House of Energy

House of IT

Houses of Dialog

Die Energiewelt wird digital

24. Oktober 2018

Ergebnisse der gemeinsamen Veranstaltung von **House of IT e.V.** und **House of Energy e.V.**

Gefördert durch

HESSEN
Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Wohnen

EUROPÄISCHE UNION
Investition in Ihre Zukunft
Europäischer Fonds für regionale Entwicklung

Inhalt

IMPRESSUM	**2**
CONCLUSIO - DAS WICHTIGSTE IN KÜRZE	**3**
EINFÜHRENDE ÜBERLEGUNGEN AUS SICHT DER ENERGIEWELT – Rolle und Herausforderungen der Digitalisierung	6
EINFÜHRENDE ÜBERLEGUNGEN AUS SICHT DER IT-WELT – Rolle und Herausforderungen der digitalen Transformation	12
SESSION 1: IT-ANWENDUNGEN IN DER ENERGIEWELT	
Entwicklung neuer Geschäftsmodelle mit Smart Home aus Sicht eines EVU	14
Quartierslösungen digitalisiert: Mehrwerte durch Energiemanagement Systeme	15
Industrie 4.0 für die Energieversorgung – ein junges Unternehmen nimmt die Digitalisierung in die Hand	17
Diskussion in Session 1 „IT-Anwendungen in der Energiewelt“	18
SESSION 2: IT-SICHERHEIT IN DER ENERGIEWELT	
IT-Sicherheit in der Energiewelt: Notwendigkeiten, Herausforderungen, Perspektiven	25
Einsatz militärischer Konzepte für die IT-Sicherheit in der Energiewelt	28
Erfahrungen mit IT-Sicherheit in der Praxis	33
Diskussion in Session 2 „IT-Sicherheit in der Energiewelt“	35

IMPRESSUM

Herausgeber: House of Energy e.V. (HoE) und House of IT e.V. (HIT)
Stand: August 2019
Redaktion: Prof. Dr. Peter Birkner, Dirk Filzek und Ivonne Müller (HoE) sowie Dr. Cornelia Herriger und Dr. Florian Volk (HIT)
Gestaltung: Caroline Enders (HoE)

Ihre Ansprechpartner:

Dirk Filzek
House of Energy e.V.
Telefon: +49 561 / 953 79-796
d.filzek@house-of-energy.org

Dr. Cornelia Herriger
House of IT e.V.
+49 6151 / 16 -75990
herriger@house-of-it.eu

Houses of Dialog: Die Energiewelt wird digital | Frankfurt am Main, 28.10.2018

CONCLUSIO - DAS WICHTIGSTE IN KÜRZE

Zentrale Erkenntnisse aus dem Houses of Dialog „Die Energiewelt wird digital“

IT-Anwendungen in der Energiewelt

1. Die **Energiewende** ist ein wesentlicher Baustein für die Erreichung der Klimaschutzziele. Ziel ist ein **erneuerbares Energieversorgungssystem mit Sektorenkopplung**, das mittels digitaler Technologien gesteuert wird. Die Energiewende stellt einen fundamentalen gesamtgesellschaftlichen Transformationsprozess dar, wobei Branchengrenzen erodieren. Treiber für die Prozessdynamik der Energiewende sind Klimaschutz, technologischer Fortschritt und Wirtschaftlichkeit.

2. IT erlaubt die Identifikation und **Nutzung von Effizienz- und Suffizienzpotenzialen**. Weiterhin erlaubt IT eine optimierte Nutzung von Infrastruktur (Smartness) und eine Orchestrierung volatiler Systeme. Energiewende setzt damit auf IT und Digitalisierung auf. Andererseits benötigt IT Energie. In Konsequenz ist die systembezogene Kosten-/Nutzenanalyse daher stets mitzudenken.

3. Die Verwebung von digitaler Welt und Energiewelt ermöglicht perspektivisch völlig **neue IT-Anwendungen** für die Systemsteuerung (Smart Grids / Smart Markets), die Optimierung unternehmensinterner Prozesse sowie für neue Dienstleistungen und Produkte.

4. Ein **intelligentes Stromnetz (Smart Grid)** wird erforderlich, um das Energieversorgungssystem bei einem zukünftig vermehrtem Einsatz erneuerbarer Energien zu managen. Das Gesamtsystem wird sich dadurch auszeichnen, dass vielfältige Energieanlagen dezentral in die Verteilnetze eingebunden sind und sehr flexibel auf die jeweilige Netzsituation reagieren. Dabei kann man sich das Stromnetz der Zukunft als zellulär organisiertes Gesamtsystem vorstellen, in dem die Verteilnetze dynamisch betrieben werden. Dies führt zu einer neuen Komplexität. Die Steuerung erfolgt über eine Verknüpfung von Energietechnik mit Informationstechnologie. Erst dadurch werden die Flexibilitätspotenziale vieler potenziell flexiblen Energieanlagen verfügbar. Derart intelligente Smart Grid-Funktionalitäten können den Ausbaubedarf der Stromnetze deutlich reduzieren.

5. **Smart Markets** werden zukünftig den Handel von Energiemengen und Energiedienstleistungen für eine Vielzahl von Akteuren ermöglichen. Dies beinhaltet sowohl Kleinsttransaktionen, als auch schnellen Echtzeithandel. Zu unterscheiden ist zwischen einem Handel zur Optimierung des Netzbetriebs (regulierter Bereich) und einem wettbewerblichen Handel bei Nutzung der Infrastruktur. Über Smart Market-Plattformen werden sich vielfältige neue Geschäftsmodelle und Produkte konzipieren und abwickeln lassen.

6. **Erzeugungsanlagen, Speicher und flexible Lasten** können mittels IT-Lösungen effizienter integriert, in dynamisch wechselnden Anlagenverbünden zu virtuellen Kraftwerken zusammengefasst und vorausschauend gewartet werden.

7. Die **Technologien** sind grundsätzlich vorhanden. Sie sind für die Praxis in der Energiewelt von morgen weiterzuentwickeln, beispielsweise in Reallaboren.

8. Um diese Systeme zu realisieren steigt die **Bedeutung von Daten**. Der Einsatz moderner Big Data-Verfahren aus der IT-Welt wird unumgänglich sein.

9. Die **IT-Infrastruktur muss resilient und energieeffizient sein.** Der Zugang aller Marktteilnehmer und auch der Datenschutz sind zu gewährleisten.

10. Neue Anwendungsfelder und Geschäftsmodelle führen zu **Marktanpassungen** und machen **Innovations- und Changemanagement** bei den Unternehmen der Energiewelt notwendig.

11. Für den Endkunden sind **Versorgungssicherheit, Komfort und Preis** ausschlaggebend – gekoppelt mit dem Vertrauen, das der Anbieter genießt. Lokalversorger verfügen im allgemeinen über Kundenzugang und Kundenvertrauen.

12. Für Energieversorger ist es wichtig, sich auf **Prosumer** (Konsument, der zugleich Energieproduzent wird) einzustellen, und zwar aus Vertriebssicht genauso wie aus Netzsicht.

13. Im **Smart Home** werden vernetzte und fernsteuerbare Geräte eingesetzt, um in Wohnungen und Häusern Wohnqualität, Sicherheit und effiziente Energienutzung zu erhöhen. Smart Home bietet lokalen Energieversorgern neue Chancen, ihren Kunden neue Dienstleistungen anzubieten. Dabei sollten die Energieversorger auf ihren Stärken aufbauen und sich z.B. auf Wärmesteuerung und Sicherheitsfunktionen fokussieren.

14. **Quartierslösungen** eröffnen neue Möglichkeiten der Selbstversorgung und Energieeffizienz sowie in der Vermarktung von Flexibilitäten. Digitalisierte Quartiere bieten ähnliche Schnittstellen wie kleinere Prosumer-Einheiten für die Vernetzung und lassen sich grundsätzlich netzdienlich in Verteilnetze einbinden. Quartierslösungen funktionieren zwar von der Idee her gut, jedoch ist die Umsetzung in der Breite mit langwierigen Prozessen verbunden. Bei Projektplanung und -umsetzung kommt es auf eine enge Kooperation aller Akteure an.

15. **Digitale Energiemanagement-Systeme** sind sowohl der Schlüssel für einen reibungslosen Steuerungsablauf (z.B. für Quartierslösungen) zur Sicherung der Energieversorgung als auch für Energieoptimierungen in Bezug auf Effizienz, Kosten und Verfügbarkeit. Weiterhin helfen digitale Energiemanagement-Systeme dabei, Synergien von Energiesystemen mit anderen Einheiten im Smart Grid zu heben.

16. Eine **automatisierte vorausschauende Steuerung** von Energiesystemen kann die Profitabilität der Energieerzeugung steigern. Im Unterschied zur klassischen Regelungstechnik, die auf aktuellen Messwerten basiert, werden dabei Prognosen zu Verbrauch, Erzeugung und Marktpreisen eingebunden.

17. **Herstellerunabhängige Lösungen** können vorteilhaft sein, wenn es darum geht, beliebige Komponenten an digitale Plattformen zur Überwachung, Analyse und Optimierung von Energiesystemen anzubinden.

18. Das **Messstellenbetriebsgesetz** (MsbG) ist in der Praxis unbeliebt. Trotzdem kann man in der Praxis mit dem MsbG arbeiten.

19. Seitdem die **Datenschutzgrundverordnung** (DSGVO) gilt, muss jedes Unternehmen über ein Datensicherheitskonzept verfügen. Viele Unternehmen haben diese Verpflichtung bereits umgesetzt. Es gibt aber immer noch Lücken und großen Nachholbedarf. Hier drohen hohe Bußgelder.

20. Für die Umsetzung der Energiewende spielt **Akzeptanz** durch die Bevölkerung eine herausragende Rolle.

21. Eine schrittweise **Anpassung des Rechtsrahmens** mit begleitenden Transparenzmaßnahmen wurde gefordert, um den Akteuren eine gute Orientierung im komplexen Prozess der Energiewende zu bieten.

22. Ein **zielgerichteter Austausch zwischen Energiewelt und IT-Welt** ist notwendig und zu fördern, um gemeinsam die Basis für tragfähige Geschäftsmodelle im Sinne der Energiewende zu entwickeln. Auf der einen Seite geht es darum, dass die Energiewelt bereits vorhandene Lösungen aus der IT-Welt erkennt und für sich einsetzt. Dabei ist der rasche technologische Fortschritt in der IT-Welt zu berücksichtigen. Auf der anderen Seite sind der IT-Welt die Probleme aus der Energiewelt nicht bewusst. Über einen gezielten Wissenstransfer können miteinander Lösungen gefunden werden.

IT-Sicherheit in der Energiewelt

1. Dezentrale Energieanlagen, die in zellulären Strukturen zusammenarbeiten, können die **Resilienz der Energieversorgung insgesamt stärken,** wenn gute Konzepte umgesetzt werden.

2. Bis 2020 werden voraussichtlich 50 Milliarden Geräte im **Internet der Dinge** (IoT) vernetzt sein. Das Anwendungsspektrum reicht von Smart Grids und Smart Home über Verkehrsleittechnik und E-Mobility bis zu Industrie 4.0. Mit der Vernetzung von immer mehr „Dingen" steigen auch die Anforderungen an die IT-Sicherheit.

3. Das **Energienetz ist eine hochkritische Infrastruktur.** Wirtschaft und Gesellschaft sind abhängig von einer stabilen und bedarfsoptimierten Versorgung mit Energie. Die Entwicklung eines intelligenten Stromnetzes (»smart grid«) und eines »smart market« in der Energiewelt erfordern nicht nur neue Möglichkeiten der Energieversorgung und -vermarktung zu untersuchen, sondern zwingendermaßen auch neue Gefahren zu betrachten.

4. Mit dem Thema **Cybersicherheit** werden **neue Gefahren** diskutiert. Pauschal ist alles angreifbar, primär technologische Systeme, genauso aber auch die Menschen, welche diese Systeme einrichten, warten, betreiben und nutzen. Die gesamte Betriebskette von Hersteller bis hin zum Endabnehmer ist ein potenzielles Einfalltor für Cyberangriffe. Dazu zählen derzeit auch Denial-of-Service-Angriffe (also das absichtliche Überlasten von Systemen, sodass diese ihre geplante Funktionalität nicht mehr erfüllen können), Fraud (Betrug mit dem Ziel, möglichst unauffällig zu sein)

und ganz klassische Cyberweapons, deren technische Evolution derzeit schnell voranschreitet und stets neue Gegenmaßnahmen, aber insbesondere auch fachliches Bewusstsein, erfordert.

5. Cyberangriffe sind inzwischen **hochgradig professionalisiert: Angreifer** haben fast immer geschäftliche Interessen und sind mit aktuellem Fachwissen und umfangreichen finanziellen Mitteln ausgestattet. Auch Industriespionage funktioniert heute digital. Zudem wird weltweit der „Ton rauher", die Angriffe gezielter, gefährlicher und zunehmend rücksichtslos.

6. Die Digitalisierung der Energiewelt sieht **cyber-physische Systeme** vor, also Verbünde aus informatischen, softwaretechnischen Komponenten mit mechanischen und elektronischen Komponenten, die über eine Dateninfrastruktur kommunizieren. In solchen Systemen ist es meist schwierig, bestehende Schutzmaßnahmen und Sicherheitskonzepte einzusetzen.

7. Die Vernetzung und Steuerung von Stromerzeugern, Stromspeichern und Stromnetzen bis hin zum Endkunden geht mit deutlich **vermehrten Kommunikationsschnittstellen** einher. Dabei stammen Lösungen, Dienstleistungen und Zugriffe von sehr unterschiedlichen Akteuren. In einem derart heterogenen Szenario implementieren nicht alle Anbieter Standards, die zueinander kompatibel sind, und nicht alle Lösungen arbeiten sicher und zuverlässig. Dadurch entstehen viele bisher unbekannter Risiken für Netzverfügbarkeit, Systemsicherheit und Datenschutz.

8. Die **Akteure berücksichtigen IT-Sicherheit oftmals nicht,** wenn Sie die Digitalisierung vorantreiben, weil diese keine funktionale Eigenschaft der Energiesysteme darstellt und mit Mehrkosten verbunden ist. Auch die Produkthaftung entfaltet bislang noch keine disziplinierende Wirkung.

9. **Cybersicherheit muss das gesamte Netz schützen:** Bisher isolierte Systeme einer kritischen Infrastruktur werden vernetzt und die Angriffsmöglichkeiten auf das Gesamtsystem erhöhen sich. Wo bisher ein Angriff auf eine einzelne Komponente des Energienetzes primär diese Komponente gefährdet, sehen wir perspektivisch Angriffe, die sich von einem „Einfallstor" hin auf das gesamte Netz ausbreiten können. Gerade in einer alten, gewachsenen und vor allem verteilten Infrastruktur, wie dem Energienetz wird man mit klassischer Perimetersicherheit keinen hinreichenden Schutz erreichen können. Neue Mechanismen sind gefragt, um Resilienz zu erzielen.

10. Für eine umfassende IT-Sicherheit im Rahmen der digitalen Energiewende braucht es klare **Richtlinien und Schutzprofile,** die einheitlich umgesetzt werden. Solche Richtlinien dürfen keine reinen IT-Richtlinien sein, sondern die Verbindung von IT-OT-IoT (Information technology / Operational technology / Internet of things) muss gesamtheitlich gedacht werden.

11. In der Welt der Digitalisierung gibt es **bereits erprobte und adaptierbare Lösungen.** Man denke nur an Design-Ansätze, wie zelluläre Netze (z.B. Modellstadt Mannheim, C/sells-Projekt) und den potentiell nächsten Schritt, holare Netze (z.B. PolyEnergy-Net-Projekt), welche zu flexibleren und resilienteren Netzen führen, die zugleich eine höhere Versorgungssicherheit und die Integration verteilter, dezentraler Prosumer ermöglichen.

12. Auf Geräteebene kann ein effektiver Schutz vor Missbrauch und vor Cyberattacken nur gewährleistet werden, wenn die Echtheit, also die **Identität und Integrität des vernetzen Geräts** über den gesamten Lebenszyklus hinweg als Komposition von Hardware, Software und Betriebsparametern gesichert ist. Nur so kann zum Beispiel mit dem Smartphone die Heizungssteuerung in der Smart Home-Umgebung sicher betrieben oder zwischen Ladesäule und Elektroauto korrekt abgerechnet werden.

