer sich noch Anteile an dieser Wertschöpfung, an diesem Value Creation, an der Value Delivery und dann entsprechend auch an dem Value Capture sichern möchte.

Ich hoffe, dass Sie mit mir und uns zusammen einen spannenden Abend mit vielen offenen und dann auch andiskutierten Fragen erleben, denn die Herausforderung einer solchen Zusammenkunft besteht ja darin, dass alle Statementlieferanten gebeten werden, sich an die Zeitbegrenzung zu halten, damit Ihnen allen genügend Zeit bleibt, die Fragen und die Bedenken, die Einwürfe, die Vorschläge, die Sie haben, vorzubringen.

17 Das Programm der Bundesregierung zu Smart Energy

Parlamentarischer Staatssekretär Hans-Joachim Otto, BMWi, Berlin

Ich möchte ausdrücklich für die Gelegenheit danken, hier beim Berliner Gespräch zu Ihnen sprechen zu können, zu einem Thema, das mir und meinem Hause sehr am Herzen liegt: Sicherheit und Datenschutz bei Smart Energy. Lassen Sie mich mit etwas beginnen, das Sie alle wissen, man sich aber immer noch einmal in Erinnerung rufen möge. Deutschland hat im Gegensatz zu vielen anderen Ländern, auch europäischen Ländern, die Grundentscheidung getroffen, seine Energieversorgung in Zukunft zu einem Hauptteil, 2050 immerhin zu 80%, aus erneuerbaren Quellen zu decken. Dabei war bereits in dem Energiekonzept aus dem Jahre 2010 im Grunde der Weg vorgezeichnet, sozusagen der Brückenbau zu den erneuerbaren Energien, der Einstieg in die erneuerbaren Energien.

Wir haben nach Fukushima die Entscheidung getroffen, die Restrisiken der Atomkraft verschärft zu bewerten und damit bis Ende 2022 aus der Atomenergie komplett auszusteigen. Wir sind hier nicht bei einer energiepolitischen Tagung, wie mir wohl bewusst ist, aber meine Damen und Herren, ich kann Ihnen sagen, dass diese Entscheidung freundlich formuliert eine sehr ambitionierte Entscheidung ist.

Ich war kürzlich bei der Jahrestagung der Internationalen Atomenergiebehörde in Wien und habe dort unter den vielen Experten keinen gefunden, der nicht voll der Bewunderung oder wenigstens des Zweifels war, wie wir das alles hinbekommen. Die einen haben uns bewundert und gesagt, dass das ein wunderbarer Showcase für die Welt ist, wenn es gelingt. Die anderen haben gesagt, dass sie es sich kaum vorstellen können. Ich sage dies alles nur, damit Sie wissen, wie wichtig das Thema ist, über das wir hier sprechen. Das ist eingebettet in eine enorm wichtige und weltweit einmalige energiepolitische Rahmensituation.

Eines zeichnet sich jetzt bereits ab, und ich nähere mich sehr schnell dem Thema, dass das zukünftige Energiesystem wesentlich vernetzter und komplexer wird. Das lässt sich an drei Trends verdeutlichen, die ich Ihnen eingangs zum Nachdenken, als Wiederholung oder Vertiefung noch einmal kurz nennen möchte:

- 1) Der zunehmende Anteil von wetterabhängigen Energien, also Wind und Sonne, führt dazu, dass der Strom möglichst dann und vielleicht auch dort verbraucht werden sollte, wenn und wo er erzeugt wird. Wir werden uns also zukünftig von der bislang vorherrschenden verbrauchsorientierten Stromerzeugung in Richtung auf einen erzeugungsorientierten Stromverbrauch bewegen müssen. Das ist in der Tat ein großer Paradigmenwechsel, der eine Menge von Konsequenzen nach sich zieht.
- 2) Wir haben eine zunehmende Dezentralisierung und Individualisierung der Stromerzeugung. So gibt es immer mehr Kleinerzeuger in Form von Photovoltaik-, Biogas-, Kraftwärmekopplungsanlagen. Wie Sie auch alle wissen, hat das natürlich erhebliche Auswirkungen auf den Stromtransfer. Die ehemals existierende und vergleichsweise einfach zu beherrschende unidirektionale Top-down Struktur der Elektrizitätsversorgung verliert immer mehr an Gültigkeit und an Gewicht. Sie wird durch eine bidirektional aufgebaute Netzstruktur abgelöst werden müssen.
- 3) Die Rolle der Kunden wandelt sich vom bisher mehr oder minder ausschließlich passiven Versorgungsempfänger zu der des aktiven Marktteilnehmers, der sich z.B. auch selbst

am Stromhandel beteiligen kann. Das erhöht die Komplexität und die Vielfalt der Marktbeziehungen.

Meine Damen und Herren, die modernen Informations- und Kommunikationstechnologien (IKT) haben vielfach bewiesen und beweisen es jeden Tag, dass sie komplexe Systeme steuern können. Die Bundesregierung misst deshalb den IKT eine ganz zentrale Bedeutung zu und hat mit „Deutschland digital 2015“ ihre Schwerpunkte, ihre Aufgaben und Projekte für den Zeitraum bis 2015 bis über die nächste Bundestagswahl hinaus in ihrer IKT-Strategie zusammengefasst.

Diese IKT-Strategie ist darauf ausgerichtet, zum einen die Wettbewerbsfähigkeit durch Einsatz von IKT in allen Bereichen unserer Wirtschaft und in allen Abschnitten der Wertschöpfungskette zu stärken. Sie zielt des Weiteren darauf ab, eine hochleistungsfähige und sichere Internetinfrastruktur zu schaffen, um den künftigen Anforderungen gerecht zu werden. Deswegen haben wir auch die Netzausbaustrategie, von der wir mit gutem Grund behaupten können, dass sie immer mehr greift und zusammen mit dem raschen Ausbau insbesondere von LTE dazu führen wird, dass wir bald eine flächendeckende Versorgung haben werden.

Weitere Punkte sind der Ausbau von Forschung und Entwicklung im IKT-Bereich sowie die schnellere Umsetzung von Forschungs- und Entwicklungsergebnissen in marktfähige Produkte. Das ist ein großes Thema des Münchner Kreises und der Alcatel-Lucent Stiftung. Deswegen bin ich bei Ihnen genau richtig, bei dieser Umsetzung von Forschung in marktfähige Produkte. Das ist beileibe nicht nur ein Thema von IKT, sondern es ist eines der zentralen Probleme überhaupt in Deutschland und eines der Schwerpunkte bei uns im Bundesministerium für Wirtschaft und Technologie.

Die IKT-Strategie zielt auch darauf ab, neue Geschäftsmodelle unter Wahrung der Individualrechte der Nutzer zu ermöglichen. Weitere Aspekte sind, die Aus-, Fort- und Weiterbildung und die Kompetenzen für die Nutzung neuer Medien zu stärken. Ein letzter Punkt, den ich erwähnen möchte, ist der Einsatz von IKT bei der Lösung vielfältiger drängender Herausforderungen der Gesellschaft, u.a. die Nachhaltigkeit und den Klimaschutz, Gesundheit, Mobilität, Verwaltung und Verbesserung der Lebensqualität der Bürgerinnen und Bürger konsequent zu nutzen.

Sie sehen: ein sehr ambitioniertes Programm, das wir uns vorgenommen haben. Wir wollen mit dieser IKT-Strategie dazu beitragen, nachhaltiges wirtschaftliches Wachstum zu fördern, die Schaffung neuer, weiterer Arbeitsplätze zu unterstützen und auch sozialen Nutzen zu schaffen. Ich erwähne das deswegen hier, weil das natürlich ein Gemeinschaftswerk ist. Diese IKT-Strategie ist keineswegs nur eine Aufgabe der Politik, schon gar nicht nur der Bundesregierung, sondern es bedarf des Zusammenwirkens von Politik, Wissenschaft und Wirtschaft. Bei diesem Prozess, der von zentraler Wichtigkeit ist, spielen die nationalen IT-Gipfel eine sehr wichtige Rolle, die ja im Übrigen – darauf darf ich noch einmal hinweisen – nicht nur in einer einmaligen Veranstaltung liegt, sondern auch in den vielen Arbeitskreisen, die zur Vorbereitung tagen. Insofern haben wir hier einen Prozess eingeleitet, der in Europa vorbildlich ist und der dazu geführt hat, dass die Kommissarin Kroes beim letzten IT-Gipfel ange-reist ist, um sich den Prozess anzuschauen um ihn vielleicht als Vorbildfunktion für andere europäische Länder zu nehmen. Der nächste IT-Gipfel findet übrigens am 6. Dezember in München statt unter dem Motto „Vernetzt und mobil – nachhaltiges Wachstum durch IKT“.

Auf unserem letzten Gipfel ging es um die Nutzung der IKT für das Energiesystem der Zukunft. Die Stichworte lauteten E-Energy oder Smart Grid made in Germany. Es geht also

um die Optimierung unseres Energiesystems durch IKT. Immer deutlicher zeichnet sich ab, dass die IKT zur effizienten Umsetzung und Bewältigung von energie- und klimapolitischen Zielsetzungen entscheidend beitragen können, also zentrale Bedeutung haben. Bereits im April 2007, das muss ich fairerweise sagen und will ich auch gern hervorheben, hat unter der Vorgängerregierung das Bundeswirtschaftsministerium in Kooperation mit dem BMU, dem Umweltministerium, mit der Ausschreibung des Forschungs- und Entwicklungstechnologieprogramms E-Energy die Initialzündung gesetzt. Man soll sich also nur begrenzt mit fremden Federn schmücken, denn bereits seit Ende 2008 – und es läuft bis 2012 – werden in sechs regional verankerten E-Energy Modellprojekten neue Smart Grid-Technologien, elektronische Energiemarktplätze, Online-Energiedienstleistungen usw. mit zahlreichen Anwendungen für das Internet der Energie beispielhaft erarbeitet. Die werden dann auch immer wieder präsentiert bei dem jeweils nächsten IT-Gipfel. Ich glaube, dass wir da sehr sinnvolle und gute Erkenntnisse haben gewinnen können und darauf auch aufbauen können.

Datenschutz und Sicherheit werden von Beginn an in diesem Technologieprogramm großgeschrieben. Schon die Systemarchitektur der E-Energy-Technologien wird von Beginn an, also von 2008 bis zum heutigen Tage, in der Weise eines Privacy by Design konzipiert. In einer projektübergreifenden Arbeitsgruppe wurden Empfehlungen zu Datenschutz und Datensicherheit erarbeitet.

Meine Damen und Herren, welche Anforderungen sollten wir an die Sicherheit von IKT-basierten intelligenten Energienetzen stellen? Oder welche müssen wir an sie stellen? Vorerst, was Deutschland anbelangt, die Beibehaltung eines sehr hohen Grades an Versorgungssicherheit. Das ist die ganz große Herausforderung. Ich brauche Ihnen nicht zu sagen, dass wir hier auf Kante genäht sind. Die Abschaltung von 7+1 Atomkraftwerken hat jetzt schon eine sehr schwierige Situation zur Folge. Man kann dieses System jetzt schon nur steuern mit einem sehr hohen Maß an intelligenter Netzsteuerung, und dazu ist IKT absolut erforderlich. Das ist eine richtige große Herausforderung. Man sieht nicht immer in der Öffentlichkeit, was die Netzbetreiber schon heute alles leisten müssen, auch mit Stromimporten aus Frankreich oder aus der Tschechischen Republik. Da ist ein sehr großes Maß an IKT-Steuerung erforderlich.

Ich will aber auch erwähnen, dass Steuer-, Tarif-, Verbrauchs-, Identitäts- und Kundendaten auf einem hohen und jeweils angemessenen Niveau vor Manipulationen geschützt werden müssen. Zu vermeiden sind also sowohl manipulative als auch systembedingte Versorgungsausfälle, Fehlsteuerungen bzw. Fehl-Bereitstellungen von Energie. Ein praktisches Problem ist aber auch, dass wir Schwierigkeiten bei der Rechnungsstellung und den Missbrauch von Kunden- und Verbrauchsdaten vermeiden müssen.

Eine unverzichtbare Kernfunktionalität der Versorgungssysteme muss auch in Krisen- und Katastrophenlagen gewährleistet sein und es müssen Mechanismen zur schnellstmöglichen Wiederherstellung auch im Falle von Totalausfällen vorhanden sein. Das ist eine Lehre aus Fukushima. Schwarzstartfähigkeit muss vorhanden sein. Auch das ist ein Kriterium, das erfüllt sein muss.

Die Novelle des Energiewirtschaftsgesetzes, das, wie Sie sicherlich wissen, im Zusammenhang mit der Energiewende verabschiedet worden ist, beinhaltet klare Regeln zu Datenschutz und Datensicherheit. Paragraph 21g regelt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten aus einem Messsystem. Der Paragraph 21e fordert die Einhaltung eines Schutzprofils, welches per Rechtsverordnung auf der Grundlage des Paragraph 21i EnWG näher bestimmt werden kann. Datenschutz und Datensicherheit im Smart Grid sind durchgehend über verschiedenste Rollen und technische Bereiche zu gewährleisten, im Haushalt,

beim Verbraucher, den wir neudeutsch schon Prosumer nennen, eine Mischung aus Verbraucher und Erzeuger, aber auch beim Energieversorger, dem Messstellenbetreiber und Dienstleister, bei Diensteanbietern und den Marktplatzbetreibern.

Aus technischer Sicht sind Einzelsysteme und ihre Verknüpfung sowohl in Bezug auf Hardware als auch auf Software abzusichern. Die Sicherheitskonzepte intelligenter Energienetze müssen eine Lehre aus vielfältigen Problemen der Vergangenheit und aus Fukushima sehr robust konzipiert sein. Die Gespräche im Zusammenhang mit unseren E-Energy-Projekten, diese sechs Modellregionen, die ich Ihnen schilderte, weiteren Smart Grid-Akteuren und der IT-Sicherheitswirtschaft haben uns gezeigt, dass im Bereich Smart Energy-Sicherheit noch sehr viel Arbeit, noch sehr viele Hürden zu nehmen sind.

Mit intelligenten Stromnetzen konzipieren wir kritische Infrastrukturen, die über die gesamte Prozesskette risikoadäquat zu schützen sind. Der Absicherung eines wichtigen Gliedes dieser Kette dient auch der Auftrag, den das Bundeswirtschaftsministerium an das Bundesamt für die Sicherheit in der Informationstechnik, Ihnen allen als BSI bekannt, zur Entwicklung und Erstellung eines Schutzprofils für Smart Meter vergeben hat.

Wir sind also auch vor allen Dingen im internationalen Vergleich auf einem guten Weg. Unter enger Einbeziehung des Bundesdatenschutzbeauftragten wird ein neuer verbindlicher Sicherheitsstandard entwickelt. Immer wenn ich von Standards und Normen spreche, sage ich, dass hier die Musik spielt. Wenn wir es schaffen, vorweg zu marschieren und Standards und Normen setzen zu können, zumindest im europäischen aber besser noch im weltweiten Bereich, dann werden wir auch die ökonomische Ernte einfahren zu können. Deswegen versuchen wir hier, was Sicherheitsstandards angeht, vorweg zu marschieren. Wir beziehen da die Unternehmen, die Verbände und Verbraucherschutzorganisationen mit ein, die auch unterstützend teilnehmen. Es gibt zahlreiche Vorschläge und Kommentare von Ihnen, meine Damen und Herren, wofür ich sehr dankbar bin und wozu ich Sie jederzeit auch ermutigen möchte, das in Zukunft zu tun.

