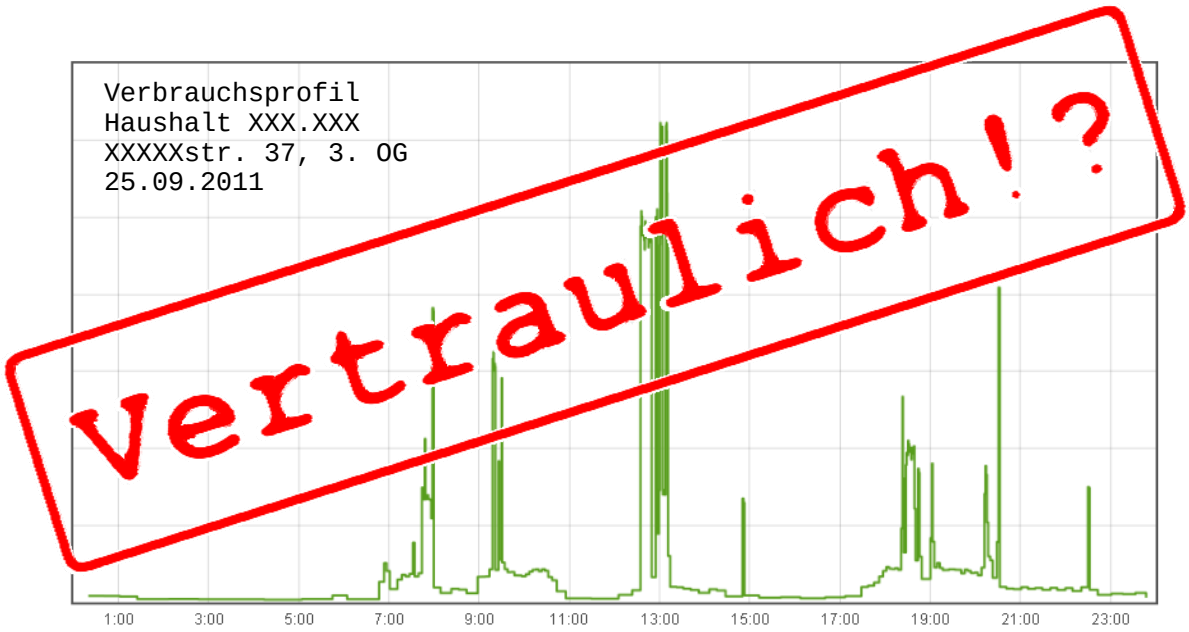
Alcatel-Lucent Stiftung für Kommunikations-forschung

Gestaltungslinien für Sicherheit und Datenschutz im Energieinformationsnetz

Dirk Fox, Katharina Fuchs, Gerrit Hornung, Dieter Klumpp, Johann Kranz, Christoph Krauß, Klaus J. Müller und Alexander Roßnagel



Alcatel-Lucent Stiftung

Impressum

Stiftungsreihe 94

Redaktion
Dr. Dieter Klumpp
(Leitung)
Petra Bonnet M.A.
Dirk Fox

Druck der Broschüre
DCC Kästl GmbH & Co. KG

Die Alcatel-Lucent Stiftung für Kommunikationsforschung ist eine nichtrechtsfähige Stiftung in der treuhänderischen Verwaltung des Stifterverbandes für die Deutsche Wissenschaft.

Angaben nach § 5 TMD/
§ 55 RfStv

Stifterverband für die Deutsche Wissenschaft e.V.
Barkhovenallee 1
45239 Essen
Telefon: (02 01) 8401-0
Telefax: (02 01) 8401-301
E-Mail: mail@stifterverband.de

Geschäftsführer:
Prof. Dr. Andreas Schlüter
(Generalsekretär)

ISSN 0932-156x

Gestaltungslinien für Sicherheit und Datenschutz im Energieinformationsnetz

Inhalt

Allianz von IT-Sicherheit und Datenschutz

Alexander Roßnagel

Energieinformationsnetze müssen sicher, aber auch datenschutzgerecht sein. Sie werden nur akzeptabel und akzeptiert sein, wenn sie die Schutzgüter der Beteiligten nicht gefährden, sondern schützen. Zu diesen Schutzgütern gehören nicht nur Gesundheit, Eigentum und Vermögen und letztlich die Funktionsfähigkeit der Gesellschaft, sondern auch die Freiheit persönlicher Entfaltung ohne Beobachtung und Datenverarbeitung durch Dritte. Diese Schutzpflichten können nicht aufgeteilt oder gegeneinander ausgespielt werden. Vielmehr ist es eine Aufgabe von Politik und Gesetzgebung, von Wirtschaft und Technik, künftige Energieinformationsnetz so zu gestalten, dass sie diese Schutzaufgaben gleichberechtigt und sich gegenseitig unterstützend gewährleisten.

Gestaltungsaufgaben

Klima- und Ressourcenschutz erfordern eine effiziente Erzeugung und Nutzung von Strom. Die Stromerzeugung muss weitgehend auf erneuerbare Energieträger übertragen werden, die jedoch in vielen Fällen ihre Energie nur diskontinuierlich erzeugen können. Zugleich muss der Stromverbrauch – möglichst ohne Komfortverlust – erheblich verringert und daher effizienter genutzt werden. Aus diesen Gründen müssen Stromerzeugung und Stromverbrauch stärker aufeinander abgestimmt werden, um unnötige Spitzen und Lücken zu vermeiden. Alle diese Maßnahmen setzen eine erheblich höhere Informationsdichte über die Stromerzeugung und den Stromverbrauch voraus und erfordern eine effiziente Steuerung beider. Hierfür sind Energieinformationsnetze, die über den notwendigen Informationsaustausch zur Stromerzeugung und zum Stromverbrauch sorgen, unabdingbar.

Mehr Informationen über die Erzeugung erneuerbarer Energien und die Nutzung elektrischer Energie führen unweigerlich zu mehr Informationen über den Nutzer, der oft Erzeuger und Verbraucher zugleich (neudeutsch: Prosumer) ist. Da jede Person und jeder Haushalt für sehr viele Tätigkeiten elektrischen Strom benötigen, sind diese Informationen je nach Informationsdichte sehr aussagekräftig und erlauben Rückschlüsse auf viele Handlungsvollzüge und – über die Zeit – auf viele Lebensgewohnheiten. Zu entscheiden, wer welche Informationen, in welchem Umfang und zu welchem Zweck haben soll, ist der Inhalt des Grundrechts auf informationelle Selbstbestimmung. Wenn Nutzerschutz in Energieinformationsnetzen gewährleistet werden soll, sind diese datenschutzgerecht zu gestalten und müssen Schutz vor unerwünschten Verbrauchs- und Lebensstilprofilen bieten.[1]

Neben dem Datenschutz ist aber auch die Datensicherheit in Energieinformationsnetzen essentiell. Dabei geht es nicht nur um die Sicherheit der Verbrauchs- und Abrechnungsdaten, die die Energieversorgungsunternehmen und die jeweils anderen Nutzer beunruhigen könnten, auch nicht nur um die Sicherheit vor dem Ausspähen von Stromverbrauchsdaten, sondern vor allem auch um die Sicherheit der Daten, die Versorgungssi-

[1] Ausführlicher zu den Datenschutzfragen eines Energieinformationsnetzes siehe z. B. *Roßnagel/Jandt*, Stiftungsreihe Nr. 88, 2010.

cherheit und Energieeffizienz sicherstellen sollen, und die Funktionsfähigkeit der Energieinformationsnetze insgesamt. Ein Ausfall des Energieinformationsnetzes hätte gravierende Folgen für die Energieversorgung der Nutzer, der Wirtschaft und der Verwaltung. Daher müssen zu deren Sicherheit Konzepte zur Gewährleistung von IT-Sicherheit in den Energieinformationsnetzen entwickelt und umgesetzt werden.

Gegenseitige Abhängigkeit

Datenschutz(recht) und IT-Sicherheit(stechnik) stehen aber nicht unverbunden nebeneinander. Datenschutz erfordert die Umsetzung von Datenschutzprinzipien durch technische Mechanismen der IT-Sicherheit. Und umgekehrt benötigt IT-Sicherheit verbindliche Sicherheitsanforderungen und rechtliche Rahmensetzungen, die IT-Sicherheit erst ermöglichen und zur Durchsetzung verhelfen. Schließlich dürfen Maßnahmen der IT-Sicherheit nicht gegen Datenschutzvorgaben verstoßen. Beide müssen nicht nur mit einander kompatibel sein, sondern sich gegenseitig unterstützen.

Diese allgemein zutreffende Erkenntnis gilt vor allem für die Gestaltung von Energieinformationsnetzen. Ihr ist auch der Gesetzgeber bei der jüngsten Novellierung des Energiewirtschaftsgesetzes (EnWG) durch das Gesetz zur „Neuregelung energiewirtschaftsrechtlicher Vorgaben“ vom 26. Juli 2011 gefolgt. Zur Gestaltung von Smart Meter und zur Vorbereitung von Smart Grids hat er unter anderem den bestehenden Rechtsrahmen für den Einsatz von Smart Meter durch miteinander verschränkte Regelungen zum Datenschutz und zur IT-Sicherheit ergänzt. Allerdings kann diese Novelle nur der erste Schritt sein, weil trotz eines richtigen Ansatzes noch viele Fragen offen und wichtige Gestaltungsvorschläge unberücksichtigt sind.

Wichtige Grundsätze der Zusammenarbeit zwischen Datenschutz(recht) und IT-Sicherheit(stechnik) müssen auch die Gestaltung künftiger Energieinformationsnetze bestimmen:

Datenschutz und IT-Sicherheit

In einem technikgeprägten Gegenstandsbereich wie Energieinformationsnetzen kann Datenschutz nur dann um- und durchgesetzt werden, wenn er in die Gestaltung der Technik Eingang findet. Dieser Datenschutz durch Technik ist in zwei Formen möglich, durch *Systemdatenschutz* und durch *Selbstdatenschutz*.

Systemdatenschutz soll durch Gestaltung der Datenverarbeitungssysteme vor allem erreichen, dass so wenig personenbezogene Daten wie möglich verarbeitet werden. Darüber hinaus kann Systemdatenschutz zur Umsetzung weiterer datenschutzrechtlicher Ziele wie der informationellen Gewaltenteilung oder der Transparenz und Kontrolleignung der Datenverarbeitung eingesetzt werden. Zum Systemdatenschutz gehören auch die Maßnahmen zur Datensicherheit wie Zugangs- und Verarbeitungskontrollen. Systemdatenschutz soll vor allem durch „Privacy by Design“ erreicht werden. Hersteller sollen Datenschutzfunktionen schon bei der Konzeption ihrer Systeme berücksichtigen – wie dies § 3a Satz 1 BDSG fordert. In einem Energieinformationsnetz betrifft dies zum Beispiel die Verteilung der Funktionen der Verbrauchsdatenerfassung und -verarbeitung sowie der Steuerung der Verbrauchsgeräte. Eine datensparsame Gestaltung der Technikkonzepte wird so viel wie möglich dieser Funktionen dezentral in den Endgeräten der Anschlussnutzer integrieren und so wenige Daten wie

möglich (nur hinsichtlich der Geräte oder gar Haushalte aggregierte personenbezogene Daten) so selten wie möglich (hinsichtlich der relevanten Zeitintervalle aggregierte Daten) an die Datenumgangsberechtigten übermitteln. Eine datenschutzgerechte Konzeption würde auf eine Übermittlung von personenbezogenen Daten – jedenfalls in engen Zeitintervallen – verzichten.

Selbstdatenschutz gibt dem Betroffenen eigene Instrumente in die Hand, damit dieser in der Lage ist, seine informationelle Selbstbestimmung selbst zu schützen. Selbstdatenschutz kann vor allem durch technische Möglichkeiten des anonymen und pseudonymen Handelns verbessert werden. Um Selbstdatenschutz zu ermöglichen, werden zunehmend „Privacy Enhancing Technologies“ entwickelt und angeboten. Auch durch Selbstdatenschutz kann der Grundsatz der Datensparsamkeit verwirklicht werden, wenn in Energieinformationsnetzen den Anschlussnutzern ermöglicht wird, Verbrauchsdaten anonym oder pseudonym zu übermitteln und gegen Ausspähung durch Verschlüsselung zu schützen.

IT-Sicherheit und Datenschutz

IT-Sicherheit wird durch Datenschutz(recht) unterstützt, indem ihr verbindliche Schutzziele (etwa Vertraulichkeit) und Sicherheitsanforderungen (etwa Ende-zu-Ende-Verschlüsselung) vorgegeben werden und ihre Ziele mit der Autorität des Rechts verpflichtend gemacht und mit den Instrumenten des Rechts durchgesetzt werden können. Zum Beispiel fordert § 21e Abs. 2 EnWG, dass Smart Meter Schutzprofilen und technischen Richtlinien genügen müssen, die technische Sicherheitsanforderungen enthalten.

Das Bundesverfassungsgericht hat in seinem Urteil zur Umsetzung der Vorratsdatenspeicherung vom 2. März 2010 festgestellt, dass das hohe Schutzbedürfnis der Telekommunikationsverkehrsdaten, aus denen über die Zeit Verhaltensprofile der Nutzer erstellt werden können, eine risikoadäquate Sicherung erfordern. Ihrem Risikopotenzial wird eine Speicherung der Daten nur dann gerecht, wenn sie einem besonders hohen und dynamischen Sicherheitsniveau entsprechend geschützt werden. Diese Anforderungen sind auf die sehr aussagekräftigen detaillierten Stromverbrauchsdaten zu übertragen. Um ihnen zu entsprechen, fordert der Gesetzgeber in § 21e Abs. 3 EnWG ausdrücklich ein dynamisches Niveau des technischen Datenschutzes: Alle an der Datenübermittlung beteiligten Stellen müssen dem jeweiligen, sich im Zeitablauf verschärfenden Stand der Technik entsprechende Maßnahmen zum Schutz der Datensicherheit, der Vertraulichkeit und Integrität der Daten sicherstellen.

IT-Sicherheit benötigt über die verpflichtende Vorgabe von Zielen hinaus aber auch geeignete Rahmenbedingungen, die eine Durchsetzung von IT-Sicherheitsanforderungen unterstützen. Solche geeigneten Rahmenbedingungen sind zum Beispiel Verfahren, die sicherstellen, dass die Umsetzung von Sicherheitsanforderungen erörtert, dokumentiert und kontrolliert wird. Dieser Zielsetzung entsprechend sieht etwa § 21e Abs. 4 EnWG vor, dass die Einhaltung der Schutzprofile für Smart Meter durch ein Zertifizierungsverfahren nachzuweisen, zu überprüfen und zu bestätigen ist. Anhand des Zertifikats können alle Interessierten sofort erkennen, das die vorgegebenen Sicherheitsanforderungen erfüllt sind.

Schließlich ist sicherzustellen, dass durch Maßnahmen der IT-Sicherheit Datenschutzanforderungen nicht verletzt werden, Datenschutz und IT-Sicherheit also kompatibel

sind. IT-Sicherheit setzt auch voraus, mögliche Angreifer zu überwachen und Schwachstellen im Sicherheitssystem zu erkennen. Dieses Ziel ist oft umso leichter zu erreichen, je mehr Daten über Nutzer vorliegen, die für Prognosen oder Analysen ausgewertet werden können.

Die Zielsetzung der Sicherheit muss jedoch mit der Zielsetzung des Freiheitsschutzes immer wieder abgeglichen und abgewogen werden. Sicherheit darf nicht dazu führen, dass sie selbst eines ihrer höchsten Schutzgüter gefährdet. Daher bedarf die Sicherheitsgewährleistung klarer und nachvollziehbarer Beschränkungen. Dementsprechend sollen die (sicherheits-)technischen Eigenschaften und Funktionalitäten von Messsystemen in der Rechtsverordnung gemäß § 21i Abs. 1 Nr. 4 EnWG ausdrücklich so geregelt werden, dass sie datenschutzgerecht sind.

Datenschutz und IT-Sicherheit dürfen nicht als Gegensätze gesehen werden, sondern sind sowohl normativ als auch praktisch aufeinander angewiesen. Nur in einer Allianz werden sie zu sicheren und datenschutzgerechten und damit akzeptablen und akzeptierten Energieinformationsnetzen beitragen.

Smart Grid-Legenden

Dirk Fox, Klaus J. Müller

Der zunehmende Anteil stark volatiler regenerativer Energiequellen im deutschen Strom-Mix, dessen Verfügbarkeit nur eingeschränkt zu prognostizieren und lediglich kurzfristig planbar ist, hat den Wunsch nach einer Steuerung des Verbrauchsverhaltens geweckt. Eine Smart Meter-Infrastruktur als Kernelement eines „intelligenten" Energieinformationsnetzes soll dies durch die Übermittlung von Verbrauchsdaten in relativ kurzen Zeitintervallen ermöglichen. Der Beitrag zeigt auf, das die für den Zweck einer Verbrauchssteuerung geforderte Verbrauchsdatenübermittlung – anders als vielfach postuliert – weder geeignet noch erforderlich ist, und nimmt eine Abschätzung des tatsächlichen Nutzens einer Verbrauchssteuerung vor.

Hintergrund

Elektrischer Strom hat sich in den vergangenen 150 Jahren zu einer überlebenswichtigen Ressource moderner Gesellschaften entwickelt. Daher sind besondere Anforderungen an eine Infrastruktur zu dessen überwiegend zentraler Erzeugung und zuverlässigen Verteilung zu stellen. Das gilt insbesondere deshalb, weil Strom – im Unterschied z. B. zu Wasser – bis heute zu vertretbaren Kosten nur in begrenztem Umfang gespeichert werden kann. Daher müssen die Einspeisung ins Stromnetz und der aktuelle Verbrauch einander jederzeit entsprechen. Der Stromverbrauch unterliegt dabei starken Schwankungen; Höchst- und Tiefstlast können im Tagesverlauf um mehr als 30 % differieren.[1]

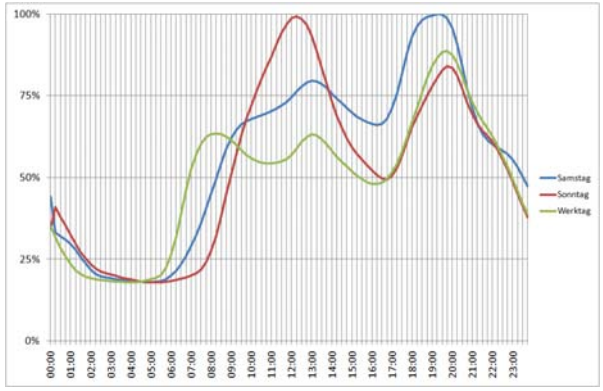


Abb. 1: Standard-Lastkurven Privathaushalte, „Wintertag" (Quelle: VDEW)

In der Praxis erfolgt die Steuerung des Stromnetzes bis heute weit überwiegend durch eine Steuerung der Einspeisung. Diese wird an die vor allem durch Tages- und Jahreszeit bedingten Verbrauchsschwankungen angepasst, indem bei Bedarf Spitzenlast-Kraftwerke zu der Grundlast-Leistung und den aktuellen Mittellast-Kraftwerken hinzugeschaltet werden. Grund- (bisher vor allem Kern- und Braunkohlekraftwerke) und Mittellast-Kraftwerke (vor allem Steinkohlekraftwerke) haben zum Teil sehr lange Anlaufzeiten, daher erfolgt die Einsatzplanung der Grund- und Mittellastkraftwerke sehr langfristig und orientiert sich an Standard-Lastkurven, mit denen die Nachfrage von In-

[1] Winter-Höchstlast am 13.12.2007: 78.500 MW; Quelle: BDEW, URL: http://www.bdew.de. Forschungsstelle für Energiewirtschaft e.V.: Demand Response in der Industrie. Dezember 2010, S. 24.

dustrie und Privathaushalten in Abhängigkeit von Wochentag, Jahres- und Tageszeit prognostiziert wird (siehe Abb. 1).

Mit der Zuschaltung von Spitzenlastkraftwerken wird sehr kurzfristig auf Lastspitzen reagiert. Dabei spielen vor allem Pumpspeicherkraftwerke eine zentrale Rolle, da diese innerhalb weniger Sekunden vom Speicher- in den Generatorbetrieb umgeschaltet werden können. Nach einigen Minuten können Gasturbinenkraftwerke die Leistung übernehmen. In Deutschland stehen Pumpspeicherkraftwerke mit einer installierten Leistung von 7.000 MW zur Verfügung; das entspricht knapp 9 % des Spitzenbedarfs und etwa 4,8 % der „Netto-Engpassleistung“ von ca. 145.000 MW aller Stromkraftwerke in Deutschland.

Schon heute stammen ca. 32 % dieser Leistung, etwa 45.000 MW, aus Wind- und Solarenergie[2], deren Erzeugung im Tagesverlauf stark schwankt. Ein Blick auf die Transparenz-Plattform der EEX[3] zeigt die Stärke der Schwankungen tagesaktuell: Bei starkem Wind und blauem Himmel stammen schon heute in den Sommermonaten bis zu 30.000 MW (fast 50 % des jahreszeitlichen Leistungsbedarfs) aus Windrädern und Photovoltaikanlagen (Abb. 2) – die aber innerhalb weniger Stunden auf unter 1.000 MW fallen können.

Ein großer Teil der Stromeinspeisung lässt sich somit schon heute nicht mehr steuern.

Diese Situation wird sich aus zwei Gründen noch deutlich verschärfen: Die im Kyoto-Protokoll (in Kraft seit 16.05.2005) vorgegebene CO_2-Reduktion in Deutschland um 21 % gegenüber 1990 bis zum Jahr 2012 wird zusammen mit dem beschlossenen Ausstieg aus der Kernenergienutzung zu einem erheblichen Verlust von Strom aus Grund- und Mittellastkraftwerken führen. Allein die Leistung der derzeit noch nicht abgeschalteten deutschen Kernkraftwerke summiert sich auf 12.700 MW[4]; 2009 lag der Beitrag der Kernenergie noch bei über 20.000 MW. Diese Leistung soll ersetzt werden durch Wind- und Solarstrom, deren Verfügbarkeit weder geplant noch gesteuert werden kann. Abgesehen von den vorgesehenen Off-Shore-Windkraftwerken leisten Wind- und Solarenergie daher weder einen Beitrag zur Grundlast noch können sie Mittel- oder Spitzenlastkraftwerke ersetzen.

Der Bau weiterer Spitzenlastkraftwerke, die kurzfristig auf Lastspitzen oder einen Abfall der eingespeisten Leistung (Windstille, Wolken) reagieren können, wird die Lücke wegen der langen Bauzeit, der geringen Zahl der geeigneten, aber noch ungenutzten Standorte und politischer Widerstände auf absehbare Zeit nicht füllen können. Hinzu kommt, dass Spitzenlastkraftwerke auf eine Nutzungsdauer von 4-8 Stunden ausgelegt sind – eine Windstille oder eine an Sonnenschein arme Zeit kann jedoch leicht länger andauern. Ein Ausbau der Gasturbinenkraftwerke würde wiederum den CO_2-Ausstoß erhöhen und könnte so die Einhaltung des Kyoto-Protokolls gefährden. Wenn man aber die Energieeinspeisung nur noch begrenzt steuern

[2] Stand: September 2010, Quelle: BDEW, URL: http://www.bdew.de; 27.214 MW installierte Windenergiekapazität (URL: http://www.wwindea.org/home/images/stories/pdfs/worldwindenergyreport2010_s.pdf) und 17.370 MW_p (Peak) installierte Photovoltaik-Nennleistung (URL: http://www.eurobserv-er.org/pdf/baro202.pdf); zusammen 44.580 MW.

[3] EEX-Transparenzplattform, URL: http://www.transparency.eex.com/de/

[4] Bundesamt für Strahlenschutz (BfS), URL: http://www.bfs.de/kerntechnik/ereignisse/standorte/karte_kw.html

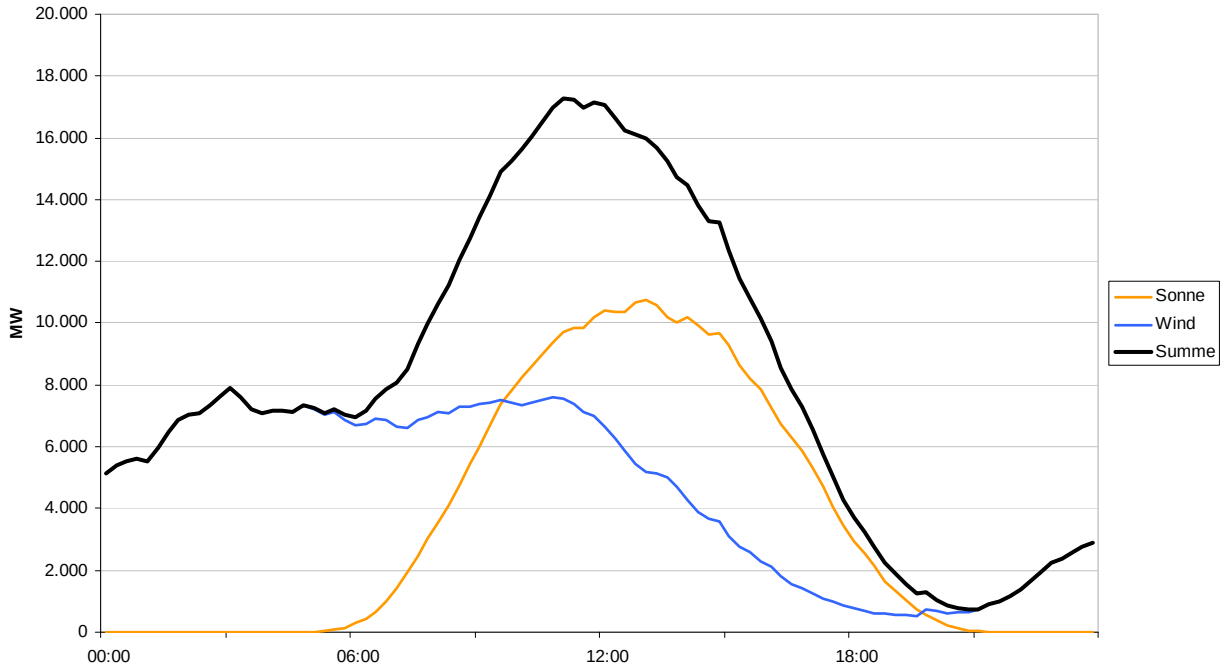


Abb. 2: Stromerzeugung aus regenerativen Energien am 17.06.2011 (Daten: EEX)

kann – was liegt da näher, als es mit der Steuerung des Verbrauchs zu versuchen?

In energieintensiven Branchen ist die Verschiebung von Lastspitzen im Tausch gegen vergünstigte Strompreise bereits üblich, und auch bei Privathaushalten gibt es mit Nachtstromtarifen und Nachtspeicherheizungen schon lange Mechanismen, die eine Lastverschiebung insbesondere auf die Nachtstunden bewirken – eine Tageszeit allerdings, in der Solarstrom gerade nicht zur Verfügung steht.

Zukünftig sollen lastvariable oder Tageszeit abhängige Tarife in Kombination mit einer verbesserten Transparenz des tatsächlichen Energieverbrauchs auch bei Privathaushalten eine gezieltere Verbrauchssteuerung ermöglichen. Zugleich soll eine Verbrauchsmessung in kürzeren Zeitintervallen die Prognosegenauigkeit der Bedarfsermittlung zur Steuerung der Grund- und Mittellastkraftwerke verbessern. Zu diesem Zweck wurden Smart Meter eingeführt – „intelligente“ Stromzähler, die die Verbrauchsentwicklung eines Haushalts anzeigen und die aktuellen Verbrauchswerte in regelmäßigen Zeitintervallen elektronisch an den Stromversorger oder einen Gerätebetreiber übermitteln können.