13. Die Sicherheitsanforderungen an **Smart Meter** sind in Deutschland sehr hoch. Das Smart Meter-Gateway dient als standardisierte IKT-Plattform, auf dessen Basis attraktive Mehrwerte für den Endkunden möglich sind. Moderne Tarife für individuelle Kundenbedürfnisse sind möglich.

14. Eine **sichere Logistikkette** ist enorm wichtig für die IT-Sicherheit, z.B. beim intelligenten Messwesen. Sicherheitsvorgaben müssen von der Herstellung bis zum Einbauort und zum Ort der Wiederverwendung oder Verschrottung erfüllt sein. Dabei ist insbesondere sicherzustellen, dass ein unautorisierter Zugriff auf Smart Meter Gateway während des Transportes ausgeschlossen ist. Dazu sind Transportfahrzeuge und Lagerräume abzusichern und eine durchgängige Nachverfolgung zu etablieren.

15. Da auch das beste IT-Konzept immer Sicherheitslücken haben wird, muss darauf geachtet werden, dass die **Energieinfrastruktur selbst** in der Lage ist, die Systemstabilität auch bei (teilweisem) Ausfall der IT-Infrastruktur autark zu gewährleisten.

Hintergründe und Details zu den einzelnen Punkten finden Sie unter *https://www.house-of-energy.org/Housesofdialog* mit

- den Ergebnissen der Diskussionen sowie
- den Zusammenfassungen der Vorträge.

Houses of Dialog: Die Energiewelt wird digital | Frankfurt am Main, 28.10.2018

EINFÜHRENDE ÜBERLEGUNGEN AUS SICHT DER ENERGIEWELT – Rolle und Herausforderungen der Digitalisierung

Dirk Filzek, House of Energy e.V., Bereich Wissenstransfer
Prof. Dr.-Ing. Peter Birkner, House of Energy e.V., Geschäftsführer

Wie kann die Digitalisierung die künftige Energiewelt unterstützen und wie fordert die Digitalisierung die Energiewelt gleichzeitig heraus? Welche Lösungsansätze gibt es? Wie lassen sich neue IT-Anwendungen intelligent für zukunftsfähige Geschäftsmodelle einsetzen?

Die beiden hessischen Houses „House of Energy e.V." und „House of IT e.V." stellen sich mit ihren Netzwerken der Aufgabe, die Digitalisierung der Energiewelt proaktiv zu begleiten. Die Energiewende ist eines der größten IT-Projekte in Deutschland. Um die Chancen und Risiken für die Akteure und die Gesellschaft zu beurteilen und Handlungswege zu skizzieren, ist es essenziell, sowohl das Wesen der Energiewende als auch das Wesen der Digitalisierung zu verstehen. In Bezug auf Digitalisierung ist anzumerken, dass dieser häufig genutzte Begriff besser durch den Terminus „Digitale Transformation" zu ersetzen wäre. Die digitale Transformation umfasst nämlich zwei Aspekte. Zum einen die Umwandlung von analogen Daten in ein digitales Format und zum anderen die damit möglich gewordene Verarbeitung von Daten zur Unterstützung von Geschäftsmodellen. Im Englischen werden für die beiden Aspekte auch zwei Begriffe, nämlich Digitization und Digitalization verwendet. Im Hinblick auf die Energiewende spielt das „Internet of Things" eine wichtige Rolle. Basierend auf Datenerfassung und -auswertung werden über Aktoren physische Reaktionen ausgelöst. Wir sind im Bereich der „Smart Grids", der intelligenten Netze.

Die Energiewende selbst ist geprägt durch drei wesentliche Treiber, die ihr eine hohe Dynamik verleihen und Wirkung entfalten:

1. Antwort auf den Klimawandel und Mittel für den Klimaschutz,
2. Nutzung des technischen Fortschritts im Energiebereich sowie
3. Mittelfristige wirtschaftliche und politische Vorteile für Deutschland gegenüber einem fossilen Szenario.

Faktor Klimaschutz

Der Klimawandel ist eine Existenzfrage für die Menschheit, die sich der Marke von 8 Milliarden nähert. Erst im Oktober 2018 erklärte der Weltklimabericht eine Erderwärmung von mehr als 1,5 °C als zu riskant, da der Menschheit dann keine realistischen und umfänglichen Anpassungsstrategien für die Folgen des Klimawandels mehr zur Verfügung stünden. Es ist von dauerhaften Schäden der Biosphäre auszugehen. Daraus lässt sich ableiten, dass uns noch ein Jahrzehnt verbleibt, um die notwendige (radikale) Wende beim globalen Ausstoß klimarelevanter Gase zu schaffen. Der weltweite CO_2-Ausstoß hat sich in den letzten Jahrzehnten allerdings immer weiter erhöht: von 9 Mrd. Tonnen im Jahr 1960 auf 35 Mrd. Tonnen im Jahr 2016 – ungeachtet der Tatsache, dass der Prozess des menschengemachten Klimawandels bereits seit den 1980er Jahren im Grundsatz bekannt ist. Das Potsdam Institut für Klimafolgenforschung hat festgestellt, dass heute mehr vom Treibhausgas CO_2 in unserer Atmosphäre ist als wahrscheinlich je zuvor in den letzten 3 Millionen Jahren. Dabei entstand die menschliche Zivilisation erst vor rund 11.000 Jahren.
Es sind daher viel stärkere Anstrengungen gefragt sind als bislang. Der politische Wille dazu ist grundsätzlich vorhanden. Dabei geht es nicht um Verbote, sondern um Alternativen. Technologie ist gefragter denn je. Der Druck auf die politischen Entscheider nimmt zu. Erst kürzlich warnte die Geschäftsführende Direktorin des Umweltprogramms der Vereinten Nationen (UNEP), Joyce Msuya: Aktuell würde die EU ihr 40 %-Ziel bis 2030 verfehlen. Das Ziel der EU müsste auf 55 % angehoben werden, wenn sie innerhalb des 1,5 °C-Ziels bei der globalen Erderwärmung bleiben will.

Die Diskussion des Klimawandels hat aber die Parlamente und die Lehrstühle verlassen. Es bildet sich eine gesamtgesellschaftliche Bewegung. Die Wirkung der globalen Schülerstreiks unter dem Motto „Fridays for Future" ist Spiegelbild dieser Entwicklung. Sie wird von

der Wissenschaft mit der Initiative „Scientists for Future" aufgegriffen. Es setzt sich die Erkenntnis durch, dass ein gesamtgesellschaftlicher und fundamentaler Transformationsprozess bevorsteht und das Wirtschaftssystem zu dekarbonisieren – besser zu „de-fossilisieren" – ist. Dies erfordert tiefgreifende Maßnahmen. Früher oder später darf also damit gerechnet werden, dass in der EU und in Deutschland wirksame Instrumente eingeführt werden.

Aktuell wird das Instrument einer CO_2-Bepreisung diskutiert. Klimaverträgliches Handeln würde dadurch wirtschaftlich belohnt, klimaschädliches Handeln hingegen würde sich wirtschaftlich nicht mehr lohnen. Die resultierenden fiskalischen Einnahmen wären den Marktakteuren an anderer Stelle (in Summe aufwandsneutral aber sinnvoll steuernd) wieder zurückzugeben, ganz im Sinne der Stärkung von Wirtschaftsstandort und Innovationen sowie zum Zweck der Vermeidung sozialer Härten.

Für die Energiewende, die ein ganz wichtiger Teil dieser gesamtgesellschaftlichen Klimawende ist, bedeutet dies, dass die Entwicklungen von Anfang an transdisziplinär erfolgen müssen. An diesem Anspruch möchte sich auch das House of Energy e.V. als „Denkfabrik" und Innovationscluster messen lassen. Dazu werden Wirtschaft, Wissenschaft und Politik an einen Tisch gebracht. In der Mitgliederstruktur wird versucht, alle Wirtschaftszweige abzubilden, die betroffen sind und die über Gestaltungsmöglichkeiten im Sinne der Klimawende verfügen.

Faktor technischer Fortschritt

Ein zentraler Treiber der Energiewende ist der technische Fortschritt. Es ist im Wesen der Menschheit verankert, dass attraktive technische Optionen auch Anwendung finden. Daher ist es sehr wichtig, dass in den Bereichen Erneuerbare Energien, Energieeffizienz und Energiespeicherung enorme Fortschritte erzielt worden sind. Das Gleiche gilt für die Informations- und Kommunikationstechnologien (IKT) sowie die Mobilität und den Wärme- bzw. Kältesektor. In allen genannten Sparten sind die Entwicklungspotenziale jedoch noch lange nicht ausgeschöpft. Die drei Technologie- und Wirtschaftszweige Elektrizität, Mobilität und Klimatisierung bieten neue technische Optionen, die unsere Welt und unseren Alltag in näherer Zukunft deutlich verändern werden. Hier ist hohe Aufmerksamkeit erforderlich. Menschen denken häufig linear, während sich Veränderungen exponentiell – und damit häufig auch disruptiv – entfalten. Veränderungsprozesse verlaufen häufig zu Beginn sehr langsam, um dann plötzlich zum Durchbruch zu kommen und ihr Veränderungspotenzial explosionsartig zu entfalten. Wie die Welt in 10, 20 oder 30 Jahren genau aussehen wird, wissen wir nicht. Die Erfahrungen aus bisherigen Entwicklungen können jedoch helfen die Richtung und Dynamik zukünftiger Entwicklungen abzuschätzen. Dies setzt voraus, dass sowohl Wirtschaft, als auch Wissenschaft zu Wort kommen und die Potenziale aus den verschiedenen Perspektiven beleuchten, z.B. aus Sicht der Materialwissenschaften, der Ressourcenverfügbarkeit oder der soziologischen und umweltpsychologischen Forschung. Zu vergessen ist auch nicht, dass Technologieanwendung und Erhalt der Biodiversität in Einklang gebracht werden müssen.

Faktor Wirtschaftlichkeit

Ob die Energiewende zum Selbstläufer wird, hängt nicht zuletzt von der Wirtschaftlichkeit ab. Volkswirtschaftlich gesehen ist die Energiewende für Deutschland ein positiver Business Case, sofern neben dem Stromsektor sowohl die Sektoren Wärme und Mobilität miteinbezogen werden. Untersuchungen von Fraunhofer IEE („Geschäftsmodell Energiewende") aber auch von BDI und Prognos („Klimapfade für Deutschland") bestätigen dies. Auch die Industriezweige, deren Produktionsverfahren auf der Nutzung kohlenstoffhaltiger fossiler Stoffe basieren, müssen hierbei berücksichtigt werden. Die Potenziale erneuerbarer Energien aus Wind und Sonne sind groß. Hierfür sind Investitionen in die notwendige Infrastruktur erforderlich. Energieanlagen sind neu zu installieren, zu warten und nach Ablauf ihrer Lebenszeit zu ersetzen. Während des Anlagenbetriebs fallen allerdings keinerlei Brennstoffkosten mehr für die Energieerzeugung an. Damit werden volkswirtschaftlich betrachtet die Kosten für bisherige Brennstoffimporte eingespart. Abgesehen von der Braunkohle, die aus Klimasicht besonders umstritten ist, werden Erdöl, Erdgas und auch Steinkohle zu über 90 % aus dem Ausland eingeführt. Die Energiewende wird Deutschland daher mittelfristig auch unabhängig von der Preispolitik der Lieferländer machen. Damit steigt auch die geopolitische Resilienz.

Als Zwischenfazit ist festzuhalten, dass die drei genannten Faktoren zu orchestrieren sind, um die größtmögliche Wirkung im Sinne einer Eindämmung des Klimawandels zu errreichen.

Anforderungen – Energiewende ist Leistungswende

Da die erneuerbaren Potenziale und die Erzeugungskosten bei Wind- und Solarenergie am günstigsten sind, stehen sie im Zentrum der Energiewende. Die erzeugte elektrische Energie ist leicht transportierbar und in andere Energieformen wandelbar. Jedoch ist die ins Stromnetz eingespeiste Energie aus Wind und Sonne von der Witterung abhängig und daher mit raschen Leistungsänderungen und ausgeprägter Nichtverfügbarkeit verbunden. Dabei sind die Leistungsgradienten dem regionalen Einfluss unterworfen und abhängig von

der installierten Anlagenleistung in einem Netzgebiet. Bereits an Pfingsten 2016 konnte der – an Feiertagen generell niedrige deutsche Strombedarf – kurzzeitig fast vollständig aus erneuerbaren Energien gedeckt werden. Allerdings sah das Bild nur wenige Stunden früher und später ganz anders aus: Der Großteil der Stromverbrauchsleistung musste aus konventionellen Kraftwerken bereitgestellt werden. Die Energiemenge ist nicht das Problem, sondern deren zeitgerechte Verfügbarkeit am richtigen Ort.

Dies bedeutet zukünftig vor allem für die Stromnetzbetreiber eine enorme Herausforderung. Szenarien des Fraunhofer IEE für das Jahr 2050 zeigen, dass in Deutschland die installierte Leistung an Windenergie- und PV-Anlagen allein für den Ersatz der heutigen fossilen und nuklearen Kraftwerke beim 4- bis 5-fachen der Verbrauchleistung liegen wird. Diese Überbauung ist notwendig, weil die Anlagen witterungsbedingt die meiste Zeit über nicht mit ihrer vollen installierten Anlagenleistung Strom erzeugen können, sondern zumeist deutlich darunter liegen. Weiterhin sind Verbrauch und Einspeisung auch dann im Gleichgewicht zu halten, wenn nicht genügend elektrische Energie aus Wind und Sonne erzeugt wird. Aus diesen Gründen ist das Versorgungssystem flexibel zu gestalten. Dazu bieten sich verschiedene Möglichkeiten an: hochflexible, steuerbare Erzeugungsanlagen, Lastmanagement (Demand-Side-Management), Speicher sowie ein dynamischer Netzbetrieb. Näheres zu diesem Thema findet sich in der Publikation „Stabilität durch Flexibilität – Das hessische Stromnetz der Zukunft", die in Kooperation vom House of Energy und der Hessischen LandesEnergieAgentur erstellt wurde.

Energiewende ist Suffizienz- und Effizienzwende

Eine zukunftsfähige Energiewende bindet neben der Stromversorgung auch die anderen Sektoren wie Wärme und Verkehr sowie perspektivisch auch die Chemieindustrie mit ein. Für Erzeugung, Transport und Verteilung ist eine entsprechende Infrastruktur bereit zu stellen. Damit diese Infrastruktur in der Lage ist, den Elektrizitätsbedarf für die verschiedenen Sektoren zu jeder Zeit zu decken, sind große Anstrengungen bei Energieeffizienz und Energieeinsparung (Suffizienz) notwendig – gerade vor dem Hintergrund, dass Effizienz- und Suffizienzerfolge in der Vergangenheit immer wieder durch Rebound-Effekte und verändertes Kundenverhalten überkompensiert wurden.

Zellulär organisiertes Stromversorgungssystem

Um hohe Leistungen zu beherrschen und die Energiepotenziale aus Wind- und PV-Anlagen auszuschöpfen – also die Abregelungszeiten auf ein Minimum zu begrenzen – wird das Stromnetz der Zukunft in aktuellen Forschungsprojekten zellulär gedacht. Im SINTEG-Projekt C/sells, bei dem das House of Energy für die Regionalkoordination Hessen verantwortlich ist, finden hierzu Untersuchungen statt.
Im herkömmlichen Versorgungssystem speisen Großkraftwerke ins Höchstspannungsnetz ein und die Energie wird unidirektional zu den Verbrauchern auf den darunterliegenden Leistungsebenen transportiert. Im erneuerbaren Energiesystem hingegen speisen viele dezentrale Energieerzeuger auf unterschiedlichen Netzebenen ein. Die Verteilung von Erzeugern und Verbrauchern weist ganz unterschiedliche Strukturen auf. Innerhalb von Netzzellen sollte ein bestimmtes Maß an Leistungs- und Energieausgleich möglich sein, ebenso zwischen verschiedenen Netzzellen auf einer Spannungsebene. Dabei könnten diese Zellen subsidiär strukturiert sein, beginnend von einer Zelle „Europa" bis hinab zu den Zellen „Ortschaft", „Quartier" oder „Gebäude". Ziel ist ein resilientes und effizientes Gesamtsystem. Ein zellulär strukturiertes und dynamisch betriebenes Netz ermöglicht auch in Zukunft mit den Übertragungsnetzkapazitäten auszukommen und hilft unnötigen Netzausbau zu vermeiden.