Darin liegt nichts Geringeres als die Chance, intelligente Energienetze, die auf Kommunikation setzen, auf dem Fundament von Datenschutz und Datensicherheit und damit Akzeptanz bei den Bürgerinnen und Bürgern aufzubauen. Alles, was wir tun, ist nicht nur eine Lehre aus Stuttgart 21. Es gibt in großen Teilen der Bevölkerung Vorbehalte gegenüber mehr oder minder jeder Form von Technik. Deswegen ist es auch so wichtig, Datenschutz und Datensicherheit aus Akzeptanzgründen, nicht nur aus Gründen der Systemstabilisierung, voranzutreiben. Der Computerwurm Stuxnet und die Meldungen über mangelnde Absicherungen von SCADA-Systemen haben den Fokus auf die Sicherheit von jetzigen und zukünftigen Infrastrukturen vor Cyberangriffen gelenkt. Das IT-Sicherheitsunternehmen, das Sie alle kennen, McAfee als Tochterunternehmen von Intel, hat im April dieses Jahres auf Basis von Umfragen schon das zweite Mal in Folge den Fokus auf die Sicherheit in IT-basierten Infrastrukturen gesetzt. Die Konvergenz zweier kritischer Infrastrukturen, nämlich IKT und Energie, erzeugt nun mal komplexe Sicherheitsproblematiken, die es zu analysieren gilt und aus denen dann die gebotenen Konsequenzen zu ziehen sind. Deswegen werden wir auch hier prüfen, ob wir Studien vergeben, um die Erkenntnisse voranzutreiben und Impulse zu setzen für die weitere Entwicklung.

Meine sehr geehrten Damen und Herren, lassen Sie mich zum Schluss kommen. Der Münchner Kreis, zu dem ich jederzeit, lieber Herr Prof. Picot, sehr gerne hinzukomme wegen der Qualität der Veranstaltungen und des Publikums, hat in vielen Jahren ein großes Spektrum neuer Entwicklungen der Informations- und Kommunikationstechniken begleitet, vielfach auch eingeleitet. Sein Selbstverständnis ist eines der Überparteilichkeit und der

Neutralität gegenüber gesellschaftlichen und wirtschaftlichen Interessen.

Neutralität und Überparteilichkeit ist etwas, was ich mir in diesen stürmischen Zeiten auch von anderen wünschen würde, den Medien zum Beispiel. Vielen Dank für die hervorragende Arbeit des Münchner Kreises. Ich möchte auch positiv hervorheben, dass die heutige Veranstaltung von der Alcatel-Lucent Stiftung, mit der wir, lieber Herr Dr. Klumpp, seit vielen Jahren in vielen Feldern von IKT und E-Energy erfolgreich zusammenarbeiten, mit vorbereitet worden ist. In diesem Berliner Gespräch heute wird der offenen Diskussion viel Zeit eingeräumt. Ich hoffe auf für Sie alle anregende Beiträge, einen intensiven Meinungsaustausch und wünsche Ihnen einen schönen Abend, weiterhin anregende Gespräche und freue mich auf einen intensiven Dialog heute und in Zukunft mit Ihnen.

18 Smart Grid – Perspektiven der Energiewirtschaft

Dr. Andreas Breuer, RWE Deutschland AG, Essen

Ich freue mich ganz außerordentlich, dass ich heute Abend hier zu Ihnen sprechen kann, auch als Vertreter des BDEW, weil die Mischung der Teilnehmer genau die ist, die wir für die Diskussion des Themas Smart Grid benötigen. Ich möchte die nächsten zehn Minuten nutzen, um mit Ihnen einen Blick in die Zukunft zu werfen. Das ist mein Blick in die Zukunft, und Sie werden sehen: das ganze Zukunftsbild ist noch sehr unscharf. Die gute Nachricht ist: Wir wissen zwar nicht exakt, was uns die Zukunft bringt. Aber es ist genau die Diskussion, die die Zukunft und damit ein Stück potenzieller Wirklichkeit gestalten wird.

So könnte die Welt in Zukunft aussehen. Wir befinden uns allesamt und insbesondere die Energiewirtschaft vor einem Paradigmenwechsel. Wenn es in der Vergangenheit noch gegolten hat, dass wir zentrale Erzeugung hatten und der Strom von der zentralen Erzeugung über die einzelnen Netzebenen zum Kunden geflossen ist und dort verbraucht wurde, muss ich sagen, dass sich das in den letzten Jahren deutlich gewandelt hat, und es wandelt sich immer mehr. Der Kunde ist nicht nur Verbraucher, sondern der Kunde entwickelt sich hin zum Erzeuger. Wir nennen das Neudeutsch, auch aus den E-Energy Projekten kommend, „Prosumer“.

Um Ihnen ein Beispiel aus meinem Unternehmen zu geben: Wir haben in den letzten Jahren 180.000 dezentrale Anlagen zur Stromerzeugung aus erneuerbaren Energien – im wesentlichen Photovoltaik und Windkraft - ans Netz geschlossen. Allein im vergangenen Jahr waren es 60.000 Anlagen, so dass man statistisch sagen kann, pro Tag kommen 164 Anlagen bei uns ans Netz. Diese Anlagen werden nicht auf Höchst- und Hochspannungsebene in Form von Großanlagen angeschlossen, sondern genau da, wo wir sie eigentlich aus reiner Netzführungssicht nicht unmittelbar gebrauchen können - nämlich als Kleinstanlagen, verstreut in der Mittelspannung und in der Niederspannung. Diese Anlagen sind zu einem großen Teil von den Launen des Wetters abhängig, daher sind sie volatil in ihrer Erzeugung bzw. im Stromangebot. Das stellt die Energiebranche und insbesondere auch die Verteilnetzbetreiber schon heute vor entsprechende Herausforderungen.

Diese Herausforderungen sind aber nicht nur technischer Natur. Lassen Sie mich kurz erläutern, wie wir als Energiebranche versuchen, die Herausforderungen, die die Zukunft an uns und an die Infrastruktur stellt, mit konkreten und effizienten Lösungen zu meistern. Es ist nicht nur die Technologie, auch nicht in Bezug auf IKT, die uns allein fordert. Der demografische Wandel in Deutschland und der Strukturwandel in Stadt und Land hat mindestens ebenso bedeutende Konsequenzen für die Art, mit der wir Strom erzeugen und verteilen.

Ich selbst habe mein Büro in Essen. Ganz deutlich kann man es im Ruhrgebiet sehen. Diese und weitere Anforderungen an uns als Infrastrukturbetreiber für Energienetze haben sich schon gewaltig verändert, und sie werden sich immer mehr ändern. Das heißt, wenn wir anhand von demografischen Entwicklungen, von Strukturwandel, von Alterung – unsere Netze unterliegen natürlich wie jede andere Technologie auch entsprechenden Alterungsmodellen – und dem Ausbau von Photovoltaik und Wind insbesondere in den ländlichen Regionen, versuchen, dies alles zu fassen, dann wissen wir, wie die Herausforderungen in der Zukunft aussehen.

Aus diesem Grund beschäftigt sich die Energiewirtschaft und vorweg RWE massiv mit einer Vielzahl von Projekten, insbesondere aus den E-Energy Projekten, wo wir versuchen, die

Versorgungsaufgabe der Zukunft zu greifen. Ein weiteres Projekt ist das Projekt ‚Netze für die Stromversorgung der Zukunft‘ oder wie wir sagen: „Smart Country“. In diesem Projekt wurde im ersten Schritt die Herausforderung definiert. Das ist ein ganz wichtiger Punkt für die Diskussion später. Denn bevor wir nicht alle wissen, welche Herausforderungen exakt auf die Netzinfrastruktur zukommen, springen wir bei der Lösung zu kurz oder vielleicht auch zu weit. Nur dann, wenn wir wissen, wie z.B. 2020, 2030 die Versorgungsausgabe in einer konkreten Region aussehen soll, können wir mit Ihnen zusammen über Lösungsmöglichkeiten diskutieren. Und wir brauchen dazu die Erfahrungen aller Beteiligten, um zu einer Lösung aus einem Guss zu kommen, ansonsten droht eine Energiewende ohne Sinn und Verstand – mit unabsehbaren Folgen für Ihre und unsere Glaubwürdigkeit in Politik und Gesellschaft. Das ist für mich ein ganz zentraler und wichtiger Punkt. Wir sitzen hier nicht nur alle aus der Energiewirtschaft kommend, sondern eine Vielzahl von Kollegen sind aus der IKT Branche, und das Essentielle der Diskussion muss sein, dass wir voneinander lernen und dass wir uns auch untereinander verstehen, sprich: die gleiche Sprache sprechen.

Eine der Kernbotschaften zum Thema Smart Grid ist, dass man sich mit dem Markt und den unterschiedlichen Marktrollen auseinandersetzen muss. Dies ist von entscheidender Bedeutung. Wir verstehen uns als Infrastrukturdienstleister oder Infrastrukturbetreiber, der es allen Marktspielern in Zukunft ermöglicht, diese Infrastruktur so zu nutzen, wie es für die einzelnen Marktrollen und deren Geschäftsmodelle notwendig ist.

Aber hier gilt es, die unterschiedlichen Rollenverständnisse zu beachten. Da gibt zum einen die Sichtweise eines Verteilnetzbetreibers. Der Verteilnetzbetreiber hat die Aufgabe, die Infrastruktur so instand zu halten und zu betreiben, dass die Marktspieler diese Infrastruktur auch nutzen können. Betreiber von virtuellen Kraftwerken, Anbieter von E-Mobility, regionaler Marktplätze, und die Bereiche Handel und Erzeugung haben ein anderes Rollenverständnis. Unsere Aufgabe als Verteilnetzbetreiber beschränkt sich auf die Infrastruktur und die damit verbundenen Aufgabe, einen sicheren und zuverlässigen Betrieb dieser Infrastruktur zu gewährleisten, damit die Lichter nicht ausgehen – oder schnell wieder angehen, wenn Sie so wollen, denn eine perfekte Welt gibt es auch in der vorbildlichen deutschen Versorgungssicherheit nicht in jeder Minute. Diese Rolle des Verteilnetzbetreibers ist eine ganz andere Rolle als wenn wir über Geschäftsmöglichkeiten oder Geschäftsmodelle sprechen. Für unsere Diskussion ist dies eine ganz wichtige Rahmenbedingung, weil IKT nicht gleich IKT ist. Als Verteilnetzbetreiber betreiben wir eine eigene IKT in Form eines Prozessnetzes. Diese IKT, die wir schon seit Jahren betreiben, dient dazu, das Netz zu steuern; Schutz, Leittechnik, nachrichtentechnische Anwendungen fallen darunter. Diese IKT ist eine ganz andere IKT als die IKT mit den unterschiedlichen Geschäftsmodellen, die Elektromobilität verbindet, die Windkraft- und Photovoltaikanlagen anbindet und deren erzeugten Strom handelbar macht und die regionale Marktplätze beflügeln soll.

Da ist es ganz wichtig, in der Diskussion immer zu wissen, über welche Marktrollen und Marktverständnisse wir jetzt reden. Also, IKT ist nicht gleich IKT, weil wir über eine Prozess-IKT und eine Consumer Information Technology reden. Die Anforderungen an diese Lösungen sind komplett unterschiedlich. Wenn eine Lösung Real Time Anforderungen stellt, braucht eine andere Lösung vielleicht nur Daten im 15-Minuten-Takt.

Eine weitere Kernbotschaft meiner Rede soll sein, dass Smart Grid nicht gleichzusetzen ist mit Smart Meter. Das bedeutet nicht, dass wir Smart Meter flächendeckend brauchen, damit wir ein Smart Grid aufbauen können. Da verweise ich auf das Markt- und Rollenverständnis. Wenn ich mir den Verteilnetzbetreiber herauspicke - und ich nehme unser Pilotprojekt „Smart Country“ im Landkreis Bitburg-Prüm in der Eifel -, haben wir dort 11 MW installierte dezentrale Leistung bei 8 MW Last bzw. Nachfrage. Wir haben also gewöhnlich mehr

Einspeisung als Verbrauch in diesem Landkreis – sofern nicht dauerhaft diesiges und windstilles Wetter herrscht - und wir nutzen dort neue Technologien, um die Versorgungsaufgabe auch zukünftig lösen zu können. Wir hätten die Möglichkeit, in diesem Landkreis 1.300 Smart Meter bei unseren Haushaltskunden zu installieren, um möglicherweise Daten für den Netzbetrieb zu nutzen. Die Lösung mit Blick auf ausschließlich die Aufgabe des Verteilnetzbetreibers ist aber, verteilt im Netz an neuralgisch wichtigen Punkten 25 Messpunkte zu installieren. Das bedeutet 1.300 versus 25. In der Diskussion rund um Smart Meter und Smart Grid ist das für mich eine ganz wichtige Unterscheidung. Smart Meter hat im ersten Schritt nichts mit Smart Grid zu tun. Das ist das Henne-Ei-Problem. Wir als Verteilnetzbetreiber und als Branche nutzen natürlich die Smart Meter-Infrastruktur, wenn diese vorhanden ist. Nehmen wir an, dass wir einen Rollout von Smart Metern hätten, dann können wir natürlich diese Daten auch entsprechend für netzrelevante Aufgaben verwenden, und zwar ohne das individuelle Verbrauchsverhalten von Kunden auszuspähen – das ist weder unser Ziel noch hilft es uns bei der Erfüllung unserer zentralen Aufgabe: die Spannung im Verteilnetz stabil zu halten. Darauf komme ich gleich nochmal zurück. Aber der Umkehrschluss, dass wir erst den Smart Meter in jedem Haushalt brauchen, damit wir unsere Versorgungsaufgabe auch in Zukunft erfüllen können, ist nicht richtig.

Im Zusammenhang Smart Meter und Smart Grid ist eines sehr wichtig, und das ist eine Tatsache, die uns schon seit Jahren in der Branche beschäftigt und woran wir auch sehr aktiv arbeiten. Das ist das Thema Datenschutz und Datensicherheit, was für die Branche jetzt nichts Neues ist. Es ist auch nichts Neues aus den Diskussionen mit Smart Grid und Smart Meter. Datenschutz und Datensicherheit hat bei uns schon immer einen sehr hohen Stellenwert gehabt. Deshalb ist der BDEW auch aktiv, um den Prozess zur Findung von Datenschutz und Datensicherheitsrichtlinien und Regularien mit zu begleiten. Der BDEW, insbesondere auch im Hinblick auf die Netzplattform des BMWi und die Kontakte hin zum BSI, ist sehr daran interessiert, entsprechende Stellungnahmen und Verbesserungsvorschläge in die laufenden Diskussionen einzubringen. Die Privatsphäre wird zu keinem Zeitpunkt der Energiewende geopfert.

Dennoch wird uns die Energiewende über die nächsten Jahre beschäftigen. Und sie wird auch unsere Verbraucher und Kunden fordern, die wir mit intelligenten Lösungen für die Energiewende begeistern müssen. Es ist keine Revolution, bei der man einen Schalter umlegt und alles ist fertig, sondern wir reden von einem Prozess einer Evolution, den wir nur gemeinschaftlich zukünftig gestalten können. Kommunikation tut nicht weh. Kommunikation schadet nicht. Vor dem Hintergrund wünsche ich mir rege Diskussionen und Kommunikation mit Ihnen.

19 Smart Grid – Perspektiven der IKT-Wirtschaft

Herbert Merz, BITKOM, Berlin

Ich freue mich, Ihnen heute die Perspektiven der IKT-Wirtschaft zum Thema Datenschutz und Datensicherheit bei Smart Energy darlegen zu können. Vielleicht sollten wir uns einmal kurz vor Augen halten, was „Smart Energy“ bedeutet. „Smart Energy“ ist das intelligente Stromnetz, die intelligente Erzeugung und der intelligente Verbrauch, die zusammen eine zuverlässige, nachhaltige und kosteneffiziente Energieversorgung auch in der Zukunft sicherstellen. Damit einher gehen neue Tarifmodelle und Services für den Endkunden wie zeitvariable Tarife, dynamische Verbrauchsregelung je nach Erzeugung und Netzlast, detaillierte und zeitnahe Informationen über den stündlichen, täglichen und wöchentlichen Verbrauch und Energiemanagementanwendungen. Auch die Elektromobilität mit der flächendeckenden Installation von Ladestationen für elektrische Fahrzeuge wird in dem Gesamtkonzept eine wichtige Rolle spielen.