1 Lastverschiebung: Begrenzte Wirkung

Etwa 26 % des bundesweiten Stromverbrauchs in Höhe von jährlich 511,8 Mrd. kWh (2010)[2] entfällt auf 40,3 Millionen private Haushalte. Analysiert man das Verbrauchsprofil eines typischen Privathaushalts, so stellt man schnell fest, dass der überwiegende Teil des Verbrauchs der „Grundlast“ geschuldet ist und nur bei wenigen Großgeräten durch eine Verschiebung des Nutzungszeitraums ein nennenswerter Effekt entsteht. Denn bei Beleuchtung, Fernseher, Herd, Fön,

Toaster oder Kaffeemaschine kann man sicherlich durch verbrauchsärmere Geräte Strom einsparen; eine zeitliche Verlagerung der Nutzung ist jedoch unsinnig, da die Nutzung bedarfsgesteuert erfolgt.

Als potenzielle Kandidaten für eine (in der Strommenge nennenswerte) Verschiebung des Energieverbrauchs im Privathaushalt verbleiben im wesentlichen drei Haushaltsgeräte: Spülmaschine, Waschmaschine und Trockner (Abb. 3). Unter der (wenig realistischen) Annahme, dass es gelänge, bundesweit alle diese Verbraucher, auf die zusammen durchschnittlich etwa 20 % des Stromverbrauchs im Privathaushalt entfällt, aus Spitzenlast-Zeiten verschieben zu können, entspräche dies etwa 5,2 % der Gesamtenergiemenge.[5]

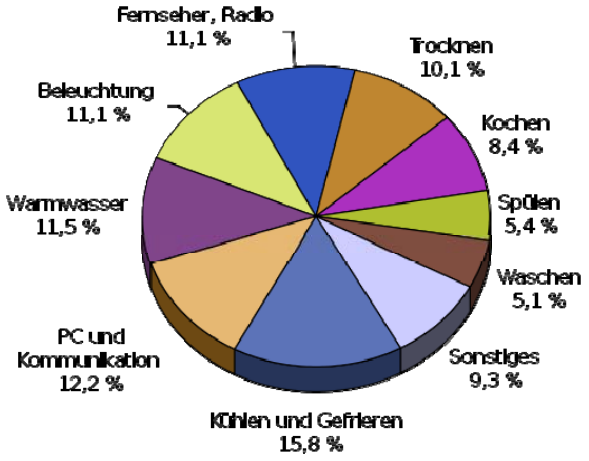


Abb. 3: Anteiliger Energieverbrauch der Haushaltsgeräte (Quelle: Energie-Agentur NRW)[6]

Realistisch dürfte – da sich die Nutzung der Geräte auf den Tagesverlauf verteilt und somit ein Teil der Geräte ohnehin in Last armen Zeiten betrieben wird – wohl eher ein deutlich niedrigerer Wert sein. Klobasa geht von ¼ aus [5], damit würde die Verschiebung deutlich weniger als 2 % der volatilen Stromeinspeisung aus Wind und Sonnenenergie ausgleichen können.[7]

Angesichts der Kosten einer Smart Grid-Infrastruktur ist das ein mageres Ergebnis: Stadtwerke kalkulieren derzeit mit Investitionskosten von 400 € je Gerät inklusive Einbau – bei einer angenommenen Geräte-Lebensdauer von (sehr optimistischen) zehn Jahren summiert sich allein dieser (vom Stromkunden zu finanzierende) Betrag auf über 1,6 Mrd. € – pro Jahr. Hinzu kommen die Investitions- und Betriebskosten des Stromversorgers sowie etwaige Mehrkosten für „Smart Grid-fähige“ neue Haushaltsgeräte.

Aber selbst wenn man auf dieses Lastverlagerungspotenzial setzen möchte: Für die Realisierung einer solchen Lastverschiebung ist – anders als vielerorts postuliert[8] – keineswegs eine Übermittlung der Verbrauchsdaten des Haushalts erforderlich. Selbst bei zeitabhängigen Tarifen genügt es, über eine Broadcast-Nachricht die aktuelle Tarifinformation an das Smart Meter zu übermitteln – und die Berechnung der Stromkosten dezentral im Smart Meter vorzunehmen [7].

---

5 *Klobasa* kommt in seiner Promotion [5] (auf der Grundlage von Zahlen aus dem Jahr 1999) zu einem etwas höheren Wert: Er bestimmt den Anteil der „verlagerbaren Energie“ an der Gesamtjahreserzeugung durch die Verschiebung von Waschmaschine, Wäschetrockner und Geschirrspüler auf 5,6% (S. 84).

6 Energieagentur NRW: Durchschnittlicher Anteil der Stromverbrauchsbereiche am Gesamtstromverbrauch, gemittelt über alle Haushaltsgrößen auf Basis von 28.242 Verbrauchsdatensätzen (3/2006). URL: http://www.ea-nrw.de/_database/_data/datainfopool/prozentuale_anteile_diagramm.pdf.pdf

7 Abhängen wird der tatsächliche Umfang der Lastverschiebung vor allem von dem angebotenen „Lastverlagerungsrabatt“: Bei einem Preis von lediglich etwa 0,22 € je kWh muss der Bonus zweifellos nennenswert sein, damit beispielsweise eine Familie mit Kindern das Spülen des Geschirrs oder das Waschen und Trocknen der Wäsche verschiebt.

8 So zunächst sogar Roßnagel/Jandt [10], S. 4; später in diesem Punkt zurückhaltender [11].

Statt einer Übermittlung des Zählerstands in festgelegten Zeitintervallen von 15 Minuten (wie derzeit geplant) oder zumindest bei jedem Tarifwechsel würde es genügen, dass das Smart Meter einmal pro Abrechnungszeitraum, also z. B. monatlich, den Rechnungsbetrag (statt wie heute den Zählerstand durch Ablesung) an den Stromversorger übermittelt. Ein solches Daten sparsames Verfahren würde nicht nur den mit der Übermittlung, Speicherung und Verarbeitung von täglich 3,8 Mrd. Zählerständen verbundenen Aufwand überflüssig machen, sondern würde zudem sogar die bestehenden Abrechnungsprozesse durch die Übermittlung der Rechnungssumme statt des Zählerstands vereinfachen.

2 Lastermittlung: Microzensus statt „Lauschangriff“

Bessere Prognosen des erwarteten Verbrauchs statt der heute verwendeten Standard-Lastprofile könnten die von Spitzenlastkraftwerken abzudeckenden „Verbrauchsspitzen“ immerhin ein wenig dämpfen. Auch zu diesem Zweck sollen Smart Meter die Verbrauchsdaten in Zeitintervallen von 15 Minuten an den Stromversorger übermitteln.

Dass eine solche Datenerhebung einen erheblichen Eingriff in die Privatsphäre der Verbraucher darstellt, wurde verschiedentlich ausführlich begründet.[9] Auch das vom BVerfG im Urteil über die so genannte „Online-Durchsuchung“ formulierte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie die verfassungsmäßig garantierte Unverletzlichkeit der Wohnung (Art. 13 GG) setzen dem „messtechnischen Lauschangriff“ eines Smart Meters enge Grenzen.[10]

Übersehen wird dabei allerdings, dass eine solche permanente Datenübermittlung für den Zweck der Lasterhebung keineswegs erforderlich ist. Denn zur Ermittlung realistischer aktueller Verbrauchsdaten wird keine haushaltsgenaue Auflösung benötigt. Vollständig genügen würde es beispielsweise, die Verbrauchsdaten über mehrere Haushalte zu aggregieren und lediglich die Durchschnittswerte an den Stromversorger zu übermitteln. Die Zusammenführung der Daten ließe sich sogar mit einem einfachen kryptografischen Protokoll wirksam anonymisieren, wie Jeske gezeigt hat [3].

Aber selbst das wäre verzichtbar: Mit statistischen Verfahren lässt sich selbst aus einer Zufallsstichprobe von wenigen tausend Haushalten eine zuverlässige Hochrechnung des aktuellen Gesamtverbrauchs vornehmen, die dem tatsächlichen Verbrauchswert sehr nahe kommt. Daher würde es völlig genügen, wenn jeder Smart Meter zu einem zufälligen Zeitpunkt einmal wöchentlich den aktuellen Stromverbrauch an den Stromversorger übermitteln würde. Aus diesen wenigen Angaben ließen sich keinerlei Verbrauchsprofile gewinnen.

3 Verbrauchsdatenanzeige: Dezentral statt zentral

Für die Anzeige der Verbrauchsdaten zur Kontrolle des Stromverbrauchs durch den Privatkunden ist schließlich überhaupt keine Übermittlung der Verbrauchsdaten erforderlich. Zwar ist es denkbar, dass Verbrauchern die Aufbereitung oder sogar Analyse der

[9] Siehe insbesondere Müller [7] und Karg [4].

[10] Siehe Hornung/Fuchs, in dieser Stiftungsreihe.

Verbrauchsdaten als Dienstleistung angeboten wird und in diesem Rahmen eine Übermittlung stattfindet; ein generelles Übermittlungserfordernis lässt sich daraus jedoch nicht ableiten.

Dazu müssen Smart Meter so gestaltet sein, dass sie eine (lokale) Übermittlung direkt an ein geeignetes Anzeigegerät (PC oder auch ein mobiles Gerät ermöglichen. Auch sollten die Messwerte in deutlich kleineren Intervallen als lediglich alle 15 Minuten erhoben werden, um eine genauere Analyse des eigenen Energieverbrauchs zu ermöglichen.

Diese Anforderungen flossen in das vom BSI entwickelte Schutzprofil[11] für Smart Metering Gateways ein, die im Rahmen der Novellierung des EnWG zur verbindlichen technischen Vorgabe geworden ist [6].

4 CC-Schutzprofil: Keine Antwort auf alle Fragen

Neben den angeführten Datenschutzaspekten wirft das Smart Grid auch in Bezug auf die Sicherheit der Erhebung und Übermittlung der Verbrauchsdaten Fragen auf [1, 2].

Zwar regelt das CC-Schutzprofil[11] des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) für das Smart Metering Gateway [6, 9] die sichere Kommunikation der Messgeräte mit und über das Gateway hinweg. Die kommende Generation von Smart Meter Gateways sollte daher den Integritäts- und Vertraulichkeitsanforderungen an diese Komponenten einer Smart Grid-Infrastruktur genügen. Außen vor bleiben dabei allerdings sowohl organisatorische Fragen wie ein Eskalationsprozess für kritische Sicherheits-Patches [9], die Sicherheit der Smart Meter selbst sowie die Sicherheit des Heimnetzwerkes (Home Area Network, HAN), welches in einem realen Szenario ebenfalls zu berücksichtigen ist (Abb. 4).

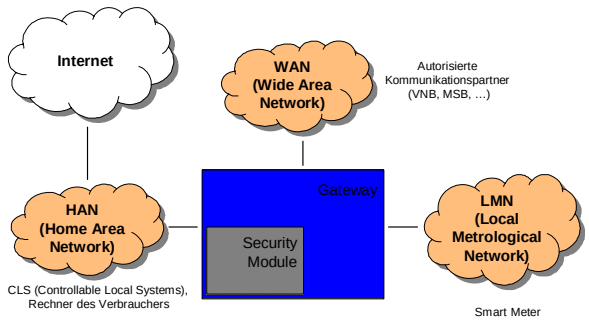


Abb. 4: Smart Metering Gateway mit angrenzenden Netzwerken

Dabei stellt ein HAN ein Netzwerk mit großem Zuwachspotenzial dar: Mit ihm sind nicht nur alle Controllable Local Systems (CLS) wie beispielsweise das Elektromobil verbunden, sondern es besitzt in vielen Fällen auch weitere Schnittstellen zum Internet und zu den durch den Nutzer betriebenen Systemen (PCs, Tablets und Smartphones). Im aktuellen Entwurf für das Schutzprofil des Smart Metering Gateways wird lediglich darauf verwiesen, dass diese Schnittstellen angemessen geschützt werden müssen – das Schutzprofil sorgt nicht dafür.[12]

[11] BSI: Protection Profile for the Gateway of a Smart Metering System, v 1.1.1 (final draft), URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile

[12] Abschnitt 1.4.6.4, S. 21: „If devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) this connection is assumed to be appropriately protected."

5 Unterbrechereinrichtungen: Netz- vs. Nutzerpriorisierung

Das aktuelle EnWG sieht die Steuerung von Lasten durch den Verteilnetzbetreiber (VNB) vor.[13] Diese bezieht sich ausschließlich auf „die Steuerung von vollständig unterbrechbaren Verbrauchseinrichtungen, die über einen separaten Zählpunkt verfügen“; als Beispiel wird das Elektromobil genannt. Der Verteilnetzbetreiber kann so in Phasen starker Nachfrage Lasten vom Netz trennen. Im Gegenzug kann er dem Endkunden ein reduziertes Netzentgelt einräumen – was sollte einen Netzbetreiber davon abhalten, diesen Preisvorteil auch für reguläre Hausanschlüsse zu gewähren, um sich damit einen Freiheitsgrad zu erkaufen?

Die Anbindung eines regulären Hausanschlusses ist zwar im EnWG nicht ausdrücklich vorgesehen, wird aber auch nicht ausgeschlossen. Ein passendes Produkt könnte beispielsweise so aussehen:

- Die Stromversorgung kann für maximal zehn Minuten am Stück und maximal drei Mal pro Tag ohne gesonderte vorherige Ankündigung unterbrochen werden.
- Das monatliche Netznutzungsentgelt wird im Gegenzug um einen festen oder verbrauchsabhängigen Betrag gesenkt.

Die ausdrücklich aufgeführte „Zumutbarkeit“ dürfte keinen Anbieter daran hindern, ein solches Stromprodukt anzubieten – schließlich steht es dem Kunden ja frei, das Angebot zu ignorieren oder eben doch ein paar Euro pro Monat einzusparen.

Zur technischen Umsetzung wird eine Unterbrechereinheit in die Stromversorgung eingebaut, die sich aus der Ferne auslösen lässt. Sie ist in den heutigen Smart Meter-Produkten bereits vorgesehen.

Hat der Verbraucher jedoch keine Möglichkeit, im Falle einer Unterbrechung die Versorgung bei Bedarf wieder einzuschalten, ist er auf die fehlerfreie Funktion der Einheit angewiesen. Denn diese Unterbrechereinheiten sind nicht nur für die VNB, sondern auch für potenzielle Angreifer interessant. Da davon auszugehen ist, dass – zumindest im gesamten Bereich eines VNB – in allen Haushalten identische oder ähnliche Geräte – mit den gleichen Schwachstellen – eingesetzt werden, kann ein Angreifer mit Kenntnis einer geeigneten Schwachstelle sämtliche auf diese Weise angebundenen Haushalte vom Stromnetz trennen [8]. Der „Wiederanlauf“ in einer solchen Situation könnte es erforderlich machen, die Unterbrechereinheit in Millionen Haushalten manuell aus der Schaltung zu entfernen.

Um einen solchen Schadensfall – mit fraglos erheblichen Gefährdungen für Leib und Leben der Betroffenen – zu verhindern, erscheint eine Unterbrecherschaltung, die vom Endverbraucher manuell überbrückt werden kann („Nutzerpriorität“), unverzichtbar.

Fazit

Die derzeitige Diskussion um Einsatz und Nutzen von Smart Metern und die Etablierung eines Energieinformationsnetzes ist von zahlreichen Postulaten durchzogen, die einer genauen Prüfung nicht standhalten. So ist festzuhalten:

- Bei Privathaushalten besteht ein theoretisches Leistungsverschiebungspotential von etwa 5,2 % der Gesamtenergiemenge – weniger als 2 % der gesamten

[13] § 14a EnWG: „Steuerung von unterbrechbaren Verbrauchseinrichtungen in Niederspannung“.

Stromeinspeisung aus Wind- und Sonnenenergie. Dem steht ein Investitionsvolumen von 1,6 Mrd. € (jährlich) allein für die Basis-Infrastruktur (Smart Meter, Einbau) gegenüber.

- Für die Abrechnung des Verbrauchs bei wechselnden Tarifen ist keine Übermittlung der Verbrauchswerte aller 40 Mio. Haushalte erforderlich – einfacher und ausreichend wäre die Berechnung des Rechnungsbetrags im Smart Meter (anhand von Broadcast-Tarifinformationen) und dessen einmalige Übermittlung.
- Auch für die Verbesserung der Verbrauchsprognosen ist keine regelmäßige Verbrauchsdatenübermittlung erforderlich; hier genügen anonym aggregierte Werte über mehrere Haushalte oder – besser noch – eine Zufallserhebung in mehreren Tausend Haushalten zur Hochrechnung des Gesamtverbrauchs.
- Für die Anzeige der Verbrauchsdaten im Haushalt ist ebenfalls keine Übermittlung erforderlich; es genügt eine Schnittstelle für den lokalen Zugriff oder deren Transfer auf ein anderes IT-System.
- Im CC-Schutzprofil sind sowohl der Umgang mit kritischen Sicherheits-Patches als auch der Internet-Zugang des privaten PC ausgeklammert – es verbleiben daher weitere zu schützende Bereiche.
- Die vorgesehene Unterbrechereinrichtung im Smart Meter macht die Infrastruktur anfällig für flächendeckende Denial-of-Service-Angriffe, die sich nur vor Ort an jedem einzelnen Zähler reparieren ließe.

Literatur

[1] Eckert, Claudia.: *Sicherheit im Smart Grid. Eckpunkte für ein Energieinformationsnetz*. Stiftungsreihe Nr. 90, Alcatel-Lucent-Stiftung für Kommunikationsforschung, 2010.
URL: http://www.stiftungaktuell.de/files/sr90_sicherheit_im_energieinformationsnetz_gesamt_1.pdf

[2] Eckert, Claudia; Krauß, Christoph.: *Sicherheit im Smart Grid. Herausforderungen und Handlungsempfehlungen*. Datenschutz und Datensicherheit (DuD), 8/2011, S. 535-541.

[3] Jeske, Tobias: *Datenschutzfreundliches Smar Metering. Ein praktikables Lösungskonzept*. Datenschutz und Dtensicherheit (DuD), 8/2011, S. 530-534.

[4] Karg, Moritz: *Datenschutzrechtliche Rahmenbedingungen beim Einsatz intelligenter Zähler*. Datenschutz und Datensicherheit (DuD), 6/2010, S. 365-372.

[5] Klobasa, Marian: *Dynamische Simulation eines Lastmanagements und Integration von Windenergie in ein Elektrizitätsnetz auf Landesebene*. DISS ETH Nr. 17324, ETH Zürich, 2007.
URL: http://isi.fraunhofer.de/isi-de/publ/download/isi07b52/Promotion-Wind-Last.pdf

[6] Laupichler, Dennis; Vollmer, Stefan; Bast, Holger; Intemann, Matthias: *Das BSI-Schutzprofil: Anforderungen an den Datenschutz und die Datensicherheit für Smart Metering Systeme*. Datenschutz und Datensicherheit (DuD), 8/2011, S. 542-551.

[7] Müller, Klaus J.: *Gewinnung von Verhaltensprofilen am intelligenten Stromzähler*. Datenschutz und Datensicherheit (DuD), 6/2010, S. 359-364.
URL: http://www.secorvo.de/publikationen/verhaltensprofile-smart-meter-mueller-2010.pdf

[8] Müller, Klaus J.: *Sicherheit im Smart Grid.* DFN-CERT & PCA Workshop „Sicherheit in vernetzten Systemen“, DFN-Bericht, Februar 2011, S. A1-A24
URL: http://www.dfn-cert.de/dokumente/workshop/2011/beitrag mueller.pdf

[9] Müller, Klaus J.: *Verordnete Sicherheit – das Schutzprofil für das Smart Metering Gateway*. Datenschutz und Datensicherheit (DuD), 8/2011, S. 547-551.
URL: http://www.secorvo.de/publikationen/schutzprofil-smart-metering-gateway-mueller-2011.pdf

[10] Roßnagel, Alexander; Jandt, Silke: *Datenschutzfragen eines Energieinformationsnetzes*. Stiftungsreihe Nr. 88, Alcatel-Lucent-Stiftung für Kommunikationsforschung, 2010.
URL: http://www.stiftungaktuell.de/files/sr88_newise_datenschutz_gesamt_1.pdf

[11] Roßnagel, Alexander; Jandt, Silke: *Datenschutzkonformes Energieinformationsnetz*. Datenschutz und Datensicherheit (DuD), 6/2010, S. 373-378.

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

Gerrit Hornung, Katharina Fuchs

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 und aus diesem Anforderungen an die Rechtsgrundlagen und die Gestaltung der verwendeten Technik abgeleitet. Die grundrechtlichen Probleme sind damit allerdings nicht ausgeschöpft: Da die Daten der häuslichen Sphäre entstammen ist zu fragen, ob nicht auch der Schutzbereich von Art. 13 GG betroffen ist. Durch die Erhebung mittels eines IT-Systems (der Smart Meter) kann auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eingreifen. Schließlich stellt sich angesichts der Kommerzialisierung der Daten im Smart Grid die Frage, ob vermögenswerte Positionen betroffen sind. Insgesamt ergibt sich: 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.

1 Hintergrund

Aus verfassungsrechtlicher Sicht weist die Idee eines nachhaltigen Energieinformationsnetzes[1] grundsätzliche Spannungsfelder auf. Der Staat verfolgt mit dem Ziel der effektiven Nutzung der im Netz jeweils erzeugten, gerade bei regenerativen Energiequellen stark schwankenden Energiemenge das Allgemeininteresse des Schutzes der natürlichen Lebensgrundlagen, das in Art. 20a GG als Staatsziel verankert ist. Dazu wird die Nutzung personenbezogener Daten der Letztverbraucher teils erlaubt, teils vorgeschrieben, sodass deren grundrechtlich geschützte Persönlichkeitsrechte[2] zu wahren sind; hinzu kommt das Interesse an günstigeren Preisstrukturen angesichts steigender Energiepreise. Auch auf Seiten der Anbieter und Betreiber von Netzen und Messgeräten bestehen mit der Berufsfreiheit (Art. 12 GG) verfassungsrechtlich geschützte Interessen an neuen Geschäftsmodellen, die mit der Auswertung der Verbrauchsdaten ermöglicht werden.

Der Gesetzgeber fördert diese Entwicklung, indem er Vorgaben für die rechtliche, technische und organisatorische Gestaltung des Energieinformationsnetzes macht. Sobald jedoch wichtige Bausteine dieser Infrastruktur –

[1] S. aus Sicht des Gesetzgebers BT-Drs. 17/6072, 76 ff.; zu den Hintergründen der Entwicklung s. z. B. *Orlamünder*, Der Einsatz von Informations- und Kommunikationstechnik in Stromnetzen – ein Nachhaltiges Energieinformationsnetz, Alcatel-Lucent-Stiftung, Stiftungsreihe Nr. 85, 2009; *Roßnagel/Jandt*, Datenschutzfragen eines Energieinformationsnetzes. Alcatel-Lucent-Stiftung, Stiftungsreihe Nr. 88, 2010, 3 ff.; *dies*., DuD 2010, 373 f.; *Pielow*, ZUR 2010, 115 ff.; *Raabe*, DuD 2010, 279 f.; *Wiesemann*, MMR 2011, 355; ferner *Güneysu/Vetter/Wieser*, DVBl. 2011, 870.

[2] Im wirtschaftlichen Umfeld können auch grundrechtlich geschützte Betriebs- und Geschäftsgeheimnisse betroffen sein (die dann auch juristischen Personen zustehen können). Dieser Aspekt bleibt im Folgenden außer Betracht.

wie etwa die in § 21d EnWG legaldefinierten „Messsysteme“ (Smart Meter) – dazu geeignet sind, allein oder in der Vernetzung mit elektronischen Haushaltsgegenständen in erheblichem Maße Informationen über die Privatsphäre der Letztverbraucher zu erheben und zu übermitteln, treffen den Staat grundrechtliche Schutzpflichten gegenüber den Betroffenen, deren Reichweite von den jeweils tangierten Grundrechten sowie der Intensität der in Rede stehenden Beeinträchtigung abhängt.

2 Betroffene Grundrechte

In der bisherigen Diskussion ist ausführlich herausgearbeitet worden, dass in praktisch allen Konstellationen aufgrund der Identifizierbarkeit der Letztverbraucher einfachgesetzlich die Regeln des Datenschutzrechts und auf verfassungsrechtlicher Ebene das Grundrecht auf informationelle Selbstbestimmung einschlägig sind.[3] Dieses schützt „die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.[4]

Derartige Daten fallen im Energieinformationsnetz in vielfältiger Weise an. So weisen regelmäßig alle Informationen, die zur näheren Ausgestaltung und Abwicklung der Vertragsverhältnisse zwischen den Energieerzeugern, den Energieversorgungsunternehmen, den Messstellenbetreibern, den Messstellendienstleistern und den Energieverbrauchern benötigt werden einen entsprechenden Personenbezug auf.[5] Hierzu gehören etwa die Zahl der verbrauchten Kilowattstunden der Anschlussinhaber und der Verbrauchszeitraum (bei tageszeitvariablen Tarifen), aber auch Informationen über den Status einzelner Verbrauchsgeräte oder Angaben über die aktuellen Energieverbrauchswerte einzelner solcher Geräte.[6] Das bedeutet indes nicht, dass alle insoweit erhobenen Daten auch im selben Maße schutzbedürftig sind: So wird die Information, dass bestimmte Haushaltsgeräte zu einer bestimmten Tageszeit aktiv sind, noch relativ belanglos sein. An der Information, dass über einen längeren Zeitraum überhaupt keine Haushaltsgeräte bedient werden, könnten demgegenüber Kriminelle ein großes Interesse haben. Schließlich greifen die in § 14a EnWG normierte externe Steuerung von Verbrauchseinrichtungen sowie das Fernwirken und Fernmessen (§ 21g Abs. 6 Satz 5 und 6 EnWG)[7] direkt in die bisher abgeschottete Sphäre der Letztverbraucher ein.

Insgesamt ist deutlich, dass Smart Meter und die mit ihnen verbundenen Infrastrukturen zumindest potentiell eine besondere Eingriffstiefe hervorrufen, die durch den großen Umfang der Datenerhebung, die Vielzahl der von ihr betroffenen Lebensbereiche, die erhöhte Aussagekraft der erhobenen Daten, die steigende Anzahl der datenverarbeitenden Stel-

3 Hiervon geht auch der Gesetzgeber aus, s. BT-Drs. 17/6072, 76 ff.; zur Diskussion s. z. B. *Göge/Boers*, ZNER 2009, 368, 370; *Karg*, DuD 2010, 365 ff.; *Raabe*, DuD 2010, 379 ff.; *Roßnagel/Jandt* (Fn. 1), 6 ff.; *dies*., DuD 2010, 373 ff.; *Müller*, DuD 2010, 359 ff.; *Güneysu/Vetter/Wieser*, DVBl. 2011, 870, 872 f.; *Art. 29 Data Protection Working Party*, Opinion 12/2011 on smart metering, 2011; *Jandt*, in: Roßnagel (Hrsg.), Nutzerschutz – Rechtsrahmen, Technikpotentiale, Wirtschaftskonzept, 2011, i.E; zu Österreich *Renner*, DuD 2011, 524 f.; zu Einzelheiten s. v. a. die Szenarien in *Raabe/Pallas/Weis/ Lorenz/Boesche*, Datenschutz in Smart Grids, 2011.