Sektorenkopplung

Wenn Windenergie und Photovoltaik die tragenden Säulen des erneuerbaren Energiesystems sind, wird Strom zur neuen Primärenergie. Die Sektorenkopplung ermöglicht, diese erneuerbare Energie auch für andere Sektoren verfügbar zu machen, z.B. für die Mobilität oder die Bereitstellung von Nutzwärme.

Damit werden direkt Effizienzpotenziale gehoben. Ein gutes Beispiel ist die Elektromobilität. Die Verbrennung von Benzin und Diesel zum Zwecke der Bewegung von PKW ist energetisch sehr ineffizient – im Gegensatz zum Elektroantrieb.

Auch für Anwendungen, die einen gasförmigen oder flüssigen Treibstoff benötigen, lässt sich dieser aus erneuerbaren Energien herstellen. In deutlich begrenzten Mengen stünde Biogas zur Verfügung. Eine Treibstoffsynthese unter Nutzung von Wind- und Solarstrom ist mit größeren Abstrichen beim Wirkungsgrad verbunden. Doch die Erzeugung könnte zukünftig an Orten sinnvoll sein, an denen die Anlagen sonst regelmäßig abgeregelt werden und ausreichende Jahresenergiemengen zur Verfügung stehen.

Wird der Power-to-X-Ansatz ergänzt durch X-to-Power, so bestehen große Flexibilitätspotenziale für das Stromversorgungssystem. Beispiel Hochtemperaturspeicher: Zu Stromüberschusszeiten wird dieser mittels elektrischer Beheizung befüllt. Später kann die gespeicherte Hitze genutzt werden, um Strom zu erzeugen. Die Funktion eines elektrischen Speichers wäre gegeben.

Neue Komplexität

Stromeinspeisung und -bezug aus den dezentral verteilten Anlagen lassen sich unterschiedlich gut prognostizieren und regeln. Wichtig ist es, die Anlagen intelligent zu steuern, um die angestrebte Effizienz und Flexibilität im Gesamtsystem auch tatsächlich zu erreichen. Neben der technischen Sicht auf ein solches intelligentes Netz (Smart Grids) ist auch die ökonomische Sicht zu berücksichtigen. Aktuell werden digitale Markplattformen für „Smart Markets" in verschiedenen Projekten erprobt. Dabei ist auch mit neuen Marktrollen zu rechnen. Das Management dieses komplexen Energiesystems benötigt eine ergänzende IT-Infrastruktur. Es sind also zwei Infrastrukturen aufzubauen: Dezentrale Energieanlagen inklusive intelligenter Netztechnik sowie die IT-Infrastruktur, die ein Internet of Things in der Energiewelt ermöglicht.

Internet of Things in der Energiewelt – Rolle von Daten

Die dargestellte Komplexität des neuen Energiesystems erfordert die Erhebung und die Analyse sowie den Austausch und die Bereitstellung großer Datenmengen. Dabei kommen moderne Big Data-Verfahren aus der digitalen Welt zum Einsatz. Aus der an sich unübersichtlichen Fülle an Daten können mittels Mustererkennung, künstlicher Intelligenz, selbstlernender Systeme, neuronalen Netzen, etc. Erkenntnisse gewonnen werden, z.B. um Energieeffizienzpotenziale zu erkennen und zu heben. Perspektivisch wird die bislang in der Energiewirtschaft übliche zeitliche Auflösung von Viertelstundenwerten nicht mehr ausreichen. Echtzeitdaten werden der neue Standard sein. Einerseits ermöglichen Echtzeitdaten das Stromnetz genau zu beobachten und zu steuern. Andererseits wird es Fortschritte bei Rechenleistung, Speicherkapazität und Übertragungsgeschwindigkeit geben.

Mögliche Anwendungsfelder für die IT

Die Verwebung von digitaler Welt und Energiewelt ermöglicht perspektivisch völlig neue IT- und OT- Anwendungen (Information Technology / Operation Technology) für die Systemsteuerung (Smart Grids / Smart Markets), die Optimierung unternehmensinterner Prozesse sowie für neue Dienstleistungen und Produkte. Schon jetzt erkennen Startups die Chance und den Bedarf. Sie entwickeln neue Lösungen und bringen diese auf den Markt – soweit der aktuelle Rechtsrahmen es ermöglicht.

Beispielhafte IT-Anwendungsfelder entlang der Wertschöpfungskette der Energiewirtschaft sind:

Erzeuger / Verbraucher / Speicher

- Intelligente Steuerungen flexibler dezentraler Energieanlagen ermöglichen eine bessere Integration von fluktuierenden erneuerbaren Energien.
- Smart Grids und Smart Markets sind aufeinander abzustimmen, um synchrone Wirkung im Sinne der Minimierung der Infrastruktur zu entfalten.
- Virtuelle Kraftwerke und intelligente, dynamisch wechselnde Anlagenverbünde sind zu etablieren.
- Vorausschauende Wartung und Instandhaltung von Energieanlagen verbessern die Systemzuverlässigkeit und senken die Kosten.
- Identifikation und Nutzung von Energieeffizienzpotentialen auf Quartiers- oder Gebäudeebene reduzieren den Energiebedarf und entlasten so die energietechnische Infrastruktur.

Netze

- Eine effizientere Netznutzung wird möglich, indem die Kapazitäten der Verteilnetze besser genutzt werden. Dazu sind die Verteilnetze dynamisch zu betreiben.
- Hierbei helfen bessere Einspeiseprognosen für regional bzw. lokal ins Netz eingespeisten Wind- und PV-Strom, bessere Prognosen zum Verhalten von Prosumern, eine automatische Netzbeobachtung und -steuerung sowie der bedarfsgerechte Abruf von Netzdienstleistungen.

Handel & Vertrieb

- Neue Marktplattformen machen den Handel mit vielfältigen neuen Produkten zwischen vielfältigen Marktakteuren möglich.
- Kleinsttransaktionen werden möglich und auf Basis von Echtzeitdaten auch ein schneller algorithmischer Handel.
- Da sprichwörtlich gesehen jeder Kilowattstunde ein Datum angeheftet werden kann, entsteht eine neue Datentransparenz, worüber das Ausstellen von Herkunftsnachweisen und die Zertifizierung von Energieprodukten vereinfacht werden.

- Auf Basis von dynamischen Tarifen werden sektorenkoppelnde Anlagen (Power-to-X) ihren Strom automatisiert vorwiegend dann beziehen können, wenn erneuerbarer Strom in großen Mengen verfügbar ist und die Anlage nicht für Netzdienstleistungen benötigt wird.

Bei neuen Energiedienstleistungen, die sich an Endkunden richten, gilt es zu beachten: Für den Endkunden sind Versorgungssicherheit, Komfort und Preis ausschlaggebend und damit Trumpf – gekoppelt mit dem Vertrauen, das der Anbieter genießt.

Anforderungen an die IT

Damit die IT bestmöglich die Energiewende und die Menschen unterstützt, sind klare Qualitätsanforderungen an die IT-Infrastruktur zu stellen.

Bei der Infrastruktur für die Energieversorgung handelt es sich um eine kritische Infrastruktur. Die Versorgungssicherheit muss zu jedem Zeitpunkt für jeden Ort gewährleistet sein. Gegenüber äußeren Einflüssen muss eine hohe Resilienz sichergestellt sein. Zugleich benötigt die große Zahl unterschiedlicher Akteure einen Zugang zu System und Märkten, der standardisiert mit geringem Aufwand möglich ist. Beide Ansprüche gilt es, miteinander in Einklang zu bringen.

Darüber hinaus sollten möglichst wenig Energie und Ressourcen für die zusätzliche IT-Infrastruktur verbraucht werden. Nicht vergessen werden darf der Energiebedarf für den Betrieb der IT. Nutzen und Aufwand sind abzuwägen. Das Zieldreieck der Energiewirtschaft (Versorgungssicherheit, Wirtschaftlichkeit und Klima- und Umweltschutz) darf trotz aller IT-Möglichkeiten nicht aus den Augen verloren werden. Neben der Bereitstellung einer ausreichenden Datenqualität und -verfügbarkeit müssen der Datenschutz und die Datenhoheit/-souveränität beachtet werden.

Da auch das beste IT-Konzept immer Sicherheitslücken haben wird, muss darauf geachtet werden, dass die Energieinfrastruktur selbst in der Lage ist, die Systemstabilität auch bei (teilweisem) Ausfall der IT-Infrastruktur autark zu gewährleisten.

Green Economy als Schnittmenge von Smart Grids und Smart City

Die Digitalisierung schreitet schnell voran und neue innovative IKT-Lösungen für die Stadt- und Regionalentwicklung werden in Konzepten mit dem Titel Smart City sichtbar. Gleichzeitig bieten städtische und ländliche Räume auf lokaler Ebene die Grundlage für die oben vorgestellte Zellenstruktur von Stromverteilnetzen. Für die verschiedenen Teilaspekte einer Smart City, seien es Gebäude & Quartiere, Mobilität & Logistik, Wasser & Abfall oder Industrie, sollte die Vision einer wirksamen Green Economy gleich mitgedacht werden. Städte sind für den überwiegenden Teil der Treibhausgasemissionen verantwortlich. Beim Aufbau der neuen Infrastrukturen sind die drei Seiten des Nachhaltigkeitsdreiecks zu berücksichtigen:

- die Umweltseite (z.B. umweltverträglicher Umgang mit Energie und Ressourcen)
- die soziale Seite (z.B. Lebensqualität und gesellschaftlicher Wandel) sowie
- die wirtschaftliche Seite (z.B. Marktvielfalt, lokale/regionale Wertschöpfung).

Marktentwicklung im Zuge von Energiewende und Digitalisierung

Die Digitalisierung der Energiewelt hat einen großen Einfluss auf die Märkte und bringt Veränderungen in Bezug auf Geschäftsmodelle & Produkte, Wertschöpfungsketten, Marktrollen und Finanzflüsse mit sich.

Marktstrukturen werden sich wandeln. Dies bedeutet im Umkehrschluss, dass traditionelle Geschäftsmodelle bedroht sind. Bei diesem Wandel wird es Gewinner und Verlierer geben. Aufgabe des Gesetzgebers ist es, die Marktentwicklung aktiv zu begleiten und den Rechtsrahmen so auszugestalten, dass der Prozess geordnet abläuft und der Wirtschaftsstandort Deutschland bzw. Hessen gestärkt daraus hervorgeht. Dies beinhaltet, dass die soziale Balance gewahrt bleibt und neue Lösungen sich am Markt erproben und beweisen können. Der regulatorische Rahmen wird erst mit einer gewissen zeitlichen Verzögerung die neuen Herausforderungen aufgreifen, die die Veränderungen in der Energie- und IT-Welt mit sich bringen. Im Bereich der Netze ist der Markt reguliert. Dadurch haben die Norm gebenden Stellen auf Bundesebene Einfluss darauf mit welcher Geschwindigkeit und Durchdringungstiefe bestimmte technische Optionen, die der Markt bereithält, zum Tragen kommen.

Für etablierte Unternehmen bedeutet dies, dass ein Innovations- und Changemanagement erforderlich ist. Das Personal ist entsprechend weiterzubilden.

Ansätze des House of Energy in diesem Zusammenhang sind: Zukunftsfragen frühzeitig identifizieren und eine „zügige Evolution" ermöglichen, anstatt „Disruption" zuzulassen. House of Energy und House of IT ermöglichen, sich gezielt auf die Zukunft einzustellen

und Synergien zwischen den Akteuren zu nutzen. Beispiele sind geförderte Innovationsprojekte sowie die Vernetzung mit kleinen innovativen Unternehmen, die sich durch Wendigkeit und Risikobereitschaft auszeichnen und Innovationen gemeinsam mit den im Markt verankerten etablierten Unternehmen vorantreiben.

Fazit:

4. Die Energiewende stellt einen fundamentalen gesamtgesellschaftlichen Transformationsprozess dar, wobei Branchengrenzen erodieren.

5. Treiber der Prozessdynamik sind Klimaschutz, technologischer Fortschritt und Wirtschaftlichkeit.

6. Eigenschaften des neuen Energiesystems: dezentral, sektorenübergreifend, zellulär strukturiert, hoch flexibel, komplex.

7. Smart Grids & Smart Markets erfordern die Digitalisierung der Energiewelt.

8. Die IT-Infrastruktur muss resilient und energieeffizient sein. Der Zugang aller Marktteilnehmer und Datenschutz sind zu gewährleisten.

9. Neue Anwendungsfelder und Geschäftsmodelle führen zu Marktanpassungen und machen Innovations- und Changemanagement notwendig.

Houses of Dialog: Die Energiewelt wird digital | Frankfurt am Main, 28.10.2018

EINFÜHRENDE ÜBERLEGUNGEN AUS SICHT DER IT-WELT – Rolle und Herausforderungen der digitalen Transformation

Dr. Florian Volk, House of IT e.V., Geschäftsführer

Auch aus Sicht der Digitalen Transformation ist die Energiewende ein wegweisendes Großprojekt: neue Geschäftsmodelle werden entstehen und Intelligenz wird im Netz verteilt werden. So jedenfalls zeichnet es sich ab.

Das Thema Cybersicherheit im Energienetz bekommt eine neue Dimension: Bisher isolierte Systeme einer kritischen Infrastruktur werden vernetzt und die Angriffsmöglichkeiten auf das Gesamtsystem erhöhen sich. Wo bisher ein Angriff auf eine einzelne Komponente des Energienetzes primär diese Komponente gefährdet, sehen wir perspektivisch Angriffe, die sich von einem „Einfallstor" hin auf gesamte Netze ausbreiten können. Gerade in einer alten, gewachsenen und vor allem: verteilten Infrastruktur wie dem Energienetz wird man mit klassischer Perimetersicherheit keinen hinreichenden Schutz erreichen können. Neue Mechanismen sind gefragt, um Resilienz erzielen zu können.

Ein großer Vorteil ist, dass die Energiebranche hier von der IT-Branche lernen kann (und natürlich auch umgekehrt); für viele Herausforderungen, die im Energiesektor durch die Energiewende neu entstehen, gibt es in der Welt der Digitalisierung schon erprobte und adaptierbare Lösungen. Man denke nur an Design-Ansätze wie zelluläre Netze (z.B. Modellstadt Mannheim, C/sells-Projekt) und den potentiell nächsten Schritt, holare Netze (z.B. PolyEnergyNet-Projekt), welche zu flexibleren und resilienteren Netzen führen, die zugleich eine höhere Versorgungssicherheit und die Integration verteilter, dezentraler Prosumer ermöglichen.

Die Möglichkeit, von der Zusammenarbeit zweier so unterschiedlicher Sektoren zu profitieren, erfordert als Vorarbeit, dass die Sektoren lernen, sich gegenseitig zu verstehen. Es gibt grundsätzlich unterschiedliche Eigenschaften und Herangehensweisen, deren man sich bewusst werden muss, um sie zusammenführen zu können.

Die Energiebranche ist geprägt von einem erzeugerzentrischen Denkbild und etablierten technologischen Lösungen. Veränderungen sind zeitaufwendig (Tiefbau, Gesetzgebungsverfahren), während die Digitalbranche als „junge Branche" eine deutlich höhere Taktzahl anlegt: häufige Updates, kurze Technologielebenszyklen von teilweise nur wenigen Jahren in Verbindung mit einer disruptiven Attitüde machen es schwierig, die Welten „Energiebranche" und „Digitalbranche" gewinnbringend zu kombinieren.

Als „Houses of" sehen wir uns als die richtigen Ansprechpartner, diese Annäherung fruchtvoll zu gestalten, indem wir unsere Expertennetzwerke in der Fragestellung der Energiewende zusammenbringen und den Wissens-, Forschungs- und Technologietransfer fördern.

SESSION 1

IT-ANWENDUNGEN IN DER ENERGIEWELT

Houses of Dialog: Die Energiewelt wird digital | Frankfurt am Main, 28.10.2018

Entwicklung neuer Geschäftsmodelle mit Smart Home aus Sicht eines EVU

Kai Wacholder, Städtische Werke AG, Kassel

Fragt man sich, was eigentlich die Assets von Stadtwerken sind, so kann man dieses vor allem mit „hohem Vertrauen" und „direktem Kundenzugang" zusammenfassen. Andere, vermeintliche Stärken von Stadtwerken wie Erzeugung, Lieferung und Abrechnung von Energie können Stadtwerke zwar auch gut, jedoch nicht wirklich besser als die Wettbewerber am Markt. Auch ist inzwischen klar, dass die Lieferung von Energie nicht den Energieversorgern vorbehalten bleibt, sondern dass auch Marktfremde den Stadtwerken zunehmend ihre Marktanteile abnehmen. Telekommunikationsriesen wie 1&1, Transportunternehmen wie die Deutsche Bahn oder auch Hersteller wie Viessmann sind inzwischen auch zu Energieversorgern geworden.