All diese Intelligenz erfordert die Erfassung und Verarbeitung großer Datenmengen, um die Netze, die Erzeugung und den Verbrauch entsprechend zu steuern und zu optimieren. Das geht, wie Sie wissen, nur mit dem netzweiten Einsatz von IKT Systemen. Auf der Endkundenseite sind intelligente Haussteuerungssysteme erforderlich, um dem Anwender den gewohnt einfachen Umgang mit elektrischer Energie auch weiterhin zu ermöglichen. Er wird keine Lösungen akzeptieren, die eine fortwährende und zeitaufwendige Beschäftigung mit komplexen Tarifmodellen und Preissignalen erfordern. Die Lösungen müssen komfortabel und transparent sein und den Kunden möglichst wenig einspannen, wie der Trend zu Flatrates im Bereich der Internet- und VoIP-Anschlüsse zeigt. Und, das hat eine Umfrage der LMU Anfang des Jahres ergeben: Die Verbraucher müssen Vertrauen in die Anbieter und die Technologie haben.

Kosten, Nutzen und Vertrauen. Diese Größen sind für den Erfolg von Smart Energy entscheidend. Dies gilt sowohl für den Verbraucher als auch für das Energieversorgungsunternehmen und den Netzbetreiber. Smart Energy erfordert Investitionen auf allen Seiten, die kurzfristig nicht immer zu Kosteneinsparungen führen. Hier zählt zuerst einmal der gesellschaftliche Nutzen, der sich in nachhaltiger Energieversorgung, CO₂ Reduktion und auch in der Erarbeitung weltmarktführender Technologie zeigt. Wir müssen es deshalb schaffen, dass die Menschen den Nutzen für die Gesellschaft auch als ihren eigenen erkennen.

Kommen wir zum Vertrauen und damit zum Thema des heutigen Abends. Datenschutz und Datensicherheit sind die vertrauensbildenden Maßnahmen schlechthin. Dies gilt sowohl für die verbraucher-spezifischen Daten beim Smart Metering als auch für die Sicherheit bei der Steuerung von kritischer Infrastruktur im Smart Grid die gegen Netzangriffe von außen geschützt sein müssen.

Entscheidend für nachhaltigen Datenschutz und Datensicherheit ist aber, dass wir es von Anfang an richtig machen. Es sollte nicht darum gehen, alles so sicher wie MÖGLICH zu machen. Denn dann wird das System zu teuer. Ein Energiesystem, das sich niemand leisten kann, braucht auch kein Nutzervertrauen. Nein, wir müssen das System so sicher wie NÖTIG machen. Um zu wissen, was nötig ist, müssen wir das Gesamtsystem betrachten. Dafür wäre eine umfassende Analyse bzw. eine Studie zur IT-Sicherheit in Smart Grids sehr hilfreich. Die Sicherheit von Smart Metering ist ein wichtiger, aber eben nur relativ kleiner Teil des gesamten Energiesystems. Wir müssen uns überlegen, welche Daten und Rollen es in diesem System gibt, auf welche Daten die jeweiligen Rollen zugreifen dürfen und welche Angriffs-

szenarien existieren. Daraus ergibt sich die Notwendigkeit für Granularität und Anonymisierung von Daten, für Verschlüsselung und Authentifizierung und für ein Rechtemanagement für den Zugriff auf die Daten.

Die Datenschutz- und Datensicherheitskonzepte müssen von Anfang an berücksichtigt werden und das nicht nur beim Smart Metering, sondern beim ganzen Smart Grid. Die technischen Verfahren und Protokolle für Datenschutz und Datensicherheit existieren bereits und werden schon in anderen Bereichen eingesetzt. Beispiele hierfür sind zahlreich, ich möchte nur Telekommunikation, Online-Banking oder Straßenmaut nennen. Das Handling von Millionen Kunden mit variablen Tarifen und die sichere Datenübertragung und Authentifizierung ist zum Beispiel im Mobilfunk Standard. Natürlich müssen die Systeme und Prozesse an die Bedürfnisse der Energiewirtschaft angepasst werden. Aber auch die Anpassung von existierenden Lösungen an neue Anforderungen ist in der IT-Branche Alltag. Weltweit akzeptierte Prinzipien und Prozesse für Datenschutz und Datensicherheit sind dabei die Grundlage. Was fehlt, sind einheitliche rechtliche Rahmenbedingungen, die es gestatten, auf Basis der existierenden Verfahren passende Lösungen zu kreieren. Es gibt 16, in Worten sechzehn, Landesdatenschutzgesetze, die teils unterschiedliche Regelungen vorsehen und zu unterschiedlichen Positionen der Landesbehörden führen.

Einheitliche Regelungen sind essenziell, um landes- und europaweit wirtschaftlich sinnvoll tätig zu werden. Die für Smart Grids notwendigen Investitionen müssen für die Marktteilnehmer attraktiv werden, sie müssen investieren wollen. Und dazu gehört Investitionssicherheit. Die gibt es natürlich nicht, wenn die Rechtmäßigkeit von Smart Metering oder Smart Grid infrage steht oder Widerrufsmöglichkeiten im großen Umfang genutzt werden können, die zum „Einreißen“ des Smart Grids führen. Auch die Definition von einheitlichen, standardisierten Schnittstellen spielt dabei eine wichtige Rolle. Sie ermöglichen Interoperabilität zwischen den verschiedenen Marktteilnehmern und Lösungsanbietern unter Berücksichtigung von Datenschutz und Datensicherheit. Deutschland hat dabei weltweit eine führende Rolle inne und trägt damit zu einer Führungsposition bei Smart Grid Technologien bei.

Der BITKOM als Verband der deutschen IKT-Wirtschaft beschäftigt sich schon seit Jahren mit dem Thema Datenschutz und Datensicherheit und hat eine eigene Arbeitsgruppe zum Thema Smart Energy. Wir versuchen, auch zusammen mit den Verbänden der anderen involvierten Wirtschaftsbereiche, einheitliche landes- und auch europaweite gesetzliche Regelungen herbeizuführen, indem wir die Politik und auch die Regulierungsbehörde auf die erforderlichen Festlegungen hinweisen und entsprechende Vorschläge unterbreiten. Auch die Information der Öffentlichkeit, des Verbrauchers ist uns ein Anliegen. Und hier sind wir wieder beim Vertrauen als Basis für Akzeptanz. Vertrauen wird auch durch Transparenz gebildet. Wir müssen dem Anwender erklären, wer welche Daten wofür nutzt und wie diese geschützt werden. Und vor allem, dass und warum das für eine umweltfreundliche, zukunfts-sichere Energieversorgung notwendig ist.

20 Smart Grid – Perspektiven der IKT-Wirtschaft

Prof. Dr. Ingo Wolff, Informationstechnische Gesellschaft im VDE (ITG), Frankfurt

Um aus dem heutigen Energieversorgungssystem ein Smart Grid zu generieren, müssen vielfache Investitionen in die notwendige Informations- und Kommunikationstechnik, die Messtechnik und die Automatisierungstechnik aufgebracht werden. Es muss allerdings generell festgestellt werden, dass bis heute noch keine realistische Abschätzung des technischen Aufbaus, geschweige denn der Investitionskosten und ihrer Refinanzierungsmöglichkeiten für die IKT-Infrastruktur des Smart Grid existiert. Um zu einer solchen Basis zu gelangen, bedarf es der Analyse der Informationsflüsse zwischen den Marktteilnehmern, der Identifikation einer geeigneten Marktrolle der einzelnen Marktpartner, einer Beschreibung der Modellunternehmen, einer Analyse der benötigten IKT-Infrastruktur, der Bewertung geeigneter Technologien und einer Technologieauswahl sowie einer monetären Bewertung der zu installierenden Infrastruktur. Insgesamt werden die aufzubringenden Kosten sicher im zweistelligen Milliardenbereich liegen. Genauere Zahlen sind aber bisher nicht in der Diskussion zu finden und auf Grund der noch fließenden Diskussionen über die Struktur des Smart Grid zurzeit auch nicht zu erwarten.

Zum Aufbau und Betrieb des internen Kommunikationsnetzes, das die Stromerzeuger, Stromhändler, Stromanbieter und die Strombörse miteinander und dann über das intelligente Verteilnetz mit den dezentralen Energieerzeugern und den Endkunden, den Messstellenbetreibern und den Messstellendienstleistern verbindet, sind die Kommunikationsnetzbetreiber mit ihrem in den letzten zwei Jahrzehnten geschaffenen Know-How gefordert. Die notwendige Software- und Middlewareentwicklung kann ein interessantes Geschäftsfeld auch für kleine und mittlere Unternehmen werden.

Der Aufbau, der Betrieb und der Erfolg des Smart Grid beruht auf dem Messen von Daten im Netz, die zur Steuerung und Regelung der Netzeigenschaften verwendet werden können. Das Stichwort heißt: „Smart Metering“. Smart Meter, also mit elektronischer Intelligenz und Kommunikationsfähigkeit ausgestattete Messstellen für elektrische Energie sind eine notwendige Voraussetzung für den Aufbau des Smart Grid. Der Markt der Smart Meter Technik sieht, wenn man die Millionen Endverbraucher betrachtet, nach einem für die IKT-Wirtschaft lukrativen Markt aus. Er ist allerdings, insbesondere in Deutschland, ein vor sich hin dümpelnder Markt. Dies liegt nicht nur daran, dass die gesetzlichen Vorschriften zum Smart Metering nicht immer stringent, sondern weich formuliert sind, sondern auch weil für die Refinanzierung der Investitionen noch nicht ausreichende Modelle vorliegen, teilweise noch technische Probleme zu lösen sind, die Standardisierung noch nicht zu einem Ergebnis gekommen ist und damit viele unterschiedliche, proprietäre Lösungen in den Markt gebracht werden.

Als letzter hoch interessanter Markt aus dem Bereich Smart Grid soll der Markt der additiven Dienstleistungen erwähnt werden, wobei der Energiemarkt viel von den bereits existierenden Diensten im Kommunikationsmarkt lernen kann. Intelligente Billingssysteme z.B. für die Abrechnung zeitlich wechselnder Preise in einem Energiesparanreizmodell entsprechen weitgehend den Abrechnungsmethoden im Mobilfunk. Für die Messung der Stromdaten und für das Management dieser Daten können sich speziell ausgerüstete Dienstleister engagieren. Dienstleister können sich aber auch in vielen anderen Bereichen engagieren. Die Möglichkeiten im Bereich intelligenter Dienstleistungen sind, wenn einmal ein Smart Grid existiert, vielfältig und ein großer, interessanter Markt.

Zusammengefasst: Smart Grid ist, wenn es zügig angegangen und richtig umgesetzt wird, ein vorzügliches Konjunkturprogramm für die deutsche und europäische IKT-Wirtschaft. Um diesen Markt zu nutzen bedarf es aber noch erheblicher Anstrengungen.

21 Diskussion / weitere Statements mit Vortragenden und allen Teilnehmern einschl. der eingeladenen Pressevertreter

Moderation: Prof. Dr. Helmut Krcmar, Technische Universität München
Prof. Dr. Heinz Thielmann, Emphasys GmbH, Heroldsberg

(Anmerkung: Es sind nicht alle Wortmeldungen dokumentiert. Schriftliche Statements einiger Teilnehmer sind im Anhang abgedruckt.)

Prof. Thielmann:

Der Münchner Kreis und das Berliner Gespräch mit diesem Format leben davon, dass wir Handlungsbedarfe formulieren, die dann vielleicht für eine nächste Veranstaltung konkreter thematisiert werden. Ich möchte gleich in die Diskussion einsteigen und dann die Redner, die auf der Liste stehen, spontan bitten, mehr in Richtung Handlungsbedarfe an verschiedene Adressaten und auch an die Politik zu formulieren. Vielleicht melden Sie sich in der ersten Runde einfach spontan und sagen, wo Handlungsbedarf in Richtung Politik besteht.

Prof. Picot:

Ich möchte einen Punkt erwähnen, der auch bei anderer Gelegenheit schon aufgekommen ist und bei dem aus meiner Sicht Klärungsbedarf besteht. Es geht um die Frage der Daten. Man braucht ja, um ein Smart Grid oder auch einen Smart Metering / Smart Grid Verbund zu betreiben, einen gewissen Datenzugang, wenn neue Märkte und neue Dienstleistungen entstehen sollen. Es kann nicht jeder, der sich ein Geschäftsmodell ausdenkt, selbst neue Sensor- und Messnetze installieren oder neue Daten erheben, sondern es sind ja Daten da. Die Frage ist, wie die Zugangsmöglichkeit zu diesen Daten organisiert wird. Handelt es sich bei diesen Daten um proprietäre Daten, die nur, wenn wettbewerbsrelevante Einschränkungen vorliegen, geöffnet werden müssen im Sinne einer essential facility? Oder handelt es sich um Daten, auf die die Öffentlichkeit einen Anspruch hat, natürlich immer unter Wahrung der Anonymität usw.? Inwieweit müssen solche Daten in einer Treuhandenschaft geführt werden, inwieweit aber können sie von privaten Organisationen in normalen Markt-zusammenhängen verwaltet werden - oder muss man das differenziert sehen je nach Datenkategorie und anderen Randbedingungen? Hier, glaube ich, ist ein dringender Klärungsbedarf, den wir nicht nur bei diesem Cyber Physical System haben, aber hier als gutes Beispiel, sondern auch bei anderen, wo wir auf großen Datenmengen, die durch irgendwelche Sensornetze erhoben werden, aufbauen. Das ist in der Mobility auch ein Thema, aber auch in Smart Factories, in E-Health usw. Ich habe den Eindruck, dass hier noch ein erheblicher Aufklärungsbedarf besteht, bei dem uns die öffentliche Hand helfen kann.

Staatssekretär Otto:

Ich fürchte, dass die Frage an mich gerichtet wurde, wobei ich Ihnen sagen möchte, zum derzeitigen Zeitpunkt – Herr Prof. Wolff hat eben darauf hingewiesen, dass viele Dinge noch im Fluss sind – würde es sicherlich wenig Sinn machen, Datenschutzaudits durchzuführen oder Datenregelungen zu treffen. Wenn ich den Trend richtig einschätze, werden wir dauerhaft eine sehr hohe Sensibilität der Bürgerinnen und Bürger haben, irgendwelche Daten durch Gesetz oder durch was auch immer privaten Anbietern zu den allerbesten Zwecken, also Energieeinsparung usw. zur Verfügung zu stellen. Ich glaube, auf das Prinzip des Opt-in, das Prinzip der Freiwilligkeit, wird man sich einstellen müssen, obwohl man aus energiepolitischen Gründen natürlich viele Überlegungen haben könnte zu sagen, dass ich die Menschen verpflichte, bestimmte Datensätze zur Verfügung zu stellen. Ich Sorge dafür, dass sie nicht missbraucht werden. Aber wie die Diskussion im Moment läuft, ohne ich, dass

man hier keine Akzeptanz finden wird. Viele von Ihnen kennen die Regelungen zu den Cookies, wo wir erhebliche Diskussionen haben, obwohl wir mit Engelszungen reden und sagen, dass Geschäftsmodelle in Gefahr sind, dass die Refinanzierung des Netzes in Gefahr steht. Aber die Leute bestehen darauf, dass sie in jedem Einzelfall ihre Zustimmung erteilen wollen.