4 BVerfGE 65, 1 (42), s. zuletzt ausführlich *Albers*, Informationelle Selbstbestimmung, 2005.

5 *Roßnagel/Jandt* (Fn. 1), 22.

6 S. die Tabelle von *Roßnagel/Jandt* (Fn. 1), 21.

7 Hierzu bestehen teilweise Regelungen in den Landesdatenschutzgesetzen, s. z. B. § 36 HDSG.

len (vor allem durch die neue Rolle des Messstellenbetreibers nach § 3 Nr. 26a EnWG) und das gesteigerte Interesse Dritter an den erhobenen Daten verursacht wird.[8]

Aus dem verfassungsrechtlichen Schutzprogramm der informationellen Selbstbestimmung lassen sich Anforderungen an eine rechtliche Regelung des Energieinformationsnetzes und an seine technische Gestaltung ableiten.[9] Der Gesetzgeber ist inzwischen aktiv geworden und hat mit dem Gesetz zur Neuregelung energiewirtschaftsrechtlicher Vorschriften (EnWRNRG)[10] mit Wirkung vom 4.8.2011 Regelungen für die Erhebung und Verwendung personenbezogener Daten im Smart Grid geschaffen.[11] Diese sehen auch Vorgaben für die Zertifizierung der Messsysteme anhand eines Schutzprofils (Protection Profile) nach Common Criteria vor (§ 21e Abs. 2 und Abs. 4 EnWG),[12] welches nicht nur datenschutzrechtliche Aspekte, sondern auch die – schon aus eichrechtlichen Gründen – überaus wichtigen Fragen der Datensicherheit berücksichtigt.[13] Auch wenn nicht alle rechtspolitischen Forderungen umgesetzt wurden,[14] hat der Gesetzgeber mit dem Instrument des Schutzprofils und mit den Vorgaben zu Verarbeitungszwecken und Erforderlichkeit der Datenverwendung (§ 21g Abs. 1 EnWG), zur Datensicherheit nach dem dynamischen Maßstab des „jeweiligen" Stands der Technik (§ 21e Abs. 3 Satz 1 EnWG), zu bereichsspezifischen Auskunftsansprüchen (§ 21h Abs. 1 EnWG), zur Anonymisierung und Pseudonymisierung (§ 21g Abs. 3 Satz 4 und Abs. 5 EnWG), zum Kopplungsverbot (§ 21g Abs. 6 Satz 3 EnWG) und zu den Informationspflichten bei „Datenpannen" (§ 21h Abs. 2 EnWG)[15] jeweils Schritte in die richtige Richtung unternommen.

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. Soweit Smart Meter in der häuslichen Sphäre der Letztverbraucher verbaut werden und in dieser Informationen erheben, kann das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 GG) betroffen sein. Dasselbe gilt für das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, welches das Bundesverfassungsgericht in der Entscheidung zur Online-Durchsuchung entwickelt hat. Angesichts des wirtschaftlichen Werts der im Smart Grid erhobenen und verwendeten Daten bestehen außerdem Anhaltspunkte für eine eher eigentums- oder vermögensrechtlich strukturierte Grundrechtsdimension. Diese drei Bereiche werden im Folgenden hinsichtlich der Betrof-

8 S. näher *Roßnagel/Jandt* (Fn. 1), 6 ff.

9 S. *Roßnagel/Jandt* (Fn. 1), 26 ff., 38 ff.; *dies*., DuD 2010, 373, 375 ff.; *Karg*, DuD 2010, 365, 366 ff.; *Raabe*, DuD 2010, 379, 381 ff.; *Art. 29 Data Protection Working Party* (Fn. 3), 16 ff.; *Raabe/Lorenz/Pallas/Weis/Malina*, DuD 2011, 519 ff.; zur technischen Umsetzung s. *Eckert*, Sicherheit im Smart Grid. Eckpunkte für ein Energieinformationsnetz, Alcatel-Lucent-Stiftung, Stiftungsreihe Nr. 90, 2011; *Cavoukian/Polonetsky/Wolf*, IDIS 2010, 275 ff.; zum Konzept einer anonymen Datenübertragung *Jeske*, DuD 2011, 530 ff.

10 BGBl. I 2011, Nr. 41, S. 1554.

11 S. dazu *Roßnagel/Jandt/Volland*, ZD 2011, i.E.

12 Dazu z. B. *Laupichler/Vollmer/Bast/Intemann*, DuD 2011, 542 ff.; *Müller*, DuD 2011, 547 ff.

13 S. näher *Eckert* (Fn. 9); *Eckert/Krauß*, DuD 2011, 542.

14 So die – allerdings auch weitreichende – Forderung nach einem „Energiegeheimnis" von *Roßnagel/Jandt* (Fn. 1), 38; s.a. *Jandt* (Fn. 3); kritisch auch *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, Stellungnahme v. 10.6.2011, https://www.datenschutzzentrum.de/smartmeter/20110615-smartmeterregelung.pdf.

15 S. dazu allgemein *Gabel*, BB 2009, 2045 ff.; *Eckhardt/Schmitz*, DuD 2010, 390 ff.; *Hanloser*, MMR 2010, 300 ff.; *Hornung*, NJW 2010, 1841 ff.

fenheit der Schutzbereiche und der Frage behandelt, welche Schlussfolgerungen für das Handeln staatlicher Stellen und etwaige Schutzpflichten gegenüber den Letztverbraucher zu ziehen sind.

3 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.[16] Geschützt wird die „räumliche Privatsphäre“;[17] historisch vor allem gegen Eingriffe bei physischer Anwesenheit von Trägern öffentlicher Gewalt. Das Bundesverfassungsgericht hat aber überzeugend dargelegt, dass „der Schutzzweck der Grundrechtsnorm vereitelt [würde], wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung […] umfasst wäre“.[18] Auch solche Maßnahmen stellen also eine Beeinträchtigung des räumlich-gegenständlichen Bereichs der Privatsphäre dar, die durch eine anschließende Speicherung und Verwendung der gewonnenen Informationen oder eine Übermittlung an andere Stellen weiter fortgesetzt wird.[19]

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 jeweiligen Haushaltsmitglieder und ihre Verhaltensweisen und Gewohnheiten gewinnen lassen: Da die Anzahl der zugleich betriebenen elektrischen Geräte in einem Haushalt begrenzt ist und sich die verschiedenen Apparate durch spezifische Lastprofile auszeichnen, ist es möglich, einen Großteil der Geräte – insbesondere solche mit hoher Leistung wie Kühlschrank, Spülmaschine oder Backofen – eindeutig zu identifizieren.[20] Ist es aber erst einmal gelungen, die Eckdaten und Lastprofile der leistungsintensiven Geräte zu ermitteln und in der Folge aus dem Lastgang des Haushalts herauszurechnen, steht auch der Identifikation kleinerer Verbraucher (z. B. Staubsauger oder Haartrockner) anhand von Kriterien wie Leistungsaufnahme, Funktionsweise, typische Arbeitszyklen, Nutzungszeitpunkte oder Verwendungshäufigkeit nichts mehr im Wege.

Letztlich werden auf diese Weise diverse Rückschlüsse auf die Lebensgewohnheiten der Haushaltsmitglieder möglich, die sonst nicht ohne herkömmliche Eingriffe in Art. 13 GG ermittelbar wären, etwa wann die Bewohner zu Bett gehen und morgens aufstehen, ob es nächtliche Toilettenbesuche gibt, wie häufig und mit welchen Geräten vorzugsweise gekocht wird, wie oft die Haushaltsmitglieder Besuch empfangen, wie häufig die Waschmaschine läuft etc.[21] Ferner geben etwa Dauer und Zeitraum der Nutzung eines Computers oder des Fernsehers Hinweise auf das Freizeitverhalten oder die Interessen des Nutzers. Selbst die Tatsache, dass in bestimmten Zeiträumen kein oder nur sehr wenig Strom verbraucht wird, kann zu Vervollständigung des Verbraucherprofils ge-

[16] BVerfGE 32, 54 (75); 42, 212 (219); 51, 97 (110); 109, 279 (309).
[17] BVerfGE 7, 230 (238); 109, 279 (309).
[18] BVerfGE 109, 279 (309); s.a. BVerfGE 120, 274 (309 f.).
[19] BVerfGE 109, 279 (327).
[20] S. *Müller*, DuD 2010, 359, 360 f.; s. zu den betroffenen Lebensbereichen auch *Roßnagel/Jandt* (Fn. 1), 7 ff.
[21] *Müller*, DuD 2010, 359, 360 f.

nutzt werden und Aufschluss über die Lebensumstände der Betroffenen, wie etwa über den Grund einer kürzeren oder längeren Abwesenheit (Arbeit, Krankenhausaufenthalt, Urlaubsreise), geben.[22] Für den Eingriff kommt es nicht darauf an, ob diese Informationen definitiv einzelnen Personen zugeordnet werden können. Bei Einpersonenhaushalten ist dies allerdings ohnehin der Fall, und bei der zur Energieeffizienzberatung gegebenenfalls notwendigen geräte- und raumgenauen Auflösung der Messdaten können mit entsprechendem Zusatzwissen auch bei mehreren Bewohnern konkrete Verhaltensprofile im innerhäuslichen Bereich ermittelt werden.[23]

Dass diese Informationen dem durch Art. 13 GG geschützten räumlichen Bereich entstammen, ist weithin eindeutig. Zweifeln kann man an der Anwendbarkeit des Grundrechts höchstens deshalb, weil die Aussagekraft gegenüber einer direkten Beobachtung herabgesetzt sein kann: Die anhand eines Lastprofils gewonnene Information, dass ein Fernseh- oder Radiogerät eingeschaltet ist, gibt zunächst noch keine Auskunft darüber, welches Programm ausgewählt wurde. Vergleichbares gilt für die Nutzung anderer elektrischer Haushaltsgeräte. Deshalb ist der Hinweis zutreffend, dass in einer solchen Situation die Verbrauchsdaten von Smart Metern nicht mit einer optischen oder akustischen Überwachung des Betroffenen in seiner Wohnung gleichgesetzt werden können.[24] Dies würde sich jedoch grundlegend anders darstellen, wenn es anhand des Lastprofils eines Fernsehgeräts doch möglich sein sollte, das eingeschaltete Programm oder den abgespielten Film zu identifizieren. Genau hierfür gibt es erste Forschungsergebnisse, die anhand des Stromverbrauchs den konsumierten Inhalt bestimmen.[25] Selbst wenn keine derartigen direkten Informationen über das Konsumverhalten in der Wohnung gewonnen werden können, kann daraus jedoch nicht der Schluss gezogen werden, Art. 13 GG sei insgesamt nicht anwendbar. Ob der Schutzbereich eines Grundrechts einschlägig ist, hängt grundsätzlich nicht davon ab, in welcher Intensität in diesen eingegriffen wird,[26] und ob der Eingriff seiner Art nach mit bisher üblichen Eingriffen vergleichbar ist. Ohnehin ist auch ohne Erkennbarkeit audiovisueller Kommunikationsinhalte zweifelhaft, ob die Eingriffsintensität wirklich geringer ist: Die Art der Erfassung von Energieverbrauchsdaten ermöglicht eine unbegrenzte Speicherung, die jederzeitige und ohne Rücksicht auf Entfernungen in Sekundenschnelle erfolgende Übermittlung sowie die Verschneidung dieser Informationen mit anderen Daten.[27] Je nach technischer Umsetzung des Energieinformationsnetzes und der im Einzelfall durch den Smart Meter erhobenen Daten erscheint es deshalb denkbar, dass ein zwar andersartiger, im Ergebnis aufgrund der gewonnenen Persönlichkeitsprofile aber doch der optischen oder akustischen Überwachung vergleichbar intensiver Grundrechtseingriff vorliegt.[28]

Gegen die Anwendbarkeit von Art. 13 GG könnte man indes vorbringen, das Bundesverfassungsgericht habe in dem vergleichbaren Fall der Online-Durchsuchung einen ent-

22 *Roßnagel/Jandt*, (Fn. 1), 2010, 8 f.
23 *Raabe*, DuD 2010, 379, 381.
24 *Göge/Boers*, ZNER 2009, 368, 369.

25 S. das Arbeitspapier des Labors für IT-Sicherheit der FH Münster, http://www.its.fh-muenster.de/ greveler/pubs/smartmeter_sep11_v06.pdf.
26 Die Intensität eines Eingriffs spielt vielmehr regelmäßig erst im Rahmen der Frage nach einer möglichen Rechtfertigung desselben eine Rolle, s. *Kube*, JuS 2003, 111, 112 (speziell zu Art. 2 Abs. 1 GG).
27 S. *Karg*; DuD 2010, 365, 366 f.
28 So auch *Müller*, DuD 2010, 359, 364; *Karg*, DuD 2010, 365, 366.

sprechenden Eingriff abgelehnt. Allerdings wurde dort entscheidend damit argumentiert, der Eingriff könne unabhängig vom Standort erfolgen, der den Behörden oftmals noch nicht einmal bekannt sei, sodass die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt bleibe.[29] Dies ist hier anders: Der Standort der Smart Meter liegt regelmäßig ebenso in dieser Sphäre wie die elektronischen Geräte, durch deren Verbrauchsmessung die beschriebenen Informationen über Verhaltensweisen innerhalb der Wohnung erhoben werden. Bei einem physischen Zugriff auf Messsysteme ist Art. 13 GG ohnehin einschlägig; das hat das Bundesverfassungsgericht auch für den Fall des Zugriffs auf IT-Systeme zur Online-Durchsuchung betont.[30]

Soweit Art. 13 GG nach diesen Kriterien anwendbar ist, wird das Grundrecht auf informationelle Selbstbestimmung verdrängt.[31] Hoheitliche Eingriffe (also der Zugriff auf die Daten, solange sich diese in der häuslichen Sphäre befinden) unterliegen den allgemeinen Anforderungen von Art. 13 Abs. 2 bis Abs. 7 GG. Da Art. 13 Abs. 3 GG zur Aufklärung von Straftaten nur technische Mittel „zur akustischen Überwachung“ zulässt, ist ein externer Zugriff auf die Daten zu diesem Zweck unzulässig. Denkbar wäre zum einen eine Datenerhebung im Rahmen einer Durchsuchung (Art. 13 Abs. 2 GG), zum anderen ein Zugriff auf die Daten, die an die Betreiber von Messstellen oder Netzen weitergeleitet wurden. Im präventiven Bereich lässt Art. 13 Abs. 4 GG demgegenüber (unter weiteren Voraussetzungen) allgemein „technische Mittel zur Überwachung von Wohnungen“ zu. Dieser Begriff ist entwicklungsoffen und beschränkt sich nicht auf die zur Zeit der Verfassungsänderung bekannten Mittel.[32] Damit ist ein externer Zugriff zur Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, zumindest prinzipiell möglich.

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)[33] bezweckt wird.

4 Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Smart Meter und eine Vielzahl elektronischer Haushaltsgeräte, deren Verbrauch sie aufzeichnen, sind IT-Systeme. Allein deshalb fallen sie allerdings noch nicht in den Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Dieses erfasst keine

[29] BVerfGE 120, 274 (310 f.); a.A. z. B. *Buermeyer*, HRRS 2007, 392, 395 ff.; *Hornung*, DuD 2007, 575, 577 f.; *Kudlich*, HFR 19-2007, 4 ff.; *Rux*, JZ 2007, 285, 292 ff.; *Schaar/Landwehr*, K&R 2007, 202, 204; *Schantz*, KritV 2007, 310 ff.; wie das BVerfG *Gercke*, CR 2007, 245, 250; *Schlegel*, GA 2007, 648 ff.

[30] BVerfGE 120, 274 (310).

[31] BVerfGE 51, 97 (105); s.a. *Di Fabio*, in: Maunz/Dürig, GG, 61. Ergänzungslieferung 2011, Art. 2 Rn. 21 ff.

[32] *Gornig*, in: v. Mangoldt/Klein/Starck, Kommentar zum Grundgesetz, 6. Auflage 2010, Art. 13 Rn. 129.

[33] Zu den externen Gefahren, die beim Einsatz von Smart Metern und Smart Grids drohen und den zu deren Abwehr unerlässlichen Schutzmaßnahmen s. *Eckert* (Fn. 9); *Eckert/Krauß*, DuD 2011, 535 ff.

Systeme, die „nach ihrer technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthalten“; erforderlich ist nach Aussage des Bundesverfassungsgerichts vielmehr, dass sie „allein oder in ihren 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“.[34]

Ob diese Voraussetzungen erfüllt sind, 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. Hierbei ist auch wichtig, dass das Bundesverfassungsgericht nicht verlangt, dass das IT-System tatsächlich besonders sensible Informationen enthält: Ausreichend ist vielmehr, dass das System hierzu potentiell in der Lage ist („enthalten können“). Dies wird weithin der Fall sein; auch die Gesetzesbegründung zum EnWRNRG spricht von „intelligenten Messsystemen“.[35] Wenn diese schließlich mit weiteren IT-Systemen im Haushalt interagieren, so kommt der Aspekt der technischen Vernetzung ins Spiel, den das Bundesverfassungsgericht besonders hervorgehoben hat: Die steuerbaren Geräte müssen dann einheitlich betrachtet werden, und dies erhöht die Wahrscheinlichkeit, dass das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme betroffen ist.

Damit eine „grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung“ besteht, verlangt das Bundesverfassungsgericht des Weiteren, dass „der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das System selbstbestimmt verfügt“.[36] Hierfür ist unerheblich, dass Messeinrichtungen und Messsysteme nach § 21b Abs. 4 Satz 1 EnWG regelmäßig nicht im Eigentum des Letztverbrauchers stehen werden: Entscheidend ist nicht die sachenrechtliche Zuordnung, sondern die selbstbestimmte Nutzung „als“ eigenes System. Die Literatur geht überwiegend davon aus, dass dies zumindest auch schuldrechtliche Zuordnungen, etwa im Arbeitsverhältnis, erfasst.[37] Soweit allerdings IT-Systeme nach ihrer Konzeption gerade darauf angelegt sind, Dritten Daten zu übermitteln – dies dürfte bei isolierter Betrachtung auf Smart Meter zutreffen –, so entfällt die Nutzung als „eigenes“ System.[38]

Jedenfalls nutzt der Letztverbraucher aber die in der Wohnung befindlichen IT-Systeme als eigene. Soweit es also nach den oben genannten Kriterien auf die (gesamte) vernetzte Haustechnik ankommt, liegt in jedem

[34] BVerfGE 120, 274 (313 f.).

[35] BT-Drs. 17/6072, 76, 78 f. in Anlehnung an die Formulierung in den Richtlinien 2009/72/EG (ABl. EU 2009 Nr. L 211 S. 91) und 2009/73/EG (ABl. EU 2009 Nr. L 211 S. 134).

[36] BVerfGE 120, 274 (315).

[37] Zu den Auswirkungen des Grundrechts auf das Arbeitsrecht s. z. B. *Stögmüller*, CR 2008, 435 ff.; *Wedde*, AuR 2009, 373 ff.; erste Gerichtsentscheidungen erkennen dies zumindest am Rande an, s. Hessischer VGH, NJW 2009, 2470; LAG Niedersachsen, MMR 2010, 639.

[38] S.a. *Luch*, MMR 2011, 75, 76.

Fall die grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung vor. Das gilt beispielsweise in dem in § 14a EnWG ausdrücklich vorgesehen 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, zweistufiger Kernbereichsschutz.[39] 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,[40] die sich insbesondere in staatlichen Schutzpflichten niederschlagen.[41] Der Gesetzgeber ist deshalb gehalten, sich „schützend und fördernd“[42] vor die Vertraulichkeit und Integrität informationstechnischer Systeme zu stellen.

Insbesondere der Schutz der Integrität der Smart Meter und der mit ihnen vernetzten IT-Systeme der Letztverbraucher gewinnt hiermit eine besondere Bedeutung. Dem ist präventiv auf technischer Ebene im Rahmen des gesetzlich geforderten „jeweiligen Stands der Technik“ (§ 21e Abs. 3 Satz 1 EnWG) durch erhöhte Anforderungen Rechnung zu tragen. Überdies schlägt sich die Schutzpflicht in einem Auftrag an den Gesetzgeber nieder, durch gesetzliche Regelungen insbesondere dort Vorgaben zu machen, wo es im Verhältnis zwischen Bürgern und großen Wirtschaftsunternehmen zu einem Machtungleichgewicht kommt. Man kann aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme insoweit nicht nur zivilrechtliche Ansprüche auf Unterlassung nicht autorisierter Systemzugriffe ableiten, sondern auch einen positiven Anspruch auf Schutz der durch einen Dienstanbieter zur Nutzung bereitgestellten Systeme vor unbefugten Zugriffen Dritter.[43] Wenn der Gesetzgeber Schutzvorgaben an den Verordnungsgeber delegiert (§ 21i EnWG), so sind diese Anforderungen auf der Verordnungsebene ebenfalls umzusetzen.

5 Kommerzialisierung der Verbrauchsdaten?

Eine letzte grundrechtliche Frage wird durch den besonderen Charakter der durch Smart Meter 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 Wertung des Gesetzgebers zum Aus-

39 BVerfGE 120, 274 (327 ff.).

40 Zum Einfluss des Grundrechts auf das Privatrecht s. *Roßnagel/Schnabel*, NJW 2008, 3534 ff.; zu § 823 Abs. 1 BGB *Bartsch*, CR 2008, 613 ff.

41 S. ausführlich *Heckmann*, in: Rüssmann (Hrsg.), Festschrift für Gerhard Käfer, 2009, 129 ff. sowie *Roßnagel/Schnabel*, NJW 2008, 3534, 3535; *Holznagel/Schumacher*, MMR 2009, 3, 6 f.; *Luch*, MMR 2011, 75, 78 f.; tendenziell zurückhaltend gegenüber der Ableitung spezifischer Schutzpflichten *Sick*, VBlBW 2009, 85 ff.

42 So die Formulierung des BVerfG zu Art. 2 Abs. 2 GG, s. BVerfGE 39, 1 (42); 46, 160 (164); 53, 30 (57); 88, 203 (251); 90, 145 (195); 115, 118 (152), 121, 317 (356); ebenso zu Art. 5 Abs. 3 GG: BVerfGE 35, 79 (113); 85, 360 (384).

43 Treffend *Luch*, MMR 2011, 75, 78 f.

druck, die § 14a Satz 1 EnWG zugrunde liegt: 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 durch elektronische Haushaltsgeräte erzeugten 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 so weit gehen, diese Position der grundrechtlichen Eigentumsgarantie zuzuordnen. Zwar schützt Art. 14 GG auch die rechtliche Zuordnung privater vermögenswerter Güter zu einem Rechtsträger, und dies geht weit über das hinaus, was umgangssprachlich und nach bürgerlichem Recht (§ 903 BGB) unter „Eigentum" verstanden wird.[44] Bei der Nutzung feingranularer Verbrauchsdaten ist aber – jenseits der Frage, ob diese sich überhaupt zu einer einigermaßen abgrenzbaren vermögenswerten Position verdichten – die Funktion der Eigentumsgarantie nicht betroffen, dem Einzelnen „die privat verfügbare ökonomische Grundlage individueller Freiheit" zu gewährleisten.[45] Das gilt insbesondere im Verhältnis zu Netz- und Messstellenbetreibern, weil diese die Energie bereitstellen, die Grundlage für die Verbrauchsdaten ist. Dennoch ist der wirtschaftliche Wert dieser Daten grundrechtlich nicht belanglos. Er wirft nämlich die grundsätzliche Frage auf, ob die oben erörterten Persönlichkeitsrechte (auch) eigentumsähnlich strukturiert sind. In Deutschland wird das für das Grundrecht auf informationelle Selbstbestimmung überwiegend abgelehnt,[46] während man in anderen Ländern offen für diese

---

[44] S. z. B. *Wieland*, in: Dreier, Grundgesetz Kommentar, Band I, 2. Auflage 2004, Art. 14 Rn. 38 ff. m.w.N.

[45] BVerfG, NJW 1998, 1934, 1936; s.a. *Depenheuer*, in: v. Mangoldt/Klein/Starck (Fn. 31). Art. 14 Rn. 11 ff.

[46] *Vogelgesang*, Grundrecht auf informationelle Selbstbestimmung?, 1987, 141 ff.; *Pitschas*, DuD 1998, 139, 148; *Simitis*, in: ders. (Hrsg.), BDSG, 7. Auflage 2011, Einl. Rn. 26; *ders.*, NJW 1998, 2473, 2476 f.; *Trute*, JZ 1998, 822, 825 ff.; *ders*., in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 2.5 Rn. 19, 21; *Weichert*, NJW 2001, 1463 ff.; *ders*., in: Taeger (Hrsg.), Informatik – Wirtschaft – Recht: Regulierung in der Wissensgesellschaft, FS für Wolfgang Kilian, 2004, 281 ff.; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 207 f., 230; s. aber anders *Ladeur*, NJW 2000, 1977, 1980: quasi-eigentumsrechtlich geschütztes Interesse am eigenen Bild (allgemeiner *ders*., DuD 2000, 12, 18 f.); darauf aufbauend für Daten in sozialen Netzwerken *Hoeren*, ZRP 2010, 251, 252.

Perspektive ist.[47] Allerdings wird auch das deutsche allgemeine Persönlichkeitsrecht – das verfassungsrechtlich die Basis der informationellen Selbstbestimmung ist – im Zivilrecht durchaus „kommerzialisiert".[48] Auf verfassungsrechtlicher Ebene scheint einer eigentums- oder vermögensorientierten Konzeption die gesellschaftlich-demokratische Dimension informationeller Selbstbestimmung entgegenzustehen: Nicht nur der Einzelne, auch die Gesellschaft insgesamt hat ein Interesse an selbstbestimmter Persönlichkeitsentfaltung, ohne die eine freiheitliche Gesellschaft nicht möglich ist, und die unbeobachtete Bereiche des Ausprobierens und der geschützten Kommunikation erfordert.[49] Soweit Daten Ergebnis von Kommunikation (oder als Informationen Ergebnis kognitiver Prozesse der verantwortlichen Stelle) sind, ist die eigentumsorientierte Sichtweise auch deswegen unzureichend, weil erhobene Daten dann immer schon auch dem Kommunikationspartner „gehören".

Allerdings besteht im Energieinformationsnetz die Besonderheit, dass die personenbezogenen Daten, die erhoben und verwendet werden sollen, einer (oder, wenn sowohl Art. 13 GG als auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eingreifen, zwei) räumlich geschützten Sphäre entstammen, die dem Letztverbraucher grundrechtlich zugeordnet ist, und in der sie „produziert" werden. Außerdem sind die Daten nach der gesetzlichen und wirtschaftlichen Konzeption des Smart Grid jenseits der Letztverbrauchersphäre ohnehin kommerzialisiert und werden (wenn auch möglicherweise in aggregierter, also nicht mehr einzelnen Verbrauchern zuordenbarer Form) zum Wirtschaftsgut, das auch den Wirtschaftsgrundrechten unterfällt. Wieso diese Dimension im Rahmen des Grundrechtsschutzes des Letztverbrauchers nicht ebenfalls eingreifen soll, leuchtet nicht ein. Dazu muss man informationelle Selbstbestimmung nicht als solche eigentums- oder vermögensähnlich konzipieren. Es spricht aber dafür, diese Dimension als Verstärkung des Schutzes der Letztverbraucher zu begreifen, deren Besonderheiten im Rahmen grundrechtlich begründeter Schutzprogramme zur berücksichtigen sind.