Grund genug, sich auf die eigenen Stärken zu fokussieren und die wahren Assets „Kundenzugang" und „Kundenvertrauen" für neue Geschäftsfelder zu nutzen. Aber nicht nur die Stadtwerke müssen lernen, jenseits der Kilowattstunde neue Geschäfte zu entwickeln. Denn auch für die Kunden muss dieser Wandel nachvollziehbar und naheliegend sein. Während sich heute noch die meisten Stadtwerke eher unterhalb der Wahrnehmungsschwelle, d.h. im wörtlichen Sinne im Keller des Kunden aufhalten, gilt es, hier die Kellerdecke zu durchdringen und mit neuen Angeboten im häuslichen Umfeld zusätzliche Deckungsbeiträge zu erwirtschaften.

Dies gilt auch für die Städtische Werke AG, die – behutsam und für den Kunden schrittweise nachvollziehbar – Dienstleistungen in und ums Haus entwickelt. Smarthome bietet dabei eine große Chance. Und die Abgrenzung zu do it yourself-Angeboten der Elektro- und Baumärkte wie schaltbare Steckdosen oder dimmbare Lampen fällt den Stadtwerken nicht schwer. Die Energieversorger fokussieren sich besser auf ihre Tugenden und bieten deshalb vorrangig Wärmesteuerung und Sicherheitsfunktionen an.

Dennoch gibt es einige Herausforderungen, die bei der Einführung von Smarthome für Stadtwerke zu beachten sind: Stadtwerke sind weder Hersteller von Hardware noch Experten für deren Lieferung an den Kunden. Kooperationen sind hier das Mittel der Wahl, denn sie entlasten die Stadtwerke bei denjenigen Teilen der Wertschöpfungskette, die nicht zu ihren bisherigen Kernprozessen passen.

Dabei sollte die Auswahl der benötigten Hardware gut überlegt sein. Verfügbarkeit, Preis, Sicherheit und Erweiterbarkeit sind Anforderungen der Kunden, die optimal befriedigt werden müssen. Zusammen mit den Kooperationspartnern haben Stadtwerke aber gute Chancen, dieses Geschäftsfeld erfolgreich zu besetzen und im Anschluss daran sogar weitere Dienstleistungen zu entwickeln. Das Stadtwerk wird so schrittweise vom Energielieferanten zum Lösungsanbieter und zurückgehende Margen aus dem Energievertrieb werden durch neue Geschäftsmodelle idealerweise überkompensiert.

Houses of Dialog: Die Energiewelt wird digital | Frankfurt am Main, 28.10.2018

Quartierslösungen digitalisiert: Mehrwerte durch Energiemanagement Systeme

Martin Volkmar, Viessmann Werke GmbH & Co. KG

Viessmann ist Hersteller von Energiesystemen mit einem breiten Produktportfolio im Bereich von Heizen, Stromversorgung und Kühlen. Der Bereich der Systems Technology bei Viessmann stellt sicher, dass die verschiedenen Wärme- und Stromerzeuger zusammen mit Services und Zubehör systemfähig werden. In diesem Zusammenhang werden insbesondere multivalente Energiesysteme in Quartierslösungen konzipiert und mit lokalen Steuerungen ausgerüstet.

Ein Quartier besteht in der Regel aus einer Menge von Haushalten mit Wärme- und Strombedarf, die aus einer gemeinsamen Energiezentrale über ein Nahwärmenetz bzw. geeignete Stromleitungen versorgt werden. Quartiere können entweder in Form von Neubauprojekten oder für existierende Wohn- und Gewerbegebiete realisiert werden. Eine besonders interessante Art von Quartieren sind die sogenannten Bioenergiedörfer, welche aufgrund der Wahl der Brennstoffe, Heiztechnologie und Stromerzeugungsverfahren komplett auf regenerativen Energiearten aufsetzen können.

Abbildung 1: Konzept eines Bioenergiedorfes

Bezüglich der Wärmeversorgung ist die Energiezentrale so ausgelegt, dass mehrere Wärmeerzeuger zu den verschiedenen Jahreszeiten den anfallenden Wärmebedarf effizient und sicher bedienen können. Die hierzu konzipierte Steuerung gibt den Betriebsablauf für die verschiedenen Wärmeerzeuger gemäß dem gemessenen Bedarf und verschiedener anderer Messwerte aus der Umgebung vor.

Abbildung 2: Jahreslastprognose für ein Bioenergiedorf. Heizlastabdeckung durch ein multivalentes Heizsystem mit übergeordneter Steuerung

Für den reibungslosen Steuerungsablauf müssen viele Statusinformationen und Messwerte von den Erzeugern, Verbrauchern, Pumpen und Umweltsensoren digital erfasst werden. Die lokal erfassten Daten können über eine geeignete Datenverbindung einem Speicher in der Cloud zugeführt werden.

Mit den Daten des Energiesystems in der Cloud können verschiedene Mehrwerte realisiert werden:

1. Visualisierung und Monitoring:
   - Überwachung des Anlagenzustandes via Leitwarte
   - Messaging und Alarmierung bei Fehlerzuständen
   - Darstellung von historischen Datenverläufen

2. Datenauswertung auf Basis der historischen Daten:
   - Errechnung von Kennzahlen zur Bewertung von verschiedenen Anlageneigenschaften
   - Energieflussanalysen über Sankey Diagramme
   - Prädiktive Analyse bzgl. Anlagenwartung
   - Optimierungsmaßnahmen

Auf Basis der Datenauswertung kann ein Energiemanagement aufgesetzt werden, welches verschiedene Mehrwerte für den Anlagenbetrieb realisieren kann:

- **Energieberichte** nach ISO 50001 und Berichte für den Nachweis bzgl. Förderbedingungen

- **Effizienzbewertungen** schaffen Transparenz für die Energieströme in der Anlage. Hierdurch können Verbesserungspotentiale identifiziert werden, die im Rahmen der ISO 50001 in überwachten Maßnahmen umgesetzt werden.

- **Condition Monitoring** stellt über KI-Methoden ein abnormes Anlagenverhalten fest, welches den nahenden Ausfall eines Anlagenteils ankündigt. Ein frühzeitiger Austausch verringert Ausfallzeiten der Anlage. Darüber hinaus können fehlerhafte Auslegungen der Anlage erkannt und korrektive Maßnahmen zur Behebung eingeleitet werden.

- **Bedarfsprognosen** ermöglichen Kostensenkungen bei der Beschaffung von Brennstoffen und Strombezug. Durch einen prognosegesteuerten Betriebsplan für Wärmeerzeuger und flexible Stromverbraucher können Effizienz, Kosten und Verfügbarkeit auf hohem Niveau gehalten werden.

- Im Rahmen der **Energieoptimierung** können Betriebsfahrpläne nach Berechnung durch den Optimierer automatisch auf die Anlagenteile abgebildet werden. Hierdurch entstehen automatisch Energiekosteneinsparungen und entsprechende Effizienzsteigerungen.

Fazit: Die digitalisierte Datenerfassung in Quartierslösungen ermöglicht ein Energiemanagement. Das Energiemanagement ist Schlüssel zu ...

- höchstem Grad der Sicherung für eine kontinuierliche Energieversorgung

- optimiertem Anlagenbetrieb -> Effizienz, Kosten, Verfügbarkeit

- Synergie mit anderen Ebenen des Energienetzes durch Vernetzung auf Cloud-Basis

Kernthesen:

- **Digitalisierte Quartiere bieten ähnliche Schnittstellen wie kleinere Prosumer-Einheiten für die Vernetzung.**

- **Aufgrund des hohen Erzeugungs- und Verbrauchspotentials eröffnen Quartiere eine neue Dimension in der Vermarktung von Flexibilitäten.**

Houses of Dialog: Die Energiewelt wird digital | Frankfurt am Main, 28.10.2018

Industrie 4.0 für die Energieversorgung – ein junges Unternehmen nimmt die Digitalisierung in die Hand

Dr. Dennis Metz, Othermo GmbH (Startup)

Die Energiewende stellt Energieversorger vor eine Vielzahl an Herausforderungen. So werden in der Versorgung von Quartieren, großen Gebäuden sowie Nahwärmenetzen aus ökonomischen und ökologischen Gesichtspunkten inzwischen meist Blockheizkraftwerke eingesetzt. Hierdurch wird die Versorgungssituation allerdings deutlich komplexer. Dies ist nicht nur durch die zusätzliche Technik bedingt, sondern auch durch die regulatorische und energetische Betrachtung, da nun neben der Wärme auch der Stromumsatz berücksichtigt werden muss. Die eingesetzte Überwachungs- und Steuertechnik hat bei der Entwicklung häufig nicht Schritt gehalten und es werden nach wie vor technologisch überholte Lösungen eingesetzt. Unter dem Schlagwort „Industrie 4.0" hat sich im industriellen Umfeld in den letzten Jahren ein Trend herausgebildet, der die Vernetzung und Digitalisierung der Produktionsprozesse beschreibt. Basierend auf den gesammelten Betriebsdaten lassen sich vielfältige Mehrwerte generieren, welche auch in Heizzentralen realisiert werden können.

othermo bietet eine Lösung für Heizzentralen, welche die Überwachung, Analyse und Optimierung von den dort verbauten Komponenten herstellerübergreifend ermöglicht.

Durch ein vor Ort installiertes Gateway werden die Betriebsdaten der einzelnen Anlagenkomponenten (z.B. Kessel, Blockheizkraftwerke, Pumpen, Druckhaltung, Zähler) kontinuierlich ausgelesen und übertragen. Die Anbindung von Komponenten ist dabei herstellerübergreifend möglich und erfolgt über Busprotokolle, um detaillierte Statusinformationen und alle Betriebsparameter zu erhalten. Gleichzeitig werden dadurch die Installationskosten reduziert, da in der Regel keine weitere Sensorik installiert werden muss.

Der Zugriff auf die gesammelten Betriebsdaten erfolgt über eine webbasierte Plattform, welche eine integrierte Betrachtung der gesamten Heizzentrale ermöglicht. Somit ist keine spezielle zentrale Software notwendig, auch die Einwahl über Modem / VPN entfällt.

Über die Plattform lässt sich sowohl der aktuelle Betriebszustand der Anlage visualisieren als auch historische Trenddaten. Mit Hilfe von diesen lässt sich das Zusammenspiel der einzelnen Komponenten analysieren, Fehler in den Parametern der einzelnen Komponenten finden, Anlagen bedarfsgerecht warten und Optimierungspotentiale identifizieren. Das regelmäßige manuelle Ablesen der Zählerstände entfällt. Die Alarmierung bei Störungen oder Grenzwertüber-/unterschreitungen erfolgt z.B. per SMS oder E-Mail. Des Weiteren sind sektorspezifische Analysetools integriert, welche die Auswertung der gesammelten Daten entsprechend den Anforderungen der Betreiber ermöglicht.

Durch solch eine Lösung lassen sich nicht nur die Effizienz und Versorgungssicherheit erhöhen, sondern es ergeben sich auch ökonomisch neue Optionen durch eine vorausschauende Steuerung. Statt der klassischen (auf aktuellen Messwerten basierenden) Regelungstechnik nutzen wir Vorhersagen über künftigen Verbrauch und Erzeugung. Somit lassen sich z.B. erneuerbare Energien optimal integrieren und Strom bedarfsgerecht lokal erzeugen, z.B. um die Profitabilität bei Mieterstrom-Lösungen zu steigern. Basierend auf historischen Verbrauchsdaten für Wärme und Strom werden dazu im ersten Schritt kontinuierlich Vorhersagen über den künftigen Verbrauch erzeugt. Diese bilden anschließend die Grundlage für eine Optimierung, welche den Betriebsablauf der Anlagen unter Berücksichtigung der Betriebskosten und Erlöse optimiert. Der jeweils optimale Fahrplan wird an die Anlage übertragen und automatisch umgesetzt.

Houses of Dialog: Die Energiewelt wird digital | Frankfurt am Main, 28.10.2018

Diskussion in Session 1 „IT-Anwendungen in der Energiewelt“

- **Wie wird die Energiewelt im Jahr 2030 aussehen?**
- **Worin besteht aktuell der drängendste Handlungsbedarf?**
- **Welche Potenziale hat die energieoptimierte Quartiersversorgung?**
- **Wie gelingt die Umsetzung im Zusammenspiel mit den Bürgern?**
- **Welche Rolle spielt die IT für die Energiewende?**
- **Welche Konsequenzen ergeben sich für Energieversorger?**
- **Was bedeutet dies für den regulatorischen Rahmen?**
- **Was bringen Messstellenbetriebsgesetz und Datenschutz-Grundverordnung?**
- **Wie kann Hessen eine Vorreiterrolle bei der digitalen Energiewende einnehmen?**

Im Anschluss an die Impulsvorträge der Session 1 „IT-Anwendungen in der Energiewelt“ fand eine moderierte Podiumsdiskussion unter Einbeziehung des Publikums statt. Dabei wurden die genannten Fragenkomplexe diskutiert.

Naturgemäß konnten die Fragestellungen im Rahmen der dreiviertelstündigen Diskussion nicht vollständig oder ganzheitlich beantwortet werden. Die textliche Zusammenfassung gibt wichtige Aspekte wider, die die Diskutanten auf Grundlage ihrer fachlichen Erfahrungen aufgegriffen und erörtert haben. Widergegebene Positionen entsprechen nicht zwangsläufig der Haltung der Geschäftsstelle des House of Energy.

Ein herzliches Dankeschön geht an die Personen, die sich intensiv in die Fachdiskussion eingebracht haben: Herr Kai Wacholder (Städtische Werke AG Kassel), Herr Martin Volkmar (Viessmann), Herr Dr. Dennis Metz (Othermo GmbH, Alzenau), Herr Arnd Böken (Wirtschaftskanzlei GvW Graf von Westphalen, Frankfurt), Herr Dr. Reinhard Mackensen (Fraunhofer IEE, Kassel), Herr Lars Rinn (node.energy GmbH, Frankfurt). Zusammenfassung der Diskussion: Dirk Filzek (House of Energy e.V., Bereich Wissenstransfer, Kassel).

Wie wird die Energiewelt im Jahr 2030 aussehen?

Die Erzeugerlandschaft wird sich weiter verändern. Mehr PV- und Windenergieanlagen werden in die Stromnetze eingebunden sein, u.a. durch Prosumer. Gerade mit Blick auf die Verteilnetze ist deshalb mit entsprechend mehr Fluktuation bei der eingespeisten elektrischen Energie zu rechnen. Dabei stellt die rasche Änderungsgeschwindigkeit der Einspeiseleistungen eine besondere Herausforderung dar. Um für einen Leistungsausgleich zu sorgen, dürften daher im Jahr 2030 viele kleine Energieversorger gefordert sein, auch die Lastseite in ihren Verteilnetzen mit zu berücksichtigen.

Die Sektorenkopplung bringt viele zusätzliche Stromanwendungen auf der Lastseite mit ins System ein. Als konkretes Beispiel für die Kopplung Strom-Wärme wurde die Wärmepumpe angesprochen: Im Jahr 2030 dürften 60-70 % aller Neubauten mit Wärmepumpen ausgestattet sein. Bei Neubauten sind Wärmepumpen gut geeignet um Energieeffizienz zu erreichen. In Altbauten sind Wärmepumpen aufgrund des größeren Wärmebedarfs der Gebäude nicht so effizient. Hier bieten sich Kombinationen aus PV-Anlagen und lokalen Stromspeichern an. Dabei könnten Second-Life-Batterien kostengünstig zum Einsatz kommen. Dies sind Batterien, die nach ihrer Erstnutzung im Elektroauto einer Zweitnutzung zugeführt werden, für die die Batteriekapazität über einen längeren Zeitraum noch gut ausreicht. Fortschritte in der Digitalisierung werden die Koordination der zahlreichen dezentralen Energieanlagen unterstützen (weiteres dazu siehe unten).

Worin besteht aktuell der drängendste Handlungsbedarf?