Wenn ich das auf die Energienetze übertrage, habe ich das Gefühl, dass der Staat sich sehr zurückhalten muss mit irgendwelchen staatlichen Vorschriften, welche Daten zur Verfügung zu stellen sind. Ich muss im Grunde dazu kommen, dass die Menschen durch Aufklärung, durch öffentliche Meinungsklima usw. dazu veranlasst werden, dass sie es freiwillig tun. Mir ist klar, je mehr Daten zur Verfügung gestellt werden, desto intensiver und desto effektiver wird ein Energiesystem, ein Smart Grid. Wenn wir hier über Geschäftsmodelle reden, sollte jeder, der sich in diesen Bereich vorwagt, sein Geschäftsmodell darauf aufbauen, dass die Datensätze, die von Privaten erforderlich sind, um hier Geschäftsmodelle aufzusetzen, auf dem Prinzip der Freiwilligkeit gegeben werden, und zwar in jedem Einzelfall. Das wird sich vielleicht ändern, aber meine persönliche Einschätzung und Erfahrung aus vielen aktuellen Diskussionen ist, dass die Reise dorthin geht, dass jeder Verbraucher sagt: Ich will bestimmen, was mit meinen Daten geschieht und ich lasse mir vom Gesetzgeber mit Sicherheit nicht vorschreiben, dass er an den Energieversorger oder an den Netzbetreiber oder an die Netzbörse irgendwelche Daten preisgibt. Das wird wohl nicht laufen und deswegen meine dringende Empfehlung, jedes Businessmodell so zu konzipieren, dass es so überzeugend ist, dass der jeweilige Verbraucher, der Inhaber eines Smart Meter freiwillig bereit ist, um Geld und Energiekosten zu sparen, seine Daten an den Netzbetreiber, an den Energieversorger usw. zur Verfügung zu stellen. Das ist wohl die Tendenz, auf die wir uns für die nächsten fünf bis zehn Jahre einstellen müssen.

Prof. Thielmann:

Vielen Dank, Herr Staatssekretär Otto. Gibt es dazu Kommentare? Herr Büttgen als Datenschutzbeauftragter?

Herr Büttgen, BfDI, Bonn:

Die aktuelle öffentliche Debatte über die datenschutzrechtlichen Aspekte von Smart Meter freut mich als Datenschützer sehr. Das intelligente Stromnetz ist noch nicht implementiert und doch wird schon jetzt über den Datenschutz bei Smart Meter diskutiert. Bislang kannte ich das anders. Die Datenschützer wurden in der Regel erst dann gerufen, wenn etwas schief gegangen war. Wurden dann datenschutzfreundliche Techniken und Verfahren eingefordert, hieß es stereotyp: Das ist zu teuer; das macht unser Geschäftsmodell kaputt. Daher ist Privacy by Design ein Ansatz, bei dem alle gewinnen. Privacy by Design bedeutet, dass datenschutzrechtliche Voraussetzungen bereits in der Planungsphase berücksichtigt werden und damit integraler Teil der Projektkonzeption sind. Insofern gebührt dem Bundeswirtschaftsministerium Dank, das bereits bei der Novellierung des Energiewirtschaftsgesetzes, d.h. in der Planungsphase von Smart Meter, in § 21g Energiewirtschaftsgesetz Datenschutzregelungen formuliert hat. Natürlich werden weitere Schritte folgen müssen. Dies betrifft die entsprechende Datenschutzrechtverordnung nach § 21i Energiewirtschaftsgesetz sowie die Technische Richtlinie und das Schutzprofil für das Smart Meter, die beide vom Bundesamt für Sicherheit in der Informationstechnik erarbeitet werden.

Zur Diskussion über das Schutzprofil folgende Anmerkung. Wir sprechen immer von dem Schutzprofil des Smart Meter. Die datenschutzrechtlich entscheidende Komponente des Schutzprofils ist das im Smart Meter integrierte Gateway, das die Kommunikation des intelligenten Stromzählers nach außen zu den Marktteilnehmern steuert. Das Schutzprofil sieht vor, dass das Gateway auch die Tarifierung der verbrauchten Energie durchführt. Aufgrund dieser Funktionalität wird eine Vielzahl von Daten durch das Smart Meter selber verarbeitet,

so dass diese Dritten gegenüber nicht preisgegeben werden. Dieses Modell der dezentralen Datenverarbeitung entspricht datenschutzrechtlichen Forderungen. Ein zentrales Billing durch Dritte sollte vermieden werden, da jede Datenübermittlung das Fehler- und Missbrauchsrisiko erhöht. Natürlich bedeutet das nicht, dass Daten nicht zu den vertraglich festgelegten Zwecken verarbeitet werden dürfen. Dies gilt letztendlich auch für die Verbrauchsdaten der Energienutzer. Aber das Beispiel Holland zeigt, dass ein angemessener Datenschutz gerade im Bereich Smart Meter notwendig ist. In Holland ist die Einführung von Smart Meter nämlich bislang aufgrund massiver Datenschutzproteste gescheitert. Für die Akzeptanz einer intelligenten Stromversorgung ist es aber auch wichtig, dass der Verbraucher für sich einen Mehrwert in der neuen Technologie erkennt. Ich glaube, dass es weniger um Einsparpotentiale beim Einzelnen geht. Wir machen das Licht auch ohne Smart Meter aus, wenn wir es nicht zum Lesen brauchen und wenn wir schlafen gehen. Ob ich wirklich aufstehe und meine Wäsche wasche, wenn der Strom nachts billiger ist, wage ich zu bezweifeln. Wichtig ist, dass das Stromnetz durch die Einführung von Smart Meter zu einem Smart Grid optimiert wird. Wenn das Netz kostengünstiger gefahren wird, führt dies letztlich auch zu wirtschaftlich positiven Effekten beim Energienutzer. Der Datenschutz ist beim Thema Smart Meter sehr gut aufgestellt. Wir haben zwar noch nicht die Rechtsverordnung nach § 21i Energiewirtschaftsgesetz, hoffen aber auf angemessene datenschutzrechtliche Regelungen. Wir wissen aber auch, dass der Markt andere Ideen hat. So wird etwa für die so genannte Home Automation geworben, zum Beispiel für den Kühlschrank, der selber Lebensmittel ordert, wenn etwas fehlt. Die weitere Entwicklung kann in Ruhe abgewartet werden. Wichtig ist, dass, wie Herr Staatssekretär Otto auch sagte, der Nutzer selber, also derjenige, der seine Daten preisgibt, der Herr seiner Daten ist und dies durch die abgeschlossenen Verträge und die rechtlichen Regelungen sichergestellt wird.

Prof. Thielmann:

Vielen Dank, Herr Büttgen, jetzt Herr Merz bitte!

Herr Merz:

Ich möchte noch einmal kurz eine Analogie zum Mobilfunk machen: Warum ist der Mobilfunk weltweit erfolgreich gewesen und warum kann man heute mit seinem Mobiltelefon in jedem Land telefonieren? Weil es eine globale Standardisierung gab, aus der sich die Hersteller wie auch die Anwender zusammengefunden haben. Man hat einen gemeinsamen Standard geschaffen welche den Datenschutz wie auch die Verschlüsselung beinhaltet. Ich glaube, dass wir hier auch so etwas Ähnliches bräuchten, wenn wir hier erfolgreich sein wollen. Zuerst im bereits angefangenen Deutschland, dann in Europa und zuletzt auf der ganzen Welt. Und wie wir schon richtig sagten, wäre der Wunsch an die Politik, einheitliche Datenschutzrichtlinien. Zwar nicht einzeln für jedes Bundesland, aber einheitlich für Deutschland.

Dr. Klumpp:

Vielleicht kann man in der Tat sagen: weil wir hinsichtlich der Zukunft nicht so recht wissen, was kommen wird, dass wir in diesem Kreis unter den Fachleuten in spätestens 1 ½ Jahren einen Kompromiss haben werden, schätze ich. Aber viel länger können wir das, was wir diskutieren und gemeinsam wollen, nicht vor einem höchsten Richter offiziell geheim halten. Irgendwann bekommt das einer offiziell mit, und von da an wissen wir ziemlich genau, was passieren wird. Die Linie ist seit Jahrzehnten berechenbar. Das Bundesverfassungsgericht wird schlichtweg das, was wir als Kompromiss aushandeln, verbieten. Es dauert dann ziemlich genau 1 ½ Jahre, bis das durchgelaufen ist. Das heißt - von heute an gerechnet - können wir nur noch optimistisch vier Jahre lang unsere Modelle machen. Dann wird es sowieso verboten und dann können wir in der Sache wieder rückwärts gehen.

Staatssekretär Otto:

Nein, nein, lieber Herr Klumpp, ich freue mich, dass es die große Allianz des Bundeswirtschaftsministeriums mit dem Datenschutzbeauftragten jetzt offensichtlich gibt. Ich glaube, dass das Bundesverfassungsgericht gar nicht so realitätsfern und gar nicht so strikt urteilt, wie Sie das befürchten. Wer das Urteil zur Vorratsdatenspeicherung richtig liest – und ich empfehle Ihnen das zu tun –, der wird feststellen, dass es hier sehr differenzierte Überlegungen gab, die auch nachvollziehbar sind. Der Grundgedanke muss sein, dass man sozusagen als unbescholtener Bürger, wie Sie sagen, Herr über seine Daten sein muss und das man bestimmen muss, in welchem Umfang man diese herausgibt. Wir haben uns gerade darüber unterhalten, dass man bei Facebook und StudiVZ usw. über alles Mögliche, z.B. Trink- und Sexualvorlieben, sich freundlichst offenbart, aber gleichzeitig von Google Street View verlangt, dass die Hausfassade verpixelt werden soll. Das sind komische Dinge, aber immerhin eine individuelle Entscheidung, die zu treffen ist. Ich bin nicht so pessimistisch. Offensichtlich gibt es Nachsteuerungsbedarf nach meinem ersten Redebeitrag. Wenn man den Menschen klarmacht, dass sie einen gewissen Datensatz liefern, der anonymisiert ist und sie damit Energie sparen können, werden viele Bürgerinnen und Bürger das so machen. Und das Bundesverfassungsgericht wird uns nicht in die Quere kommen.

Wenn wir uns aber – und das war die Frage zum Handlungsbedarf von Prof. Picot – auf den irrsinnigen Gedanken begeben würden, durch Gesetz das Energiesparen zu regeln und zu bestimmen, dass jede Nutzerin und jeder Nutzer seine Datensätze an einen Netzbetreiber, einen Energieversorger oder wer auch immer die Akteure in diesem Feld sind, geben muss, dann werden wir scheitern.

Das heißt, wir haben ein hohes Maß an Überzeugungsarbeit zu leisten. Deswegen bin ich mit dem Datenschutzbeauftragten völlig einer Meinung, dass wir es uns nicht so leicht machen können. Die Politik soll entscheiden, soll Gesetze machen und dann werden Datensätze einfach rübergeschoben – so wird das nicht laufen. Das scheitert an verfassungsrechtlichen Gründen, aber, lieber Herr Dr. Klumpp, wir scheitern nicht an verfassungsschutzrechtlichen Gründen, wenn wir die Verbraucher aufklären. Wir scheitern nicht daran, wenn wir in einer Aufklärungskampagne sagen, dass man die und die Vorteile hat, wenn man die und die Datensätze liefert, Datensätze, die nicht sehr individuelle Daten enthalten, letztlich geht es nicht um sexuelle Vorlieben oder Trinkgewohnheiten.

Dr. Klumpp:

Waschmaschinenverhalten bestimmter Gruppen?

Staatssekretär Otto:

...auch da, lieber Herr Klumpp, Waschmaschinenverhalten. Ist es wirklich ehrabschneidend, wenn herauskommt, dass ich meine Waschmaschine in der Nacht laufen lasse, wenn der Strom billiger ist als tagsüber um 12 Uhr? Bei der Diskussion um Google Street View hatte ich manchmal das Gefühl, dass die Diskussion völlig abgehoben ist.

Dr. Klumpp:

Beim Energieverhalten können wir nicht mit Terrorprävention argumentieren, zumindest kein entsprechendes Verhalten am Verbrauch ablesen. Das war mein Punkt. Wohingegen wir Energieverbrauchsdaten sehr wohl brauchen können, wäre gezielte Werbung bis hin zur Kontrolle der „ecologic correctness“ eines Bewohners. Wollen wir das?

Staatssekretär Otto:

Also, Sie sehen, meine Damen und Herren, dass wir hier bei wirklich komplexen Diskussionen angekommen sind. Ich will es vereinfachen und klarstellen. Die Erwartungen an die Politik, dass sie durch Verordnungen oder Gesetze die Bürger dazu verpflichtet, bestimmte

Datensätze aus ihren Smart Meter, aus ihrem privaten Bereich an einen Dienstleister welcher Art auch immer preiszugeben haben: Vergessen Sie diese Überlegung! Egal, wer an der Regierung ist. Das wird nicht gehen. Da fehlt die Akzeptanz der Bürger und das wäre auch mit dem Bundesverfassungsgericht nicht zu machen. Da ist der Bundesdatenschutzbeauftragte wahrscheinlich auch völlig meiner Meinung.

Deswegen müssen wir uns beim Energiesystem der Zukunft darauf konzentrieren, bestimmte technische Vorgaben für Smart Meter zu setzen, damit das funktioniert, damit das System stabil dargestellt ist. Ob aber letztendlich ein Smart Meter dann im optimalen Sinne genutzt wird, dass der Strom nachts fließt für Waschmaschinen, die Gefrierbox usw., wird nicht laufen, wenn der Verbraucher sagt, dass er das nicht will.

Darauf, und das ist meine persönliche Einschätzung und Erwartung aus langjährigen Diskussionen, sollten Sie sich nicht einstellen. Wenn das Businessmodell nur so läuft, dass Sie darauf setzen, dass der Gesetzgeber die Verbraucherinnen und Verbraucher dazu verpflichtet, alles abzuliefern, wird das nicht passieren. Aber ich bin nicht so pessimistisch, um das noch einmal zusammenzufassen, dass uns bei einer freiwilligen Preisgabe von zentralen Datensätzen in einem Smart Grid der Zukunft das Verfassungsgericht in die Quere kommt. Es verlangt nur, dass jeder Verbraucher Herr über seine eigenen Daten ist, und wenn das nicht alle tun, dann ist es unsere gemeinsame Aufgabe, die Menschen davon zu überzeugen, dass sie im ökonomischen und energiepolitischen Sinne etwas Richtiges tun, wenn sie die Datensätze liefern, um dieses System zum Laufen zu bringen.

Prof. Thielmann:

Vielen Dank. Wir haben jetzt vier Wortmeldungen. Bitte sehr!

Herr Jähn:

Ich fasse mich ganz kurz. Wer sich mit Reiseberichten und historischen Reiseführern beschäftigt, stößt irgendwann auf Berichte, da gab es noch keine Fotos. Ich würde vorschlagen, die Fotos in den Pässen wieder zu verbieten, denn da kann man die Leute erkennen. Das ist ja datenschutzmäßig eigentlich völlig daneben.

Aber meine andere Anregung für die Runde hier. Ich habe sehr viel mit jungen Leuten zu tun und wenn ich mit denen Datenschutz und Facebook diskutiere, erscheint die Meinung, dass es Missbräuche in allen Bereichen gibt, man kann auch Fotos missbrauchen. Ich glaube, dass wir künftig bei solchen Diskussionen junge Leute mit einladen sollten, die diese Themen sehr kritisch sehen und vielleicht völlig andere Sichtweise mit reinbringen, weil ich glaube, dass wir da schlichtweg schief liegen.