6 Gestaltungsziele für Sicherheit und Nutzerschutz

Im Ergebnis haben alle drei untersuchten 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 andere (und 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 Verhältnismäßigkeitsebene auch dann zu berücksichtigen, wenn die Daten nicht beim Letztverbraucher, sondern bei

[47] Insbesondere in den USA, s. die Nachweise bei *Ladeur*, DuD 2000, 12, 18 f.; Simitis (Fn. 466), Einl. Rn. 26.

[48] Seit BGHZ 26, 348 (Herrenreiter-Entscheidung).

[49] S. BVerfGE 65, 1 (43): „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."

Netz- und Messstellenbetreibern durch staatliche Stellen erhoben werden.[50]

Für den Bereich der Umsetzung zwischen privaten Betreibern und Letztverbrauchern ergeben sich ebenfalls höhere Anforderungen, als dies bei isolierter Betrachtung des Grundrechts auf informationelle Selbstbestimmung der Fall wäre. 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 zusätzlich einschlägigen Grundrechte Rechnung tragen müssen.

[50] Daraus lässt sich ein zusätzliches Argument für den Vorschlag eines Energiegeheimnisses ableiten, s. dazu *Roßnagel/Jandt* (Fn. 1), 38.

Akzeptanz von Smart Metering

Johann Kranz

Politisch gewollt, technisch realisierbar und für eine grundlegende Modernisierung der Energieinfrastruktur hin zu einem intelligenten Energieversorgungssystem unerlässlich: Im Grunde steht der flächendeckenden Einführung von Smart Metering kaum mehr etwas im Wege. Dennoch fehlen bislang entsprechende Angebote für Endkunden. Dies hängt u. a. mit der geringen Nachfrage nach intelligenten Zählern von Privathaushalten zusammen, obwohl Studien zeigen, dass die Mehrheit der Stromkunden der neuen digitalen Zählertechnologie grundsätzlich positiv gegenübersteht. Der vorliegende Beitrag setzt sich deshalb näher mit den Einflussfaktoren, die die Akzeptanz von privaten Endverbrauchern in Bezug auf Smart Metering determinieren, auseinander und zeigt auf, wie die Nachfrage und Nutzungsabsicht gesteigert werden kann.

Einführung

Beim Umbau des Energieversorgungssystems zu einem intelligenten „e-Energy"-System oder Smart Grid, gibt es kaum ein Thema, das kontinuierlich derart kontroverse Debatten hervorruft wie Smart Metering. Die Diskussion wird dabei häufig von technischen und rechtlichen Fragestellungen dominiert. Es ist zu beobachten, dass die Wünsche, Vorbehalte und Interessen der privaten Endverbraucher häufig zu kurz kommen. Dabei haben die Verbraucher bei der Verbreitung und v. a. beim nachgelagerten Nutzungsverhalten der neuen Zählerinfrastruktur eine Schlüsselrolle inne. Denn obwohl der Roll-Out der neuen Zählergeneration durch EDL 21 zumindest gesetzlich beschlossene Sache ist, hängt die Rentabilität der substantiellen Investition in hohem Maße davon ab, ob private Stromverbraucher die neuen Möglichkeiten, die durch intelligente Zähler ermöglicht werden, mehrheitlich annehmen und gebrauchen (Faruqui et al. 2010, IEE 2011, Intellieкon 2011).

Die Smart Metering Technologie (SMT) ist ein integraler Bestandteil eines intelligenten Energieversorgungssystems. Durch die zeitnahe, präzise Bereitstellung von Verbrauchsinformation durch die neuen Zähler lassen sich deutliche Effizienzsteigerungen in der gesamten Wertschöpfungskette von Erzeugung, Verteilung, ggf. auch Speicherung, Handel und Vermarktung sowie nicht zuletzt beim Verbrauch von Energie erzielen. Insbesondere ermöglicht die bessere Informationsversorgung der beteiligten Akteure eine wesentlich effizientere Abstimmung innerhalb der Wertschöpfungskette, mit der sich kurzfristige Schwankungen volatiler erneuerbarer Energien besser ausgleichen und Kapazitäten für Regelenergie und Spitzenlasten reduzieren lassen.

Die SMT stellt im Energiesystem der Zukunft das kommunikative Bindeglied zwischen dem traditionellen Energienetz und der neu zu integrierenden Kommunikationsschicht dar (siehe Abbildung 1).

Auf Basis der neuen Zählertechnologie sind private Energieverbraucher erstmals kommunikativ mit den übrigen Akteuren im Energiesystem „end-to-end" vernetzt. Dadurch ergeben sich u. a. hinsichtlich der Energieeffizienz, Gebäudeautomatisierung, Prozessoptimierung und des so genannten *Demand*

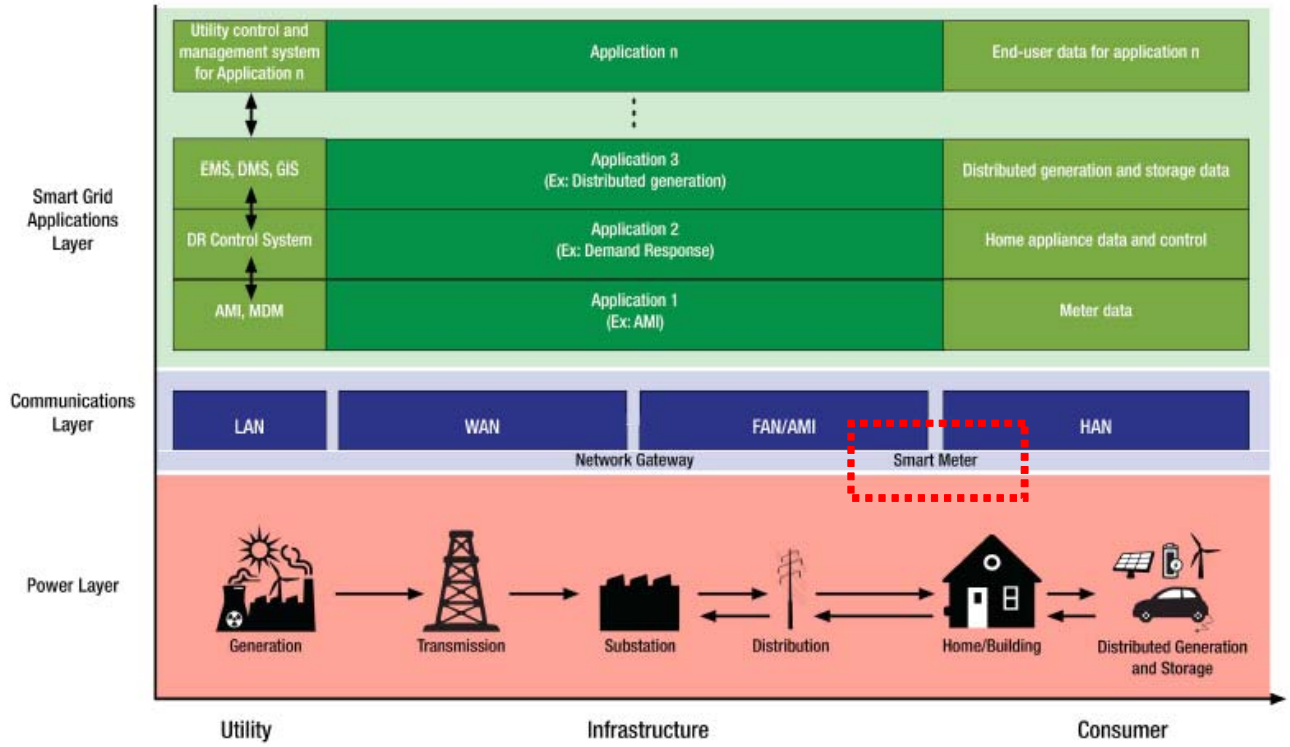


Abbildung 1: Smart Grid Infrastruktur (basierend auf Leeds 2009)

Response Managements (automatisierte Lastkontrolle und -verschiebung) neuartige und zukunftsweisende Möglichkeiten für Energieversorger, Stromverbraucher und -erzeuger. Die SMT fungiert dementsprechend als zentrales in-House Gateway, das innovative Dienste durch bidirektionale Kommunikation ermöglicht. Dieses Technologieverständnis liegt auch dem vorliegenden Beitrag zugrunde.

Smart Metering in Deutschland

Mit der Liberalisierung des Zähl- und Messwesens und der indirekten Vorgabe zum Einbau von intelligenten Stromzählern in Neubauten und grundrenovierten Gebäuden ab Anfang 2010 sowie dem Angebot von last- und zeitabhängigen Tarifen ab Ende 2010 hat der Gesetzgeber wesentliche Rahmenbedingungen zum Rollout der neuen Zählergeneration geschaffen.

Am Markt werden auch bereits die ersten Smart Meter angeboten und in den von der Bundesregierung geförderten Modellregionen werden die Geräte in großflächigen Tests von E-Energy-Ansätzen verwendet, doch insgesamt fehlen noch wichtige Voraussetzungen, die dringend für einen zügigen Roll-Out zu schaffen sind. So mangelt es derzeit z. B. noch an durchgängigen und offenen technischen (Mindest-)Standards zur Verknüpfung der diversen Komponenten in einer integrierten e-Energy Welt, ferner einem Datenmanagement-Konzept, insbesondere für die Sicherheit und den Schutz der Privatsphäre, aber auch für den fairen Zugang zu den anfallenden ungeheuren Datenmengen, und nicht zuletzt an nachhaltigen Geschäftsmodellen für neue Dienstleistungen.

Zwar versuchte die Bundesnetzagentur im letzten Jahr durch ein Positionspapier die Unklarheiten in Bezug zu den Anforderungen an Messeinrichtungen nach § 21b Abs. 3a und 3b EnWG zu beseitigen, doch nach wie

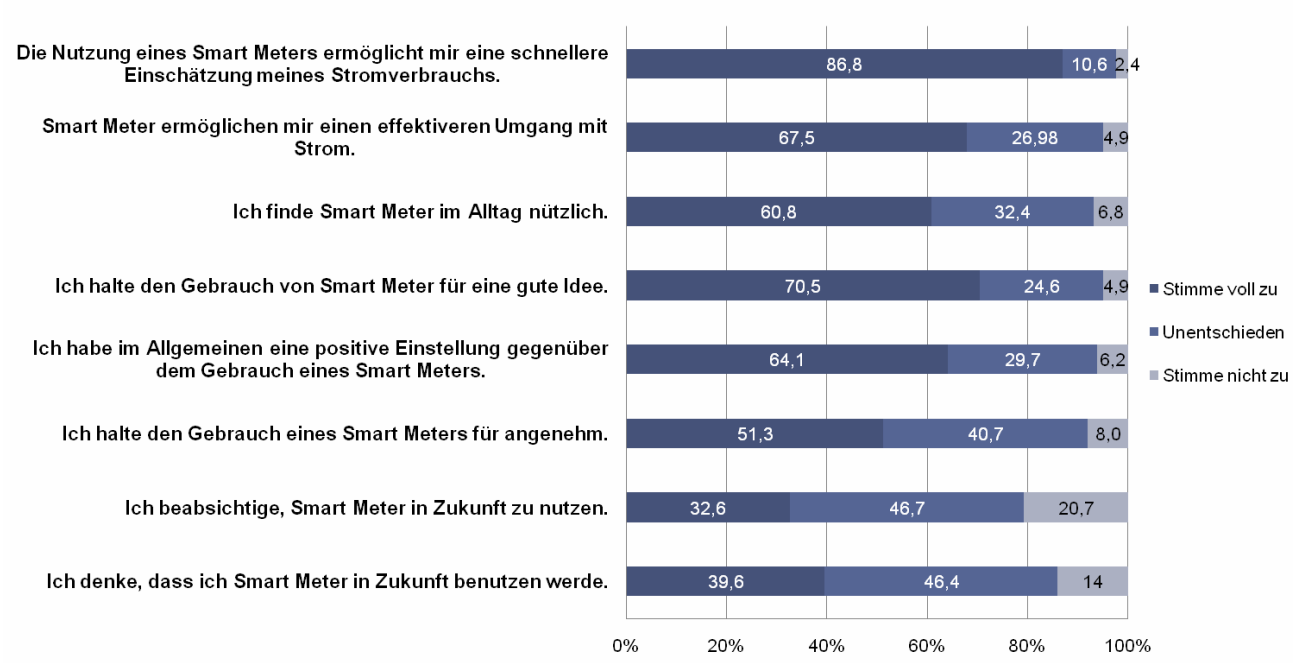


Abbildung 2: Einschätzung der Nützlichkeit von und Einstellung gegenüber Smart Metering (basierend auf Kranz 2011)

vor trifft man im Smart Metering Markt auf eine klassische Henne-Ei Problematik. Das Wissen und die konkrete Handlungsabsicht der Konsumenten sind derzeit zu gering, um Marktdynamik zu erzeugen. Unter diesen Voraussetzungen sind folgerichtig nur sehr wenige Anbieter willens in den Markt einzutreten.

Aus diesem Grund ist das Ziel der Bundesregierung, bis 2020 eine nahezu flächendeckende Verbreitung der SMT zu erreichen, unter Beibehaltung der derzeitigen Regulierungsbestimmungen sehr unrealistisch. So kann es durchaus dazu kommen, wie z. B. in den Niederlanden geschehen, dass der deutsche Messstellen-Markt von einer derzeit wettbewerblichen Organisation wieder auf ein reguliertes Marktmodell umgestellt wird. Aber auch in einem regulierten Zählermarkt bleibt es wichtig, die Einflussfaktoren auf die Akzeptanz der Stromverbraucher zu verstehen, um eine möglichst hohe Nutzung der neuen Technik und darauf aufsetzender Produkte und Dienstleistungen zu erreichen.

Einflussfaktoren auf die Nutzerakzeptanz

Der Begriff „Smart Meter“ ist trotz zunehmenden Medieninteresses noch weitgehend unbekannt. Über 90 % der Verbraucher können sich unter dem Begriff nichts vorstellen (Donath 2009, VZBV 2010), was sicherlich nicht zuletzt mit der englischen Namensgebung zusammenhängt. Klärt man die Konsumenten allerdings über die aktuellen und zukünftigen Funktionen eines intelligenten Stromzählers auf, ist das Echo überwiegend positiv (VZBV 2010, Kranz 2011). Mehr als 80 % der Verbraucher stehen der Einführung und Nutzung der digitalen Zähler positiv gegenüber.

Allerdings ist diese positive Einschätzung keineswegs mit einer konkreten Handlungsabsicht gleichzusetzen. Es ist eher so, dass die große Mehrheit der Konsumenten zwar die neuen Informations- und Energiemanagementoptionen schätzt, der Anreiz aber nicht ausreicht, um die Stromverbraucher zu aktivieren (siehe Abbildung 2). Dies spiegelt sich auch in den Erfahrungen der wenigen Anbieter von Smart Metering-Lösungen wider.

Aus Sicht der Verbraucher werden insbesondere Funktionen im Hinblick auf Transparenz, ver-brauchsgenaue und häufigere Abrechnungen, Kostenkontrolle, Sicherheit, das Aufspüren von Stromfressern, Umweltschutz, die Erleichterung eines Anbieterwechsels und Energiemanagement als positiv bewertet. Als potentielle Nutzungsbarrieren hingegen werden eine zunehmende Fremdkontrolle, Datenschutzaspekte, zeitlicher und finanzieller Mehraufwand, technische Abhängigkeit und Strahlenbelastung angeführt. Auf einige der genannten Aspekte, denen bei der Endkundenakzeptanz eine Schlüsselrolle zukommt (siehe Kranz 2011), wird im Folgenden näher eingegangen.

In der Öffentlichkeit werden Kosteneinsparungen stets als zentraler Vorteil von Smart Metering genannt. Allerdings zeigt sich hierbei ein ambivalentes Bild. Zwar ist der Stromverbrauch mit Smart Metering durchaus zu senken, allerdings sind diese Einsparungen in den meisten Haushalten absolut gesehen nicht groß und attraktiv genug, um die Verbraucher zu aktivieren. Durch die eindimensionale Fokussierung auf Einsparungen jedoch werden bei den Konsumenten überzogene Erwartungen erzeugt, die bei Nicht-Erfüllung ein gewisses „Enttäuschungspotential“ besitzen. So besteht denn auch zwischen dem erwarteten Einsparpotential (9 %) und der tatsächlich in einer kürzlich vorgestellten Studie (Intelliekon 2011) erzielten Reduzierung (3,7 %) – zumindest derzeit noch – eine erhebliche Diskrepanz. Außerdem zeigen Umfragen, dass Kosteneinsparungen für Verbraucher zwar nicht unwichtig sind, aber bei weitem nicht das entscheidende Kriterium bei der Entscheidung pro oder contra Smart Metering sind (VZBV 2010, Kranz 2011).

Ein Faktor, dessen Wichtigkeit bei der Akzeptanz hingegen nicht überbetont werden kann, ist der Datenschutz. Die Studien von Kranz (2011) zeigen, dass bezüglich der Datensicherheit und des Schutzes der Privatsphäre bei den Endverbrauchern teils erhebliche Bedenken bestehen (siehe Abbildung 3). Die Angst vor Datenmissbrauch sollte demzufolge als Querschnittsthema der Digitalisierung von allen Beteiligten sehr ernst genommen werden; denn nur so können nachhaltige Ansätze realisiert und die dauerhafte Akzeptanz der SMT gewährleistet werden.

Eng mit der Datenschutzproblematik zusammen, hängt auch das geringe Vertrauen der Verbraucher in die Stromversorger und die SMT. Das festzustellende Vertrauensdefizit wirkt sich negativ auf die Nutzungsabsicht aus. Die Kunden befürchten, dass die Technologie wie auch die Versorger die Interessen der Verbraucher nicht in ausreichendem Maße berücksichtigen und so bspw. die Preise zu Ungunsten der Konsumenten manipulieren oder die Daten gar missbraucht werden. Da Vertrauen in die Technologie und den Anbieter aber ein zentrales Kriterium bei der Entscheidung ist, Smart Metering zu nutzen, erscheint es umso wichtiger, dass die Verbraucher transparent darüber informiert werden, was mit ihren Daten geschieht und wieso diese Daten in einem zunehmend von dezentraler Einspeisung und moderner Informa-

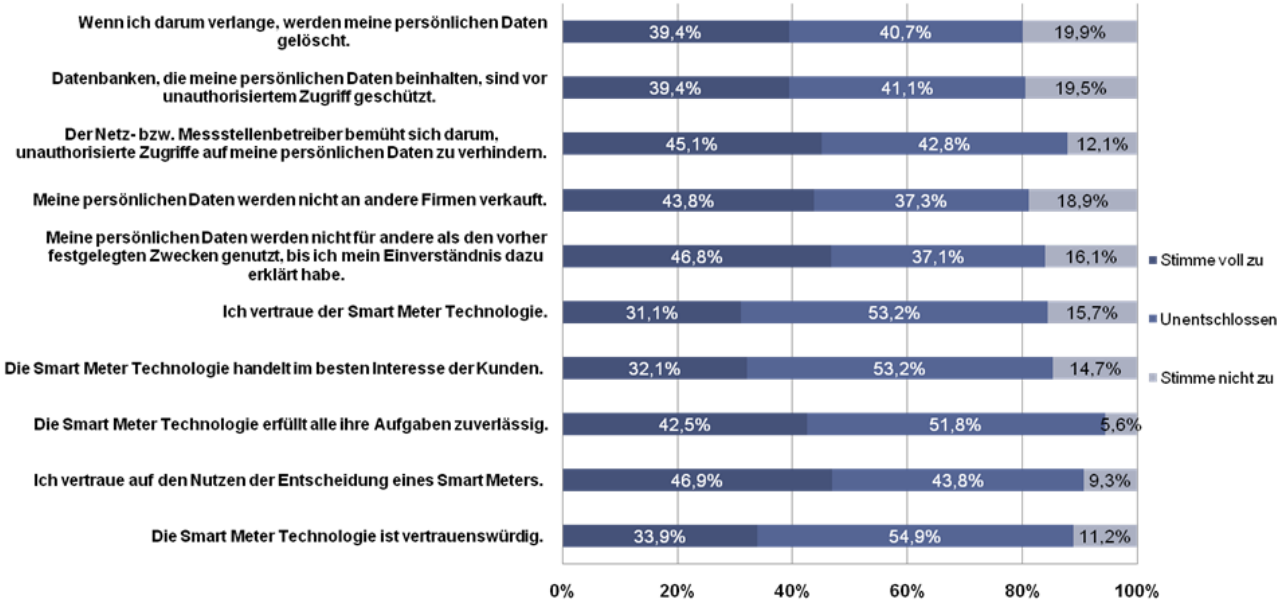


Abbildung 3: Einschätzung des Datenschutzes und Vertrauens (basierend auf Kranz 2011)

tions- und Kommunikationstechnik geprägten Energiesystem von zentraler Bedeutung sind.

Ein weiterer – oft vernachlässigter – Einflussfaktor auf die SMT-Akzeptanz ist das Umweltbewusstsein der Verbraucher. Wie bereits erwähnt, spielen Smart Meter beim Umbau zu einem nachhaltigeren Energieversorgungssystem eine wichtige Rolle, da die fluktuierende Einspeisung regenerativer Energien durch Steigerung der Nachfragelastizität besser ausgeglichen werden können. So trägt die SMT zur Reduzierung der negativen Auswirkungen der Energiewirtschaft auf die Umwelt bei. Eine große Mehrheit von 80 % sieht demnach den Umweltschutz auch als (sehr) großen Vorteil der SMT an (VZBV 2010). Demzufolge ist bei Konsumenten mit größeren Umweltbedenken eine höhere Nutzungsabsicht festzustellen (Kranz 2011).

Schlussfolgerung und Ausblick

Trotz umfangreicher Bemühungen ist es in Deutschland – wie auch in weiten Teilen Europas – bisher nicht gelungen, digitale Zähler in größerem Ausmaß privaten Stromkunden verfügbar zu machen. Abgesehen von wichtigen – teils noch ungeklärten – technischen und rechtlichen Fragestellungen ist hierfür auch die fehlende Endverbrauchernachfrage verantwortlich.

Zwar zeigen die vorgestellten Studienergebnisse, dass die Einstellung zu Smart Metering grundsätzlich positiv ist, aber die Funktionen nicht ausreichen, um die Konsumenten von sich aus aktiv auf die neue Zählertechnologie umsteigen zu lassen und diese auch zu nutzen.

Hierbei spielt sicherlich eine Rolle, dass Strom (noch) ein *low involvement* Produkt ist, dessen Kosten trotz der jüngsten Preissteigerungen in Relation zum Komfort für die meisten Haushalte überschaubar sind. Doch spätestens seit der Nuklearkatastrophe von Fu-

kushima und der daraufhin besiegelten Energiewende ändern sich diese Rahmenbedingungen zunehmend.

Doch die Frage bleibt: Wie kann man die überwiegend positive Einstellung der Verbraucher in konkrete Handlungen und Nutzungsabsicht transformieren?

Die empirischen Studien haben zwar keine Patentlösung parat, können aber wertvolle Hinweise geben, wie man die Akzeptanz und Nachfrage nach intelligenten Zählern steigern kann.

- Weniger als 10 % der deutschen Bevölkerung kann den Begriff „Smart Meter“ richtig zuordnen. Deshalb sollte sich die deutsche Politik, Wirtschaft und Wissenschaft auf einen deutschsprachigen Begriff für die neue Zählergeneration verständigen, um die öffentliche Wahrnehmung und das Verständnis zu verbessern.
- Die geringe Bekanntheit der SMT geht mit einem hohen Informationsbedürfnis und einem noch höherem Wissensdefizit einher. Die teils diffusen Vorbehalte und Ängste der Verbraucher gilt es frühzeitig, vor der Einführung, der neuen Geräte auszuräumen. Wichtig ist insbesondere klar zu machen, wieso die intelligenten Zähler gebraucht werden, um die Energieversorgung nachhaltiger zu gestalten, ohne dass gleichzeitig die Kosten explodieren. Um eine generelle Ablehnung der SMT zu vermeiden, müssen die Nutzer zusätzlich über die implementierten Datenschutz- und Sicherheitsmerkmale informiert werden.
- Ein ebenfalls bedeutender Aspekt in der Kommunikation ist auch, dass nicht nur auf Einsparungen abgezielt wird, sondern vor allem Umweltaspekte in den Vordergrund rücken. Denn das Umweltbewusstsein spielt bei der Absicht, Smart Meter zu nutzen, eine nicht zu unterschätzende Rolle.
- Für einen digitalen Basiszähler liegt die ungefähre Zahlungsbereitschaft bei einmalig zwischen 50 und 100 Euro (VZBV 2010). Diese Zahlungsbereitschaft und auch das Verbraucherinteresse könnten durch Zusatzfunktionalitäten, z. B. in den Bereichen *Home Automation* und *Security* sowie der automatisierten Steuerung von Haushaltgeräten zusätzlich gesteigert werden. Auch aus diesem Grund präferieren die Konsumenten einen modularen Zähleraufbau (VZBV 2010).
- Egal ob Basis- oder fortgeschrittener Zähler, die Nutzer möchten, dass ein Smart Meter im Alltag unauffällig und für ein breites Publikum leicht zu kontrollieren ist. Die Verbraucher haben neben Automatisierung auch ein starkes Bedürfnis nach Selbstbestimmung und Einflussnahme, was den Stromverbrauch und die Verbrauchsdaten angeht.
- Im Hinblick auf die Bedenken der Verbraucher vor Datenmissbrauch und der geringen wahrgenommenen Kontrolle über die Daten bietet sich ein so genannten Opt-In-Verfahren an. Bei dieser Vorgehensweise ist eine explizite Zustimmung der Verbraucher zur Nutzung der Daten, die über ein grundlegendes Informationsbedürfnis der Energieversorger (z. B. zu Abrechnungszwecken) hinausgehen, erforderlich. Darüber hinaus müssen Politik und Industrie das Vertrauen und den wahrgenommenen Schutz der Privatsphäre durch transparente und verständliche Datenschutzbestimmungen erhöhen. Das Vertrauen und der Schutz der

Privatsphäre können bspw. durch die Schaffung eines zentralen, unabhängigen Datendepots (wie in Großbritannien beschlossen) gesteigert werden.

Letztlich jedoch wird die Akzeptanz und Nutzungsintensität der SMT von privaten Stromverbrauchern ganz erheblich davon abhängen, ob es gelingt, Produkte und Dienstleistungen, die auf der digitalen Zählerinfrastruktur aufbauen, für ein breites Publikum hinreichend attraktiv zu gestalten. Sollte dies zeitnah gelingen, könnte sogar das ehrgeizige Ziel der Bundesregierung noch zu erreichen sein.

Literatur

Donath, T. (2009). Private Stromkunden in Deutschland 2009: Smart Metering, Hilden: Nordlight Research.

Faruqui, A., Harris, D. and Hledik, R. (2010). Unlocking the [euro]53 billion savings from smart meters in the EU: How increasing the adoption of dynamic tariffs could make or break the EU's smart grid investment. Energy Policy, Vol. 38, No. 10, pp. 6222-6231.