Als herausragendes Thema wurde die Umsetzung der Klimaschutzziele wahrgenommen. Dabei leitet sich der aktuelle Handlungsbedarf aus dem angestrebten Dekarbonisierungspfad für die Wirtschaft ab. Ziel ist ein erneuerbares Energieversorgungssystem mit Sektorenkopplung, wobei die vielen dezentralen Energieanlagen mittels eines intelligenten Stromnetzes (Smart Grid) aufeinander abgestimmt gesteuert werden. Für die konkrete Umsetzung wurde herausgestellt, dass der weitere Ausbau der erneuerbaren Energien alleine nicht ausreicht, und sowohl die Notwendigkeit besteht, Effizienzpotenziale systematisch zu erschließen, als auch den gesamtgesellschaftlichen Energieverbrauch zu reduzieren.

Deutschland wurde von Diskutanten in Sachen Energiewende nicht mehr als Vorreiter, sondern eher als Bremser wahrgenommen. Es wurde festgestellt, dass die Technologien grundsätzlich bereits vor-

handen sind und es gilt, sie für die Praxis weiterzuentwickeln, wobei der Blick vor allem auf technisch-systemische Weiterentwicklung, IKT-Vernetzung sowie regulatorische Fragestellungen zu richten ist. Als ein Beispiel wurden neue Speichertechnologien genannt: Mögliche Anwendungsfälle gilt es jetzt weiterzuentwickeln und im Praxistest zu erproben, denn – auch wenn ihr Einsatz derzeit noch nicht erforderlich bzw. wirtschaftlich ist ist – sie werden zukünftig notwendig.

Welche Potenziale hat die energieoptimierte Quartiersversorgung?

Um die Klimaziele zu erreichen wurde vorgeschlagen, in der nächsten Stufe von der Wärmeseite aus zu denken und von dort aus konzeptuell auf die Sektorenkopplung zu schauen. Eine energieoptimierte Quartiersversorgung könnte ein Ansatz sein. Für ein Quartier lässt sich die Energieversorgung oftmals effizienter und umweltfreundlicher gestalten, als dies für Einzelobjekte möglich ist.

Eigenerzeugungsanlagen in Quartieren und Einzelgebäuden dienen der Selbstversorgung mit Strom und Wärme zu einem gewissen Grad. Diese lassen sich netzdienlich in die Verteilnetze einbinden, sofern sie über die entsprechenden regelbaren Einheiten verfügen. Dadurch könnten Netzbelastungen und Netzentgelte sinken. Netzdienlichkeit ist jedoch nicht automatisch gegeben. Nicht auszuschließen ist, dass sich Prosumer-Haushalte etablieren, deren Energieoptimierung sich ausschließlich auf den Strom- und Wärmebedarf im Haushalt selbst bezieht und die die Perspektive des Verteilnetzes ausschließen. Prosumer-Haushalte gilt es, in das Smart Grid mit einzubinden.

Quartierslösungen zur energetischen Optimierung funktionieren zwar von der Idee her gut, jedoch wurde die Realisierung, und damit ein Ausrollen in die Breite, als ein zäher Prozess beschrieben. Bei Projektplanung und -umsetzung kommt es auf eine enge Kooperation aller Akteure an. Im Einzelfall entscheidet die richtige Kommunikation genauso über den Projekterfolg wie die Ergebnisse der technisch-ökonomischen Analyse. Die jährliche Zahl an Quartiersneubauten ist begrenzt. Bestandsquartiere sind zwar in Fülle vorhanden. Dort sind aufgrund der Bestandsstrukturen unter Umständen aber die Möglichkeiten begrenzt oder es steht nur eine rudimentäre Datenbasis zur Verfügung. In der Praxis gibt es Hindernisse bei der Einbindung der Mieter in die Quartiers-Energieversorgung, z.B. aufgrund der freien Stromanbieterwahl durch die Mieter oder aufgrund von Heizungsbestandsanlagen. Mit Blick auf die Klimaschutzziele für das Jahr 2030 wurde gefolgert, dass Quartiere noch eine nachrangige Rolle spielen dürften. Es wurde die Einschätzung geäußert, dass eine weiterentwickelte Regulatorik hilfreich wäre, um Quartierslösungen zielgerichtet zu unterstützen.

Eine Besonderheit im Bereich der Quartierslösungen ist das Bioenergiedorf. Dabei wird nicht der einzelne Kunde als Erzeuger gesehen, sondern das gesamte Dorf. Vorteil ist, dass sich Ausgleichseffekte im Netz ergeben und Lastspitzen abgefangen werden. Entscheidend ist das Engagement der Akteure. Während es bereits für Quartiersprojekte aktive Personen braucht, die die Umsetzungschancen sichern, gilt für alternative Modelle wie ein Bioenergiedorf umso mehr, dass die Akteure Idealismus mitbringen müssen, denn bei den relativ niedrigen Energiepreisen und den schwankenden Preisen für Biomasse stellt ein Bioenergiedorf aus ökonomischer Sicht nicht gleich und verlässlich einen Vorteil dar.

Wie gelingt die Umsetzung im Zusammenspiel mit den Bürgern?

Es wurde als Gegensatz wahrgenommen, dass die Umsetzung der Energiewende eine gesamtgesellschaftliche Herausforderung darstellt, sich andererseits aber die Endverbraucher kaum mit dem Thema Energie beschäftigen. Bei Energie handelt es sich um ein Commodity-Produkt: Endverbraucher erwarten eine gesicherte, kostengünstige und unkomplizierte Versorgung. Daran dürfte sich auch perspektivisch nicht viel ändern und Ansätze, den Kunden diesbezüglich umzuerziehen, dürften zum Scheitern verurteilt sein. Nichtsdestotrotz muss der Umsetzungswille für eine gelingende Energiewende – so wurde hervorgehoben – von der Bevölkerung ausgehen, was praktisch bedeutet, dass der Einzelne Verantwortung für Klimaschutz und Energiewende übernimmt. Da der Transformationsprozess mit deutlichen Veränderungen einhergeht, setzt dies einen persönlichen Willen zur Veränderung voraus.

Aufbauend auf diesen Überlegungen wurde darüber diskutiert, wie sich in der Gesellschaft ein solcher Mentalitätswechsel herbeiführen lässt. Eine Bewusstseinsbildung dafür, dass Energie als wertvolle Ressource gesehen wird, sollte dazu führen, dass Einsparungen beim Energieverbrauch realisiert werden. Im konkreten Fall wurde die Beobachtung geschildert, dass auch in Neubauten immer wieder veraltete Technologien eingesetzt werden, was mit unnötig hohen Verbräuchen und Emissionen über die Lebenszeit der Geräte hinweg einhergeht. Als weiteres Problem wurde die Überkompensierung von Energieeffizienz-Zugewinnen angesprochen: durch Mehrverbräuche und höhere Komfort-Standards werden Effizienzzugewinne in vielen Fällen überkompensiert - auch im Haushalt.

Für die Realisierung von Projekten zur Umsetzung der Energiewende wie Windenergieanlagen oder Stromleitungen spielt die Akzeptanz eine herausragende Rolle.

Für den Mentalitätswechsel wurden folgende Lösungsvorschläge geäußert:

- Sensibilisierung für die Gefahren des Klimawandels und Aufklärung über wirksame und umsetzbare Klimaschutzmaßnahmen.
- Ausweitung der Energieberatung für Verbraucher (auch verpflichtende Energieberatungen wurden diskutiert).
- Weiterbildungen für Multiplikatoren, etwa für Kundenberater von Heizungsherstellern.
- Eine Energiepreisgestaltung, die dabei hilft, den Wert der Energie und die Auswirkungen auf das Klima besser einzuschätzen. Wichtig dabei sind Transparenz und sozialer Ausgleich.
- Energieprodukte, die eine positive Beziehung zwischen Verbrauchern und Energieanlagen unterstützen, wie z.B. Strom aus regionalen Anlagen, die mit Bürgerbeteiligung errichtet werden.
- Berücksichtigung der sozialen Perspektive: Mieterstromprojekte bringen diese soziale Dimension mit, da so auch Mieter in den Genuss von Vorteilen kommen, die ansonsten Besitzern von PV-Anlagen gegenüber reinen Stromverbrauchern vorbehalten sind.

Welche Rolle spielt die IT für die Energiewende?

Es wurde die Frage diskutiert, wie die IT im Zuge der Digitalisierung dazu beitragen kann, dass die Vision einer sozial-ökologisch transformierten Energieversorgung Realität wird.

Erst die Digitalisierung ermöglicht eine intelligente Koordination der vielen dezentralen Energieanlagen und damit ein zukünftig vollständig auf erneuerbaren Energien basierendes Energieversorgungssystem. Durch die Digitalisierung können die Flexibilitätspotenziale besser genutzt werden. Über die Kopplung der Sektoren Strom-Wärme-Mobilität werden Flexibilitätspotenziale vermehrt verfügbar. Zugleich können unnötige Lastspitzen vermieden werden, die durch einen unkoordinierten zeitgleichen Strombezug dezentraler Anlagen entstehen würden.

Stromüberschüsse aus Wind und Sonne können durch digitale Vernetzung und intelligente Nutzung der zur Verfügung stehenden Informationen sinnvoll verteilt und bedarfsorientiert in Form der vor Ort benötigten Energieformen bereitgestellt werden. Weiterhin ermöglicht die Digitalisierung ein intelligentes Management der Stromverteilnetze und damit einen besseren Leistungsausgleich innerhalb der Stromverteilnetze. Die Fluktuation der eingespeisten Energie aus Wind- und PV-Anlagen kann in einem Verbund aus lokalen Netzzellen ausgeglichen werden. Dies führt im Gesamtsystem zu Synergien, die dabei helfen, Netzbelastungen und Netzentgelte gering zu halten. Weiterhin wurde festgestellt, dass die IT die Energieversorgungsunternehmen darin unterstützen kann, Lösungen bereitzustellen, die zugleich dem Klimaschutz als auch dem Komfort für den Kunden dienen. Dabei wurde die IT als „unsichtbarer Erfüllungsgehilfe“ beschrieben, der dabei hilft Effizienzpotenziale zu erschließen, die heute noch nicht gehoben werden können – und zwar ohne, dass der Endkunde es merkt.

Ein auf kleinere Einheiten bezogener Energiehandel könnte dabei helfen, bislang unentdeckte Potenziale für erneuerbare Energieerzeugung zu erschließen. Als Beispiel wurde ein Gewerbegebiet genannt, für das im alltäglichen Kontext nicht deutlich wird, wieviel Energie von A nach B fließt, welche Kosten an welcher Stelle entstehen und welche weiteren PV-Anlagen eingebunden werden könnten. Dies kann durch digitale Systeme abgebildet werden. Dazu werden die verfügbaren technischen und wirtschaftlichen Informationen zusammengeführt, analysiert und genutzt.

Welche Konsequenzen ergeben sich für Energieversorger?

Für Energieversorger ist es wichtig, sich auf die Prosumer einzustellen, und zwar aus Vertriebssicht genauso wie aus Netzsicht. Die Eigenerzeugung durch die Prosumer führt zu einem geringeren Stromabsatz. Wenn zusätzlich die gesellschaftlich erwünschten Energiesparmaßnahmen greifen, reduziert sich der Absatz von Strom und Wärme weiter. Zugleich werden bei den Prosumern die (Rest-) Lastprofile für den Strombezug komplexer. Unterstützende Systeme könnten es Prosumern auch ermöglichen, die von ihnen erzeugten Energiemengen auch selbst zu handeln. Etwas abmildernd wurde die Einschätzung geäußert, dass nicht alle Stromkunden zu Prosumern werden bzw. für ihren Strombezug auf Peer-to-Peer-gehandelten Strom vertrauen dürften..

Neben den Prosumern gibt es weitere Veränderungen, auf die sich die Vertriebe der lokalen Energieversorger vorbereiten müssen. Traditionelle Geschäftsmodelle verändern sich mit neuen Mitbewerbern am Markt, die sich die Möglichkeiten der Digitalisierung zunutze machen. Welche Geschäftsmodelle für die Kunden der Energieversorger attraktiv sind und sich schlussendlich durchsetzen, bleibt aktuell eine offene Frage. Bislang ließ sich beobachten, dass die Kunden ihren lokalen Energieversorgern in der Mehrzahl treu bleiben.

Die zwei bedeutendsten Assets der EVU sind Vertrauen und Kundenzugang. Daraus lassen sich auch neue Geschäftsmodelle entwickeln. Um die Kundenbindung zu verstetigen wird es darum gehen, den Kunden Mehrwerte zu bieten, für die sie möglichst nichts extra bezahlen müssen. Die Rolle der EVU bestünde darin, diese neuen Geschäftsmodelle im Hintergrund zu managen. Auch eine Flatrate für Strom, ähnlich wie bei der Telekommunikation, könnte aus vertrieblicher Sicht Sinn machen, sofern ein solches Produkt betriebswirtschaftlich funktioniert.

Zur Umsetzung der neuen Geschäftsmodelle werden Energieversorger ihre Strukturen umbauen müssen. Es wurde festgestellt, dass die im Zusammenhang mit dem Unbundling vorgeschriebene Trennung von Netz und Vertrieb für lokale Energieversorger dabei nicht immer ideal sei.

Was bedeutet dies für den regulatorischen Rahmen?

Der Rechtsrahmen für Energiethemen wird grundsätzlich auf Bundesebene geregelt. Bei der Diskussion bestand weitgehende Übereinstimmung darin, dass der regulatorische Rahmen Wirtschaftlichkeit für diejenigen ermöglichen muss, die die Energiewende umsetzen. Ökonomische Anreize werden als Motor für eine beschleunigte Transformation gesehen. Schlechte Regularien hingegen führen zu Ausweichmodellen, nicht jedoch zielgerichtet zur Umsetzung des angestrebten Transformationspfades.

Es wurde bemängelt, dass den Akteuren bislang Anreize fehlen, die ein Handeln im Sinne der Energiewende fördern, und dass weiterhin Anreize gegeben werden, die das herkömmliche Energiesystem stützen. Eine schrittweise Anpassung des Rechtsrahmens wurde gefordert, und zwar im Zusammenspiel mit Transparenzmaßnahmen, um den Akteuren eine gute Orientierung im komplexen Prozess der Energiewende zu bieten.

Bei der Gestaltung der Anreize gilt es zu berücksichtigen, dass Investitionen in neue Infrastruktur teils mit langen Abschreibungszeiträumen von 30-50 Jahren einhergehen. Hinzu kommen divergierende Geschwindigkeiten bei der Entwicklung unterschiedlicher Technologien und Innovationen. Nahwärmenetzwerke zum Beispiel werden für die nächsten 30 bis 40 Jahre gebaut. In der Zwischenzeit wird eine enorme technologische Entwicklung stattfinden und weitere Rahmenbedingungen werden sich verändern. Die Entscheidung für eine teure Investition muss aktuell in einem Umfeld günstiger Energiepreise getroffen werden. Ist die Investition einmal auf langfristige Sicht getätigt, darf sie später nicht mehr „von außen“ gestört und damit unwirtschaftlich werden. Investitionsentscheidungen sind aktuell mit vielen Unsicherheiten verbunden.

Es stellt sich die Frage, wie man die Akteure darin unterstützen kann, von vorn herein solche Investitionsentscheidungen zu treffen, die im Sinne von Klimaschutz und Energiewende geeignet sind. Die Investoren benötigen Vertrauen in die Wirtschaftlichkeit und Anreize für langfristige Investitionen. Die Politik kann beispielsweise unterschiedliche Maßnahmen zur Reduzierung des Investitionsrisikos ergreifen. Zusätzlich erleichtert ein klarer politischer Umsetzungspfad in Kombination mit einem verlässlichen Rechtsrahmen den Investoren eine Einschätzung dessen, welche Infrastrukturprojekte tragfähig sind. Ebenso wäre besser beurteilbar, welche Infrastrukturprojekte innerhalb der Abschreibungszeit zu gestrandeten Investitionen werden könnten, weil diese den Umsetzungspfaden für Energiewende und Klimaschutz nicht entsprechen.

Kritisch gesehen wurde die Zahlung von Ablösesummen für bestehende fossile Kraftwerke aus öffentlichen Mitteln, da dies zu einem Festhalten an bestehenden Modellen führen kann.

Als zielführende und wirksame Maßnahme wurde die Anpassung von Steuern und Umlagen genannt. Dabei könnten CO_2-Emissionen für die verschiedenen Sektoren mit eingepreist werden, um die Nutzung von Energie aus fossilen Quellen zu verteuern. Gleichzeitig wäre die Nutzung von Strom günstiger zu machen, damit dieser für die Sektorenkopplung genutzt werden kann. Weiterhin wurde der Vorschlag geäußert, die Bepreisung der Netzentgelte ggf. stärker auf die physikalischen Gegebenheiten im Netz auszurichten. Im Zentrum der Preisgestaltung stünde die elektrische Leistung in Form von Netzkapazität, Netzlast und der zur Verfügung gestellten Flexibilität. Dabei könnten lokale und zeitlich variierende Anreize gesetzt werden. Zugleich wäre darauf zu achten, dass die Kunden in Netzregionen, in denen die Energiewende zügig erfolgt, nicht benachteiligt werden gegenüber Netzregionen, in denen die Umsetzung länger dauert.