Prof. Eckert:

Ich möchte eine ganz andere Thematik anschnitten. Vorhin hatten Sie, Herr Mayer, im Fachkongress ganz zum Schluss diese Frage hochgebracht. Ich möchte das gern in der Runde noch einmal aufgreifen. Wir sprechen viel über Smart Meter, und wir waren eigentlich heute Nachmittag da stehengeblieben, dass Smart Meter wichtig sind, aber worauf es wirklich ankommt, sind die kritischen Infrastrukturen, um die Versorgungssicherheit zu gewährleisten.

Meine Frage: Wie sieht die Politik das? Gibt es hier einen Handlungsbedarf, Prozesse zu regulieren, Vorschriften zu machen, so dass beispielsweise gewisse Komponenten und Netzbereiche redundant auszulegen sind, um einen notwendigen Grad an Robustheit zu garantieren? Dies hätte ja auch alle Nachwirkungen und Auswirkungen finanzieller Art.

Schlicht die Frage: Kritische Infrastrukturen sind das Herz der Smart Grids. Da müssen wir IKT sicher, robust, verlässlich etablieren. Gibt es Überlegungen, Anregungen, Vorstellungen, hier von Seiten der Politik Vorgaben zu machen?

Staatssekretär Otto:

Sie haben ein sehr wichtiges Thema angesprochen. Ein Thema, dessen Bedeutung in Zeiten der Vernetzung dramatisch zunehmen wird. Wir haben viele kritische Infrastrukturen und wir müssen in der Tat dafür sorgen, denn das ist Lebensnerv unseres Wohlstandes und unserer Sicherheit, dass wir kritische Infrastrukturen stabil auslegen, Redundanzen schaffen, uns vor Manipulationen weitestgehend bewahren.

Die Frage ist, ob das alles durch Gesetz erfolgen muss. Die Erwartung an die Politik ist immer: macht ein Gesetz! Sobald ein Problem entsteht, fordern viele Menschen ein Gesetz. Das kennen Sie.

Ich glaube, dass wir sehr viel besser daran tun, kritische Infrastrukturen durch Selbstregulierungen, durch Selbstverpflichtungen usw. zu sichern, weil das viel wirksamer ist und viel flexibler, viel schneller reagiert. Aber eines muss gewährleistet sein. Wenn das existentiell notwendige Infrastrukturen sind, muss der Staat gewährleisten, dass die Regeln, die dort gesetzt worden sind, auf welchem Wege auch immer, durch staatliche oder Selbstregulierung oder Vereinbarung eingehalten werden müssen. Es gibt viele Modelle. Manche Modelle funktionieren schon. Bei manchen tasten wir uns noch vor. Aber die Regeln müssen eingehalten werden. Es ist wie bei Europa. Die tollsten Regeln, wie der Maastricht-Vertrag, helfen nichts, wenn sie später bei der ersten kritischen Gelegenheit beiseitegelegt werden.

Wir laufen in ein Zeitalter, ein Jahrzehnt, ein Jahrhundert vielleicht, der Vernetzung hinaus. Das erlaubt es einzelnen Menschen, die vielleicht ökonomisch oder politisch oder kriminell negative Absichten haben, ein Volk, eine Volkswirtschaft oder wenigstens Teile davon lahmzulegen. Deswegen müssen wir uns wirklich in diesem Bereich sehr gut überlegen, wie wir – Sie haben Redundanzen, Abschirmungen genannt – Regeln setzen.

Nur diese Regeln müssen, und das will ich ganz klar erwidern, nicht immer staatlicher Art sein. Die Einhaltung muss von einer Instanz gewährleistet sein, die das dann auch durchsetzen kann. Wenn also die Regeln nicht eingehalten werden und das Energiesystem, das Datensystem, das Telekommunikationssystem, das Transportsystem usw. nicht ausreichend geschützt sind, muss der Staat eingreifen.

In meinen Überlegungen habe ich eher die Bitte oder die Anregung, auch an den Münchner Kreis und an andere, sich Gedanken zu machen, wie wir hier zu verbindlichen Regeln kommen, die flexibel sind, die angepasst werden, State of the Art, wir es aber trotzdem schaffen, dass nicht irgendwelche ökonomischen Einzelinteressen oder wettbewerblichen Einzelinteressen oder noch schlimmer kriminelle Einzelinteressen ein ganzes System aufs Spiel setzen können.

Beim Energiesystem ist es so, ich erwähnte vorhin das Stichwort Versorgungssicherheit, dass eine Nanosekunde Unterbrechung in unserer Volkswirtschaft bereits Schäden, die in das Gigantische gehen, bedeuten kann. Wir müssen eine absolut lückenlose Versorgung im Energiebereich und Informationsbereich haben. Das Problem haben viele noch gar nicht erkannt, dass Sie an einer einzigen Stelle nur einen Teil herausbrechen müssen, beispielsweise bei der Informationsverarbeitung, bei den IKT-Strukturen, und die gesamte Energieversorgung eines Landes kann gestört werden oder teilweise zusammenbrechen.

Wenn wir hier über das Thema Sicherheit und Datenschutz bei Smart Energy reden, muss Ihnen bewusst sein, dass wir zwei kritische Infrastrukturen zusammenfassen, vernetzen, d.h. die Gefahren werden noch größer. Das ist vielleicht, lieber Herr Picot, eines der nächsten Themen: Wie setzen wir überhaupt die Regeln, Sicherheit und Datenschutz, die heute diskutiert worden sind, später durch? Es ist nicht nur die Frage, wer die Regeln setzt. Auch privat gesetzte Regeln, Vereinbarungen, Selbstverpflichtungen usw. müssen konsequent durchgesetzt werden. Und da sehe ich eher die Aufgabe des Staates, dann später das zu gewährleisten.

Ich bin als Liberaler eher der Meinung, dass wir uns bei der Gesetzgebung zurückhalten sollten, weil die Gesetzgebung vielen politischen Opportunitäten, vielen faulen Kompromissen folgt und, ich bin selbstkritisch, viel zu langsam ist. Wir müssen schneller reagieren

können und deswegen müssen die Beteiligten der Energiebranche und der IKT-Branche sich sehr schnell zusammentun und zur Sicherung der Systeme Selbstregulierungsinstanzen und Regeln aufsetzen.

Herr Uhl, Deutsche Wolke:

Ich wollte noch etwas sagen zum Thema Bereitschaft, (Verbrauchs-)Daten zur Verfügung zu stellen. Wer in diesem Raum nimmt an keiner der vielen angebotenen Bonusprogramme teil, die wir als Konsumenten ständig angeboten bekommen? Man wird häufig gefragt: „Sammeln Sie Punkte?“ Meist sage ich dann: „Nein, Privatsphäre“. An der Kasse einer Drogeriemarktkette zieht man damit meist nur fragende Blicke auf sich. Aus meiner Sicht ist es also eine Frage der Anreize. Wenn Sie den Leuten klar machen, dass es sinnvoll und notwendig ist, anonymisiert Verbrauchsdaten ins Netz zu geben, werden diese bereit sein es auch zu tun. Sind Sie beispielsweise mit einem Auto unterwegs, so sind Sie froh, wenn Sie Staumeldungen bekommen. Auch hier werden Sie irgendwie erfasst, egal durch wen. Das ist hoffentlich noch anonym. Wenn Sie heute unterwegs sind, müssen Sie Daten freigeben, damit Sie auch von Staumeldungen profitieren können. Wenn Sie also an der Möglichkeit Energiekosten sparen zu können, teilnehmen wollen, müssen Sie Daten über sich und Ihre Verbräuche freigeben. Besonders aus der Ecke Deutschlands (Baden- Württemberg), aus der ich komme, geben manche Leute noch ganz andere Dinge frei, nur um irgendwo etwas zu sparen. Die Transparenz, was mit den Verbrauchsdaten geschieht ist hier entscheidend. Das können Sie sowohl einer Jugend klar machen als auch der Seniorität. Ich habe beispielsweise auch meinen Vater nach einiger Diskussion davon überzeugen können, dass er auf eine alternative Energieversorgung umsteigt, obwohl er Atomenergie eigentlich befürwortet hat, nachdem er die Chancen einer alternativen Energieversorgung für Deutschland verstanden hatte.

Prof. Tenbohlen:

Ich möchte noch einmal etwas zu diesen Weltuntergangsszenarien sagen, die hier hervorgerufen durch das Versagen der IKT hinsichtlich unserer Energieversorgung aufgezeigt werden. Das Netz wird stabil gehalten durch eine Leistungsfrequenzregelung. Am Erzeuger wird dabei die Frequenz gemessen und demnach die einzuspeisende Leistung geregelt. In diesen Prozess greift die hier diskutierte IKT nicht ein. Dementsprechend sehe ich dieses Szenario nicht, dass IKT das Netz zum Zusammenbrechen bringen würde.

Eine zweite Sache, die ich zum Thema Smart Meter sagen wollte. Hier wird häufig davon geredet, dass ich durch die Beeinflussung der Kühlschränke oder auch der Waschmaschine eine Steuerung der Last entsprechend der Erzeugung erreichen kann. Wenn wir einen durchschnittlichen Haushalt nehmen mit 3650 KWh im Jahr, das durch die 365 Tage teilen, kommen wir auf 10 KWh am Tag Verbrauch. Was würden Sie schätzen, wie viel Sie davon beeinflussen können? Vielleicht 1KWh Last. Das entspricht Stromkosten von ca. 23 Cent. Daraus ein Geschäftsmodell zu machen, wird nicht ganz einfach werden. Die Strompreise mögen steigen. Aber damit daraus ein Geschäftsmodell werden könnte, dürfte ein Anstieg um eine Größenordnung also Faktor 10 notwendig sein. Ich glaube, dass die Politik das ja wohl nicht haben möchte.

Man könnte vielleicht andererseits postulieren, dass die Lastbeeinflussung im Haushalt netzgetrieben ist, d. h. diese Lastbeeinflussung ist notwendig, um die Netzstabilität zu gewährleisten. Jetzt frage ich Sie, ob Sie von einem Energieversorgungsnetz versorgt werden möchten, das davon abhängt, dass die Waschmaschinen nachts laufen? Ich glaube, hinsichtlich der Versorgungsqualität kann das doch wohl nicht unser Ziel sein.

Dies stellt sich etwas anders dar, wenn ich die Elektromobilität zusätzlich betrachte. Dort habe ich deutlich mehr steuerbare Leistung und auch Energie, die nachgeladen werden muss. Da ist das Lastverschiebungspotential um etwa den Faktor 10 größer. Wenn Sie 50 km am Tag fahren, haben Sie 10 KWh, die Sie an Energie brauchen beim Nachladen in der Nacht.

Da könnte sich Lastbeeinflussung lohnen. Aber nicht für den normalen privaten Haushalt ohne große Verbraucher. Da wird sich Lastbeeinflussung durch Smart Meter nicht wirtschaftlich darstellen lassen.

Staatssekretär Otto:

Die erste Bemerkung: jede Steuerung der Übertragungs- und der Verteilnetze ist heute schon eine große IKT-Leistung. Gehen Sie zu den großen Übertragungsnetzunternehmen. Die haben Rechner ohne Ende. Wir sind jetzt schon da drin. Was Sie aus fachkundiger Sicht sagen, machen wir in dem Bereich, ist schon sehr weit IKT.

Zum zweiten: Ja, die Berechnungen sind mir nicht unbekannt. Das ist natürlich ein sehr zentraler Punkt. Wie weit schaffen wir es, sozusagen durch intelligente Verbrauchssteuerung, Spitzen abzufangen? Sie haben selber E-Mobility, also Elektrofahrzeuge, angesprochen und ich sage Ihnen, dass der Bereich der Heizung und Energieversorgung in Privathaushalten und vor allen Dingen im gewerblichen Bereich, die erhebliche Nachfrager sind, wenn wir es nicht schaffen, dass bestimmte Energiebedarfsspitzen abzudecken, haben wir richtig ein Problem. Deswegen mag es sein, dass Ihre Berechnung eine intelligente Bemerkung ist und wir das Problem allein mit der Waschmaschine nicht hinbekommen.

Aber wir müssen unser Energiesystem in der Tat so umbauen, um die Energiebedarfe etwas zu glätten. Wir laufen jetzt in ein Zeitalter, in dem es nicht mehr so leicht möglich ist, Spitzen hoch und runter zu fahren. Und das ist unser gesellschaftlicher Wille. Es ist nicht unbedingt meiner, um das ganz klar zu sagen. Aber 80% der Bevölkerung wollen erneuerbare Energien, wollen die Kernenergie loswerden. Dann müssen wir konsequent auch unser Leben und unsere Bedarfsanforderungen umstellen. Deswegen bitte ich Sie, die Verbraucher und uns alle nicht zu demotivieren mit Ihren Berechnungen mit den 23 Cent. Das ist der derzeitige Stand der Dinge. Wir werden uns in der Tat Systeme überlegen müssen, Connecting Home usw., intelligente Systeme sowohl in privaten Haushalten im Wohnen als auch vor allen Dingen im gewerblichen Bereich, um die Energiebedarfe glätten zu können. Das ist meine dringende Bitte auch an Sie. Wenn Sie überall in der Welt jetzt herumgehen und sagen, dass wir wegen 23 Cent eine Energiewende und Smart Grid machen, wird das natürlich scheitern. Deswegen habe ich mich herausgefordert gefühlt, bei dieser Gelegenheit auch Sie zu bitten, darüber nachzudenken, wie wir unsere Energiebedarfe in intelligenterer Weise als nur durch die Steuerung der Waschmaschine glätten.

Prof. Thielmann:

Vielen Dank. Ich möchte bitten, dass wir in der nächsten Stunde die Diskussion doch auf das Thema Sicherheit und Datenschutz fokussieren.

Prof. Krcmar wird jetzt übernehmen.

Prof. Krcmar:

Ich denke, dass wir jetzt einen Diskussionsblock machen, der sich dediziert um Fragen Schutzprofil, Risikomanagement, Risikoabwägungen kümmern kann, wenn es denn Fragen gibt. Frau Eckert bitte!

Prof. Eckert:

Eigentlich weniger eine Frage als noch einmal eine Anmerkung. Ich will eine Lanze für das Protection Profile brechen. Das Protection Profile hat ja nicht den Anspruch, eine Schutzarchitektur für Smart Grid zu sein, wie auch Herr Kowalski das vorhin sagte, sondern es soll eine Vorgabe für eine Komponente sein. Es wird definiert: was soll die Komponente leisten, was sind die Annahmen an die Umgebung?

Ihr schönes Bildchen mit dem Tor im Nirgendwo – natürlich müssen wir mehr tun und die Architekturen definieren, und wir müssen irgendwo anfangen. Ich denke, dass das Protection

Profile für den Smart Meter ein guter Anfang ist, und das sollten wir uns nicht nehmen lassen. Wir sollten – und der Redebeitrag gerade eben hat mir sehr gut gefallen – das weiter treiben, standardisieren und jetzt nicht nachlassen.

Prof. Krcmar:

Vielen Dank, Frau Eckert. Im Sinne einer lastabhängigen Regelung hat sich jetzt Herr Habel gemeldet.

Herr Habel:

Wir brauchen als Städte und Gemeinden im Bereich Sicherheit und Datenschutz bei Smart Energy schnell Klarheit. Das ist ganz wichtig, weil wir Kommunen diejenigen sind, die die Energiewende mit den Bürgern zusammen umsetzen müssen. Das werden wir nur schaffen, wenn wir in diese Technologie auch hineingehen, die wir heute hier dargestellt haben. Wenn wir hier zu zögerlich sind, wird uns das nicht gelingen.