Institute for Electric Efficiency (IEE) (2011). The Costs and Benefits of Smart Meters for Residential Customers. URL: http://www.edisonfoundation.net/iee/reorts/-IEE_BenefitsofSmartMeters_Final.pdf

Intelliekon (2011). Smart metering in Germany and Austria – results of providing feedback information in a field trial. URL: http://www.isi.fraunhofer.de/isi-de/e/download/working-papers-sustainability-and-innovation/WP6-2011_smart-metering-in-Germany.pdf.

Kranz, J. (2011). Studies on Technology Adoption and Regulation of Smart Grids (Dissertation). epubli Verlag, Berlin.

Leeds, D. (2009). The Smart Grid in 2010: Market Segments, Applications and Industry Players. URL: http://www.gtmresearch.com/report/smart-grid-in-2010.

Verbraucherzentrale Bundesverband (VZBV) (2010). Erfolgsfaktoren von Smart Metering aus Verbrauchersicht. URL: http://www.vzbv.de/mediapics/smart_metering_studie_05_2010.pdf.

Sicherheit im Smart Grid: Sicherheitsarchitekturen für die Domäne Privatkunde

Christoph Krauß

Der Beitrag gibt einen ersten Überblick über Sicherheitsarchitekturen für die Smart Grid Subdomäne Privatkunde, indem relevante Anwendungsfälle vorgestellt werden, welche Sicherheitsanforderungen sich ergeben und wie diese mittels Sicherheitskomponenten in einer Sicherheitsarchitektur realisiert werden können. Erste Schritte in Richtung Sicherheitsarchitektur und deren Umsetzung wurden vom BSI durch die Spezifikation eines Schutzprofils für Gateways vorgenommen. Dieses deckt jedoch nur einen Teil der Subdomäne Privatkunde ab. Dieser Beitrag versucht auch auf die weiteren Komponenten und Schnittstellen einzugehen.

Einleitung

Energie ist eine Grundlage des heutigen Lebens und der Bedarf steigt durch die fortschreitende Industrialisierung immer weiter an. Im Moment befindet sich die Energiewirtschaft in einem starken Umbruch. Katastrophen wie in Fukushima, die immer knapper werdenden fossilen Rohstoffen und der Klimawandel führen zur Abkehr von der Energieerzeugung in großen Atom- oder Kohlekraftwerken. Stattdessen wird Energie in Zukunft vermehrt durch erneuerbare Energien wie Wind-, Sonne- oder Wasserkraft erzeugt.

In der Energiewirtschaft ist die Versorgungssicherheit von zentraler Bedeutung. Diese muss auch bei einer verteilten Energieerzeugung und dem vermehrten Einsatz erneuerbarer Energien gewährleistet sein. Fluktuationen bei der Energieerzeugung und Lastspitzen müssen durch intelligente Steuerungen ausgeglichen werden. Energie muss zwischengespeichert oder bedarfsgerecht transportiert werden, um eine effiziente Energienutzung zu erreichen. Hierfür wird eine Informations- und Telekommunikations- (IKT) Infrastruktur zur dynamischen Steuerung benötigt. Die Kombination der Energietechnik mit der IKT wird auch als Energieinformationsnetz oder im Englischen als Smart Grid bezeichnet.

Das Smart Grid stellt jedoch eine kritische Infrastruktur dar, dessen Ausfall oder partielle Störung gravierende gesellschaftliche und wirtschaftliche Auswirkungen haben würde. Wie der Stuxnet-Wurm [1] Mitte 2010 gezeigt hat, stellen erfolgreiche Angriffe auf Automatisierungstechnologien wie *Supervisory Control and Data Acquisition* (SCADA) Systeme eine große Bedrohung dar. Ein wichtiger Bestandteil eines Smart Grids sind somit geeignete Schutzmaßnahmen, die in die IKT-Infrastrukturen zu integrieren sind, um Angriffe abzuwehren oder zumindest deutlich abzuschwächen. Angriffe können sich zum einen gegen die IKT selber richten (z. B. Stören der Datenübertragung), zum anderen können sich aber auch gezielt der IKT-Strukturen bedienen, um z. B. physische Anlagen zu schädigen. Fragestellungen der Informationssicherheit und des Datenschutzes sind aber aus noch vielen weiteren Gesichtspunkten relevant. So möchte beispielsweise der Energieversorger verhindern, dass sich ein Kunde kostenlos Energie erschleicht indem er Abrechnungsdaten verfälscht. Aus

Kundensicht ergeben sich beispielsweise Fragestellungen der Privatsphäre wenn sich sein Nutzungsverhalten über die erfassten Daten ablesen lässt [8, 12]. Sicherheit muss somit von Beginn an („*Secure by Design*“) und auch während der Laufzeit („*Secure during Ope-ration*“) elementarer Bestandteil des Smart Grids sein [5, 6]. Eine umfassende Einführung in die Thematik der IT-Sicherheit ist u. a. in [4] zu finden.

Im Smart Grid wird zwischen verschiedenen Rollen, denen Aktivitäten zugeordnet sind, unterschieden: Produzent, Energienutzer, Übertragungsnetzbetreiber (TSO), Verteilungsnetzbetreiber (DSO), Energielieferant, Bilanzkreisverantwortlicher, Bilanzkreiskoordinator, Energiehändler, Energiebörse (EEX), Kommunikationsnetzbetreiber, Messstellenbetreiber (MSB), Messdienstleister (MDL), Energiemarktplatzbetreiber, weitere Energiedienstleister, Hersteller (Gerätehersteller, Netzanlagenhersteller, Elektrofahrzeughersteller etc.) und indirekte Rollen (z. B. Standardisierungs- oder Normierungorganisationen) [3]. Diese Rollen sind in einer oder mehreren Domänen aktiv. Eine Domäne grenzt einen Systembereich ab, in dem technische und ökonomische Anwendungsfälle ablaufen. Unterschieden werden die Domänen Erzeugung, Übertragung, Verteilung, Kunde, Märkte, Betrieb und Service [3]. Diese lassen sich noch in weitere Subdomänen unterteilen. Beispielsweise lässt sich der Kunde in Privat- / Haushaltskunde, Gewerbekunde oder Industriekunde unterteilen.

Mit jeder dieser Rollen sind spezifische Sicherheitsanforderungen (z. B. möchte der Kunde seine Privatsphäre gewahrt haben), sowie weitere, meist ökonomische Anforderungen (z. B. möchte der Energielieferant eine möglichst kostengünstige Lösung) verbunden. Die Umsetzung der oftmals entgegengesetzten (Sicherheits-) Anforderungen stellt eine große Herausforderung bei der Entwicklung von Sicherheitsarchitekturen im Smart Grid dar. Um die Komplexität der Aufgabenstellung zu reduzieren, schlagen wir vor, die einzelnen Domänen differenziert zu betrachten, generische Muster für Sicherheitsarchitekturen zu entwerfen, so dass damit systematische Handlungsempfehlungen für die verschiedenen Stake¬holder eines Smart Grid entstehen können. Anhand der Privatkunden-Domäne soll im Folgenden der verfolgte Ansatz in seinen Grundzügen exemplarisch dargestellt werden.

Dieser Artikel präsentiert eine generische Sicherheitsarchitektur für die Domäne Privatkunde. Es werden zunächst sicherheitsrelevante Anwendungsfälle im Smart Grid identifiziert. Aus diesen werden die sich ergebenden Sicherheitsanforderungen abgeleitet, welche durch die Sicherheitsarchitektur erfüllt werden sollen. Die Sicherheitsarchitektur wird anhand eines generischen Netz-Referenzmodells beschrieben, bei dem an definierten Referenzpunkten die wichtigsten Sicherheitskomponenten und deren Schnittstellen erläutert werden.

Dieser Artikel ist eine kurze Vorabversion für eine kommende Publikation im Rahmen des NEWISE-Projekts. Diese wird noch detaillierter auf die Realisierung von Sicherheitsarchitekturen für das Smart Grid eingehen und betrachtet zusätzlich noch die Domäne Verteilnetz und die Einbindung der Elektromobilität in das Smart Grid.

1 Grundlagen

Die Subdomäne Privatkunde stellt aufgrund der vielen Hausanschlüsse eine wesentliche Komponente des Smart Grids dar. Die dort installierten Smart Meter ermöglichen eine zeitgenaue Verbrauchsdatenerfassung welche erst eine bessere Steuerung des Smart Grids ermöglichen. In diesem Abschnitt wird zunächst ein kurzer Überblick über diese Subdomäne gegeben, indem zunächst die beteiligten Rollen kurz beschrieben werden. Anschließend wird eine typische Netztopologie erläutert.

1.1 Rollen und Netztopologie

In der Subdomäne Privatkunde sind die folgenden Rollen relevant: Energienutzer, Verteilnetzbetreiber, Energielieferant, Kommunikationsnetzbetreiber, Messstellenbetreiber (MSB), Messdienstleister (MDL), ggf. weitere Energiedienstleister und Hersteller (z. B. von Smart Metern oder Geräten zur Heimautomatisierung). Der Privatkunde steht in der Rolle Energienutzer im Mittelpunkt dieser Subdomäne. Dieser bezieht Energie von einem Energielieferanten, (der z. B. neben Strom auch Gas und Wasser liefern kann) der als Wiederverkäufer die Energie vom Verteilnetzbetreiber bezieht. Alternativ könnte der Privatkunde seine Energie auch direkt von einem Verteilnetzbetreiber (z. B. Stadtwerke) beziehen. Der Messdienstleister erfasst beim Energienutzer die verbrauchte Energie (mit Hilfe der dort installierten Smart Meter) und liefert diese Information an den Energielieferanten, um damit eine Abrechnung zu ermöglichen. Die Installation und Wartung der Messstellen (d. h. der Smart Meter) erfolgt durch den Messstellenbetreiber. Die Kommunikation aller Rollen untereinander wird durch ein oder mehrere Kommunikationsnetzbetreiber realisiert.

In Zukunft könnte man sich auch vorstellen, dass die Rollen Energiehändler und Energiemarktplatzbetreiber ebenfalls Teil dieser Subdomäne sind, wenn Prosumer ihre erzeugte Energie selbst auf dem Markt anbieten (und nicht wie bisher feste Verträge mit einem Verteilnetzbetreiber haben). Ein Prosumer ist ein Kunde (consumer), der auch selbst Strom z. B. mittels einer Fotovoltaik-Anlage erzeugt und ins Stromnetz einspeist (producer).

Abbildung 1 zeigt eine Referenzarchitektur der Netztopologie der Subdomäne Privathaushalt. Die linke Seite stellt einen Privatkunden in den Rollen Energienutzer und Energielieferant, also als Prosumer dar.

Komponenten in der Abbildung sind Energieverbraucher (z. B. eine Waschmaschine), Energieerzeuger (z. B. die o. g. Fotovoltaik-Anlage), Smart Meter, ein Gateway und ein internetfähiger PC. Der Energienutzer bezieht Strom vom Verteilnetzbetreiber, der Teil des Stromnetzes ist. Der Verbrauch wird durch Smart Meter erfasst, welche durch den Messstellenbetreiber installiert und gewartet (in der Abbildung nicht dargestellt) werden. Ebenfalls wird der vom Prosumer erzeugte Strom gemessen. Die erfassten Messwerte werden zunächst zum Gateway und von dort weiter zum Energieversorger gesendet. In einem Mehrfamilienhaus kann beispielsweise ein einzelnes Gateway die Daten vieler Smart Meter bündeln und weiterleiten [11]. Alternativ können beispielsweise in einem Einfamilienhaus auch Smart Meter direkt in das Gateway integriert sein [2].

Neben Stromzählern können auch weitere Zähler, wie Gas oder Wasser, an ein Multi-Utility-Gateway angeschlossen sein. Diese

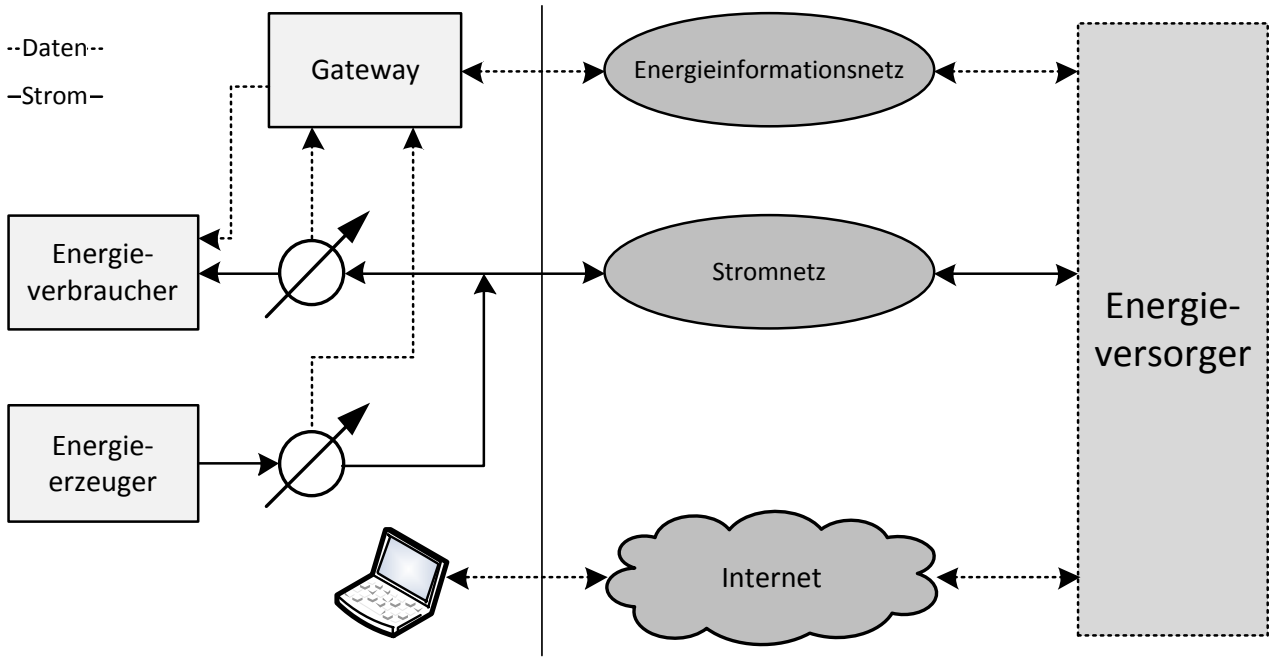


Abb. 1: Netztopologie der Subdomäne Privathaushalt

Zähler werden nach heutigem Stand der Diskussion batteriebetrieben sein und über eine Funkschnittstelle mit dem Gateway kommunizieren.

Die Energieverbraucher sollen in Zukunft auch durch den Energieversorger (in gewissem Maße) über das Energieinformationsnetz per Fernzugriff ferngesteuert werden, um ggf. Engpässe kompensieren zu können (z. B. können die Einsatzzeiten einer Klimaanlage in gewissen Grenzen variiert werden). Weiterhin können Daten (z. B. Preisinformationen) über das Energieinformationsnetz an den Energienutzer gesendet werden.

Daten, d. h. Messwerte oder Kontroll- und Steuersignale, werden zwischen Gateway und Energieversorger über das Energieinformationsnetz ausgetauscht, welches von einem oder mehreren Kommunikationsnetzbetreibern betrieben wird.

Der Energieversorger repräsentiert zur Vereinfachung die Rollen Energielieferant und Messdienstleister, d. h. er sorgt dafür, dass der Energie-nutzer mit Strom versorgt wird, Messwerte erfasst werden, Rechnungen gestellt werden und das Stromnetz optimal genutzt wird. Neben dem Energieinformationsnetz kann der Energieversorger auch Daten über das Internet an den Energienutzer senden oder von dort erhalten.

1.2 Anwendungsfälle

Im Folgenden werden repräsentative Anwendungsfälle (engl. *Use Cases*) und schon erste relevante Schutzziele beschrieben, um daraus anschließend die Sicherheitsanforderungen der einzelnen Rollen abzuleiten. Die Anwendungsfälle basieren größtenteils auf den in [10] beschriebenen sicherheitsrelevanten Anwendungsfällen. In den Anwendungsfällen muss berücksichtigt werden, dass den Rollen

auch gewisse Rechte und Pflichten zugeordnet sind, die sie erfüllen müssen. Beispielsweise sind gewisse Datenschutzanforderungen oder Protokollierungen gesetzlich vorgeschrieben.

Messwerterfassung und -übertragung

Dieser Anwendungsfall beschreibt das Auslesen der Messwerte, um Rechnungen stellen zu können. Zu schützen ist die Vertraulichkeit der beim Kunden erfassten Messwerte (z. B. im Gateway, während der Übertragung und in den verschiedenen (Rechnungs-) Datenbanken. Hierbei sind ebenfalls Datenschutzanforderungen zu erfüllen. Für eine korrekte Abrechnung müssen die Daten authentifiziert und integer sein. Das heißt, es ist sicher zu stellen, dass die Daten von einer eindeutig identifizierbaren Instanz stammen und nicht manipuliert wurden. Weiterhin muss eine Verbindlichkeit gewährleistet sein, so dass der Kunde Rechnungen, die über den Stromverbrauch ausgestellt werden, nicht abstreiten kann. Grundsätzlich muss auch die Verfügbarkeit der Daten gegeben sein. Die entsprechenden Anforderungen sind jedoch nicht sehr hoch; so sind keine Echtzeitanforderungen einzuhalten.

Gewährleistung der Einnahmen

Dieser Anwendungsfall beschreibt den Schutz vor illegalem Energiediebstahl, beispielsweise durch Manipulationen am Smart Meter. Zu schützen ist die Integrität, also der Manipulationsschutz der Messwerte und es muss gewährleistet sein, dass ein Energienutzer die Nutzung nicht abstreiten kann.

Fernanschaltung / Fernabschaltung

Anstatt durch einen Mitarbeiter vor Ort, soll die Energieversorgung durch die installierten Smart Meter über das Smart Grid aktiviert oder deaktiviert werden können, z. B. wenn ein Mieter neu in ein Haus ein- oder auszieht. Zum Schutz gegen unautorisierte Aktivierungen bzw. Deaktivierungen müssen Kontroll- und Steuersignale authentifiziert und integer sein. Weiterhin ist die Verfügbarkeit wichtig, um bei Bedarf den Strom über einen Smart Meter zu aktivieren.

Erkennung und Behandlung von Ausfällen

Dieser Anwendungsfall beschreibt das rechtzeitige Erkennen von Ausfällen (oder auch Fehlsteuerungen des Stromflusses), die schnellstmöglich gemeldet werden sollen. Zu schützen ist die Integrität der Warnmeldungen, damit Ausfälle korrekt gemeldet werden. Da Ausfälle innerhalb weniger Sekunden gemeldet werden sollen, ist die Verfügbarkeit der Kommunikation wichtig.

Wartung

Smart Meter (und Gateways) müssen gewartet werden, z.B. müssen Firmware Updates installiert werden. Die Authentizität und Integrität der Kontroll- und Steuersignale oder Firmware Updates muss gewährleistet sein, um unautorisierte Manipulationen zu verhindern. Verfügbarkeit ist in schwacher Ausprägung (Stunden oder sogar Tage) ebenfalls relevant. Falls personenbezogene Daten während der Wartung übertragen werden, müssen ebenfalls Vertraulichkeit und Datenschutz gewährleistet sein.

Erkennung von Manipulationen

Dieser Anwendungsfall beschreibt die Fähigkeit eines Smart Meters (oder Gateways etc.), ein unautorisiertes Entfernen oder ähnliche physikalische Manipulationen zu erkennen und zu melden. Dies dient dem Schutz

vor Energiediebstahl, dem Schutz gespeicherter Daten wie Zugangs-Passwörtern oder Schlüsseln und soll zudem vor der Installation von Malware durch manipulierte Software schützen.

Echtzeit-Preise

Entsprechend der Verfügbarkeit der Energie werden Preise variabel gestaltet und diese Preisinformationen über AMI, Internet oder andere Datenkanäle an den Kunden gesendet. Dadurch erhält der Kunde die Möglichkeit, seine Energienutzung an den aktuellen Preis zu koppeln und seine Kosten zu reduzieren. Authentizität, Integrität, Verfügbarkeit und Verbindlichkeit der Preisinformationen muss gewährleistet sein da es sonst zu großen finanziellen oder rechtlichen Auswirkungen kommen könnte. Vertraulichkeit und Datenschutz sind hauptsächlich für die Reaktion des Kunden auf die Preisinformationen relevant. Zu berücksichtigen ist hierbei auch, dass die Preise für eine gewisse Zeit garantiert werden müssen. Andernfalls könnte ein Anbieter die Preise kurzzeitig senken bis die Kunden Verbraucher mit einer längeren Laufzeit aktivieren (z. B. Waschmaschine), um dann den Preis anzuheben.

2 Sicherheitsanforderungen

Basierend auf den sicherheitsrelevanten Anwendungsfällen die im vorigen Kapitel vorgestellt wurden, werden nun für die Rollen Energienutzer, Verteilnetzbetreiber, Energielieferant Kommunikationsnetzbetreiber, Messstellenbetreiber (MSB), Messdienstleister (MDL) und Hersteller deren Sicherheitsanforderungen identifiziert. Nicht betrachtet wird aus Platzgründen die Rolle weiterer Energiedienstleister.

Energienutzer

Der Energienutzer hat i.d.R. hohe Anforderungen an den Datenschutz, d. h. die Vertraulichkeit und der Datenschutz der erfassten Messwerte und weiterer Kontroll- und Steuernachrichten (z. B. Reaktionen auf Preisinformationen) muss gewährleistet werden. Dies umfasst zum einen den Schutz gegen externe Dritte, angefangen bei der Erfassung, über die Übertragung, bis zur Speicherung der Daten in (Rechnungs-) Datenbanken des Energielieferanten oder Messdienstleister. Zum anderen sollten auch der Energielieferant und der Messdienstleister nicht in der Lage sein, personenbezogene Daten des Energienutzers auszuwerten.

Weiterhin sollen die Abrechnungen korrekt sein, d. h. gesendete Messwerte müssen korrekt erfasst und, ebenso wie Kontroll- und Steuernachrichten, unverändert an den Energielieferanten oder Messdienstleister übertragen werden, sowie dem richtigen Nutzer zugeordnet werden. Somit muss zum einen die Plattform-Integrität von Smart Meter und Gateway etc. gewährleistet sein, da sonst fehlerhafte oder manipulierte Systemsoftware zu falschen Abrechnungen führen könnte. Dies schließt ebenfalls die korrekte Installation durch den Messstellenbetreiber mit ein. Zum anderen muss die Authentizität und Integrität der Daten bei der Übertragung gewährleistet sein.

Neben den gesendeten Daten müssen auch die empfangenen Daten geschützt werden. Die Authentizität, Integrität, Verfügbarkeit und Verbindlichkeit von Preisinformationen muss gewährleistet werden, damit der Energienutzer rechtzeitig reagieren kann und der Energieversorger diese Preise nicht abstreiten kann. Weiterhin muss die Authentizität und Integrität von Kontroll- und Steuernachrichten

(z. B. vom Energielieferanten zur entfernte Steuerung von Geräten oder Aktivierung / Deaktivierung von Smart Metern) und Firmware Updates (z. B. vom Messstellenbetreiber oder Energielieferant) gewährleistet werden.

Neben dem Schutz der IKT-Komponenten des Smart Grids muss natürlich auch das Stromnetz und dessen Verfügbarkeit gewährleistet sein. Der Energienutzer möchte keine Einschränkungen in der Verfügbarkeit der Energie. Hierzu müssen zum einen etablierte Verfahren der Energiewirtschaft eingesetzt werden, auf die in diesem Beitrag jedoch nicht eingegangen wird. Zum anderen müssen aber auch Verfahren zur Absicherung der IKT eingesetzt werden, da Angriffe auf die IKT-Komponenten potentiell zu Ausfällen oder Fehlsteuerungen des Stromflusses führen können. Hierauf wird nachfolgend bei der Beschreibung der Sicherheitsanforderungen der Verteilnetzbetreiber eingegangen.

Zusammengefasst sind die Sicherheitsanforderungen für den Energienutzer die folgenden:

- Vertraulichkeit und Datenschutz der Messwerte und Kontroll- und Steuernachrichten, die an den Energielieferanten gesendet werden
- Integrität der Plattformen von Smart Meter, Gateway etc.
- Authentizität und Integrität der gesendeten Daten
- Authentizität, Integrität, Verfügbarkeit, Verbindlichkeit von erhaltenen Preisinformationen
- Authentizität und Integrität von empfangenen Kontroll- und Steuernachrichten und Firmware Updates
- Verfügbarkeit der Energie.

Verteilnetzbetreiber

Der Verteilnetzbetreiber hat als eine Hauptanforderung, dass sein Stromnetz verfügbar ist. Neben den oben erwähnten etablierten Verfahren der Energiewirtschaft müssen auch Verfahren der IT-Sicherheit etabliert werden. Beispielsweise müssen Kontroll- und Steuernachrichten zur Steuerung des Verteilnetzes gegen Manipulation geschützt werden. Weiterhin müssen Schutzmaßnahmen gegen Distributed Denial of Service (DDoS) Angriffe getroffen werden bei denen ein Angreifer eine Vielzahl an Smart Metern oder Gateways mit einem Trojaner infiziert, um durch koordiniertes Senden von Falschinformationen das Netz aus dem Tritt zu bringen. Hierzu müssen wirksame Maßnahmen getroffen werden, um das Risiko und die Auswirkungen derartiger Angriffe zu minimieren.

Weiterhin hat der Verteilnetzbetreiber die Anforderung, dass die an Energielieferanten oder Energienutzer gelieferte Energie korrekt abgerechnet wird. Hierzu ist sicherzustellen, dass die Abrechnungsdaten korrekt sind, d. h. keine Manipulationen möglich sind. Dies beinhaltet zum einen die korrekte Installation von Smart Metern, Gateways etc. und den Schutz vor Hardware-Manipulationen. Zum anderen muss die Authentizität und Integrität der erhaltenen Messwerte, die vom MDL erfasst wurden, gewährleistet sein und die Messwerte müssen verfügbar (aber keine Echtzeitanforderungen) sein.

In Zukunft ist mit einer vermehrten Kommunikation zwischen Verteilnetzbetreiber und Energienutzer bzw. Energieerzeuger (Prosumer) zu rechnen, um Aufgrund von Angebot und Nachfrage das Smart Grid besser zu steuern. Beispielsweise werden die Preise

entsprechend von Angebot und Nachfrage geregelt, um den Verbrauch an das Stromangebot anzupassen. Hierzu werden Nachrichten mit Preisinformationen an den Energienutzer gesendet und dieser antwortet z. B. mit der Annahme eines passenden Tarifs. Somit müssen die Authentizität, Integrität und Verfügbarkeit jeglicher Kontroll- und Steuerungsdaten sichergestellt sein.

Auch ist mit einem Anstieg der Kommunikation innerhalb des Verteilnetzes und zwischen Verteilnetz und Übertragungsnetz zu rechnen, um eine möglichst gute Steuerung des Smart Grids zu realisieren.

Zusammengefasst sind die Sicherheitsanforderungen für den Verteilnetzbetreiber die folgenden:

- Verfügbarkeit des Stromnetzes
- Korrekte Abrechnung mit Energielieferant bzw. Energienutzer
- Authentizität, Integrität und Verfügbarkeit von Kontroll- und Steuerungsdaten.