Was bringen Messstellenbetriebsgesetz und Datenschutz-Grundverordnung?

Daten wird eine zentrale Bedeutung für die Zukunft beigemessen, denn über sie lassen sich neue Geschäftsmodelle konzipieren und abwickeln. In diesem Zusammenhang wurde ausführlicher über Smart Home-Systeme gesprochen, die Energievertrieben die interessante Möglichkeit bieten, Energielieferungen und -dienstleistungen mit weiteren Zusatznutzen für die Kunden zu verknüpfen. Funktionen der Haussteuerung können mit der Erfassung der Zählerstände kombiniert werden. Mit der intelligenten Vernetzung wird das Ziel verfolgt, die Wohn- und Lebensqualität, die Sicherheit und die Energieeffizienz für den Verbraucher zu verbessern. Typische Elemente von Smart Home-Systemen sind Aktoren bzw. Endgeräte, die in die Steuerung einbezogen werden, Eingabegeräte und Sensoren, ein Gateway, das die zentrale Steuereinheit darstellt, sowie die Vernetzung per Funk

oder Kabel mit dem Energieversorger. Die Datenerhebung und Versendung von Steuersignalen kann über verschiedene Systeme realisiert werden. Von Vorteil sind Systeme, die die herstellerübergreifend und variabel für unterschiedliche Geschäftsmodelle einsetzbar sind.

Mit intelligenten Stromzählern (Smart Metern) soll eine sichere und standardisierte Kommunikation in den Energienetzen der Zukunft ermöglicht werden. Die intelligenten Messsysteme speichern den Stromverbrauch und versenden die erhobenen Daten. Informationen über Verbrauch und Erzeugung sollen dabei helfen, flexibel auf Netzsituationen zu reagieren. Weiterhin können Marktsignale an Verbraucher und Erzeuger transportiert werden. Smart Home-Systeme machen dem Smart Meter Konkurrenz. Zwar können Smart Home-Systeme unter Einbindung von Smart Metern eingerichtet werden, aber es gibt aus Sicht der Energieversorger attraktive Alternativen zum Smart Meter.

Der Einsatz von Smart Metern ist im Messstellenbetriebsgesetz (MsbG) von 2016 geregelt. Dies ist Kernstück des Gesetzes zur Digitalisierung der Energiewende und das zentrale Gesetz für Regelungen rund um Einbau und Betrieb von intelligenten Messsystemen und Zählern. Um ein einheitliches und sehr hohes Sicherheitsniveau zu gewährleisten, erklärt das Messstellenbetriebsgesetz (MsbG) Schutzprofile und Technische Richtlinien für intelligente Messsysteme zur Gewährleistung von Datenschutz, Datensicherheit und Interoperabilität für verbindlich. Ab dem Jahr 2020 können Messstellenbetreiber das Smart Meter-Rollout auf Haushaltskunden erweitern, wenn ein nutzenorientierter Kostendeckel eingehalten wird. Abseits der Vorgaben zur Versorgung mit Strom und Gas enthält das MsbG keine Anforderungen für Smart Home-Anwendungen.

Es wurde sehr ausführlich über die Herausforderungen diskutiert, die sich aus dem MsbG und den Anforderungen an die Datensicherheit ergeben. Dabei wurde deutlich:

1. Das Messstellenbetriebsgesetz (MsbG) ist in der Praxis unbeliebt. Unternehmen versuchen die Anwendung zu vermeiden und stattdessen mit alternativen Methoden Daten zu erheben. Es ist nachvollziehbar, dass das Gesetz unbeliebt ist, denn es ist aus Sicht der Diskutanten unnötig kompliziert geraten. Es wurde festgestellt, dass dem Gesetzgeber auch Fehler unterlaufen seien, denn er hat es nicht geschafft, das Gesetz an die Vorgaben der Datenschutz-Grundverordnung (DSGVO) anzupassen. Die seit Mai 2018 geltende DSGVO löst die Europäische Datenschutzrichtlinie aus dem Jahr 1995 mit dem Ziel der Harmonisierung und Modernisierung des europäischen Datenschutzrechts ab. Trotzdem kann man in der Praxis mit dem MsbG arbeiten. Wichtigster Grundsatz ist, dass Daten verarbeitet werden dürfen, wenn dies zur Vertragserfüllung erforderlich ist. Das muss man bei der Vertragsgestaltung berücksichtigen. Für Dinge, die darüber hinausgehen, benötigt man die Einwilligung des Anschlussnutzers. Hier muss man vorsichtig sein, denn die rechtlichen Anforderungen an Einwilligungen sind hoch. Wenn man diese Vorgaben berücksichtigt und sorgfältig vorgeht, lässt sich aber mit dem Gesetz arbeiten.
2. Die Anforderungen an die Datensicherheit und die hiermit verbundenen Risiken werden häufig unterschätzt. Die Hersteller von Hardware wie Routern, u. ä. meinen, dass sie nicht haften, sondern dass die Betreiber von Anlagen für Schäden verantwortlich sind. Das ist so nicht richtig. Wenn Produkte nicht dem Stand der Technik entsprechen, droht auch dem Hersteller eine Haftung. Zum Stand der Technik gehören auch angemessene Schutzmaßnahmen gegen Cyberangriffe. Seit dem 25. Mai 2018, als die DSGVO in Kraft getreten ist, muss jedes Unternehmen über ein Datensicherheitskonzept verfügen. Viele Unternehmen haben diese Verpflichtung bereits umgesetzt. Es gibt aber immer noch Lücken und großen Nachholbedarf. Hier drohen hohe Bußgelder. In der Vergangenheit bestand nach Datenverlusten oder anderen Datenschutzverstößen kein großes Haftungsrisiko. Die Vorgänge waren kompliziert und für die Geschädigten meistens nicht überschaubar. Die materiellen Schäden, also Vermögensverluste auf Grund von unberechtigten Zugriffen auf personenbezogene Daten waren meistens nur gering oder nicht nachweisbar. Der Gesetzgeber der DSGVO hat sich zum Ziel gesetzt, diesen Zustand zu ändern. Um den Geschädigten höhere Schadensersatzansprüche zukommen zu lassen, hat er eine umfangreiche Dokumentationspflicht der Unternehmen und eine Beweislastumkehr eingeführt. Unternehmen müssen sich künftig entlasten und müssen nachweisen, dass sie alle Sicherheitsmaßnahmen eingehalten haben. Der Gesetzgeber hat auch Schadenersatz für immaterielle Schäden vorgesehen. Wenn Daten in falsche Hände geraten, so verpflichtet allein schon das Bekanntwerden personenbezogener Daten zur Zahlung von Schadensersatz. Es bleibt den Gerichten überlassen, welche Beträge sie hier ansetzen. Man muss aber befürchten, dass sie die Absicht des Gesetzgebers aufgreifen und Schadensersatz in deutlicher Höhe zusprechen.

Wie kann Hessen eine Vorreiterrolle bei der digitalen Energiewende einnehmen?

Abschließend waren die Diskutanten dazu aufgerufen, zu äußern, welche Punkte sie als besonders wichtig dafür ansehen, Hessen in die Lage zu versetzen, eine Vorreiterrolle bei der digitalen Energiewende einzunehmen. Es bestand Einigkeit darin, dass ein intensiver Austausch zwischen Energiewelt und IT-Welt stattfinden muss und zu fördern ist. Es wurde festgestellt, dass die Veranstaltung eindrücklich die Notwendigkeit eines zielgerichteten Austausches gezeigt hat.
Auf der einen Seite geht es darum, dass die Energiewelt bereits

vorhandene Lösungen aus der IT-Welt erkennt und für sich einsetzt. Dabei ist der rasche technologische Fortschritt in der IT-Welt zu berücksichtigen. Auf der anderen Seite sind der IT-Welt die Probleme aus der Energiewelt nicht bewusst. Über einen gezielten Wissenstransfer können miteinander Lösungen gefunden werden. Darüber hinaus wurde festgestellt, dass der Dialog der verschiedenen Sparten innerhalb der Energiewelt (z.B. Energieversorger, Anlagenhersteller, Systemanbieter, etc.) sowie innerhalb der IT-Welt zu verstärken ist. Letztlich geht es darum, zu tragfähigen Geschäftsmodellen im Sinne von Energiewende und Klimaschutz zu finden. Dazu sind Geschäftsideen wichtig, die solch einen Dialog fördern kann. In diesem Zusammenhang wurde hervorgehoben, dass die digitale Energiewende nicht an Gesetzen scheitern muss. Auch der aktuelle Rechtsrahmen bietet bereits viele Möglichkeiten, die Chancen der Digitalisierung wirtschaftlich zu nutzen.

Ergänzend wurde die neue Landesregierung in Hessen dazu aufgerufen, neue Wege zu beschreiten, mit denen sich das Land Hessen von anderen Ländern positiv abhebt. Die Zukunftsfähigkeit wird sich daran entscheiden, mit welcher Ernsthaftigkeit die Modernisierung der Infrastruktur angegangen wird. Wenngleich das Energiethema grundsätzlich auf Bundesebene geregelt wird, so bestehen auf Landesebene viele Möglichkeiten, die diskutierten Ansätze aufzugreifen und die hessische Wirtschaft und Wissenschaft bei ihren Bemühungen für die Umsetzung der Energiewende zu unterstützen. Chancen schaffen und Optionen bieten.

SESSION 2

IT-SICHERHEIT IN DER ENERGIEWELT

Houses of Dialog: Die Energiewelt wird digital | Frankfurt am Main, 28.10.2018

IT-Sicherheit in der Energiewelt: Notwendigkeiten, Herausforderungen, Perspektiven

Andreas Fuchs, Fraunhofer SIT

Bis 2020 werden voraussichtlich 50 Milliarden Geräte im Internet der Dinge vernetzt sein. Das Anwendungsspektrum reicht von Smart Grids und Smart Home über Verkehrsleittechnik und E-Mobility bis zu Industrie 4.0. Mit der Vernetzung von immer mehr „Dingen" steigen auch die Anforderungen an die IT-Sicherheit.

Die Akteure berücksichtigen IT-Sicherheit oftmals nicht, weil

- dies keine funktionale Eigenschaft eines Systems ist, sondern das System erst mal bei den gewünschten Funktionen nur verteuert
- die Produkthaftung bislang faktisch nicht funktioniert. Dies wird sich erst nach dem ersten großen Skandal ändern, wenn ein die Gesellschaft betreffender Schaden eingetreten ist und erstmalig bestimmte Leute zur Verantwortung gezogen werden.
- die Reputation eines Herstellers bislang noch nicht infrage gestellt wurde.
- noch immer viele Menschen eine Blue Screen quasi als höhere Gewalt ansehen und nicht als etwas, dem vorzubeugen wäre.

Wenn IT-Sicherheitsprinzipien nicht eingehalten werden, ist dies als fahrlässig bzw. grob fahrlässig einzustufen. Auf der anderen Seite ist zertifizierte hohe Qualität ist ein gutes Verkaufsargument.

Smart Grid & Smart Home

Die Sicherstellung der Energieversorgung, auch bei vermehrtem Einsatz erneuerbarer Energien, benötigt ein intelligentes Stromnetz (englisch Smart Grid), bei dem die Energietechnik mit Informationstechnologie kombiniert wird, um eine effiziente und zuverlässige Steuerung zu ermöglichen. Im Smart Home werden vernetzte und fernsteuerbare Geräte eingesetzt, um in Wohnungen und Häusern Wohnqualität, Sicherheit und effiziente Energienutzung zu erhöhen.

Da Cyber-Physical Systems jedoch oftmals besondere Eigenschaften mit sich bringen, z.B. Ressourcenbeschränkungen, physikalische Zugreifbarkeit oder Echtzeitfähigkeit, ist es meist schwierig, bestehende Schutzmaßnahmen und Sicherheitskonzepte einzusetzen. Es ist jedoch essentiell, von Beginn an geeignete Sicherheits- und Datenschutzmaßnahmen in Cyber-Physical Systems zu integrieren (Security and Privacy by Design). Ohne geeignete Sicherheitsmaßnahmen könnten Anwendungsbereiche wie Smart Grid und Smart Home nicht realisiert werden.

Herausforderungen für den Bereich der Energienetze

Die speziellen Herausforderungen für den Bereich der Energienetze sind im Fraunhofer Strategie- und Positionspapier Cyber-Sicherheit 2020 beschrieben (Auszug):

Das Energienetz ist eine hochkritische Infrastruktur. Wirtschaft und Gesellschaft sind abhängig von einer stabilen und bedarfsoptimierten Versorgung mit Energie. Die Entwicklung eines intelligenten Stromnetzes (»smart grid«) erfordert nicht nur, neue Möglichkeiten der Energieversorgung zu untersuchen, sondern zwingendermaßen auch neue Gefahren zu betrachten.

Die Vernetzung und Steuerung von Stromerzeugern, Stromspeichern und Stromnetzen bis hin zum Endkunden bedeutet eine deutliche Erhöhung von Kommunikationsschnittstellen. Dabei stammen Lösungen, Dienstleistungen und Zugriffe von sehr unterschiedlichen Akteuren. In einem derart heterogenen Szenario implementieren nicht alle Anbieter Standards auf Weisen, die zueinander kompatibel sind, und nicht alle Lösungen arbeiten sicher und zuverlässig. Dadurch entsteht eine Vielzahl bisher unbekannter Risiken für Netzverfügbarkeit, Systemsicherheit und Datenschutz. Für die Komponente Smart Meter hat das BSI mit dem Schutzprofil für Smart Meter einen Schritt in die richtige Richtung getan. Für alle anderen Systeme und Prozesse im Smart Grid fehlen solche Vorgaben bisher. Beispielhafte Sicherheitsrisiken im Smart Grid sind:

- Sabotage des Energienetzes (Synchronisation der Power Management Units) zur fehlerhaften Netzbetriebsführung bis hin zum Kontrollverlust
- Sabotage von Energieerzeugungsanlagen durch Vorgabe manipulierter Sollwerte bis hin zu Kommunikationsausfall und Kontrollverlust über die Anlage
- Angriffe auf Infrastrukturkomponenten wie SCADA-Systeme analog zum Stuxnet-Wurm 2010
- Missbrauch und Manipulation von Messwerten (Smart Meter) für Verhaltensanalysen oder zum wirtschaftlichen Vorteil oder Schaden des Endkunden

Ein intelligentes Stromnetz bedingt neue Geschäftsprozesse, u.a. zur erhöhten Integration erneuerbarer Energien und zur Ausbildung regionaler Energiemärkte. Dazu gehören auch Prozesse zu Bilanzierung, Regelleistung, Messwerterfassung und -übermittlung, Energieangebot und -nachfrage und zur Energieabrechnung .

Diese Geschäftsprozesse sowie die beteiligten Hard- und Softwaresysteme gilt es gegen Manipulation und ungewollten Informationsabfluss zu schützen, um weitreichende wirtschaftliche Schäden zu verhindern und eine stabile Energieversorgung zu gewährleisten.

Elektromobilität

Im Projekt DELTA entwickelt Fraunhofer SIT zusammen mit Projektpartnern ein Schutzprofil für sicheres und datenschutzgerechtes Laden und Abrechnen von Elektrofahrzeugen. Außerdem Richtlinien zur technischen Umsetzung und Testverfahren zur Validierung der IT-Sicherheit sowie einen Prototyp einer sicheren Ladesäule.

Elektrofahrzeuge sind über Ladesäulen mit vielen Infrastrukturkomponenten vernetzt. Sicherheitsfragen betreffen deshalb nicht nur das Elektrofahrzeug an sich, sondern auch die Anbindung zum intelligenten Energienetz (Smart Grid) oder zu Backendsystemen zum Abrechnen von Ladevorgängen. Herausforderungen stellen z.B. der Schutz vor Stromdiebstahl, Verhinderung von Angriffen aber auch das Unterbinden von Bewegungsprofilen durch Aufzeichnung der genutzten Ladesäulen dar. Weitere Informationen finden Sie unter www.delta-elektromobilitaet.de

Sichere Geräteidentität und -integrität im Internet der Dinge

Ein effektiver Schutz vor Missbrauch und vor Cyberattacken kann nur gewährleistet werden, wenn die Einzelgeräteechtheit der vernetzten Objekte gesichert ist – das heißt genauer: die Identität und Integrität eines Geräts als Komposition von Hardware, Software und Betriebsparametern. Nur so kann zum Beispiel mit dem Smartphone die Heizungssteuerung in der Smart Home-Umgebung sicher betrieben oder zwischen Ladesäule und Elektroauto korrekt abgerechnet werden.