Die Kommunen haben drei Funktionen. Sie sind Energieerzeuger, Energieverteiler und Energieverbraucher. Allein für Strom geben wir 2,6 Mrd. € pro Jahr aus. Wenn ich an die öffentliche Infrastruktur denke, die wir managen und verantworten müssen, so sind dies 176.000 öffentliche Gebäude, davon 50.000 Schulen, 40.000 Kindergärten, 10.000 Bibliotheken, 10.000 Rathäuser, etwa 800 kommunale Krankenhäuser, 1.400 Stadtwerke und 700 Rechenzentren und 9,6 Millionen Straßenlampen. Warum erwähne ich die Straßenlampen? Weil wir diese Straßenlampen bis zum Jahre 2020 komplett auf LED umstellen werden, Energieersparnis etwa 70%. Diese neue Technik können wir auch für Sicherheitsmaßnahmen nutzen, weil wir damit Farbspektren in der Beleuchtung verändern können. Die Stadt Langen im Norden Deutschlands ist die erste Stadt in Europa, die komplett auf LEDs bei den Straßenlampen umgestellt hat.

Weil diese gesamte Abwicklung ziemlich kompliziert ist, möchte ich mich noch einmal stark machen für eine Energy Cloud. In einer solchen Cloud können Stadtwerke und kleine oder mittlere Kommunen auch alle Sicherheits- und Smart Energy Maßnahmen abwickeln, damit wir nicht wieder parzellenhaft in allen Städten Deutschlands dieses Thema angehen, sondern hier gemeinsam auch mit Unternehmen kooperieren. Wir brauchen die Unternehmen auch als Technologiepartner, weil die Energiewende nur mit einer neuen Zusammenarbeit der großen Energieversorger, die ich ausdrücklich mit einbeziehe, der Technologiepartner, der Kommunen und der Bürger umzusetzen ist.

Prof. Krcmar:

Herr Habel, ganz herzlichen Dank für die klare Ansage und für das uns ins Gedächtnis rufen der großen Zahlen, die sich hinter diesem netten Statement „Die Kommunen“ verbergen. Jetzt gehen wir ein bisschen mehr in IT hinein, und ich habe Herrn Mayer vom OFFIS da.

Dr. Mayer, OFFIS

(Der Text des Statements ist unter Ziffer 12.3 abgedruckt)

Prof. Krcmar:

Herr Mayer, ganz herzlichen Dank. Sie haben fast zum Abschluss noch einmal einen ganzen Strauß an neuen Themen aufgeworfen. Üblicherweise ist es so, dass wir mit Ladies first beginnen. Hier machen wir es gerade anders herum. Frau Straube von T-Systems International bekommt die Aufgabe, den Vorschluss zu machen, bevor Arnold Picot die nette Aufgabe bekommt, das alles zusammenzufassen. Frau Straube!

Frau Straube

(Der Text des Statements ist unter Ziffer 12.5 abgedruckt)

Prof. Krcmar:

Frau Straube, auch Ihnen ganz herzlichen Dank. Es wird Ihnen so ähnlich gegangen sein wie mir, dass Sie nämlich eine ganze Menge neuer Aspekte mitgenommen haben. Wer dachte, dass unter dem Thema Sicherheit und Datenschutz nur Sicherheit und Datenschutz betrachtet werden, hat sich bei den gehörten Statements getäuscht. Wir haben vom Gartentürchen bis zum Kundennutzen ein großes Feld gestreift. Wir haben Transformationsbedingungen gehört, was als erstes, was als letztes. Eines ist offenbar geworden: die Fragen, wer ist Kunde, was ist der Wert beim Kunden und wie will die Organisation Geld verdienen, sind noch nicht alle beantwortet. Das Finden der letzten Antworten ist jetzt die Aufgabe von Arnold Picot, der die Gesamtzusammenfassung aller Themen nochmals vornimmt.

22 Schlusswort

Prof. Dr. Arnold Picot, Ludwig-Maximilians-Universität

Meine sehr verehrten Damen und Herren, herzlichen Dank an Sie alle, dass Sie aufmerksam ausgeharrt und mitdiskutiert haben. Sie haben damit bewiesen, dass diese Thematik wichtig und prioritär, aber auch vielschichtig ist und dass es nicht ratsam ist, sehr simple Antworten auf die vielen relevanten Fragen zu geben, dass aber Orientierung möglich ist, um die nächsten Schritte gehen zu können. In der Tat sind schon viele Schritte eingeleitet worden, sei es vom Gesetzgeber, sei es bei den praktischen Entwicklungen, sei es bei den Geschäftskonzepten, sei es bei den Pilotversuchen im Feld. Wir stehen also keineswegs bei null, aber es ist ein komplexer Prozess und ein nicht kurzer Weg, der zu gehen ist.

Ich fand die Diskussionen des heutigen Abends außerordentlich interessant. Einige teils überraschende Dinge sind wichtig. Natürlich muss man die Sicherheitsthematik als eine integrale Komponente eines funktionierenden Systems sehen; das wussten die meisten von uns bereits. Aber dass man dabei zum Teil überraschende Wege prüfen muss, die verstopft werden müssen, damit nicht irgendetwas passiert, was wir alle nicht wollen, das wurde heute deutlich angesprochen. Ich glaube, dass noch viel Kreativität und Lernprozesse erforderlich sind, damit man als Anwender, als Nutzer, nicht über die Sicherheit erst im Nachhinein, wenn etwas passiert ist, nachzudenken beginnt, sondern von Anfang an vertrauensvoll mit diesen Infrastrukturen arbeiten kann. Unsere Industrie- und Dienstleistungsgesellschaft tut das auf anderen Feldern, etwa der Luft- und Raumfahrt auch, und das sollte auch auf dem von uns diskutierten Feld selbstverständlich sein.

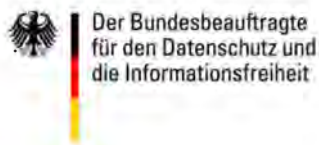
Ich glaube, dass unsere Diskussion in gewisser Weise paradigmatisch ist. Denn dies ist nicht der einzige Bereich in unserer Gesellschaft, in dem solche Konstellationen auftreten, wo kritische Infrastrukturen mit verschiedensten Dienstleistern, Anbietern und Nutzern sowie unglaublichen Datenmengen zu tun haben. Ich bin sehr dankbar, dass Sie noch einmal herausgestellt haben, welche enorme Herausforderungen in Bezug auf die Datenvolumina und deren Bewältigung entstehen. In solchen Konstellationen treten verschiedenste Interessenten und Akteure mit neuen Ideen auf, die mit diesen Daten arbeiten wollen. Politik und Gesellschaft sind herausgefordert, wie sie damit umgehen wollen und können.

Diese Veranstaltung war sicherlich nicht die letzte zu diesem großen Themenkreis. Wir werden das fortsetzen, vermutlich mit stärker spezialisierten Themenzuschnitten. Denn man wird nicht immer die ganze Breite behandeln können, wie wir das heute den ganzen Tag lang und am Abend getan haben.

Anhang

Statement zu Aspekte und Handlungsbedarf bei Sicherheit, Datenschutz und Verbraucherschutz

Statement von Herrn Peter Böttgen



Berliner Gespräch

Berlin, d. 29.09.2011

Smart Meter und Datenschutz

Die Sicherstellung einer nachhaltigen Energieversorgung stellt ein wichtiges energiepolitisches Ziel Deutschlands dar. Smart Metering ist Grundvoraussetzung für eine Ressourcen schonende, umweltfreundliche und effiziente Produktion, Verteilung und Nutzung von Energie. Hierfür sind neue Tarife, wie etwa lastvariable Tarife und Zeitzonentarife, erforderlich.

Eine effiziente Energieverteilung und Energiennutzung darf aber nicht mit datenschutzrechtlichen Kollateralschäden einhergehen.

Datenschutzgefahren von Smart Metering machen sich an der anfallenden Datenmenge fest. Heute wird 1 x Jahr und künftig (bei einem viertelstündlichen Messrhythmus) 35.040 x Jahr „Strom abgelesen“.

Der Detaillierungsgrad der Daten birgt ebenfalls datenschutzrechtliche Risiken. Die Möglichkeit von differenzierten und engmaschigen Nutzungs- und Verhaltensprofilen in den Haushalten schafft ein großes Ausforschungspotenzial. Ein gläserner Energiekunde bzw. -nutzer muss vermieden werden.

Datenschutzrechtlich problematisch stellen sich auch die neuen Rollen bei Energienutzung, Lieferung und Abrechnung dar. Neue Akteure bedeuten, dass mehr personenbezogene Daten als bisher verarbeitet und genutzt werden. Damit steigt das Fehler- und Missbrauchsrisiko.

Anforderungen für Datenschutz und Datensicherheit:

- Bereichsspezifische gesetzliche Datenschutzregelungen
- Strikte Zweckbindung der anfallenden Daten
- Nutzung personenbezogener Daten nur soweit erforderlich
- Grundsatz der Datensparsamkeit
- Transparente Information über die Datenverarbeitungstatbestände
- Datenhoheit beim Verbraucher (z.B. bei Fernmessen und Fernwartung)
- Dezentrale Datenhaltung
- Wahlfreiheit für datenschutzfreundliche Tarife
- Vertraulichkeit und Manipulationssicherheit der Messeinrichtungen
- Verschlüsselung der Daten

Statements der Marktteilnehmer / Internationale Aktivitäten

Statement von Herrn Stephan Gerhager, E.ON Energie AG, München

Informationssicherheit im zukünftigen Smart Grid

Informationssicherheit ist keine Technologie sondern ein Prozess.

Zukünftige Smart Meter könnten eine zentrale Rolle in den Kommunikationsbeziehungen zwischen den Kunden (Internet), dem „Smart Home“ und den „Smart Grids“ spielen. Aus diesem Grund werden diese Geräte ein interessantes Ziel für die unterschiedlichsten Gruppen von Angreifern darstellen.

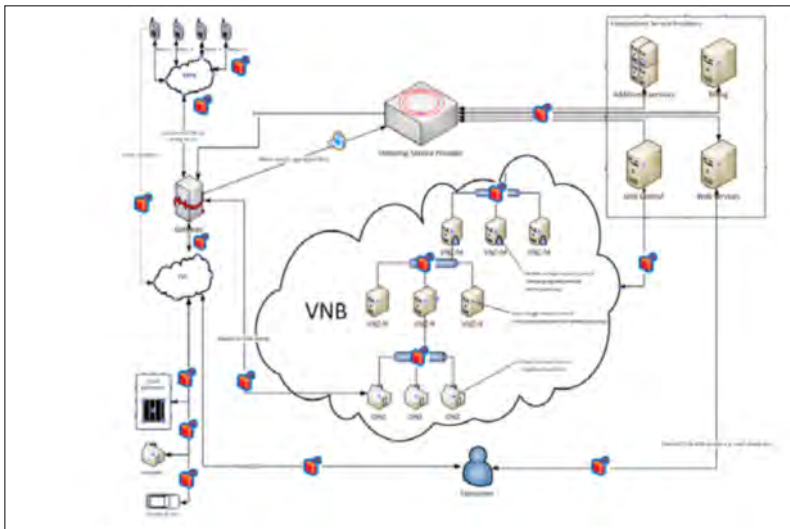
Lassen Sie uns gemeinsam ein zukünftiges Smart Grid aus der Sicht eines Angreifers sehen:

- Was hätte ein Angreifer davon einen Smart Meter anzugreifen?
- Welche Gruppen von Angreifern hätten ein Interesse daran?
- Welche Möglichkeiten stehen diesen Gruppen zur Verfügung?
- Auch Angreifer betreiben ein Risikomanagement und suchen danach Ihre Angriffsszenarien aus.

Wozu also eine sichere Smart Meter / Smart Grid Architektur?

Die neuen Informationsrisiken und Bedrohungen, die mit der Kopplung der o.g. „Welten“ entstehen, können nicht ausschließlich auf der technischen Ebene z.B. von Geräten identifiziert werden. Vielmehr muss ein Modell mit allen beteiligten Rollen definiert werden und darin die verschiedenen Prozesse (bestehend wie neue) abgebildet werden.

Erst wenn das Modell mit allen notwendigen Prozessen definiert ist, können darin die sensiblen Informationen und Prozesse identifiziert werden und darauf bekannte Angriffsszenarien gespiegelt werden. Danach müssen diese mit einer durchgängigen Sicherheitsarchitektur minimiert, sowie verbleibenden Restrisiken dokumentiert werden.



Wird zuerst eine technische Vorgabe für ein einzelnes Gerät erstellt, so kann diese richtig, je nach Angriffsvariante aber auch falsch sein. Für uns Sicherheitsexperten stellt dies ein unlösbares Problem dar. Ich lade Sie ein, dies in der Diskussion in einem gemeinsamen Experiment zu verifizieren.

Statement von Herrn Thomas Koelzer und Herrn Steffen Heyde, secunet Security Networks AG

IT-Sicherheit und Datenschutz im Smart Grid

1 Smart Grid – Zukunft der Stromwirtschaft mit Sicherheit

Die Stromversorgung steht vor völlig neuen Herausforderungen: Der fortschreitende Klimawandel, die Liberalisierung der Energiemärkte und der politisch gewollte Ausstieg aus der Atomenergie machen einen tiefgreifenden Umbau der Elektrizitätsinfrastruktur innerhalb der nächsten Jahre erforderlich.

Als Konsequenz wird die Stromerzeugung aus regenerativen Energiequellen – Wind, Photovoltaik, Wasserkraft, Bioenergie und anderen erneuerbaren Energieträgern – massiv ausgebaut. Wurde Strom in Deutschland bislang zentral in rund 300 Kraftwerken produziert und in Richtung der Verbraucher verteilt, so wird er künftig verstärkt aus regenerativen Energieträgern an einer Vielzahl von Standorten – also dezentral – erzeugt. Dezentrale Erzeugung bedeutet aber auch eine komplexere Verteilung. Für diese Anforderungen sind die heutigen Stromnetze nicht ausgelegt. Auch der weitere Ausbau von großen On/Offshore Windparks mit hohen Leistungskapazitäten lässt die Infrastruktur zunehmend an ihre Leistungsgrenzen stoßen. Zu Spitzenzeiten sind die Netze bereits heute „verstopft“, regenerativ erzeugter Strom kann deshalb häufig nicht sinnvoll genutzt werden.

2 Voraussetzung: Lastausgleich im Stromnetz

Die Erzeugungsleistungen erneuerbarer Energien sind nicht konstant. In der Regel sind sie von Wetter, Wind und Sonne abhängig. Eine Hauptaufgabe wird also sein, einen Lastausgleich im Stromnetz zu schaffen und die Versorgungssicherheit zu gewährleisten. Zentrale und dezentrale Erzeugung müssen intelligent kombiniert werden. Die zahlreichen neuen Erzeuger müssen vollständig und effizient in das Stromnetz integriert werden. Dies kann nur gelingen, wenn Stromerzeuger, -verbraucher und -speicher sowie die für die Übertragung und Verteilung notwendige Infrastruktur unter Einhaltung einer hohen Versorgungssicherheit intelligent miteinander vernetzt werden. Ein Umbau der heutigen Netze ist nötig.

3 Die Netze müssen „intelligent“ werden

Das sogenannte Smart Grid – auch als Internet der Energie bezeichnet – wird die Zukunft unserer Energieversorgung bestimmen. Es wird Erzeugung, Transport, Speicherung, Verteilung und Verbrauch von Strom steuern und kontrollieren. Möglich wird das durch den verstärkten Einsatz von IT, insbesondere Technologien, die seit Jahren in der Kommunikations- und Datentechnik vielfältig und preiswert zur Verfügung stehen, wie beispielsweise das TCP/IP-Protokoll.