Energielieferant

Der Energielieferant als „Wiederverkäufer“ der vom Verteilnetzbetreiber gelieferten Energie hat implizit ähnliche Sicherheitsanforderungen wie der Verteilnetzbetreiber, d. h. Verfügbarkeit des Stromnetzes und korrekte Abrechnung mit Verteilnetzbetreiber und Energienutzer, sowie die Authentizität, Integrität und Verfügbarkeit von Kontroll- und Steuerungsdaten. Eine Ausnahme bilden ggf. die Kontroll- und Steuerungsdaten, die nur für den Verteilnetzbetreiber zum Betrieb seiner Infrastruktur notwendig sind.

Zusammengefasst sind die Sicherheitsanforderungen für den Energielieferanten die folgenden:

- Verfügbarkeit des Stromnetzes
- Korrekte Abrechnung mit Verteilnetzbetreiber und Energienutzer
- Authentizität, Integrität und Verfügbarkeit von Kontroll- und Steuerungsdaten.

Kommunikationsnetzbetreiber

Ein oder mehrere Kommunikationsnetzbetreiber stellen die Infrastruktur für die Kommunikation im Smart Grid. Sicherheitsanforderungen sind die Verfügbarkeit der Kommunikationsnetzinfrastruktur und die Authentizität und Integrität von Abrechnungsdaten für die Nutzung des Kommunikationsnetzes.

Zusammengefasst sind die Sicherheitsanforderungen für den Kommunikationsnetzbetreiber die folgenden:

- Verfügbarkeit der Kommunikationsnetzinfrastruktur
- Authentizität und Integrität von Abrechnungsdaten für die Nutzung des Kommunikationsnetzes.

Messstellenbetreiber (MSB)

Das Geschäft des MSB ist die korrekte Installation und Wartung von Messstellen wie Smart Metern und Gateways. Der MSB hat somit die Sicherheitsanforderung, dass Messstellen gegenüber Manipulationen geschützt sind. Dies beinhalten sowohl Manipulationen mittels physischen Zugriff, als auch über Kommunikationsschnittstellen. Zur Wartung der Messstellen, dürfen nur autorisierte Entitäten auf die Messstellen zugreifen.

Zusammengefasst sind die Sicherheitsanforderungen für den Messstellenbetreiber die folgenden:

- Schutz von Messstellen gegen Manipulationen

- Autorisierung von Zugriffen auf Messstellen.

Messdienstleister (MDL)

Die Sicherheitsanforderungen des Messdienstleisters sind die Authentizität, Integrität und die Verfügbarkeit (keine Echtzeitanforderungen) der Messwerte, die vom Energienutzer erfasst werden. Diese sind für eine korrekte Abrechnung mit dem Energielieferanten bzw. Verteilnetzbetreiber notwendig.

Zusammengefasst sind die Sicherheitsanforderungen für den Messdienstleister die folgenden:

- Authentizität, Integrität und Verfügbarkeit der Messwerte.

Hersteller

Auf die Sicherheitsanforderungen der Hersteller soll hier nur kurz eingegangen werden. Neben offensichtlichen Anforderungen, wie den Schutz des geistigen Eigentums, spielen aber noch weiter Punkte eine Rolle. Ein Hersteller von Smart Metern und Gateways für die Endkunden-Domäne möchte in erster Linie seine Geräte verkaufen. Um diese verkaufen zu können, müssen sie bestimmten Sicherheitsanforderungen genügen bzw. Sicherheits-Funktionalitäten bereitstellen. So müssen zum einen die Geräte bestimmte gesetzliche Bestimmungen, Normen oder Standards erfüllen. Neben der Einhaltung von Normen zur Funktionssicherheit (z.B. IEC 61850, ISO 9506, IEC 61508) werden beispielsweise Gateways voraus-sichtlich das vom BSI erarbeitete Schutzprofil [2] einhalten müssen. Zum anderen müssen die vom Hersteller produzierten Geräte noch weiteren Sicherheitsanforderungen genügen; beispielsweise aus Akzeptanzgründen. So schreibt das BSI Schutzprofil zwar den Einsatz eines Hardware-Sicherheits-Moduls (HSM) zum Schutz vor Manipulationen des Gateways vor. Für einen Smart Meter, der nicht in ein Gateway integriert ist, ist solch ein HSM jedoch nicht verpflichtend. Wie Sicherheitsanalysen in den Laboren des Fraunhofer AISEC in München jedoch gezeigt haben, sind solche ungeschützten Smart Meter leicht angreifbar. Mittels sehr einfacher Angriffe konnten handelsübliche Smart Meter so manipuliert werden, dass Daten eingeschleust, verändert, abgehört oder unterdrückt werden. So ist es beispielsweise leicht möglich, die Firmware inklusive aller gespeicherten kryptografischen Schlüssel auszulesen und beliebige Manipulationen vorzunehmen. Hierdurch kann sich ein Angreifer beispielsweise leicht kostenlose Energie verschaffen oder mit einem gezielten Angriff einen sehr hohen Energiebedarf vorspiegeln und damit die Versorgungssicherheit eines ganzen Segments gefährden.

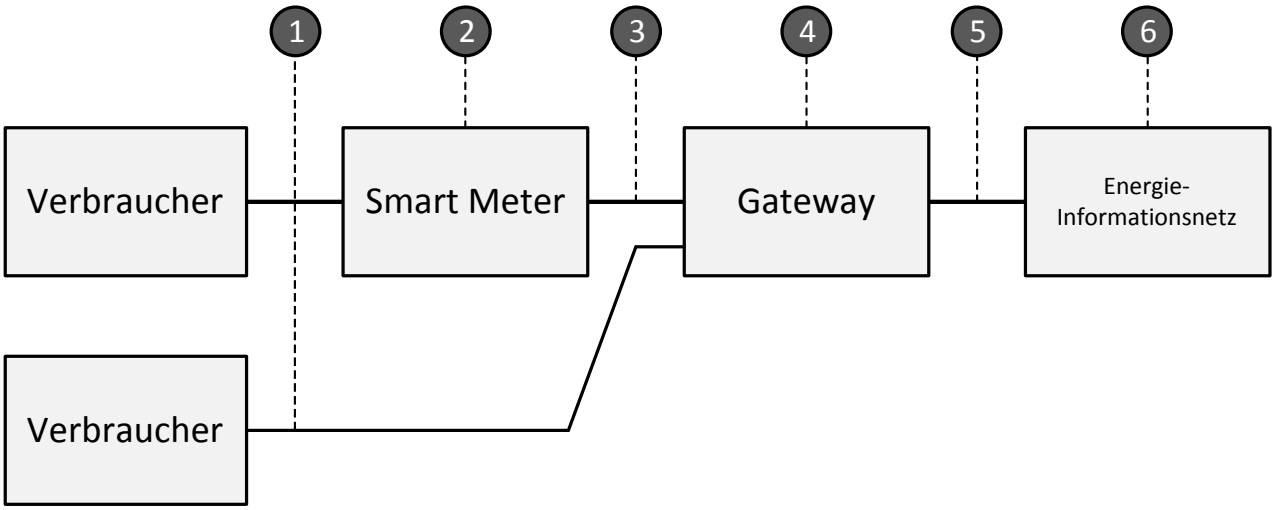


Abb. 2: Netz-Referenzmodell der Subdomäne Privathaushalt mit Referenzpunkten

3 Sicherheitsarchitektur

Im Folgenden wird eine generische Sicherheitsarchitektur für die Smart Grid Subdomäne Privatkunde vorgestellt, welche die in Kapitel 2 beschriebenen Sicherheitsanforderungen erfüllt. Hierzu werden auf einem in diesem Schritt zwangsläufig noch relativ hohem Abstraktionsniveau die wesentlichen Sicherheitskomponenten und deren Schnittstellen anhand eines Netz-Referenzmodells auf der Basis von definierten Referenzpunkten beschrieben. Weiterhin werden schon einige Konzepte zur Umsetzung erläutert.

3.1 Netz-Referenzmodell

Abbildung 2 verallgemeinert Abbildung 1 und zeigt das Netz-Referenzmodell der Subdomäne Privathaushalt. Dargestellt sind die Komponenten Verbraucher (falls der Kunde ein Prosumer ist, könnte dies auch ein Erzeuger sein), Smart Meter, Gateway und das Energieinformationsnetz, sowie deren Beziehungen zueinander. Anhand der Referenzpunkte 1 bis 6 werden nachfolgend die Sicherheitskomponenten der Sicherheitsarchitektur für die Komponenten und Schnittstellen beschrieben.

3.2 Referenzpunkt 1

Referenzpunkt 1 beschreibt die Kommunikation zwischen Verbraucher und Gateway. Dies kann beispielsweise der Fall sein, wenn Verbraucher ferngesteuert werden sollen, z. B. zum Ein- und Ausschalten der Heizung oder Einschalten der Waschmaschine. Dies sollen nur berechtigte Entitäten durchführen dürfen. Somit sind die umzusetzenden Sicherheitskomponenten:

- Mechanismen zur Authentifizierung und Autorisierung zugreifender Entitäten.

Wie eine Umsetzung dieser Sicherheitskomponente aussehen könnte, wird an Referenzpunkt 4 in Kapitel 3.5 beschrieben.

3.3 Referenzpunkt 2

Die Sicherheitskomponenten für Smart Meter leiten sich im Wesentlichen aus den Anforderungen nach korrekter Abrechnung und der Einhaltung des Datenschutzes ab. Es muss sichergestellt werden, dass Smart Meter nicht manipuliert werden und nur Entitäten (Rollen) zugreifen dürfen, welche die entsprechenden Berechtigungen haben. Wenn personenbezogene Daten verarbeitet werden, muss der Datenschutz gewahrt werden. Die umzusetzenden Sicherheitskomponenten sind somit:

- Mechanismen zum Schutz der Plattformintegrität
- Mechanismen zur Authentifizierung und Autorisierung zugreifender Entitäten
- Mechanismen zum Schutz personenbezogener Daten.

Zur Umsetzung des ersten Punktes kann beispielsweise spezielle Hardware eingesetzt werden. Da Smart Meter direkt beim Energienutzer aufgestellt sind (vgl. Abbildung 1), können diese leicht durch direkten physikalischen Kontakt angegriffen werden, um die Firmware zu manipulieren oder um Daten wie kryptografische Schlüssel auszulesen. Ein Angreifer kann hier beispielsweise über zugängliche Schnittstellen (z. B. JTGA, USB) angreifen oder auch fortgeschrittene Angriffstechniken wie Seitenkanalangriffe nutzen.

Bei klassischen Zählern erfolgt der Schutz der Plattformintegrität vor Manipulationen über die Kontrolle der Unversehrtheit von Plomben, die das Gehäuse des Zählers versiegeln. Dies erfordert grundsätzlich eine regelmäßige Überprüfung der Unversehrtheit der Plombe, was einen erheblichen Aufwand und damit Kosten bedeutet. Für Smart Meter bietet sich als Alternative der Einsatz von Hardware Security Modulen (HSM) an, die eine sichere Ausführungsumgebung für (kryptografische) Operationen und sichere Speicherbereiche (z. B. für kryptografische Schlüssel) bieten. Um Manipulationen an Software (außerhalb des HSMs) zu erkennen, bieten viele HSMs Funktionen wie z. B. Plattformintegritätstests, oder Funktionen wie *Remote Attestation*, um die Unversehrtheit der installierten Software gegenüber Dritten nachzuweisen. Durch den Einsatz von HSMs entstehen zusätzliche Kosten, was der Anforderung der Betreiber nach einer möglichst kostengünstigen Lösung widerspricht. Hier ist ein entsprechender Kompromiss zwischen Sicherheit und Wirtschaftlichkeit zu finden. Gegebenenfalls sind für einige Szenarien auch günstigerer HSMs, die geringere Sicherheit bieten, ausreichend. Neben Stromzählern können ggf. auch weitere Zähler wie Gas- und Wasserzähler die an ein Multi-Utility-Gateway angeschlossen sind, mit einem HSM ausgestattet werden.

Eine Authentifizierung kann durch kryptografische Protokolle umgesetzt werden, die beispielsweise die Kenntnis eines Passworts oder kryptografischen Schlüssels überprüfen. Die anschließende Autorisierung kann beispielsweise über Zugriffskontrolllisten oder Rollen-basierte Zugriffskontrolle [7] realisiert werden.

Zum Schutz personenbezogener Daten muss ein ganzheitliches Datenschutzkonzept Teil der Sicherheitsarchitektur sein. Dies wird in Kapitel 3.7 diskutiert.

3.4 Referenzpunkt 3

Referenzpunkt 3 beschreibt die Kommunikation zwischen Smart Meter und Gateway. Hier können unterschiedliche drahtgebundene (z. B. M-Bus [9], Power Line Communica-

tion (PLC)) oder drahtlose (z. B. Wireless M-Bus, Bluetooth, IEEE 802.15.4 Zigbee) Kommunikationstechnologien verwendet werden. Entsprechend der Sicherheitsanforderungen sind die übertragenen Daten vor Abhören und Manipulation zu schützen und es müssen Schutzmaßnahmen gegen (Wieder-) Einschleusen von Daten vorhanden sein. Ebenfalls ist die Verfügbarkeit der Kommunikation sicherzustellen. Die umzusetzenden Sicherheitskomponenten sind somit:

- Mechanismen zur Sicherstellung der Vertraulichkeit der übertragenen Daten
- Mechanismen zum Schutz der Authentizität und Integrität der übertragenen Daten
- Mechanismen zur Sicherstellung der Verlässlichkeit der Kommunikation.

Die Umsetzung dieser Sicherheitskomponenten kann beispielsweise durch die Nutzung der in die jeweilige Technologie integrierten Sicherheitsmechanismen (z. B. Verschlüsselungsmechanismen) erfolgen. So spezifiziert beispielsweise IEEE 802.15.4 Zigbee bereits einsetzbare Mechanismen und viele PLC Geräte haben bereits ebenfalls entsprechende Mechanismen integriert. Gegebenenfalls sind auch keine weiteren Maßnahmen nötig, wenn es sich um ein vollkommen geschlossenes System handelt.

3.5 Referenzpunkt 4

Die Sicherheitskomponenten für Gateways sind relativ ähnlich zu denen der Smart Meter. Da jedoch an Gateways häufig viele Smart Meter angebunden sind, werden hier oftmals höhere Sicherheitsstandards gefordert (vgl. BSI Schutzprofil für Smart Meter [2]). Die umzusetzenden Sicherheitskomponenten sind somit:

- Mechanismen zum Schutz der Plattformintegrität
- Mechanismen zur Authentifizierung und Autorisierung zugreifender Entitäten
- Mechanismen zum Schutz personenbezogener Daten.

Die Umsetzung von Sicherheitskomponenten für Gateways wird detailliert im BSI Schutzprofil [2] beschrieben. Dieses schreibt beispielsweise auch den Einsatz eines HSMs im Gateway vor, um, wie in Kapitel 4.3 beschrieben, die Plattformintegrität zu sichern. Für Smart Meter, die nicht in das Gateway integriert sind, ist aber kein HSM vorgeschrieben.

3.6 Referenzpunkt 5

Referenzpunkt 5 beschreibt die Kommunikation zwischen Gateway und dem Energieinformationsnetz. Diese Kommunikation erfolgt über einen oder mehrere Kommunikationsnetzbetreiber und kann über verschiedene, schon vorhandene Netze, erfolgen, z.B. Telefonnetz, DSL-Anschluss, Kabelnetz, Mobilfunk aber auch PLC oder Glasfaser (*Fiber to the Home*). Die umzusetzenden Sicherheitskomponenten sind ähnlich zu Referenzpunkt 3 müssen aber insbesondere noch den Datenschutz berücksichtigen:

- Mechanismen zur Sicherstellung der Vertraulichkeit der übertragenen Daten
- Mechanismen zum Schutz der Authentizität und Integrität der übertragenen Daten
- Mechanismen zur Sicherstellung der Verlässlichkeit der Kommunikation

- Mechanismen zum Schutz personenbezogener Daten.

Die Umsetzung dieser Sicherheitskomponenten kann mit Protokollen wie TLS (vgl. auch [2]) erfolgen. Die Umsetzung von Mechanismen zum Datenschutz wird in nachfolgendem Kapitel 4.7 diskutiert.

3.7 Referenzpunkt 6

Referenzpunkt 6 beschreibt die Kommunikation im Energieinformationsnetz, welche auch die Kommunikation in Verteilnetzen und Übertragungsnetzen umfasst. Weitere Details zu Sicher-heitskomponenten in Verteilnetzen (und zur Anbindung der Elektromobilität) werden in einer kommenden Publikation des Projekts NEWISE vorgestellt. Grundsätzlich sind die umzusetzenden Sicherheitskomponenten:

- Mechanismen zur Sicherstellung der Vertraulichkeit der übertragenen Daten
- Mechanismen zum Schutz der Authentizität und Integrität der übertragenen Daten
- Mechanismen zur Sicherstellung der Verlässlichkeit der Kommunikation
- Mechanismen zum Schutz personenbezogener Daten.

Die ersten drei Punkte werden detaillierter in der kommenden NEWISE Publikation beschrieben. Hier soll aber noch kurz auf den Aspekt des Datenschutzes eingegangen werden, da die in der Privatkunden-Domäne erfassten personenbezogenen Daten ein ganzheitliches Datenschutzkonzept erforderlich machen. Um ein Abhören dieser Daten zu verhindern sind Verschlüsselungsmechanismen notwendig. Jedoch ist Verschlüsselung alleine nicht ausreichend, da sich meist auch aus verschlüsselten Daten Rückschlüsse ziehen lassen, oder bestimmte Rollen wie der Energieversorger selbst Zugriff auf die unverschlüsselten Daten hat. Dementsprechend sind weiterführende Mechanismen wie Pseudonymisierungs- und Anonymisierungsdienste in die Sicherheitsarchitektur zu integrieren. Weiterhin kann der Datenschutz durch konzeptionelle Ansätze gewahrt werden, indem beispielsweise personenbezogene Daten mehrerer Privatkunden aggregiert werden und somit keine individuellen Rückschlüsse mehr möglich sind.

3 Ausblick

In einer kommenden Publikation im Rahmen des NEWISE-Projekts werden diese Überlegungen noch detaillierter weiter geführt und auf die Domäne Verteilnetz ausgeweitet. Weiterhin werden die Sicherheitsaspekte bei der Integration der Elektromobilität in das Smart Grid diskutiert.

Literatur

[1] M. Brunner, H. Hofinger, C. Krauß, C. Roblee, P. Schoo, S. Todt. Infiltrating critical infra-structures with next-generation attacks: W32.Stuxnet as a showcase threat. Technical report, Fraunhofer SIT Munich, December 2010.

[2] Bundesamt für Sicherheit in der Informationstechnik BSI. Protection Profile for the Gate-way of a Smart Metering System, 2011.

[3] Deutsche Kommission Elektrotechnik Informationstechnik im DIN und VDE. Die deutsche Normungsroadmap E-Energy / Smart Grid, Version 1.0. Technical report, DKE, März 2010.

[4] C. Eckert. IT-Sicherheit: Konzepte, Verfahren, Protokolle. 7. Auflage. Oldenbourg-Verlag. 2011

[5] C. Eckert, C. Krauß. Sicherheit im Smart Grid – Herausforderungen und Handlungsempfehlungen. Datenschutz und Datensicherheit, 8:535–541, 2011.

[6] C. Eckert, C. Krauß, P. Schoo. Sicherheit im Smart Grid – Eckpunkte für ein Energieinformationsnetz. Stiftung-Verbundkolleg / Projekt Newise Nr. 90, 2011.

[7] D. Ferraiolo, D. Kuhn. Role-based access control. In 15th National Computer Security Conference, 1992.

[8] Heise Online. Intelligente Stromnetze: Ich weiß, ob du gestern geduscht hast. http://www.heise.de/security/meldung/Intelligente-Stromnetze-Ich-weiss-ob-du-gestern-geduscht-hast-864221.html.

[9] M-Bus standard. EN 13757. http://www.m-bus.com.

[10] NIST. Guidelines for Smart Grid Cyber Se-curity: Vol. 3, Supportive Analyses and Ref-erences. NISTIR 7628, August 2010.

[11] H. Orlamünder. Der Einsatz von Informations- und Kommunikationstechnik in Stromnetzen – ein nachhaltiges Energieinformationsnetz. Stiftung-Verbundkolleg / Projekt Newise Nr. 85, 2009.

[12] D. L. U. Greveler, B. Justus. Hintergrund und experimentelle Ergebnisse zum Thema „Smart Meter und Datenschutz“. Technical Report, FH Münster, September 2011.

Forschungsfragen zum Energieinformationsnetz

Dieter Klumpp

Auch wenn es 2011 schon Produkte für Smart Metering und Dienste eines Smart Grid zu kaufen gibt, so ist doch unübersehbar, dass eine Marktreife im Sinne eines für alle Beteiligten akzeptablen Infrastrukturguts noch nicht gegeben ist. Bei der auch im politischen Raum absolut einhelligen Einschätzung, dass ein „Smart Grid" einen wunderbaren Beitrag für alle unsere Energie- und Umweltnöte darstellt, wird noch übersehen, dass eine gemeinsam gewünschte Zukunft die Gegenwart realweltlich noch nicht entscheidend verändert. Alle einzelnen Punkte in diesem Beitrag müssen deswegen noch mit einem Fragezeichen als „vorläufig" versehen werden. Es gibt – vollends nach Fukushima – eine weltweit und auch in Deutschland hoch wogende Diskussion über die Möglichkeiten eines „intelligenten" Stromnetzes (eines „Smart Grid"), aber keinen strukturierten Diskurs. Denn in allen Fällen eines Diskurses (wenn er denn keine Kreislaufdiskussion werden soll) muss erst einmal ein „prädiskursives Einverständnis über den Diskursgegenstand" (C. F. Gethmann) hergestellt sein. Dies schließt im Frühstadium methodisch ein Ausrufezeichen aus. „Gewissheiten" stehen erst am Ende eines Fachdiskurses. Um es auch aktuell (nicht nur für Stuttgarter) deutlich zu machen: Ein transparent geführter früher Expertendiskurs erspart den späten Schlichter.

Schon die ersten beiden Konferenzen der Alcatel-Lucent Stiftung im Rahmen des Projekts NEWISE (Nachhaltiges Energieinformationsnetz[1] – Sicherung Energieversorgung) in Stuttgart[2] und Berlin[3], insbesondere aber die intensive Nachbereitung in der transdisziplinären Arbeitsgruppe aus Wissenschaft und Praxis zeigten zahlreiche Forschungsfragen auf, vor allem aber die dringende Notwendigkeit einer diskursiven Auseinandersetzung mit den Gestaltungsanforderungen für ein Nachhaltiges Energieinformationsnetz. Denn es geht nicht nur um Messwerte oder andere exakte Zahlen allein, es müssen auch für den Akteurskreis Empfehlungen für konsensuelle Festlegungen erarbeitet werden. Während zum Beispiel – bei aller Unterschiedlichkeit der jeweiligen Definition – im Punkt „Nachhaltigkeit" über das Ziel Einigkeit herrscht, sind bei Punkten wie „Datensicherheit"; „Datenschutz" und „Wettbewerb" noch deutliche Unterschiede in der global geführten Diskussion erkennbar.

Die Gemengelage von freiem Marktmechanismus hier und den der sozialen und ökologischen Marktwirtschaft immanenten Ordnungsprinzipien und Ordnungsmechanismen bis hin zu Regulierung und Intervention wird meist mit dem Begriff „Rahmenbedingungen" gearbeitet. Auch 20 Jahre nach dem weltweiten Fiasko der „bürokratisch-dirigistischen Staatszwangswirtschaften" schaudert es manchen Diskutanten (speziell in der Politik) bei Worten wie „Planung" oder „Rahmenziehung" immer noch. Als positiv besetzten Ausdruck spricht man zum Beispiel in der EU von

---

1 Der Begriff „Energieinformationsnetz" wurde im Rahmen von NEWISE als deutsche Sachbezeichnung (ohne „smart") eingeführt.

2 Vgl. Roßnagel, Alexander; Jandt Silke: Datenschutzfragen eines Energieinformationsnetzes, Stiftungsreihe Nr. 88, Stuttgart 2009

3 Siehe im Web www.stiftungaktuell.de http://www.stiftungaktuell.de/index.php?article_id=32; Vgl. Raabe, O./ Pallas, F./ Weis, Eva/ Lorenz, Mieke/Boesche, K.V. (Hrsg.), Datenschutz in Smart Grids, London/Berlin 2011

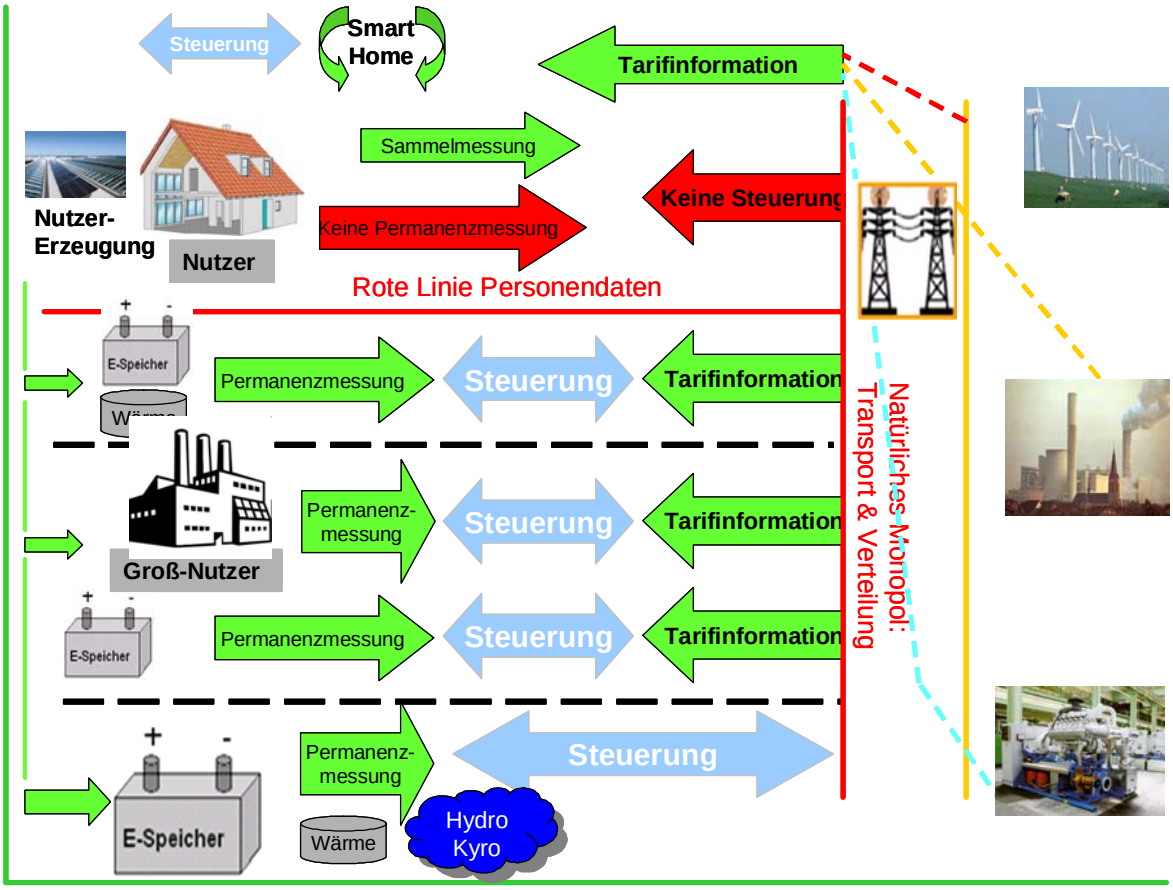
„Innovation Framework“, dem nach meinem Vorschlag der deutsche Ausdruck „Innovationsrahmen“ entspräche.