Wie die Identität und Integrität vernetzter Geräte gewährleistet werden kann, hat die Taskforce „Sichere Geräteidentität und -integrität im Internet der Dinge" koordiniert durch VDE und Fraunhofer SIT in einem Positionspapier dargestellt. Das Positionspapier gibt einen Überblick über die Ziele, und Herausforderungen sowie Potenziale von sicheren Identitäten im Internet der Dinge. Dabei werden Anwendungsszenarien aufgezeigt, Anforderungen und Voraussetzungen beschrieben, Konzepte und Ansätze präsentiert und Herausforderungen dargelegt.

Das Thema „Identität und Integrität von Geräten und Systemen" zählt neben den Themen „Security by Design", „Machine-to-Machine Communication" sowie „Hardware-Vertrauensanker" wie beispielsweise dem Trusted Platform Module (TPM) zu den Fokusthemen der VDE/Fraunhofer SIT-Taskforce. Deren Ziel ist es, Anforderungen der Industrie zu sammeln, gemeinsame Lösungen zu identifizieren, sichere Schnittstellen zu entwickeln und Standards zu erarbeiten, um eine anwendungsunabhängige und -übergreifende technologische Basis für die sichere Einzelgeräteechtheit zu schaffen. Die Integration in die einzelnen Anwendungsdomänen, deren Prozesse und Lebenszyklen stellt dabei eine zentrale Herausforderung dar.

Anforderungen und Voraussetzungen für Geräteidentität und -integrität

(Auszug aus dem Positionspapier:)
Die Potenziale von Industrie 4.0 werden sich nur dann nutzen lassen, wenn die zugrunde liegende Infrastruktur in ausreichendem Maße sicherstellen kann, dass sich die Vertrauensverhältnisse zwischen einzelnen Akteuren der physischen Welt auch auf den Cyberspace abbilden lassen. Dabei muss der Identität und Integrität von Geräten besondere Aufmerksamkeit zukommen.

1. Vertrauenswürdige Funktionalität
Die Sicherheit von IKT-Geräten beginnt bei der Konzeption und Entwicklung ihrer Hardware- und Softwarekomponenten. Hierbei muss sichergestellt werden, dass das Produkt die erwartete Funktionalität aufweist und insbesondere frei von ungewollter Funktionalität ist. Diesem Ziel können jedoch einige Umstände und Interessen entgegenwirken. So erschweren die zunehmende Komplexität von Software und Hardware auf der einen und der zunehmende Preis- und Zeitdruck auf der anderen Seite das Entwickeln von sicheren und

verlässlichen Komponenten und Geräten. Probleme werden häufig erst beim Kunden bzw. Endanwender entdeckt. Hier können z.B. die Normenreihen VDI/VDE 2182, ISO/IEC 25000, ISO/IEC 62443, ISO/IEC 27000 oder ISO/IEC 15408, als Leitfaden für die Sicherstellung einer hohen Qualität dienen.

Jedoch unterscheidet sich häufig auch die Erwartung des Kunden bzw. Endanwenders an die Funktionalität eines Gerätes von der des Herstellers oder Anbieters. Es gibt unzählige Beispiele von gelieferten Systemen, die zusätzliche Funktionen aufweisen, die dem Benutzer nicht bekannt waren. Dies beginnt bei intransparenten Zugriffen auf die Cloud, bei der personenbezogene Daten übertragen werden, um einen vermeintlich besseren Service zu liefern, geht über Kassenterminals, die in krimineller Absicht Bankkartendaten ins Internet übertragen bis hin zu Audiotechnologien, die als Wanzen missbraucht werden können.

Eine wesentliche Voraussetzung für das Vertrauen in das Internet der Dinge ist daher die Überprüfbarkeit der Funktionalität von Geräten. Das kann nach verschiedenen Herangehensweisen durchgeführt werden – entweder über die Transparenz gemäß des neuen Standard-Datenschutz-modells oder anhand von Zertifizierungen von Software, Prozessen oder Funktionalitäten.

Ähnliche Herausforderungen finden sich auch im Bereich der Hardwaresicherheit. Die Gefahren von Hardwaretrojanern sind insbesondere aufgrund der erschwerten Detektierbarkeit ein aktuelles Forschungsfeld. Hard- und Software ist zudem das Problem der Lieferkettenintegrität gemein.

Offensichtlich ist jedoch auch, dass z.B. die reine Existenz einer vertrauenswürdigen Komponente nicht ausreicht. Vielmehr muss es ausgehend von Komponenten mit vertrauenswürdiger Funktionalität auch eine Möglichkeit geben, sicherzustellen, dass diese im konkreten Fall tatsächlich auch zum Einsatz kommen. Die Selbstauskunft einer Komponente, insbesondere einer Softwarekomponente, lässt sich in der Regel leicht fälschen. Dies gilt umso mehr, da in Szenarien des Internets der Dinge der Angreifer physischen Zugriff auf die Geräte haben kann, während die Überprüfung aus der Ferne geschehen muss.

2. Datenschutz

Das Internet der Dinge bringt vor allem ein Mehr an Sensoren und intelligenten Systemen, welche zuvor nicht verfügbaren Daten automatisiert verarbeiten. Es gibt viele Unternehmen, deren Geschäftsmodell in der Sammlung möglichst umfangreicher Daten besteht. Daten als Rohstoff der Zukunft werden auch zur weiteren Wertschöpfung genutzt werden; über direkte Endkundenbelange bis hin zum Mining von Erkenntnissen aus Prozessdaten. Ziel muss es sein, dass persönliche Daten unter der Souveränität des Eigentümers verbleiben. In der Smart City oder Industrie 4.0 sind dort anfallende Daten zwar größtenteils nicht personenbezogen, aber sehr wohl kritisch für den Geschäftserfolg. Mit diesen Daten muss daher genauso sorgsam umgegangen werden.

Eng verknüpft mit dem Datenschutz ist das Prinzip der Datensparsamkeit. Zur Erbringung eines (gewollten) Dienstes sollten nur jene Daten übermittelt werden, die unbedingt notwendig sind. Wo möglich sollten Daten nur anonymisiert (oder ggf. pseudonymisiert) weitergegeben werden. Die Einhaltung dieser Prinzipien sollte bereits im Entwicklungsprozess berücksichtigt werden (Privacy-by-Design). Ansätze dies umzusetzen existieren bereits, etwa mit ABC4Trust.

3. Skalierbarkeit

Das Internet der Dinge wird Milliarden von Geräten umfassen. Hieraus ergeben sich hohe Anforderungen an die Skalierbarkeit und Massentauglichkeit des Nachweises der Einzelgeräteechtheit, sprich der Geräteidentität und -integrität. Dazu zählen insbesondere eine automatisierte Verwaltung, eine anwenderfreundliche Konfiguration der Geräte sowie eine Unterstützung über den gesamten Lebenszyklus der Geräte hinweg.

Dabei muss insbesondere der Entwicklung genüge getan werden, dass Updatezyklen und Fehlerbeseitigungen in immer kürzeren Abständen erfolgen müssen. Dies muss insbesondere in großen Stückzahlen im Feld möglich sein, ohne dass hierbei unzumutbarer Mehraufwand oder ein Angriffspotenzial für den Normalbetrieb entsteht. Standards und Industrienormen erleichtern diesen Vorgang.

4. Verfügbarkeit

Wenn Geräte mit sicherheitsrelevanter Funktionalität, also z.B. physische Aktoren, involviert sind, stellt sich die Frage der Verfügbarkeit und des Umgangs mit Fehlerfällen. Hier zeigen sich deutlich die wechselseitigen Abhängigkeiten zwischen der funktionalen Sicherheit (Safety) und der Informationssicherheit (Security). Insbesondere darf z.B. eine nicht erfolgreich überprüfbare Geräteidentität nicht dazu führen, dass eine Anlage komplett ausfällt oder die funktionale Sicherheit des Gesamtsystems in irgendeiner Weise beeinträchtigt wird.

Das Papier steht *hier zum Download* bereit.

Houses of Dialog: Die Energiewelt wird digital | Frankfurt am Main, 28.10.2018

Einsatz militärischer Konzepte für die IT-Sicherheit in der Energiewelt

Thomas Blumenthal, QGroup und Dirk Filzek, House of Energy e.V.

1. Bedeutung kritischer Infrastrukturen

Zu den Kritischen Infrastrukturen (KRITIS) werden in Deutschland Organisationen und Einrichtungen aus den Bereichen Energieversorgung, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur gezählt. Die ausgeprägte Widerstandsfähigkeit (Resilienz) dieser kritischen Dienstleistungen gegen vielfältige Bedrohungen bildet eine wesentliche Grundlage für das Funktionieren der Gesellschaft. (1)

Die Energieversorgung ist ein zentraler Bereich Kritischer Infrastrukturen, der sich im Fall von Ausfällen oder Störungen extrem und unmittelbar auch auf die anderen Sektoren und somit auf Staat, Wirtschaft und Gesellschaft auswirkt. Vorhandene Schwachstellen und Verwundbarkeiten sind zu identifizieren und mit Bezug auf das resultierende Risiko zu analysieren. Dabei sind angemessene und allgemeingültige Sicherheitsanforderungen zu erstellen sowie möglichst konkrete Maßnahmen zur Reduzierung vorhandener Verwundbarkeiten vorzuschlagen. (1)

2. Lage der IT-Sicherheit in Deutschland

Im Bericht des BSI (Bundesamt für Sicherheit in der Informationstechnik) „zur Lage der IT-Sicherheit in Deutschland 2018" wird festgestellt, dass die Gefährdungslage in den Kritischen Infrastrukturen insgesamt auf hohem Niveau, aber in den verschiedenen Branchen unterschiedlich ausgeprägt ist. Im Zeitraum 1. Juli 2017 bis 31. Mai 2018 erreichten das BSI 145 Meldungen aus den KRITIS-Sektoren; die meisten aus dem Bereich IT und Telekommunikation, die zweitmeisten aus dem Energiesektor. (2)

KRITIS-Betreiber wie zum Beispiel Energieversorger (siehe Vorfall EnBW/Netcom) sehen sich, zusätzlich zu normalen Angriffen aus dem Internet, auch neuen oder fortschrittlicheren Angriffen (APTs/ Advanced persistent threads) ausgesetzt. Andere Branchen stehen ebenfalls unter permanenten Angriffen und sehen sich mit Attacken konfrontiert, die in den exponierteren Branchen bereits beobachtet wurden. Die verwendeten Angriffsmethoden wurden aber mittlerweile hochgradig automatisiert und werden von den Angreifern inzwischen flächendeckend eingesetzt. Sobald Betreiber Auffälligkeiten entdecken, die auf einen Angriff hinweisen könnten, sollten Informationen darüber möglichst umgehend an das BSI gemeldet werden. Hierdurch wird anderen Betreibern beim Schutz ihrer Anlagen geholfen, da das BSI diese Informationen über den Angriff in Form von Warnungen sanitarisiert weitergibt. (2)

KRITIS-Betreiber aus dem sogenannten ersten „Korb" der BSI-KRITIS-Verordnung (die Sektoren Wasser, Ernährung, Energie sowie Informationstechnik und Telekommunikation) mussten bis 3. Mai 2018 „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer Informationstechnischen Systeme, Komponenten oder Prozesse treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind." (§ 8a Abs. 1 BSIG) und dies gegenüber dem BSI nachweisen. (2) Soweit die Theorie.

3. Herausforderungen bei der Umsetzung von IT-Sicherheit in der Energiewelt

Das Energieversorgungssystem wird in wachsendem Maße von automatisierten Systemen und IT-Anbindungen abhängig, um eine funktionierende Energieversorgung zu gewährleisten. Dabei wird zwischen IT (Informationstechnologie) und OT (Operational Technology) unterschieden, obwohl diese mitunter auf identischen Technologien aufsetzen, die jedoch unterschiedlich angewendet werden. IT- und OT-Lösungen steuern die Stromnetze, verbessern die Nutzung erneuerbarer Energien und ermöglichen neue Geschäftsmodelle. Die Unterstützung durch IKT-Systeme bringt zwar viele Vorteile; mit der wachsenden Abhängigkeit von diesen Systemen gehen jedoch auch Risiken für die Versorgungssicherheit einher. Um die Vorteile moder-

ner IKT auch in Zukunft sicher nutzen zu können, ist es daher wichtig, einen angemessenen Schutz gegen Bedrohungen für IKT-Systeme, die für einen sicheren Netzbetrieb notwendig sind, zu etablieren.

Besondere Herausforderungen sind die zunehmende Dezentralisierung der Energieversorgung sowie der Schritt in die Echtzeit-Energiewirtschaft. Dies führt zu einer unüberschaubar großen Zahl an aktiven Elementen im Stromversorgungssystem. Zwischen diesen aktiven Elementen werden mittels einer Vielzahl elektronischer Geräte enorme Datenmengen in kurzer Zeit ausgetauscht. Für all diese Daten sind Datenintegrität und Datenschutz zu gewährleisten.

Dies erfordert, dass neben den Betreibern der kritischen Netzinfrastrukturen auch Anlagenbetreiber, Vermarkter, Aggregatoren und weitere Beteiligte am Energieversorgungssystem in die Verantwortung für die IT-Sicherheit mit einbezogen werden. Dazu zählen auch die Industriebetriebe, die ihre steuerbaren Lasten, Erzeuger oder Speicher in das Energiesystem integrieren. In dezentralen Energieanlagen finden wir heute kein ausreichendes „Security by Design". Es lässt sich beobachten, dass für Sicherheitssysteme nicht in einem angemessenen Maße Geld investiert oder bei der Entwicklung neuer Produkte berücksichtigt wird. Netzleitstellen für Energieanlagen sind grundsätzlich mit erhöhter Sicherheit ausgestattet. Jedoch auch dort sind die Anbindungen nach außen vielfach nur lückenhaft abgesichert. Dabei fällt auch auf, dass die Definition von Sicherheit in der Energiewirtschaft eine ganz andere ist, als im Bereich der Cybersicherheit. Vermeintlich hohe Sicherheitsmaßnahmen im Energiebereich entsprechen oft nur normalen bis mittleren Sicherheitsmaßnahmen anderer Fachbereiche.

Gerätehersteller sind in der Pflicht, die notwendigen Sicherheitsfunktionen für ihre Geräte zu garantieren und diese bedarfsgerecht zu aktualisieren. Auf Seiten der Geräteanwender besteht die Pflicht, die Sicherheitsfunktionen korrekt anzuwenden und ein sicheres Umfeld zu schaffen. Gleichzeitig muss es sich für die Hersteller lohnen, gute Produkte auf den Markt zu bringen.

Aktuell sind die Anwender noch nicht ausreichend für das Thema sensibilisiert, sondern kaufen Produkte ausschließlich nach fachlichen Aspekten. Vielfach wird die verfügbare Technik genutzt, ohne die Risiken und den Umgang damit zu thematisieren. Ein Großteil der Nutzer informiert sich nur im offensichtlich gewordenen Problemfall mit dem Thema IT-Sicherheit. Weiterbildungsangebote können hilfreich sein, damit die Anwender eine intrinsische Motivation entwickeln und konkretes Handlungswissen besteht.

Probleme bereitet vor allem der Umgang mit kritischen Gefahren auf Grund von

- Definitionsdefiziten für Sicherheitsanforderungen,
- Skalierungseffekten,
- neuen Entwicklungen, die auf dem Echtzeitaustausch große Datenmengen in der Fläche basieren, wie z.B. das autonome Fahren im Bereich der Mobilität,
- Einsatz von Künstlicher Intelligenz.

Was Rechenleistung und Speicherkapazität anbetrifft, beobachten wir ein exponentielles Wachstum. Wenn wir alle verfügbaren Technologien so schnell, wie dies möglich ist, parallel nutzen, erschaffen wir aus Sicht der IT-Sicherheit eine unüberschaubare Zahl an Systemfehlern, die nicht mehr systematisch kontrolliert werden können. In der exponentiell ansteigenden Angriffsfläche liegt ein beachtenswertes Bedrohungsszenario.