Intelligente, kommunikative Stromzähler, sogenannte Smart Meter sind Kernstücke des Smart Grids und werden auch in Privathaushalten Einzug halten. Sie ermöglichen die digitale Erfassung der Verbrauchsdaten und deren Übermittlung zur Abrechnung und Steuerung. Gleichzeitig werden über die Kommunikationsschnittstellen auch Tarifinformationen oder auch weitere Daten zur Steuerung von Verbrauchsgeschäften, aus dem Energienetz geladen. Die Steuerung des Energieflusses erfolgt maßgeblich auf Basis der durch die Smart Meter viertelstündlich übermittelten aktuellen Verbrauchsdaten. Durch diese Informationen wird die Lastenregelung vereinfacht, der Stromfluss gesteuert und ggf. die Stromerzeugung und die -verteilung möglichst genau an den Bedarf angepasst.

4 IT-Sicherheit macht Smart Grid möglich

Dreh- und Angelpunkt für das Gelingen dieses Umbruchs in der Stromwirtschaft ist die Einhaltung von Sicherheitsanforderungen. Dazu zählen die Sicherheit vor Angriffen auf die IT-Infrastruktur („Security“), die Betriebssicherheit („Safety“), aber auch die Datenschutzaspekte („Privacy“). Mit dem zunehmenden Einsatz von Informations- und Kommunikationstechnologie beim Smart Grid steigt auch die Verwundbarkeit. Künftig können über das IT-Netzwerk eine Vielzahl von Hackern bzw. Terroristen das Smart Grid auch aus der Ferne angreifen. Voraussetzung für Konzeption und sicheren Betrieb ist ein angemessenes hohes IT-Sicherheitsniveau, um beispielsweise Schutz vor

- Stromausfall;
- Manipulation der Tarifinformationen oder Zählerstände;
- Zahlungsausfällen aufgrund von fehlerhaften bzw. manipulierten Identitätszuweisungen;
- unberechtigter Abstreitbarkeit bei Rechnungsstellungen;
- Fehlsteuerungen des Stromflusses oder
- Missbrauch von Kunden- und Verbrauchsdaten zu etablieren.

Die Stromversorgung gilt aufgrund ihrer Bedeutung und überlebensnotwendigen Funktion für Bevölkerung und Wirtschaft als kritische Infrastruktur. Die unverzichtbare Kernfunktionalität der Versorgungssysteme muss auch in Krisenlagen („Graceful Degradation“) aufrechterhalten und Mechanismen zur schnellstmöglichen Wiederherstellung nach Totalausfällen (Schwarzstartfähigkeit) vorhanden sein. Dazu ist es notwendig, die einzelnen Netz-Teilstrukturen sehr widerstandsfähig zu konzipieren und aufrechtzuerhalten.

Es wird gefordert:

- Berücksichtigung von IT-Sicherheitsaspekten bereits in der Planungsphase
- Etablierung eines hohen bzw. teilweise sehr hohen Niveaus hinsichtlich der Sicherheitsziele im gesamten Smart Grid (Vertraulichkeit, Integrität, Authentizität, Nicht-Abstreitbarkeit, Verfügbarkeit, Verbindlichkeit, Zuverlässigkeit)
- Vorgaben von IT-Sicherheitsstandards durch Politik bzw. Gesetzgebung
- Überwachung der Umsetzung von Sicherheitsvorgaben
- Regelmäßige Prüfung und Anpassung der Sicherheitsvorgaben an geänderte Rahmenbedingungen
- Definition von Schutzprofilen und Zertifizierungsprozessen für kritische Komponenten
- Aufbau und Nutzung von vertrauenswürdigen Sicherheitsinfrastrukturen und Dienstleistungen
- Angemessene Notfall-/Krisen- und Business Continuity-Konzepte und der Nachweis der Umsetzbarkeit dieser Konzepte

5 Datenschutz vermeidet gläsernen Kunden

Mit der Einführung des Smart Grids in der Energiewirtschaft werden große Mengen unterschiedlicher Energiedaten auf verschiedenen Aggregationsstufen erzeugt und übertragen. Das Schädlichkeitspotenzial bzgl. personenbezogener Daten in einem nicht ausreichend gesicherten Smart Grid ist außerordentlich hoch.

Datenschutz muss deswegen – und auch wegen der hohen Sensibilität und des Misstrauens der Verbraucher – ausdrücklich eine hohe Priorität in der Konzeption und Umsetzung des Smart Grids haben. Vertrauliche Kommunikation zwischen Endkunden und ihren Dienstleistern sowie rechtssichere elektronische Transaktionsmechanismen müssen von vornherein konzipiert und umgesetzt werden. Einmal aufgetretene Fehler und die daraus entstehende Ablehnung machen eine nachträgliche Implementierung unter Umständen nicht mehr möglich oder aufwändig und teuer. Erst eine klare und transparente gesetzliche Regelung von

Zugriffsrechten und -beschränkungen sowohl für Daten aus Mess- und Verbrauchseinheiten als auch für den steuernden Zugriff auf Erzeuger und Verbraucher kann die notwendige Akzeptanz für diese neuen Technologien schaffen. Wenn nötig, ist das Datenschutzgesetz in diesem neuen Umfeld entsprechend anzupassen. In diesem Sinne ist IT-Sicherheit eine Voraussetzung für den Aufbau und Betrieb eines von allen Beteiligten akzeptierten Smart Grids.

Es wird gefordert:

- Klare und transparente Regelungen zu Zugriffsrechten auf Daten aus Mess- und Verbrauchseinheiten in Smart Grids
- Praxisnahe Datenschutzvorgaben und datenschutzkonformes Design des Smart Grids

6 Akzeptanz braucht Vertrauen und Sicherheit

Jedes neue Thema oder Großprojekt erfordert, dass alle Beteiligten frühzeitig „mitgenommen“ bzw. über Änderungen und deren Auswirkungen sachlich und neutral informiert werden. Innerhalb der Gesellschaft muss ein breiter Konsens über die Notwendigkeit zur Realisierung des neuen Projektes geschaffen werden. Die Diskussion um den Kraftstoff E10 hat gezeigt, dass die Integration neuer Lösungen in existierenden Märkten durchaus mit Problemen einhergehen kann.

Die Akzeptanz in der Bevölkerung steht und fällt auch mit der Sicherheit der Netze und auch dem Schutz der anfallenden Verbrauchsdaten. Erforderlich ist eine offene Kommunikation mit allen Beteiligten – und das bereits während der Konzeption und Errichtung des Smart Grids. Neben den Chancen und Freiheiten, die Smart Grids bieten, dürfen die Risiken nicht außer Acht gelassen werden. Maßnahmen, die die Eintrittswahrscheinlichkeiten der Risiken reduzieren, müssen ergriffen werden und sich ergebende Restrisiken müssen plausibel, transparent und verständlich dargestellt werden.

Es wird gefordert:

- Offene Kommunikation über Chancen und Risiken sowie akzeptierte Restrisiken.

Statement von Andreas Kießling, MVV Energie AG, Mannheim

Informationssicherheit als Basis von Versorgungssicherheit und Nutzerakzeptanz im Smart Grid

Neue Anforderungen führen zur Vernetzung

Um die ökologischen und energiepolitischen Ziele umzusetzen, wird ein zügiger Ausbau Erneuerbarer Energien sowie die Steigerung der Energieeffizienz benötigt. Dabei muss das schwankende Angebot Erneuerbarer Energien sowie die dezentrale Erzeugung integriert und berücksichtigt werden, um im Gesamtenergiesystem langfristig Atom- und Kohlekraftwerke zu ersetzen. Dafür wird im Vergleich zur gegenwärtigen Situation eine höhere Flexibilität von Erzeugung und Verbrauch benötigt, die mit dynamischer Leistungssteuerung, Energiespeichern auf allen Netzebenen, integrierten Energiesystemen aus Elektrizität, Wärme und Gas sowie zellularen, robusten Systemen erreicht werden soll. Um dies voranzubringen, werden intelligent gesteuerte Energienetze (Smart Grids) sowie intelligente Messsysteme (Smart Metering) benötigt, die bei sehr unterschiedlichen Anforderungen und Akteuren aber nicht zwingend die gleichen Kommunikationseinrichtungen nutzen müssen.

Diese Netzwerke funktionieren als territorial organisierte und sich selbst ausgleichende Einheiten mit Strom-, Gas- und Wärmeerzeugern, Energiespeichern und Energienutzern. Die Netzwerke berücksichtigen im Strombereich gleichzeitig die regionale Situation wie auch Vorgänge in anderen Regionen - wie zentrale Quellen, beispielsweise als offshore-Windparks. Dies ermöglicht die Nutzung regionaler Chancen durch Kommunen, aber auch die Beteiligung am Nutzen der neuen Systeme durch alle Bürger.

Dafür ist das bisherige Energieversorgungssystem auf der letzten Meile im Niederspannungsbereich bis hin in die Objekte der Kunden mit einem Energieinformationssystem aus Kommunikationssystem und Automatisierungssystem zu verbinden. Es entwickelt sich das intelligente Energieversorgungssystem (Smart Grid) als Netzwerk aller Komponenten mit mehr Informationen über Erzeugung und Verbäuche.

Datenschutz grundlegend sichern

Mit diesen Informationen sind aber Datenschutz und Informationssicherheit nicht nur in Deutschland sondern international zunehmend ein wichtiges Akzeptanzkriterium. Die Möglichkeit, Daten ohne Zustimmung des Energieproduzenten/Energieabnehmers (Prosumer) zu speichern und zu übertragen, muss schon in den Geräten bzw. im Design der Dienste und durch vorgegebene Standardeinstellungen ausgeschlossen werden. Weiterhin ist mit der Nutzung von Datenobjekten zugeordneten Datenschutzklassen Transparenz und strikte Einhaltung der Zweckbindung erforderlich, um die Nutzerrechte zu schützen.

Auf der Grundlage der Schutzklassen sollte nur der Vertragsnehmer von Energielieferanten und Energiedienstleistern durch vorgegebene Standardeinstellungen Zugriff auf personalisierte und haushaltsbezogene Daten haben. Darüber hinaus sollte die Möglichkeit bestehen, dass Prosumer bewusst und informiert jederzeit darüber entscheiden können, wer darüber hinaus in welcher Rolle und zu welchem Zweck Zugriff auf schützenswerte Daten hat.

Informationssicherheit und Verbraucherschutz (Ende-zu-Ende)

Informationssicherheit ist also eine entscheidende Grundlage bei der Vernetzung einer kritischen Infrastruktur und wird durch technische aber auch durch organisatorische Maßnahmen definiert, um die Erfassung, Nutzung, Verarbeitung, Speicherung, Übertragung und Löschung aller Informationen auf dem der einzelnen Datenschutzklasse und dem Dienst entsprechenden Niveau zu regeln. Anforderungen und Implementierungen gemäß Sicherheits-

niveau müssen nachhaltig auf den jeweils aktuellen Stand der Technik ein- und nachgeführt werden. Die Regulierung sollte deshalb bezüglich der Smart Grid Informationssicherheit die grundlegenden Anforderungen (primäre Schutzziele) definieren und Systemvorgaben machen.

Die Detaillierung der technischen Implementierung sollte aber auf Grundlage der durch die Regulierung definierten Rahmenbedingungen durch den Markt erfolgen. Es ist deshalb die falsche Richtung, im EnWG den steuernden Zugang zu Geräten und Anlagen allein mit dem BSI-Gateway für die Messeinrichtung zu verbinden, da hier massiv ein offener und wettbewerblicher Markt behindert wird, der die eigentliche Grundlage für die Entwicklung des Smart Grids ist. Dabei ist ebenso zu betonen, dass Funktionen im Smart Grid sowie im Bereich Smart Metering sehr unterschiedlichen Anforderungen bezüglich Echtzeitfähigkeit, Standards und Widerstandsfähigkeit genügen müssen. Ebenso führen detaillierte Festlegungen an die Ausstattung technischer Komponenten anstatt der Festlegung grundlegender Systemanforderungen zu geschlossenen Lösungen, die einer technologischen Offenheit und Zukunftsfähigkeit entgegenstehen.

Grundsätzlich kann der Sonderweg der Detaillierung einer technischen Implementierung mittels BSI-Gateway, technischer Richtlinie und Zertifizierung an der datenschutz- und eichrechtlich besonders kritischen Komponente des Meter Gateways bei alleinigem Fokus auf das Messen unterstützt werden. Dieser Weg läßt sich aber nicht auf die Gesamtheit der Komponenten für das Energiemanagement im Smart Grid über alle Systemdomänen und Handlungsebenen vom Feldprozessen bis zu zentralen Marktmechanismen übertragen. Aus diesem Grund wird empfohlen, zwar eine Schnittstelle für steuernde Mechanismen im Smart Meter Gateway verpflichtend vorzusehen, deren Nutzung aber allein dem Markt zu überlassen, um die Entwicklung eigenständiger marktgetriebener Energiemanagementsysteme ohne Bezug zu Smart Metering zuzulassen. Dies entspricht vollständig der europäischen Sicht, dass die Domänen Smart Grid und Smart Metering zwar überlappende Bereiche besitzen, aber nicht zwingend voneinander abhängen. Es gilt die Entwicklung eines offenen wettbewerblichen Marktes zuzulassen.

Deshalb wird der Weg zur Herstellung der Ende-zu-Ende-Sicherheit über die gesamten Prozessketten durch Spezifikation von Anwendungsfall-Ketten (Use Cases) und genutzten Datenobjekten mit verbundenen Datenschutzklassen und Sicherheitsniveaus empfohlen, womit dann jeweils Implementierungsvorschriften für den Markt definiert sind. Darüber hinaus sind übergeordnete Überwachungs- und Sofortmaßnahmen notwendig, um Fehlanwendungen und Missbräuche von Marktimplementierungen zu erkennen und abzuwehren.

Statement von Dr. Christoph Mayer, OFFIS, Oldenburg**These 1**

Ein gelungener Migrationsprozess hin zu Smart Grids bedarf der gelungenen Synchronisation vieler Handlungsfelder auch auf internationaler Ebene. Um diesen Prozess zu koordinieren, muss eine stimmige von allen Akteuren getragene Gesamtstrategie entwickelt und umgesetzt werden. Diese Strategie muss mindestens die nächsten zwei Jahrzehnte umfassen. Eine nationale Umsetzung muss sich am internationalen Vorgehen orientieren, auch um als Referenz für andere Länder dienen zu können und so den beteiligten Unternehmen Wettbewerbsvorteile zu verschaffen. Die Koordination benötigt eine nationale Smart Grids Initiative.

These 2

Das Dringende zuerst: Viele der wesentlichen Schritte müssen kurzfristig angegangen werden, um die Energiewende erfolgreich zu meistern. Die dringendsten Schritte sind der Aufbau einer Energieinformationsinfrastruktur, die Erarbeitung von Standards, die Ausstattung der Verteilnetze mit mehr Intelligenz und Automatisierung. Diese Maßnahmen helfen gleichzeitig im internationalen Wettbewerb. „Smart Meter“ spielen für die deutsche Energiewende in den ersten Schritten keine entscheidende Rolle und bergen eher die Gefahr von Investitionsruinen, u.a. durch die Konstruktion und Installation unflexibler oder nicht zukunftssicherer Konzepte. Da viele Länder hier bereits weiter fortgeschritten sind, ist eine Konzentration auf das Thema der Zähler kontraproduktiv, soweit dieser nicht kundengetrieben erfolgt.

These 3

Die Energiewende benötigt Netzbetreiber, die eine aktive gestalterische und innovative Rolle bei der Einführung von Smart Grids wahrnehmen wollen und dürfen. Dies ist auch nötig, um international eine führende Rolle einnehmen zu können. Die intelligente Koordination von Akteuren und Anlagen benötigt neben technologischen Innovationen auch neue Ideen bei der Regulierung. Die Versorgungssicherheit bleibt die Hauptaufgabe des nun intelligenten Verteilnetzes, ist nun aber auch zu interpretieren als Sicherheit im Sinne von Security und wird mit vielen neuen IKT-bezogenen Technologien unterstützt werden müssen.