Der Begriff „Innovationsrahmen“ soll ein verfolgbares und umsetzbares Leitbild in der (als Sammelbegriff verstandenen) Informationsgesellschaft beschreiben, das auf frühzeitige Rahmengestaltung für Technologien, Märkte und Gesellschaftsorganisationen im Zusammenwirken von Wissenschaft, Wirtschaft, Politik und Gesellschaft abzielt. Besonders gilt die Notwendigkeit zur Darstellung des Innovationsrahmens für „große“ (sprich: lang laufende und/oder teure öffentliche) Projekte. In Deutschland würde ein präzise erarbeiteter Innovationsrahmen einer offenen Welt zum Beispiel signalisieren, dass über 8 % des IKT-Weltmarkts zu Importen locken oder auch, dass zunächst 80 Millionen Menschen in Deutschland und weiteren 350 Millionen EU-Menschen zum Nachweis der Akzeptanz im Markt eingeladen werden. Nur wer den Innovationsrahmen nicht einhält, der bleibt beim deutschen Markt eben außen vor.

„Akzeptanz“ kann allerdings erst empirisch erfasst werden, wenn ein Sachverhalt eingetreten ist. Dies kann der Griff in den Geldbeutel für ein Konsumgut ebenso sein wie die Zustimmung der Bürger zur Ausgabe öffentlicher Gelder, eben die „Abstimmung an der Wahlurne des Marktes“, wie sie F. A. von Hayek treffend beschrieben hat. Nicht nur Juristen, auch Ökonomen lieben den Sachverhalt und beurteilen diesen gerne, nur leider: die Zukunft aber ist kein Sachverhalt. Nun muss man die Zukunft mit ihren künftigen Sachverhalten aber nicht gleich ausschließlich den Zukunftsforschern zuschieben, alle Wissenschaftsdisziplinen samt der Praxis können mit dem Leitbild der „Akzeptabilität“ sehr wohl umgehen. Mit der methodischen Beachtung der „Akzeptabilität“ als Gestaltungskriterium[4] kann verhindert werden, dass der Akteursgeleitzug über der Zeitachse der Realisierung gegen bereits heute klar erkennbare künftige Grenzen anrennt. Plastisch ausgedrückt: Wenn erst einmal intelligente Ingenieure oder Physiker auch intelligente Juristen oder Ökonomen zu verstehen lernen, braucht man kein „intelligenteres“ Stromnetz als das heutige. In Hochglanzbroschürensprache: Kein Chip kennt die Zukunft. Auch in der jüngeren Innovationsgeschichte der IKT sind hinreichend Fälle bekannt, in denen unverantwortlicher Weise mit einem Euphemismus auf eine „hohe Anpassungsflexibilität“ von Verfassungen, Gesetzen oder gar des Verbraucherverhaltens spekuliert wurde. Es gilt also, die notwendigen interdisziplinären Analysen im Zusammenwirken der gesellschaftlichen Subsysteme mit diskursgestützten konsensuellen Empfehlungen gerade aus dem Expertenkreis zu verbinden.

Mit der heuristischen Skizze wird versucht, die Komplexität der noch offenen Diskussionspunkte so weit zu reduzieren, dass Einzelpunkte bearbeitet werden können, ohne den Systemzusammenhang aus dem Auge zu verlieren. Dabei flossen bereits – durchaus vorläufige – „Annahmen“ in die Darstellung ein. So sind hier die drei Sektoren „Privatnutzung“, „Gewerbe-/Großnutzung“ und „Energie-Massenspeicher-Nutzung“ deswegen als unterschiedliche Ebenen dargestellt, weil sich bei „privater“ oder „gewerblicher“ Nutzung die Frage nach dem Schutz der Personendaten sehr unterschiedlich stellt.

[4] Vgl. Grunwald, Armin, Zur Rolle von Akzeptanz und Akzeptabilität von Technik bei der Bewältigung von Technikkonflikten. In: Technikfolgenabschätzung – Theorie und Praxis, Nr. 3, 14. Jahrgang – Dezember 2005, S. 54-60



In allen drei Sektoren wiederum ist der Charakter des Wettbewerbs jeweils ein anderer: Während der Privatnutzer seine Nachfragemacht über verkürzte Stromanbieterwechsel voll zur Entfaltung bringen kann (und soll), will der gewerbliche Nutzer vor allem mittelfristige Berechenbarkeit. Je größer der Nutzerbetrieb, desto eher will er mit „seinem“ Versorger in bilaterale Preisverhandlungen über das nächste Planjahr (bei öffentlichen Unternehmen das nächste Haushaltsjahr) eintreten, wobei in der Praxis die Drohung mit einem Anbieterwechsel eher als Ultima Ratio erscheint. Kein Unternehmen kann und will wie der einzelne Verbraucher auf „Sonderangebote“ oder auf eine bestimmte Energieproduktion hin reagieren, es zählen Betriebswirtschaft und Berechenbarkeit, also der günstigste Preis über den längsten Zeitraum. Dafür bedarf es keines Smart Meters in jedem Büro.

Unstrittig ist in der Diskussion, dass der Wettbewerb als Instrument vor allem für die Endverbraucher von erheblichem Vorteil ist. In diesem Zusammenhang wird noch eine „Goldene Linie“ für den Wettbewerb gesucht, der – richtig eingesetzt – zu einem Innovationstreiber wird, der aber wie (vice versa) ein Monopol auch zu einer veritablen Innovationsbremse werden kann, wenn er zu „ruinösem Wettbewerb“ ausartet. Bei Infrastrukturen führt ruinöser Wettbewerb dazu, dass alle mitmachen, aber keiner beginnen will. Es bietet sich für ein Smart Grid kein Infrastrukturwettbewerb an, jedoch ein „Wettbewerb der Tarife“, die untersucht und gestaltet werden

müssen. Ob die Wettbewerbsmuster der in Europa 1998 liberalisierten Telekommunikation im Detail übernommen werden können, ist noch nicht abschließend untersucht, eine kurze Studie aus der Universität Gießen vom April 2010 war Fragen auf.

Beim dritten Sektor, der Makro-Energiespeicherung, ist hingegen noch kein Ansatz bekannt geworden, inwieweit ein Anbieter-Wettbewerb an einem Standort eine Funktion übernehmen könnte. Hingegen deuten sich neue Formen der Gemeinschaftlichkeit an, von einer „Energienachbarschaft“ über „Kommunal-Korporatismus“ bis hin zu „Globaler Energiesolidarität“. Solche neuen energieökonomischen Modelle harren noch der Ausarbeitung.

1 Gefunden? Grüne Linie Nachhaltigkeit

Für alle drei Sektoren gilt das umfassende Ziel der Nachhaltigkeit des globalen Energieversorgungssystems. In diesem Rahmen findet sich das von den Werbeagenturen höchst erfolgreich platzierte Wort von der „Green IT“ („selbst sparsam und/oder bei anderen sparend“) ebenso wieder wie der Anteil der Energieerzeugung für (bzw. gegen) das klimatische Gleichgewicht. Kein Zweifel darf bestehen, dass diese externen Faktoren auf die „Grüne Linie“ einwirken: Wenn es denn knapp und teuer wird, beginnt diese Linie zu oszillieren, sprich: sie muss angepasst werden. Umso wichtiger ist es, diese in der Diskussion vorgefundene konsensuelle „Grüne Linie“ exakter und ausführlicher als die Hochglanzbroschüren zu definieren und sie auf mittlere und längere Planungszeiträume kalkulierbar auch festzuschreiben. Im Verfolg der Kyoto-Vereinbarungen wird dies zumindest angestrebt.

Aber gerade für ein „Nachhaltiges Energieinformationsnetz“ gilt schon heute, dass es auch für denkbare künftige Anforderungen spezifiziert werden muss. Schon an dieser Stelle sei schon auf die Diskrepanz der zeitlichen Planungshorizonte im Akteurskreis hingewiesen. Während die Ökonomien der Energieversorger und der Hauseigentümer, sich hinsichtlich Investitionen durchaus auf zwanzig oder dreißig Jahre ausrichten, ist dies im IKT-Sektor schon längst nicht mehr der Fall. Die ehemaligen Fernmelde-Monopolisten werden sogar als abschreckendes Muster für „mangelnde Umsetzungsgeschwindigkeit“ bis heute auch in Fachkreisen vorgeführt, weil ihr Planungshorizont für die Verkabelung eines Standorts mit Kupfer-Doppeladern im Durchschnitt 15 Jahre betrug. Noch beim Aufbau des Kupfer-Koaxialnetzes für TV-Verteilung, der in weniger als zehn Jahren nach 1984 erfolgte, pochten die Haus- und Grundstücksbesitzer bei Neubauten auf eine „nachhaltige“ Hausverkabelung mit einer Planungsreichweite von 30 Jahren.[5] Die mittlerweile entstandene „Software-Ökonomie“ gerade in der IKT-Branche hingegen läuft (wie viele andere Branchen mit Unterstützung der Banken) auf einen Nahhorizont von maximal drei Jahren für den Payback der getätigten Investitionen hinaus.

Als bereits gesichert kann auch aus der bisherigen NEWISE-Diskussion gelten, dass ein Energieinformationsnetz (sofern es nicht auf den vorhandenen, von der Quelle zur Senke unveränderten Kabel-Infrastrukturen implementiert wird) baulich auf mindestens Jahrzehnte hin „zukunftssicher“ realisiert werden

[5] So wurden 1997 ff von einem in Berlin ansässigen Kabelbetreiber in Abstimmung mit dem Hausbesitzerverband Neubauten „vorsorglich“ mit einem Sternnetz in Koaxialtechnik anstelle des um Faktoren preisgünstigeren Baumnetzes ausgerüstet.

muss. Wer auch immer die Software für dieses Netz bereitstellt, sollte davon ausgehen, dass sowohl Energieversorger wie Hauseigentümer dem regelmäßigen „Upgrade“ (inklusive eines „patching“) der Software sehr kritisch gegenüberstehen, einen regelmäßigen Vor-Ort-Einsatz von Servicetechnikern aus Kostengründen sogar kategorisch ablehnen.

Eine durch externe Faktoren wie absoluten Energiemangel nicht auszuschließende „Flexibilisierung“ (Kontrolle, Steuerung, Abschaltung) der Grundarchitektur eines Energieinformationsnetzes in Richtung einer notwendigen Zwangsbewirtschaftung ist in der fachöffentlichen Diskussion noch nicht erfolgt. Diese sollte im Zuge der „Sicherung Kritischer Infrastrukturen“ alsbald nachgeholt werden. Denn wenn nach bestem Wissen der neutral ausgewiesenen Experten damit gerechnet werden muss, dass im Planungszeitraum auch für die Privatnutzer „Stromkontingentierung“ (in unterschiedlichen Granularitäten) erfolgen muss, sollte dies in die Spezifikation aufgenommen werden. Friktionen mit dem Schutz der Personendaten, vor allem aber der Unverletzlichkeit der Wohnung, wären nicht auszuschließen. Hingegen erscheint im gewerblichen Bereich insbesondere der Großnutzer eine derartige „Notstands-Flexibilität“ durchaus diskutierbar zu sein.

Zum „Nachhaltigkeitsziel“ für ein System der Energieversorgung gehört auch die Lösung der Notstromversorgung in einer zunehmend von Strom abhängigen Gesellschaft. Ein temporärer Stromausfall bedroht in unseren geographischen Breiten und entwickelten Gesellschaften kein Menschenleben. Ganz im Gegenteil haben große „Blackouts“ wie der zweitägige Blackout in New York am 13./14. Juli 1977 trotz oder wegen des Ausfalls von TV und Klimaanlagen schon 1978 positive familienstatistische Folgen gezeitigt, die vielleicht für manche kriminelle Taten wie Plünderung und Brandstiftung einen Trost boten. In einer „alternden“ Bevölkerung mit einem hohen „Single-Anteil“ muss jedoch damit gerechnet werden, dass die Gesundheit von Menschen, die von stromgespeisten Apparaten abhängig sind, schon bei einem nur mehrstündigen Stromausfall ernsthaft gefährdet ist. Ebenso gilt, dass Schutz vor dem Ausfall von (über die Akku-Kapazität hinausgehenden) elektrischen Kommunikationseinrichtungen gerade im Vorfeld einer „Telemedizin“ durch eine Notstromversorgung gesichert sein muss. Wenn alte und kranke Menschen als Alleinstehende auf ein automatisiertes Tele-Monitoring angewiesen sind, darf es überhaupt keinen Netzausfall geben. Das durchaus mit anschaulichen Projekten wie „Erfolgreiche Geschäftsmodelle telemedizinischer Dienstleistungen“ erforschte Anwendungsgebiet der Telemedizin sieht solche Ausfälle nicht vor.[6]

Eine Notstromversorgung für das Heim wäre nach dem Stand der Diskussion über das „Smart Home“ gewiss vorgesehen und würde zwar von den Pionierkonsumenten im Elektroniksupermarkt schon allein zur Sicherung des High-Definition-Plasmaschirms mitgekauft werden. Dem Telemedizin-Patienten hingegen bliebe nur der Versuch, einen leistungsstarken Notfall-Akku zusammen mit der Telemonitoring-Einrichtung und anderen medizinischen Hilfsgeräten vom staatlichen Gesundheitssystem zu beziehen.

Auch hierüber steht eine rechtzeitige Expertendiskussion aus. So hat selbst ein Basispapier der ITG den Notstromaspekt noch nicht

[6] Vgl. für viele http://www1.vde.com/WBB/PMM/-Telemonitoring+Vorteile/

behandelt.[7] Es kann an dieser Stelle nur vermutet werden, dass angesichts der absehbaren Alterspyramide eine Nutzung von „Nachbarschaftsspeichern" für die Notstromversorgung auch der ökonomisch günstigste Weg wäre. Eine umfassende Studie mit gemeinschaftlich zu normierenden Gestaltungsempfehlungen steht dazu noch aus.

2 Vorgeschlagen? Rote Linie Personendaten

Einigkeit herrscht bei allen Akteuren darüber, dass die „Sicherstellung des Datenschutzes unabdingbarer Bestandteil aller Kommunikationsnetze ist". Aber anders als bei der noch etwas oszillierenden „Grünen Linie Nachhaltigkeit" stellt sich die Einschätzung beim Datenschutz etwas präziser und damit polarisierbarer dar. Die in der Heuristik getroffene Unterscheidung der Sektoren „privat, geschäftlich, gemeinschaftlich" lenkt die Aufmerksamkeit direkt auf den Sektor der privaten Nutzer, also auf das Haus und die Wohnung, denn ohne Zweifel ist die Privatheit dort residual. Zugespitzt: Für von natürlichen Personen *geschäftlich* genutzte Energie gilt wahrscheinlich kein „Energieverbrauchsgeheimnis". Auch wenn es doch ein gewisses Abgrenzungsproblem zwischen Privatnutzer und Geschäftsnutzer gibt (der „ambulante Blumenhändler aus dem Hamburger OLG-Urteil zur elektronischen Steuererklärung" ist ja geläufig), so erscheint dies lösbar. Eine „Rote Linie Personendaten in der Wohnung" ist also im Prinzip schon gezogen. Die entsprechenden Punkte aus der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010 lauten hierzu:

„Die detaillierte Erfassung des Energieverbrauchs kann zu tief greifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch die langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff sind weitere Gefährdungen der Privatsphäre der Betroffenen zu befürchten."

Vor einem oberflächlichen Abwägungsprozess zwischen zwei gleichermaßen erstrebenswerten Zielen wird zu Recht gewarnt: „Eine effiziente Energiedistribution und -nutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen einhergehen. Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen im Energiewirtschaftsgesetz schützen die Privatsphäre der Betroffenen jedoch nur unzureichend." Aber gerade die Datenschutzexperten des ULD in Kiel wissen, dass ein intensiver Abwägungsprozess unvermeidlich, aber nur diskursiv zu lösen ist.

Allerdings gehen die Datenschutzbeauftragten noch vom 2010 vorherrschenden Bild eines „sekundengenauen Smart Grid" aus: Die Erklärung sagt: „Digitale Zähler ermöglichen die sekundengenaue Erfassung des Verbrauchs. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können". Auch das Gutachten des ULD sieht sekundengenaues: „Abrechnungsrelevante Daten sind die Informationen, die Auskunft über die entnommene Energiemenge (kWh) geben. (…) Steuerungsrelevante Daten bein-

[7] (ITG 2010) Energieinformationsnetze und –systeme. Bestandsaufnahme und Entwicklungstendenzen. Ein Positionspapier der Informationstechnischen Gesellschaft im VDE (ITG), Frankfurt 2010

halten zusätzliche Informationen darüber, wann in welcher Menge Energie durch den Abnehmer verbraucht wird. Letztere sind erforderlich, um ein individuelles Lastprofil, d. h. den zeitlichen Verlauf der abgenommenen Energieleistung über einen bestimmten Zeitraum zu erstellen. Lastprofile für elektrische Energie werden in der Regel in 15minütigen Zeitintervallen erstellt. Dadurch können im Jahr über 35.000 Messpunkte entstehen. Außerdem besitzen die Zähler die Fähigkeit, sekundengenau Verbräuche zu erfassen. Damit wird die Identifizierung einzelner Geräte über den spezifischen Energieverbrauch möglich."[8]

Die im Smart Grid tatsächlich stattfindende „sekundengenaue Messung" könnte ein größeres Missverständnis nach sich ziehen. Denn diese sekundengenaue Messung gibt es schon immer auch beim analogen Ferrariszähler[9], was das sich drehende waagrechte Rädchen auch anzeigt. Dennoch wurde dieser sekundengenaue Zähler bekanntlich nur einmal pro Jahr „abgelesen". Dass ein „sekundengenaues Smart Grid" droht, ist auch deswegen wenig wahrscheinlich, weil die erzeugte Datenmenge allein in Deutschland die Datenmenge aller weltweiten E-Mails zusammen übersteigen würde. Dirk Fox und Klaus J. Müller haben in ihrem Beitrag in dieser Stiftungsreihe darauf hingewiesen, dass antizipierte Einschätzungen der Interessen der anderen Seiten zur Legendenbildung beitragen können.

Aber zutreffend ist, dass es im Smart Grid um die Granularität des Ablesens respektive des Datenabfrageintervalls geht. Hierbei werden sich absehbar aufgrund der überwiegend monatlichen Zahlungsmodelle von Großanbietern und Großabnehmern nicht einmal fünfzehnminütige Intervalle einrichten lassen, sondern monatliche Rhythmen (Zahlung mit Dauerauftrag bzw. Bankeinzug) durchsetzen bzw. Modelle, die sich auf die Kündigungsfrist beim Anbieterwechsel beziehen. Die Frage nach der erforderlichen Granularität der „Ablesungsintervalle" ist durch ganz praktische Fragen geprägt: Was wird in der Wertschöpfungskette, in der Versorgungskette, in der Informationskette an Daten benötigt? Und dabei kommen in der Diskussion vor allem Anforderungen aus dem „Wettbewerb der Tarife", die untersucht werden müssen. Die Übertragung von Energienutzungsdaten aus dem Haushalt hin zu einem Energienetz-Betreiber, zum Messstellenbetreiber bzw. zu einem intermediären „Energieinformations-Dienstebetreiber" werden aus verschiedenen Perspektiven als „Business Modell" angedeutet, sind aber nirgends konzise dargelegt. Ein übergreifender Ansatz von „Geschäftsmodellen für Infrastrukturen" gerade auch für die Privatwirtschaft ist noch nicht erkennbar.

Es erscheint also bereits eine klare „Rote Linie Personendaten" heute und auch für den Planungszeitraum der nächsten Jahrzehnte. Während der CCC-Sicherheitsexperte beim „Smart Metering" (und anderen Diensten wie z. B. DE-Mail) auf dem jüngsten CCC-Jahreskongress unter dem Beifall aller nur noch nach „Popcorn!" rufen konnte (id est: „Man kann als Experte nur staunend zuschauen, welch absehbarer Unsinn dort unerbittlich realisiert wird"), beschrieb Alexander Roßnagel auf der jährlichen Stiftungskonferenz „Allianz von Recht und Technik 2010 in

[8] Karg, Moritz, ULD Schleswig-Holstein, Datenschutzrechtliche Bewertung des Einsatzes von „intelligenten" Messeinrichtungen für die Messung von gelieferter Energie (Smart Meter), Kiel, 25.09.2009

[9] Bildnachweis unter www.econitor.de/magazin/wohnen/strom/smart-meter-verbraucher-freundliches-energiemanagement-1351.html

Stuttgart neben anderen Akzeptabilitätskriterien den erforderlichen rechtspolitischen Innovationsrahmen.[10] Demnach gilt es, die Einführung eines „Energiegeheimnisses“ sogar als strafgesetzliche Verpflichtung zur Geheimhaltung (wie bei Anwälten oder Ärzten) zu verankern. Dies bedeutet für einen Dienstebetreiber auch strafrechtliche Sanktionen bei Pflichtverstoß (§ 203 StGB – Verletzung von Privatgeheimnissen).

Auch wenn Internet-Juristen wie Thomas Hoeren[11] eine denkbare Problemlösung noch auf der Ebene eines novellierten Bundesdatenschutzgesetzes, also noch nicht als Offizialdelikt, sehen, so ist doch eine erhebliche Erkenntnis selbst für die powerpointigsten Interessensvertreter unvermeidlich. So oder so: Was bislang für die Amerikaner und einige Europäer als Datenfluss eines „Smart Grid“ erstrebenswert oder noch tolerabel erscheint, wird im Geltungsbereich des Grundgesetzes und den meisten EU-Länder-Verfassungen keinen Bestand haben.

Gerade dieser Punkt führt in der deutschen Diskussion stets zu einer Lagerbildung: Eine Seite sieht den Standort Deutschland durch “überzogene und typisch deutsche“ Datenschutzanforderungen gerade im globalen Bereich gefährdet und fordert „die Politik“ per TV-Nachrichten zum Handeln auf, während das andere Lager in ein vielstimmiges „Warten auf Karlsruhe“ und per Tweet oder Facebook in tiefe Skepsis gegenüber „der Politik“ verfällt. Beide Lager räumen angesichts der Realität zwar übereinstimmend ein, dass „die USA in einer Sondersituation sind“, wobei von den einen immer noch das Erfolgsmuster des amerikanischen Business-Modells, von den anderen die Rolle der weltpolitischen Supermacht einschließlich ihres dauerhaften Kriegszustandes als Erklärung herangezogen wird.

Beiden Lagern muss man entgegenhalten, dass in Wirklichkeit „die Amerikaner“ der europäischen und damit auch der deutschen Datenschutzdiskussion um mehrere Jahre voraus sind. So schreiben Blumberg und Eckersley im August 2009 für die „Electronic Frontier Foundation“ als „Conclusion” ihres Beitrags „Lokationsdatenschutz und wie man vermeidet, die Privatheit für immer zu verlieren“ in zwei Sätzen die schlichte rechtsstaatliche Lösung für das Gegebene und die ebenso überzeugende Grundlage für das Künftige:

“In the long run, the decision about when we retain our location privacy (and the limited circumstances under which we will surrender it) should be set by democratic action and lawmaking. Now is a key moment for organizations that are building and deploying location data infrastructure to show leadership and select designs that are responsible and do not surrender the locational privacy of users simply for expediency.”[12]

Dies sind nun nicht etwa hilflose Appelle, auch das US-Businesssystem zeigt seine Lernfähigkeit: Wenn denn ein Fehler entdeckt wird, bedarf es keiner Verordnung, diesen zu korrigieren. Im Februar 2010 zeigte die Web-Site “Please Rob Me” (eingerichtet, um Bewusstsein über das eigene Informationsweitergabeverhalten aufzubauen), dass Lokati-

[10] Vgl. Roßnagel, A. (Hrsg.), Nutzerschutz – Rechtsrahmen, Technikpotenziale, Wirtschaftskonzepte, Schriftenreihe des Instituts für Europäisches Medienrecht (EMR), Band 41, Baden-Baden 2011 (im Erscheinen).

[11] Im E-Mailing mit dem Verfasser, Dez. 2010

[12] Blumberg, Andrew J / Eckersley, Peter, On Locational Privacy, and How to Avoid Losing it For-ever. Electronic Frontier Foundation, eff.org, August 2009, S. 7

onsdaten per Twitter über den Dienst Foursquare sogar zum kriminellen Gebrauch einluden. Als der "Weißhut-Hacker" Jesper Andersen dies entdeckte, brauchte das Soziale Netzwerk nicht lange für die Abhilfe: CheckinMania - Currently we're looking through the emails we've received regarding the future of the website. As soon as we've thought of a suitable way to continue, you'll find it right here. We're not showing the Twitter messages anymore, as they no longer add anything. If you don't want your information to show up everywhere, don't over-share ;-). Trotz des "Smileys" ist der Ernst der Einschätzung unübersehbar. Für die Akteure eines erkenntnisoffenen und lernoffenen Standorts heißt dies ganz pragmatisch, dass Altes mit „patches" (von der Informatik bis zur Gesetzgebung) nachgebessert und Neues optimal gestaltet werden muss. Die Diskussion in den USA ist indes dynamisch: Wenn in absehbarer Zeit kein verstärkendes Echo aus Europa kommt, könnten sich die änderungsfeindlichen und beharrenden Kräfte wieder in den Vordergrund bringen.

Die Kernergebnisse einer Studie der LMU München[13] zur Akzeptanz von Smart Metern bei Endverbrauchern zeigt auf, dass Endkunden großes Interesse an intelligenten Stromzählern zeigen, aber auch dass insbesondere bei älteren Menschen bezüglich der Datensicherheit und der subjektiven Kontrolle die Skepsis überwiegt. Wie erwähnt: Dafür kann ein präzise gezogener Innovationsrahmen nur hilfreich sein. Der Stand der Diskussion zeigt bereits, dass weder eine „profilbildende" permanente Messung noch gar eine „Außensteuerung" durch Dritte[14] vorgesehen werden sollte. Noch einmal: Das freiwillig ausgestattete „Remote Smart Home" wird dadurch nicht behindert, aber auch „Otto Normalverbraucher 2.0" will sich nicht vollständig von seinem Smartphone steuern lassen. Zusätzlich ist sicherzustellen, dass nicht etwa „Vierte" sich dieser Datenflüsse bemächtigen, sei es zum Handel mit Verbraucherprofilen oder zum Veranstalten eines lustigen „Blinking Light Event". Festzustehen scheint bereits, dass der einzelne Haushalt nicht „ferngesteuert" werden soll und dass er die Tarifsonderangebote nicht ständig interaktiv nachrecherchieren will, ein reiner Downstream oder sogar ein Broadcast sind völlig akzeptabel.

3 Erlaubt? Universelles Smart Home

Als ein Zwischenergebnis im bisherigen Verlauf der Diskussion lässt sich erkennen, dass ein E-Infonetz nicht wie das Smart Grid in einem Smart Home konvergiert. Positiv ausgedrückt: Im Haus, in der grundgesetzlich geschützten Privatheit, gibt es keinerlei rechtliche oder technische Einschränkungen für Datenerfassung und Datenverarbeitung. Es ist im Prinzip alles erlaubt. Für Sensoren in der Wohnung gibt es ebenso wenig Grenzen wie für elektronische Geräte, eine vom Bewohner individuell eingerichtete kontrollierte automatische Steuerung ist in vollem Umfang möglich. Als Sinnspruch könnte man prägen. „My Home is my Data!"

Allerdings gilt für jegliche Übertragung nach außerhalb dieser Privatheit erstens die gut li-

[13] Picot, Arnold/ Kranz Johann/ Bilecki, Simon, Studie zur Akzeptanz von Smart Metern bei Endverbrauchern, LMU München 2009

[14] Eine „Fernsteuerung" durch den Bewohner oder andere Autorisierte bleibt separat im Rahmen des „Smart Home" selbstverständlich möglich.

berale Nachbarschaftseinschränkung. Anders als beim Schillerschen „bösen Nachbarn“ aus Wilhelm Tell kann auch ein guter Nachbar durch unerwünschte akustische („Sub-Woofer) oder visuelle Signale (TV-Projektion, Laserpointer) gestört werden, man kennt so etwas schon lange. Neu ist hingegen die Nachbarschafts-Störung durch Funkfrequenzen oder elektrischen Störungen, die durchaus dem Nutzer von Inhaus-Geräten aus dem Elektronik-Supermarkt angelastet werden kann. Für die Endgeräte einer Infrastruktur haftet hingegen der Betreiber, dies kann und sollte schon als erhärtete These näher untersucht werden.

Ein solches „voll aufgerüstetes“ Smart Home ist bislang an die gängige Telekommunikation bis hin zum Breitbandkabel angeschlossen und unterliegt selbstverständlich allen Vor- und Nachteilen derselben. Wenn zum Beispiel Mobiltelefone ihre jeweiligen Lokationsdaten senden (und dies tun 2011 auf der ganzen Welt etwa fünf Milliarden Mobiltelefone), dann übertragen sie auch den Standort des Smart Home. Auch bei reiner Bereitschaftsschaltung kann dies mit einer Silent SMS festgestellt werden. Der Nutzer muss dies erst wissen, bevor er nach einer Abwägung sagen kann, ob er es will oder nicht.

Insofern ist der – ansonsten weiterhin zutreffende – Wikipedia-Eintrag (Januar 2011) zum Smart Home („Intelligentes Wohnen“[15]) in dieser Hinsicht einzuschränken: „Diese Aspekte der Gebäudeautomation, Hausautomation, Hausgeräte-Automation und Vernetzung im Bereich der Consumer-Electronics (Unterhaltungselektronik) werden in erster Linie durch eine Vernetzung von Haustechnik (Energiezähler, Alarmanlagen, Heizungs- und Lichtsteuerung etc.), Elektrohaushaltsgeräten (Herd, Kühlschrank etc.) und Multimedia-Geräten (Fernseher, Videorekorder, Tuner, zentraler Server etc.) mit Hilfe von Bussystemen (per Kabel, Powerline oder Funk) oder direkte Funkanbindung erreicht.“

Generell kann in Bezug auf die IT-Sicherheit festgehalten werden, dass in der Kombination von „intelligenten“ Geräten, Techniken und Diensten das bekannte „Geleitzugprinzip“ herrscht: Der Langsamste (in unserem Beispiel der Unsicherste) ist entscheidend. Die seit 40 Jahren (verständliche) Begeisterung für alles “Universelle” (Geräte, Netze etc.) bedarf einer tiefgreifenden Neubewertung. Die unterschiedlichen Spezifikationen sind (dies zeigt zum Beispiel die „Clean-Slate Diskussion über NGN) nach heutiger Erkenntnis nicht „konvergent“ gestaltbar.

In den USA ist das – von Bill Gates mit einem noch relativ teuren Prototyp vorgestellte – Smart Home schon seit vielen Jahren insbesondere als „ferngesteuertes“ Heim[16] in der Implementierungsphase: „In October 2008, AT&T launched a remote home-monitoring service to let users control home lighting and appliances via live video, viewable on Cingular Wireless phones or their PCs, for $10 a month. A slew of startups are looking to other service providers to bundle their solutions.” Der dahinter stehende Milliardenmarkt konnte wirklich nur begeistern: “Analysts have high hopes for the burgeoning smart home market: Now an estimated $1.3 billion, it's expected to balloon to nearly $10 billion worldwide by 2010, according to research firm Frost & Sul-

[15] Oft synonym verwendete Begriffe für Intelligentes Wohnen sind: „eHome“, „Smart House“, „Smart Home“, „Smart Living“, „Elektronisches Haus“, „Vernetztes Haus“, „Intelligentes Haus“ usw.

[16] Lev-Ram, Michal, Smart Homes Get an Upgrade, Bill Gates's smart home cost $113 million. Now you can have the same kind of remote control over your dwelling for as little as $10 a month. In: Business 2.0 Magazine 15. März 2007

livan." Dass die Amerikaner wiederum für den Rahmen dieses „Zehnmilliardenmarkts" spezielle Vorleistungskosten etwa der Wissenschaft im Sinne einer Akzeptabilitätsabschätzung hinsichtlich „privacy" aufgewendet hätten, ist nicht bekannt. Dass die Verantwortlichen in der US-Netzpolitik diesen Privatheitsschutz wollen und dabei speziell auf den deutschen Beitrag dazu warten, ist eine der Merkwürdigleiten einer unübersichtlichen Diskussionslage.

In der deutschen Diskussion wird das „Smart Home" auch dank der europäischen und deutschen Förderprogramme zu „Ambient Assisted Living" (AAL) anwendungszentriert und nicht technikzentriert behandelt. Nicht nur die völlig anderen Wohnstrukturen mit ihren großen Entfernungen und andere Unterschiede führen zu anderen Leitbildern. So erklärt der große Jahreskongress von VDE und BMBF zu AAL[17] schon im Vorspann unmissverständlich: „Das ‚Ambient Assisted Living'-Modell ist „untrennbar verbunden mit aktuell vorherrschenden gesellschaftlichen Leitbildern. Daher wird der Mensch in den Focus gerückt und Aspekte wie Ethik und Datenschutz verstärkt betrachtet. Nur so kann es gelingen innovative Produkte und Dienstleistungen in den Markt zu bringen und einen weiteren Schritt zur Lösung der besonderen Herausforderung des demographischen Wandels zu gehen."

Noch einmal die Feststellung: Es bleibt jedermann unbenommen, die Einschränkungen beim Datenschutz freiwillig hinzunehmen, sei es über die Nutzung bekannter Teledienste bis hin zu einem Speicherstick mit allen Haushaltsdaten eines Smart Home. Aber harte Bedingung ist: Diese „Freiwilligkeit" muss im Sinne eines „Opt-In" unter klarer Kenntnisnahme des „Kleingedruckten" erfolgen. Für ein nachhaltiges Energieinformationsnetz ist es deswegen ratsam, von vorneherein eine prinzipiell datenschutzverträgliche Lösung diesseits der „Roten Linie Personendaten" anzustreben, denn Mieter wie Hausbesitzer wechseln schneller als Infrastrukturen. Zum wiederholten Male sei daran erinnert, dass infrastrukturelle Akteure wie die Energieversorger oder die Hausbesitzer ihre Investitionen in langfristigen Zyklen von Jahrzehnten vornehmen. Wo immer möglich, sollten in der Wohnung Personendaten und Dinge-Daten getrennt bleiben, was trivialer erscheint als es ist. So war selbst von ausgewiesenen Experten im Juli 2010 noch zu hören, dass die Daten selbstverständlich getrennt werden. Der Hinweis, dass der Energielieferant sein Geld dann wohl bei einem technischen Gerät namens Smart Meter anmahnen müsse, weckte Nachdenklichkeit.

Wenn es eine Rote Linie Datenschutz im Haushalt gibt, so ist dennoch zu prüfen, ob es nicht mögliche Fernsteuerungstechniken diesseits der Roten Linie gibt. Ein "entpersonalisierter" Energiespeicher in einem Haushalt könnte dazu beitragen, den Nachtstrom zu nutzen und die Stromspitzen zu kappen. Hierzu sind in deutschen Forschungslabors neue Lösungsmöglichkeiten in inventorischer Arbeit, über die erst bei Veröffentlichung diskutiert werden kann. Bei der Energienutzung gilt der Satz „Strom für Geld", das Messgerät dafür ist der Verbrauchszähler bzw. Bezugszähler. Bei der Energieerzeugung lässt sich der Satz umkehren: Der Lieferant bekommt Geld für Strom, das Messgerät hierfür ist der Einspeisezähler.

[17] BMBF/VDE (Hrsg.), Altersgerechte Assistenzsysteme – Aus der Forschung in den Markt. 4. Deutscher AAL-Kongress, Berlin 2011, www.aal-kongress.de

4 Bemerkt? Einspeisung ist „Geld für Strom“

Die Betrachtung galt bislang einem Nutzerhaushalt, der seinen Strom ausschließlich wie bisher vom Versorger geliefert bekommt. Dieser Haushaltstyp wird noch lange dominierend sein. Beim künftig denkbaren „Prosumenten“, also einem Haushalt, der über den eigenen Bedarf hinaus „alternative“ Energie aus Solarstrom oder Wind produziert, gelten zunächst ganz besondere Bedingungen für IT-Sicherheit im Sinne von infrastrukturell gesicherter Ausrüstung.

Eine der ersten Bedingungen scheint richtigerweise die Trennung von Einspeise- und Bezugszähler zu sein. Die Vorstellung eines Universalgeräts, das „bidirektional“ Verbrauchs- und Erzeugungswerte misst und miteinander zu einem „gemeinsamen“ Messwert bringt, graust nicht nur den Informatikern. Selbst bei sprunghaftem Fortschritt der Mikroelektronik wäre ein solches Gebilde wegen mangelnder Transparenz und nicht darstellbarer Fail-Safe-Eigenschaften nicht brauchbar.[18]

Die erforderlichen Einspeisezähler und die Übertragung ihrer Daten müssen sehr sicher und robust sein. Denn es gibt – darauf haben Weißhut-Hacker schon früh hingewiesen – im Falle eines „Cracking“ die gänzlich neue Möglichkeit, durch Fälschung der Einspeisedaten virtuell echtes Geld zu erzeugen, das der Energielieferant an den Betrüger bezahlen muss. Im Unterschied zum „Stromdiebstahl“ (§ 248c StGB), vor dem der verplombte Verbrauchszähler bzw. der Smart Meter grosso modo schützt, und der plausiblerweise nicht unauffällig unter Null manipuliert werden kann, ist der Betrug mit falschen Einspeisezahlen nach oben nicht begrenzt. Dies gilt insbesondere bei Hochautomatisierung ohne aufwändige Plausibilitätskontrollen.

Ein neuer Begriff für den denkbaren Straftatbestand muss sogar noch gefunden werden, es wird so etwas wie einen „Stromeinspeisebetrug“ (ggf. im Umfeld des § 263 StGB) geben müssen, dies gilt es ebenfalls genauestens juristisch zu untersuchen, um zu einer Empfehlung an den Gesetzgeber zu kommen.[19]

5 Vergemeinschaftet? Makro-Energiespeicher

Wie bei der Entstehung des Internet, bei dem Menschen mit dem Leitbild „es geht doch um menschliche Kommunikation zwischen gutmeinenden Leuten“ implizit zugrunde gelegt wurden, ist auch im Kontext des Smart Grid ein positives Leitbild – „es geht doch um Energiesparen und unsere Umwelt“ – präsent, das die Augen davor verschließt, dass die Anhänger der guten Visionen immer noch eine Minderheit im weltweiten Alltagsverhalten sind. Dennoch birgt auch ein nachhaltig strukturiertes Energienetz anscheinend gute Potentiale für neue kooperative „Geschäftsmodelle“, die von „Nachbarschaftsversorgung“ bis hin zu genossenschaftlichen Modellen auch im makroökonomischen Bereich. Die dritte Ebene in der Heuristik bezieht sich deswegen auf die (volkswirtschaftlich betrachtet) großen Speicher, die hier als Makro-

[18] Diese Einsicht wird die erwähnten Pioniere des Smart Home jedoch nicht daran hindern, dies alles mit einer App im SmartPhone zu vereinen. Spätestens im Weihnachtsgeschäft verkauft es sich.

[19] Dies schließt strafrechtlich „Beihilfe“, aber auch „Bandenverbrechen“ hoch pönalisiert ein. „Sechs Monate bis zehn Jahre“ passen in keinen Businessplan. Denkbare Messbetreiber müssen ein entsprechendes „Risk Assessment“ anhand der IT-Architektur vornehmen.

Energiespeicher bezeichnet sind, also z. B. Stauseen mit Wasserkraft-Energieerzeugung. Andere Makro-Energiespeichereinrichtungen als die Turbinen-Stauseen (Wärme, Kälte, Wasserstoff etc.) könnten definitorisch gleichgestellt werden. Definitorisch können dies sogar auch energietechnisch vernetzte Kleinspeicher in einem Landstrich bzw. einer Kommune sein. Es ist sogar zu untersuchen, ob nicht grundsätzlich alle Energiespeicher bis hin zur Autobatterie als „diesseits der Roten Linie Personendaten“ zu betrachten sind.

Über die makroökonomische Bedeutung hinaus weist auch die dem Energienetz zugeordnete Eigenschaft einer „kritischen Infrastruktur“, will heißen: bei ihrem Ausfall entstehen erhebliche Folgeschäden, die es zu vermeiden gilt.

Es wurde schon darauf hingewiesen, dass etwa die Aufteilung der deutschen Stauseen mit Stromturbinen zwischen den großen und kleinen Energieversorgern nicht realisierbar erscheint. Dies gilt für alle Groß-Speichertechniken bis hin zu Wärme und Gas. Hier bietet sich von vorne herein eine gemeinschaftliche Nutzung im Sinne eines „Kollektivguts“ an, wobei die Organisation desselben durchaus eine Herausforderung für die Organisationsforschung darstellt. Wie eingangs gesagt: „Gewissheiten“ stehen erst am Ende eines transparent geführten Fachdiskurses, aber nicht ohne Fragezeichen.

Hingegen gilt ohne Fragezeichen: Ein früher Expertendiskurs erspart den späten Schlichter.

Autoren

Dirk Fox befasst sich seit 1984 mit Fragen der Kommunikationssicherheit und Kryptografie, zunächst in der Fernmeldeaufklärung, ab 1988 in Forschung und Entwicklung. Seit 1997 ist er Herausgeber der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)“, seit 1998 leitet Dirk Fox die von ihm gegründete Secorvo Security Consulting GmbH als geschäftsführender Gesellschafter. 2002 wurde er für seine unternehmerische Tätigkeit mit dem Landespreis Baden-Württemberg für junge Unternehmen ausgezeichnet. 2007 war er Gutachter des Bundesverfassungsgerichts anlässlich des Verfahrens zur „Online-Durchsuchung“. Dirk Fox ist Autor von mehr als 150 Publikationen und (Mit-) Herausgeber mehrerer Buchveröffentlichungen.

Dipl.-Jur. (Univ.) Katharina Fuchs studierte Rechtswissenschaften an der Universität Passau. Danach Tätigkeit als wissenschaftliche Mitarbeiterin am Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht von Prof. Dr. Dirk Heckmann. Seit Mai 2011 wissenschaftliche Mitarbeiterin am Lehrstuhl für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik von Prof. Dr. Gerrit Hornung.

Prof. Dr. Gerrit Hornung, LL.M., studierte Rechtswissenschaften und Philosophie an den Universitäten Freiburg und Edinburgh. 2005 Promotion über Rechtsprobleme von Chipkartenausweisen (Wissenschaftspreis 2006 der Deutschen Stiftung für Recht und Informatik). 2004 bis 2006 Referendariat am Hanseatischen Oberlandesgericht. 2006 bis 2011 Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) und Habilitand an der Universität Kassel. Seit 2011 Professor für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau. Arbeitsschwerpunkte: Technik- und Multimediarecht aus öffentlich-rechtlicher Perspektive, insbesondere verfassungsrechtliche Grundlagen, E-Government, Rechtsfragen informationstechnischer Ermittlungs- und Gefahrenabwehrmaßnahmen, Datenschutzrecht, Recht der elektronischen Signatur, neue Kommunikationstechnologien. Regelmäßige Veröffentlichungen und Vorträge zu diesen Themen.

Dr. Dieter Klumpp, Direktor Alcatel-Lucent Stiftung für Kommunikationsforschung. Studium Politikwissenschaft und Geschichte an der Universität Stuttgart, Promotion im Fach Kommunikationswissenschaft an der FU Berlin. Seit 1978 SEL AG, Zentralbereich Technik, den heutigen Bell Labs Germany. 1995 Mitglied Enquête-Kommission „Multimedia“ Landtag von Baden-Württemberg, 1996-98 Mitglied des Wissenschaftlichen Beirats der Enquête „Zukunft der Medien“ des Deutschen Bundestags, 1999 Juryvorsitz BMBF-Programm Mensch-Technik-Interaktion, 1999-2002 Beirat Media@Komm des BMWi, Sprecher Fachbereich „Informationsgesellschaft und Fokus-Projekte“ der ITG im VDE. Vorstand Förderverein Stiftungsverbundkolleg e.V., Stuttgart/Berlin. Deutsche UNESCO-Kommission, Mitglied FA Kommunikation/Information. Beirat Institut für Europäisches Medienrecht, Saarbrücken, Beirat Forschungszentrum für Informationstechnik-Gestaltung, Universität Kassel, Kompetenzzentrum Technik-Diversity-Chancengleichheit, Bielefeld. Beirat Fraunhofer e-Government-Zentrum, Mitglied der AK „Electronic Government“ der Initiative D21 und BITKOM. Beirat der Stiftung Digitale Chancen, Wissenschaftlicher Beirat Internationales Zentrum für Kultur- und Technikforschung (IZKT), Universität Stuttgart; Veröffentlichungen und Lehre zum

transdisziplinären Spektrum der Informationsgesellschaft, u. a. Seminar „Leitbilder für die Informationsgesellschaft“ seit 2009 am Institut für Informatik der Universität Potsdam.

Dr. Johann Kranz studierte an der Universität Leipzig und der Universidad de Deusto in San Sebastian Wirtschaftsinformatik. Im Oktober 2007 begann er am Institut für Information, Organisation und Management (Leitung: Prof. Dr. Dres. h.c. Arnold Picot) als wissenschaftlicher Mitarbeiter. Während seiner Tätigkeit erwarb er an der Ludwig-Maximilians-Universität München den Master of Business Research (MBR) und war zu einem mehrmonatigen Forschungsaufenthalt an der Columbia University in New York zu Gast. In seiner Promotion beschäftigte er sich mit der Konvergenz zwischen Informations- und Kommunikationstechnologien (IKT) und dem Energieversorgungssystem („e-Energy“ bzw. „Smart Grid“). Der Schwerpunkt seiner kumulativen Dissertation lag auf Studien zur Technologieakzeptanz und Regulierung von innovativen IKT-Technologien und -Infrastrukturen in Smart Grids.

Dr. Christoph Krauß ist Leiter des Bereichs Innovation & Strategie am Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC) in München und Ansprechpartner für das Thema Smart Grid Security.

Klaus J. Müller erwarb sein Diplom in Elektrotechnik mit dem Schwerpunkt Angewandte Informatik 1997 an der Fachhochschule Offenburg. Von 2000 bis 2010 arbeitete er als Freiberufler für verschiedene Industrieunternehmen. Klaus J. Müller war darüber hinaus über mehrere Jahre als Lehrbeauftragter auf dem Gebiet IT-Sicherheit an der Hochschule Offenburg tätig und ist seit 2010 Security Consultant bei der Secorvo Security Consulting GmbH. Seit 2009 setzt er sich mit dem Thema „Smart Metering“/„Smart Grid“ auseinander.

Prof. Dr. Alexander Roßnagel, Studium der Rechtswissenschaften, 1981 Dissertation, 1991 Habilitation, Universitätsprofessor für Öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes an der Universität Kassel, wissenschaftlicher Leiter der „Projektgruppe verfassungsverträgliche Technikgestaltung (provet)“ und wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR) in Saarbrücken. Seit 2003 Vizepräsident der Universität Kassel. 1993 erhielt er den Forschungspreis Technische Kommunikation der Alcatel-Lucent Stiftung, 1995/96 war er Stiftungsgastprofessor der Alcatel-Lucent Stiftung am Zentrum für Interdisziplinäre Technikforschung der Technischen Universität Darmstadt. Seit 1999 Herausgeber des wissenschaftlichen Kommentars zum Informations- und Kommunikationsdienste-Gesetz und Mediendienste-Staatsvertrag „Recht der Multimedia-Dienste“, 2001 Erstellung des Gutachtens „Modernisierung des Datenschutzrechts“ für das Bundesinnenministerium, 2003 Herausgabe des Handbuchs Datenschutzrecht.

Nachhaltiges Energieinformationsnetz: Stiftungsprojekt NEWISE

Das transdisziplinäre Schwerpunktprojekt NEWISE („Nachhaltiges Energieinformationsnetz – Wettbewerb, Information und Sicherung für die Energieversorgung“) wurde von der Alcatel-Lucent Stiftung im Mai 2009 gestartet und soll im Rahmen des Stiftungs-Verbundkolleg bis 2013 durch Sachstandsanalysen und Diskursveranstaltungen wichtige Erkenntnisse und Ergänzungen zum Themenfeld erbringen. In Kooperation mit dem Förderprojekt EEnergy der Bundesregierung und der wissenschaftlichen Begleitforschung beim Bundesministerium für Wirtschaft und Technologie (BMWi) ergänzt das Diskursprojekt mit transdisziplinären Forschungsansätzen und Informationen insbesondere für kommunale Entscheider in Politik und Verwaltung die Themenschwerpunkte „Erfordernisse und Anforderungen für Datenschutz, Privatheits- und Verbraucherschutz“, für ganzheitlichen „Nutzerschutz“. Erforscht werden Potentiale der Sicherung von versorgungskritischen Infrastrukturen vor dem Hintergrund neuer IKT-Systeme und Netze. Besondere Aufmerksamkeit gilt den Potentialen des Wettbewerbs sowie der Regulierung im „Konvergenzraum“ von Energie-, Informations- und Kommunikationsversorgung.

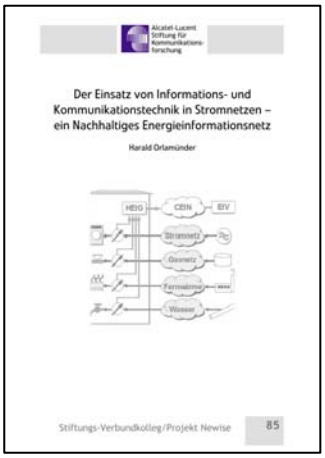
Eine langfristige und drängende Aufgabe des Standorts in Europa ist der Aufbau eines Energieinformationsnetzes. Dieses Informationsnetz soll für die heutigen und künftigen Elektrizitätsnetze alle erforderlichen Daten für die Messung, den Verbrauch und die Steuerung des Energieeinsatzes vom Einzelhaushalt, eines Areals bis hin zu einer Kommune bereitstellen. Der IKT-Einsatz im Zuge eines „Smart Grid“ zielt auf die Sicherung im kontinentalen Maßstab. Die unterschiedlichen Zugangsnetze und Hausnetze sowie die entsprechenden Dienste sind noch nicht hinreichend definiert und bedürfen der Gestaltung. Die in einem Energieinformationsnetz „konvergent“ zu integrierenden Informations- und Kommunikationssysteme müssen wie die Energienetze selbst von vorneherein auf Nachhaltigkeit (ökologisch, ökonomisch, rechtlich, gesellschaftlich) hin angelegt sein.

Die interdisziplinäre Gestaltungsaufgabe für eine große Akteursarena in Wissenschaft, Wirtschaft, Politik und Gesellschaft besteht darin, in der Ordnung des marktwirtschaftlichen Wettbewerbs mithilfe modernster, intelligent definierter IKT-Systeme koordiniert und konzentriert das Ziel einer ökologisch verträglichen, ökonomisch möglichen, sicheren und gesetzeskonformen Datenverarbeitung sowie einer Sicherung für die Energieversorgung zu realisieren.

Veranstalter der NEWISE-Konferenzen sind die Alcatel-Lucent Stiftung zusammen mit dem Bundesministerium für Wirtschaft und Technologie, dem Deutschen Städte- und Gemeindebund sowie der Informationstechnischen Gesellschaft ITG im VDE. Die Inaugurationsveranstaltung zu NEWISE-Konferenz fand am 9. Dezember 2009 im Porsche Museum in Stuttgart-Zuffenhausen statt. Die NEWISE-Konferenz 2010 mit dem Schwerpunkt „Nutzerschutz im Energieinformationsnetz“ wurde in enger Kooperation mit der E-Energy-Begleitforschung am 17. Juni 2010 im Bundeswirtschaftsministerium durchgeführt. Eine überregional ausgelegte Konferenzreihe in NRW startete mit Unterstützung der Stiftung unter der Reihenbezeichnung „Smart Energy“ am 29. Oktober 2010 in Dortmund, sie wird am 11. November 2011 fortgesetzt. Am 29. September 2011 fand die dritte NEWISE-Fachkonferenz in Berlin zusammen mit dem Münchner Kreis für Kommunikationsforschung statt, der für seine „Berliner Gespräche“ die höchste Aufmerksamkeit gerade auch der Bundespolitik genießt. Eine Dokumentation ist im Erscheinen.

Publikationen

Die Publikationen können kostenfrei über das Stiftungsbüro der Alcatel-Lucent Stiftung bezogen werden.



Harald Orlamünder
Der Einsatz von Informations- und Kommunikationstechnik in Stromnetzen – ein Nachhaltiges Energieinformationsnetz

Stiftungsreihe Nr. 85

Alexander Roßnagel, Silke Jandt
Datenschutzfragen eines Energieinformationsnetzes

Stiftungsreihe Nr. 88

Claudia Eckert
Sicherheit im Smart Grid. Eckpunke für ein Energieinformationsnetz

Stiftungsreihe Nr. 90

Alcatel-Lucent Stiftung

Die Alcatel-Lucent Stiftung für Kommunikationsforschung ist eine gemeinnützige Förderstiftung für Wissenschaft insbesondere auf allen Themengebieten einer „Informationsgesellschaft“, neben allen Aspekten der neuen breitbandigen Medien speziell der Mensch-Technik-Interaktion, des E-Government, dem Medien- und Informationsrecht, dem Datenschutz, der Datensicherheit, der Sicherheits-kommunikation sowie der Mobilitätskommunikation. Alle mitwirkenden Disziplinen sind angesprochen, von Naturwissenschaft und Technik über die Ökonomie bis hin zur Technikphilosophie.

Die Stiftung vergibt jährlich den interdisziplinären „Forschungspreis Technische Kommunikation“, Dissertationsauszeichnungen für WirtschaftswissenschaftlerInnen sowie Sonderauszeichnungen für herausragende wissenschaftliche Leistungen.

Die 1979 eingerichtete gemeinnützige Stiftung unterstützt mit Veranstaltungen, Publikationen und Expertisen ein eng mit der Praxis verbundenes pluridisziplinäres wissenschaftliches Netzwerk, in dem wichtige Fragestellungen der Informations- und Wissensgesellschaft frühzeitig aufgenommen und behandelt werden.

www.stiftungaktuell.de

Kontakt

Alcatel-Lucent Stiftung
Lorenzstraße 10, 70435 Stuttgart
Telefon 0711-821-45002
Telefax 0711-821-42253
E-Mail office@stiftungaktuell.de
URL: http://www.stiftungaktuell.de