Statement von Herrn Kai Paulssen, Bundesnetzagentur, Bonn

Abschichtung der Diskussion um die Energiezukunft durch „Smart Grid“ und „Smart Market“

Smart Grid ist ein *nicht genügend definierter Begriff* und bedarf der Klärung. Vorschlag BNetzA:

- Smart Grid = netz“interne“ Themen (intelligenter Netzausbau, Management von Netzkapazitäten, Netzzuständen, Netzsteuerung etc.)
- Smart Market = (verändertes) Nutzerverhalten durch Preise und Anreize im Bereich Energiemengenaustausch (z.B. Lastverlagerung von SLP-Kunden, Energiedienstleistungen, Energieeinsparung u.v.m.)
- Problem BNetzA: Definitionen zu ungenau, zu wenig rollenscharf
- Sorge: Unbundling-Aspekte finden zu geringe Berücksichtigung

Smart Meter sind ein Teil der Energiezukunft, nicht jedoch ihre Grundvoraussetzung

- primäre Aufgabe: Bereitstellung digitaler Daten und Weiterleitung an Berechtigte hochaufgelöste Daten für den Netzbetrieb nur in Ausnahmefällen erforderlich (z.B. problematische Stellen im Netz wie z.B. gewisse lokale Einspeisepunkte, kritische Strangpunkte im Verteilernetz)
- Daten sind die Basis für vielerlei Produkte und Dienstleistungen der Energiezukunft
- intelligente Einspeisezähler werden für die Marktintegration erneuerbarer Energie wichtig werden
- Schaffung von Verbraucherakzeptanz und damit verbundener aktiver Nutzung
 - es beteiligen sich die, die Smart Metering wollen...
 - das sind genau die, die das System auch nutzen...
 - ansonsten werden Smart Meter zu ungenutzten „Investitionsruinen“
- Der Hauptnutzen von Smart Metern liegt im Marktbereich (Smart Market-Komponente)
- Grundsatz für Effizienz: Es sollten nur diejenigen einen Smart Meter erhalten, die auch den Nutzen daraus ziehen wollen

Das Smart Grid entwickelt sich evolutionär, nicht revolutionär

Deutschland mit seinen über 800 Elektrizitätsnetzbetreibern wird nicht von heute auf morgen über intelligente Netze verfügen. Abgesehen davon, dass Übertragungsnetze heute schon „smart“ geführt werden, gibt es auch in einigen Verteilernetzen bereits jetzt einen großen Umbau druck, während in anderen Netzen überhaupt noch keine Notwendigkeiten für Veränderungen gesehen werden. Eine einheitliche Vorgehensweise ist aufgrund der unterschiedlichen Situationen in den 850 Verteilernetzen ineffizient.

Statement von Herrn Rajchowski, BDEW, Bonn

Aspekte und Handlungsbedarf zu Sicherheit, Datenschutz und Verbraucherschutz – Ausgangspunkt: Schutzprofile für Smart Meter“

Der BDEW bewertet die Einführung von intelligenten Messsystemen als wichtigen Beitrag zur Umsetzung von intelligenten Verteilernetzen. Sie bilden die Voraussetzungen, um die erneuerbaren Energien und dezentrale Erzeugungsanlagen noch stärker und effizienter zu integrieren. Zusätzlich ermöglichen intelligente Messsysteme, den Verbraucher für den effizienten Umgang mit Energie weiter zu sensibilisieren.

Die zentrale Zielstellung bei der Einführung muss es dabei sein kosteneffizient, die Messsysteme in die bestehenden Technologien der Marktteilnehmer, in die Marktprozesse und die Aufgaben der Marktrollen einzufügen.

Datenschutz und Datensicherheit bilden eine wichtige Voraussetzung. Die Unternehmen der Energiewirtschaft sind sich dessen bewusst. Schon vor über 10 Jahren vereinbarte die Branche Grundsätze und Empfehlungen für den sicheren Datenaustausch. Ebenfalls für den Einsatz elektronischer Haushaltzähler existiert seit einigen Jahren eine Brancheempfehlung. Sie orientiert sich streng am BDSG. Die Themen Datenschutz und Datensicherheit sind also mitnichten bisher unbeachtet.

Die Marktteilnehmer achten diese Empfehlungen. Passend zur Diskussion „Wer darf welche Daten sehen?“. Es darf nicht vergessen werden, dass jede Marktrolle zwingend ausgewählte Daten für die Erfüllung ihrer jeweiligen Aufgabe benötigt. Das EnWG sieht dafür gezielt Berechtigungen vor, diese müssen gestärkt werden und nicht durch Einwirkungsmöglichkeiten eingeschränkt. Diese bereichsspezifische Regelung ist für die Einführung neuer Messsysteme sehr wichtig. Eine einheitliche Erklärung der Landesdatenschützer zu diesem Thema lag und liegt leider nicht vor.

Der derzeitige Fokus auf den Datenschutz und die Datensicherheit führt leider dazu, dass wir das Ziel für diesen umfangreichen Umbau in den Verteilnetzen aus den Augen verlieren. Das Ziel ist die effizientere Integration der Erneuerbaren Energien. Prämisse muss dabei auch die Kosteneffizienz sein. Ein gangbarer Weg wäre es auch gewesen, im Vorfeld Handlungsbedarf zu identifizieren und die kosteneffizientesten Maßnahmen umzusetzen. Das EnWG sieht aber jetzt bereits umfangreiche Einbauverpflichtungen vor, die bei den Verteilnetz- und den Messstellenbetreibern zu erheblichen Aufwänden führen. Ein Treiber dafür, sind die Auswirkungen des Schutzprofils auf die Praxis der betroffenen Marktrollen.

Statement von Kerstin Straube, T-Systems International GmbH

Die Energienetze der Zukunft: Neue Herausforderungen für Datenschutz und Datensicherheit

Aus Verbrauchern werden „Prosumer“. Intelligente Stromnetze lassen den Anwender durch dezentrales Einspeisemanagement und neue Technologien zur echtzeitbasierten Verbrauchsmessung über seinen ehemals passiven Verbraucherstatus hinaus zum aktiven Energiemarktteilnehmer werden. Das heisst:

- Die Anzahl der aktiven Netzkomponenten vervielfacht sich und diese sind in der Fläche verteilt
- Im Rahmen von Smart Grids und Smart Metering werden Massendaten generiert, die Marktteilnehmer vor neue Herausforderungen stellen.

Kritische Infrastruktur und Daten müssen geschützt werden

- Zum einen geht es hier um den Schutz vor verheerenden Auswirkungen von Angriffen
 - Von außen („Hacking“, „Viren“, ...)
 - Von innen („Datenmanipulation“, ...)
- Zum anderen muss der Diebstahl sensibler Kundendaten verhindert werden

Prinzip Hoffnung gilt nicht – die Risiken sind real:

In einer neuen Studie des Allensbach Instituts wird deutlich, dass Datensicherheit und Datenschutz einen hohen Stellenwert sowohl für Endkunden als auch Unternehmen haben: Die Risiko-liste von Führungskräften wird durch drei IT-Sicherheitsrisiken angeführt: 1) Datenbetrug im Internet (67%), 2) Datenmissbrauch (64%), 3) Computerviren (59%).

Zwei Drittel Deutscher Unternehmen wurden bereits von IT-Attacken heimgesucht. Spätestens nach der Verbreitung des Stuxnet Virus ist klar, dass auch Energienetze angreifbar sind.

Trotzdem fehlen bei den heutigen Smart Grid Technologien eine ausreichende Sicherheitsarchitektur, oder es werden nur Teilaspekte beleuchtet. Power Line Communications (PLC) wird eingesetzt, obwohl hier alle Daten der Verbraucher unkontrolliert an die Konzentratoren außerhalb des Hauses gesendet werden, was aus Datenschutzsicht nicht dem Grundsatz der Datensparsamkeit entspricht.

Erfüllung höchster Sicherheitsanforderungen - auf Basis bewährter Standards

Auf Basis langjähriger Erfahrungen im IKT-Bereich, setzen wir auf eingeführte offene Standards, die ein hohes Maß an Sicherheit gewährleisten, und deren Umsetzung durch hohe Stückzahlen bezahlbar bleibt.

Dabei bauen wir auf ein Dreischichten-Modell mit Ende-zu-Ende Sicherheitsarchitektur:

- 1) Eigenständige Netze
- 2) Authentifizierung auf Basis von Zertifikaten zur Steuerung von Rechten & Rollen
- 3) Verschlüsselung der zu übertragenden Daten mit eindeutiger „Chain of Trust“, die ab dem Zeitpunkt der Installation nicht mehr unterbrochen wird

Die aktuelle Diskussion über Schutzprofile macht deutlich: Wir brauchen klare und verlässliche Rahmenbedingungen, die auch in der Praxis umsetzbar und bezahlbar bleiben, und internationale Gültigkeit erlangen können. Der Datenaustausch muss über eine sichere Kommunikationsinfrastruktur erfolgen, um Datensicherheit und Datenschutz für alle verbrauchsbezogenen und persönlichen Daten inkl. Nachweispflicht über Transport und Speicherort zu gewährleisten.

Liste der Referenten und Moderatoren

Dr. Andreas Breuer
RWE Deutschland AG
Leiter Neue Technologien/Projekte
Kruppstr. 5
45128 Essen
andreas.breuer@rwe.com

Prof. Dr. Dr. h.c. Manfred Broy
Technische Universität München
Institut für Informatik
Boltzmannstr. 3
85748 Garching
broy@in.tum.de

Ministerialrat Peter Büttgen
Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit (BfDI)
Leiter Referat IV
Husarenstr. 30
53117 Bonn
peter.buettgen@bfdi.bund.de

Prof. Dr.-Ing. Jörg Eberspächer
Technische Universität München
Lehrstuhl für Kommunikationsnetze
Arcisstr. 21
80333 München
joerg.eberspaecher@tum.de

Prof. Dr. Claudia Eckert
Institutsleiterin
Fraunhofer Institut AISEC
Parkring 4
85748 Garching
claudia.eckert@aisec.fraunhofer.de

Dirk Fox
Geschäftsführer
Secorvo Security Consulting GmbH
Ettlinger Str. 12-14
76137 Karlsruhe
dirk.fox@secorvo.de

Stephan Gerhager
Information Security Officer
E.ON Energie AG
Brienner Str. 40
80333 München
stephan.gerhager@eon-energie.com

Dr. Andreas Goerdeler
Leiter der Unterabteilung
Informationsgesellschaft; Medien
BMW
Scharnhorststr. 34-37
10115 Berlin
andreas.goerdeler@bmwi.bund.de

Dr. Peter Heuell
Vors. d. Geschäftsführung / CEO
Landis+Gyr GmbH
Humboldtstr. 64
90459 Nürnberg
peter.heuell@landisgyr.com

Steffen Heyde
Portfolio Manager
secunet Security Networks AG
GB Business Security
Alt-Moabit 91c
10559 Berlin
steffen.heyde@secunet.com

Prof. Dr. Gerrit Hornung
Lehrstuhl für Öffentliches Recht,
IT-Recht und Rechtsinformatik
Universität Passau
Innstr. 39
94032 Passau
gerrit.hornung@uni-passau.de

Dipl.-Phys. Andreas Kießling
MVV Energie AG
Technologie & Innovation
Luisenring 49
68159 Mannheim
andreas.kiessling@mvv.de

Alexander Kleemann
BMWi
Referat III B 1 Energierecht
Scharnhorststraße 34-37
10115 Berlin
alexander.kleemann@bmwi.bund.de

Bernd Kowalski
Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
bernd.kowalski@bsi.bund.de

Dr. Johann Kranz
Ludwig-Maximilians-Universität München
Institut für Information, Organisation und
Management
Ludwigstr. 28
80539 München
kranz@lmu.de

Prof. Dr. Helmut Krcmar
Technische Universität München
Lehrstuhl für Wirtschaftsinformatik
Boltzmannstr. 3
85748 Garching
krcmar@in.tum.de
Prof. em. Dr.-Ing. Dr. h.c. mult. Paul J. Kühn
Universität Stuttgart
IKR, Studiendekan Int. Studienprogramme
Pfaffenwaldring 47 - ETT II
70569 Stuttgart
paul.j.kuehn@ikr.uni-stuttgart.de

Prof. Dr. Wolf-Dieter Lukas
BMBF
Leiter Abt. Schlüsseltechnologien
Heinemannstr. 2
53175 Bonn
wolf-dieter.lukas@bmbf.bund.de

Dr. Christoph Mayer
Bereichsleiter FuE
OFFIS e.V.
Escherweg 2
26121 Oldenburg
christoph.mayer@offis.de

Herbert Merz
Mitglied des Vorstandes
Nokia Siemens Networks GmbH & Co. KG
St. Martin-Str. 76
81541 München
herbert.merz@nsn.com

Rolf Müller-Hermes
Head Center of Excellence Smart Energy
Detecon International GmbH
Oberkasseler Str. 2
53227 Bonn
Rolf.Mueller-Hermes@detecon.com

Christian Müller-Elschner
Younicos AG
Am Studio 16
12489 Berlin
mueller-elschner@younicos.com

Hans-Joachim Otto, MdB
Parlamentarischer Staatssekretär
BMWi
Scharnhorststr. 34-37
10115 Berlin
hans-joachim.otto@bundestag.de

Kai Paulssen
Bundesnetzagentur
Referent Energieregulierung
Tulpenfeld 4
53113 Bonn
kai.paulssen@bnetza.de

Prof. Dr. Dres. h.c. Arnold Picot
Ludwig-Maximilians-Universität
Institut für Information, Organisation
und Management
Ludwigstr. 28
80539 München
picot@lmu.de

Dr. Oliver Raabe
Karlsruher Institut für Technologie
Institut für Informations- und
Wirtschaftsrecht
Vincenz-Prießnitz-Str. 3
76131 Karlsruhe
raabe@kit.edu

Arne Rajchowski
Fachgebietsleiter Beschaffung, Logistik, IT
BDEW
Reinhardtstr. 32
10117 Berlin
arne.rajchowski@bdew.de

Prof. Dr. Dr. h.c. Ortwin Renn
Universität Stuttgart
Institut für Sozialwissenschaften
Abt. für Technik- und Umweltsoziologie
Seidenstr. 36
70174 Stuttgart
sekretariat.renn@sowi.uni-stuttgart.de

Martin Rost
Unabhängiges Landeszentrum
für Datenschutz (ULD)
Holstenstr. 98
24103 Kiel
ULD32@datenschutzzentrum.de

Kerstin Straube
T-Systems International GmbH
Strategic Market Energy
VP Technical Management -
End2End Smart Energy
Dingolfinger Str. 1-15
81673 München
Kerstin.Straube@t-systems.com

Prof. Dr. -Ing. Stefan Tenbohlen
Universität Stuttgart
Institut für Energieübertragung
und Hochspannungstechnik
Pfaffenwaldring 47
70569 Stuttgart
stefan.tenbohlen@ieh.uni-stuttgart.de

Prof. Dr.-Ing. Heinz Thielmann
Geschäftsführer
Emphasys GmbH
Eichenstr. 11
90562 Heroldsberg
heinz.thielmann@t-online.de

Michael Wedler
Projektleiter E-Energy
B.A.U.M. Consult GmbH
Gotzinger Str. 48/50
81371 München
m.wedler@baumgroup.de

Prof. Dr.-Ing. Ingo Wolff
Geschäftsführer
IMST GmbH
Carl-Friedrich-Gauß-Str. 2-4
47475 Kamp-Lintfort
wolff@imst.de

Peter Zoche M.A.
Fraunhofer-Institut für
System- und Innovationsforschung ISI
Breslauer Str. 48
76139 Karlsruhe
peter.zoche@isi.fraunhofer.de