Die Konsequenz sollte sein, die Digitalisierung mit mehr Bedacht und in einem nicht zu hohen Tempo voranzutreiben, sich also eher „gemütlich ins Abenteuer Digitalisierung zu stürzen". Die vielfältigen Möglichkeiten, die die Digitalisierung bietet, sollten immer nur so weit ausgeschöpft werden, dass eine akzeptable Sicherheitslage gewährleistet ist.

Ein positives Beispiel für einen besonnenen Umgang mit Gefahren und Komplexität ist das Smart-Meter-Rollout. Das BSI entwickelt im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) Schutzprofile und Technische Richtlinien sowie Prüfverfahren für das Smart-Meter-Gateway als zentrale Kommunikationsplattform intelligenter Messsysteme. Im Zusammenhang mit den technischen Standards des BSI schafft das Gesetz zur Digitalisierung der Energiewende nun verbindliche Rahmenbedingungen für den sicheren und datenschutzkonformen Einsatz und zeigt bereits perspektivisch die Ausgestaltung von Mindestanforderungen zur sicheren Integration der Ladesäuleninfrastruktur von Elektromobilen in das intelligente Stromnetz auf. Für die Weiterentwicklung der Standards wird es nach der BMWi-BSI-Roadmap („Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende") die drei Schwerpunkt-Cluster „Smart- & Sub-Metering", „Smart Grid & Smart-Mobility" und „Smart Home & Building & Services" geben. (2)

4. Geregelte Umsetzung von Informationssicherheit in der Energiewirtschaft

Nach der Verabschiedung eines IT-Sicherheitsgesetzes durch die Bundesregierung hat die Bundesnetzagentur in Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einen IT-Sicherheitskatalog gemäß § 11 Absatz 1a EnWG veröffentlicht. Dieser gilt insbesondere für Kritische Infrastrukturen der Energiewirtschaft und soll die für den sicheren Netzbetrieb wichtigen und notwendigen Telekommunikations- und Datenverarbeitungssysteme vor Bedrohungen (Cyber-Attacken) schützen. (3)

Für den Nachweis der Informationssicherheit in der Energiewirtschaft ist die Norm ISO/IEC TR 27019 „Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry" erschienen.

Der Standard ISO/IEC 27019 betrifft die folgenden Themengebiete:

- Prozesssteuerung und Automatisierungssysteme
- IT-Systeme in der Prozesskontrolle (Monitoring, Visualisierung, Dokumentation)
- IT-Infrastruktur für Prozessleitsysteme (z.B. Netzwerke, Remote-Zugriffe)
- Schutz- und Sicherheitssysteme (z.B. Relais, SPS-Steuerungen)
- Verteilte Komponenten von intelligenten Stromnetzen

Telekommunikationssysteme und -komponenten, die in der Prozesssteuerungsumgebung verwendet werden, fallen nicht direkt in den Geltungsbereich von ISO / IEC TR 27019: 2013. Diese werden von ISO / IEC 27011: 2008 abgedeckt.

Um eine garantierte Versorgung zu gewährleisten und um mögliche Angriffe auf die IKT und die angeschlossenen Energieversorgungssysteme zu unterbinden, sind die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit der Daten bzw. der notwendigen IT-Systeme zu gewährleisten. Um nachhaltigen Schutz zu sichern, sind folgende Kernforderungen zu erfüllen:

- Aufbau und Betrieb eines Informationssicherheits-Managementsystems (ISMS)
- Erstellung und Pflege von Netzstrukturplänen
- Definition und Durchführung eines Prozesses und einer Methodik zu Risikoeinschätzung und -management

Dabei ist nicht nur der Aufbau der IT-Sicherheit von Wichtigkeit, sondern auch der Betrieb sowie die kontinuierliche Verbesserung des Informationssicherheits-Managementsystems stellen Kernforderungen dar.

5. Individuelle IT-Sicherheitsmaßnahmen im Unternehmen

Es gibt keine 100%ige Sicherheit. Das liegt in der Natur der Sache, denn grundsätzlich kann jedes System gehackt werden. Wenn jedoch entsprechende Ratschläge berücksichtigt und Beratungsangebote genutzt werden, können Unternehmen ihr Risiko massiv reduzieren – einfach durch Minimierung des auftretenden Schadens mittels geeigneter resilienter Technologien.

Aber selbst ohne spezielle technische Sicherheitslösungen muss man feststellen, dass in den meisten Fällen die Angreifer einfache Ziele suchen und gar nicht mit anspruchsvollen Angriffstechniken arbeiten. Daher ist die Bedeutung der Einhaltung der üblichen normalen Sicherheitsstandards (z.B. BSI Grundschutzmaßnahmen) nicht zu unterschätzen. Für die meisten ordinären Systeme sind die Grundschutzmaßnahmen ausreichend. Bei Sicherheitsüberprüfungen (wie z.B. dem Check4Hack der QGroup GmbH) werden diese Standards überprüft. Das Problem ist jedoch, dass selbst diese Mindeststandards oft nicht eingehalten werden. In Umgebungen mit hohem oder sehr hohem Schutzbedarf sind die Anforderungen noch höher und die Lücke zwischen Bedarf und Realität umso größer. Da eine Sicherheitsüberprüfung immer nur eine Momentaufnahme darstellt, ist eine kontinuierliche Überwachung des Schutzniveaus– und ob dieses den Schutzbedarf übersteigt – dringend notwendig und stellt inzwischen den Stand der Technik da.

Überall, wo Menschen agieren, sind Sicherheitsrisiken gegeben. Professionelle Hacker haben es nicht eilig und warten ab, bis sich ein Einfallstor ergibt, um dann Schritt für Schritt Zugang zu den sensiblen Bereichen zu erlangen. Dabei können sie leicht unerkannt bleiben, wenn sie sich beispielsweise mittels gehackter Passwörter als rechtmäßige User ausgeben und dabei das übliche Nutzungsverhalten der Kontobesitzer kopieren. Unsichere Passwörter, das unreflektierte Öffnen von Anhängen wie vermeintlichen Bewerbungen oder Rechnungen wie auch vollumfängliche Datenzugriffsrechte für IT-Administratoren sind von Kriminellen gerne genutzte Wege ins Unternehmensnetz.

Problematisch ist, dass die derzeit am Markt gängigen Betriebs-

systeme, die wir z. B. in PCs, Kameras, Smartphones, Tablets und Navigationssystemen als Basistechnologie verwenden, im Hinblick auf die IT-Sicherheitsarchitektur nicht dem Stand der Technik entsprechen. Aufgrund ihrer Entwicklungshistorie wurden sie ursprünglich nicht für die Einsatzzwecke entwickelt, für den sie heute genutzt werden. Sicherheitsfunktionalitäten wurden – wenn überhaupt – nachträglich implementiert.Es gibt jedoch keine stimmige, grundlegende Sicherheitsarchitektur. Dies geht mit massiven Sicherheitsrisiken einher.
Für die Resilienz gegen Cyberbedrohungen können Hürden errichtet werden, die nicht nur die Eintrittswahrscheinlichkeit eines möglichen Angriffes minimieren, sondern auch dessen Schaden. Aufgrund des Kräfteungleichgewichts von Angreifer und Verteidiger (der Verteidiger muss alle Schwachstellen schließen, der Angreifer muss nur eine einzige Lücke finden), muss nicht nur mit einem erfolgreichen Angriff gerechnet werden – dieser erfolgreiche Angriff ist unvermeidbar.

Empfehlenswerte Maßnahmen sind:

A) Konzeptionelle Maßnahmen:
Zunächst muss mit einfach zu implementierenden, wartungsarmen Lösungen eine Übergangssicherheit geschaffen werden und die kritischsten Löcher müssen beseitigt werden. Man benötigt „Augen" im Netzwerk, die einen überhaupt erst in die Lage versetzen, Angreifer zu entdecken. Eine forensische Analyse des Netzwerktraffics hat sich hier als best practice bewährt.

Hat man sich durch diese ersten pragmatischen Maßnahmen etwas Luft verschafft, geht es an die konzeptionelle, analytische Phase. In dieser muss man zunächst eruieren, welche Informationen man hat, wie schützenswert diese in Bezug auf Verfügbarkeit, Vertraulichkeit und Integrität sind und welche Nutzer Zugriff auf diese Informationen benötigen. Bei der Bewertung sind allgemeine Richtlinien wie die europäische Datenschutzgrundverordnung (DSGVO), das Geschäftsgeheimnisgesetz (GeschGehG), sowie spezielle Richtlinien wie Vertraulichkeitsvereinbarungen (NDA) zu beachten.

Steht die Klassifizierung der Informationen, muss zunächst der passende organisatorische Rahmen geschaffen werden: Welche Person erhält welche Freigaben (Clearances) und welchen Zugriff erhält dieser Nutzer (lesen, schreibend, weitergebend...)

Die theoretische Definition muss sowohl organisatorisch und technologisch umgesetzt werden:

- Die organisatorische Umsetzung erfolgt über Prozesse und Dienstanweisungen.

- Die technische Umsetzung erfolgt über Multilevel IT-Security Systeme, die systemseitig die Einhaltung der Regeln sicherstellen.

B) Technische Maßnahmen:

1. Datenverbleib im Rechenzentrum: Befinden sich die sensiblen Daten zentral im Rechenzentrum, bestehen gute technische Möglichkeiten für die IT-Sicherheit. Befinden sich Daten auf einer Vielzahl an Endgeräten wie Notebooks, Desktops, Smartphones oder Tablets, so ist die zu verteidigende Angriffsfläche unnötig vergrößert. Sobald ein Angreifer ein Gerät physikalisch in seinen Händen hält, ist es nur eine Frage von Aufwand, Zeit und Geld, um an die darauf gespeicherten Informationen zu gelangen, egal mit welchen Sicherheitsmaßnahmen das Endgerät ausgestattet ist.

2. Fachgerechte Authentifizierung der Anwender: Vielfach ist die Identität eines Users nicht ausreichend bekannt. Man definiert zwar, dass ein bestimmter User auf eine bestimmte Information zugreifen darf, kann aber hinterher nicht mehr feststellen, ob es sich bei dem Zugriff um die rechtmäßige Person handelte oder um jemanden, der dessen Usernamen und Passwort kennt. Biometrische Systeme können hier helfen.

3. Nutzung sicherer Betriebssysteme, im Fachterminus Trusted Operating Systems (OS). Trusted OS haben andere Eigenschaften als herkömmliche Betriebssysteme und sollten in besonders sensiblen Bereichen eingesetzt werden. Das wird weltweit noch wenig genutzt, weil vielfach das Know-how fehlt und derartige Projekte technisch aufwändig werden können. Wir erkennen aber klar, dass Betriebssysteme sich ändern und Sicherheitsfunktionalitäten in den Vordergrund rücken müssen. Es gibt bisher leider nur wenige Betriebssysteme, die z. B. Informationsklassifizierung nach dem Bell LaPadula-Sicherheitsmodell oder Integritätssicherung nach dem Biba-Sicherheitsmodell ermöglichen.

4. Umsetzung von Multilevel Security (MLS). Bei MLS werden Daten entsprechend ihrer Klassifizierung in unterschiedlichen Kategorien und Klassen segmentiert, so dass immer nur ein Teil der Daten von einem Hack betroffen ist. Die Umsetzung erfolgt auf Basis entsprechender Hardware, Software und operationellen Prozeduren.

5. Musterhaft macht die Firma QGroup vor, wie IT-Security 2.0 in der Praxis umgesetzt werden kann: Der QTrust Server sichert das eigene Rechenzentrum ab. Dieses System basiert auf dem sicheren Betriebssystem Pitbull der Firma General Dynamics, das Isolation auf Prozessebene, Multilevel Security und die technische Exekution von Informationsklassifizierung ermöglicht. Darauf aufbauend werden Applikationszugriffe von mobilen Endgeräten mit QTrust ID umgesetzt. Teil dessen ist eine 3-Faktor-Authentifizierung inklusive biometrischer Erkennung.

6. Quellenangaben

(1) Informationen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu kritischen Infrastrukturen im Sektor Energie, *https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/Energie/Energie_node.html* (zuletzt aufgerufen am 12.07.2019)

(2) Die Lage der IT-Sicherheit in Deutschland 2018, Bundesamt für Sicherheit in der Informationstechnik, *http://docs.dpaq.de/14069-bsi_lagebericht_2018.pdf* (zuletzt augerufen am 12.07.2019)

(3) IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz, *https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf?__blob=publicationFile&v=2* (zuletzt aufgerufen am 12.07.2019)

Houses of Dialog: Die Energiewelt wird digital | Frankfurt am Main, 28.10.2018

Erfahrungen mit IT-Sicherheit in der Praxis

Julian Zimpel und Marcus Hörhammer, Voltaris GmbH

Um „IT-Sicherheit im intelligenten Messwesen" ging es im Impulsvortrag der VOLTARIS. Der Experte für Messstellenbetrieb, Gatewayadministration und Energiedatenmanagement begann mit der Begriffsdefinition für das intelligente Messsystem, welches sich aus einer modernen Messeinrichtung und einem Smart-Meter-Gateway (SMGW), der Kommunikationseinheit, zusammensetzt und um eine Steuerbox ergänzt werden kann. Gemäß Messstellenbetriebsgesetz sollen vorrangig größere Verbraucher und Stromerzeuger mit intelligenten Messsystemen ausgestattet werden. Dazu zählen erneuerbare-Energie- oder Kraft-Wärme-Kopplungs-Anlagen ab 7 kW Leistung und Kunden mit über 6000 kWh Jahresstromverbrauch. Voraussetzung dafür sind die wirtschaftliche Vertretbarkeit durch Einhaltung von Preisobergrenzen sowie die technische Machbarkeit (Feststellung durch das Bundesamt für Sicherheit in der Informationstechnik, BSI). Dazu müssen SMGW, sowie Akteure in deren Umfeld, die Vorgaben aus den Schutzprofilen, Technischen Richtlinien und Zertifizierungsrichtlinien erfüllen. Das BSI setzte dabei auf einen „Security-by-Design"-Ansatz.

Der Vortrag vertiefte die technische Richtlinie BSI TR 03109 und kryptographische Verfahren in der Kommunikation der SMGW. Anschließend wurden anhand von Abbildung 1 Komponenten und Akteure in der SMGW-Systemumwelt, sowohl für das Interims- wie auch für das Zielmodell erläutert. Im Interimsmodell organisiert der Verteilnetzbetreiber die Aufbereitung und Verteilung von Messwerten. Das Zielmodell sieht eine sternförmige Kommunikation direkt vom SMGW zu den Marktteilnehmern vor. Eine Sonderrolle kommt dabei dem SMGW-Administrator zu. Diesem obliegt der technische Betrieb von intelligenten Messsystemen.

Es folgte ein Überblick über den aktuellen Stand der technischen Umsetzung. So war bis zum Zeitpunkt der Tagung keines von neun sich in Zertifizierung befindlichen SMGW zertifiziert. Mit einer Marktfeststellung wird derzeit frühestens Anfang 2019 gerechnet. Als ein Praxisbeispiel vertiefte VOLTARIS das Thema „Sichere Logistikkette". Hierbei müssen Sicherheitsvorgaben für die SMGW-Logistik von der Herstellung bis zum Einbauort und zum Ort der Wiederverwendung oder Verschrottung erfüllt sein. Dabei ist insbesondere sicherzustellen, dass ein unautorisierter Zugriff auf SMGW während des Transportes ausgeschlossen ist. Dazu sind Transportfahrzeuge und Lagerräume abzusichern und eine durchgängige Nachverfolgung zu etablieren.
Zur Digitalisierung der Energiewende hat das Bundesministerium für Wirtschaft und Energie (BMWi) in seiner Standardisierungsstrategie das SMGW als sichere Plattform für verschiedene Einsatzbereiche festgelegt. Grundsätzlich dienen intelligente Messsysteme der Erhebung, Verarbeitung und Übermittlung von Messdaten, die den tatsächlichen Verbrauch sowie die Nutzungszeit widerspiegeln. Die Erhebung kann sektorübergreifend für z. B. Elektrizität, Gas, Wärme oder Wasser erfolgen. Ein SMGW bietet hierbei verschiedene Tarifprofile an, mit denen Kunden individuelle Tarife und Abrechnungsmodelle angeboten werden können. Zusätzlich binden SMGW Erzeugungsanlagen und steuerbare Verbraucher kommunikativ an. So lassen sich momentane Einspeisewerte oder Leistungsreduzierungen nach dem erneuerbaren Energien Gesetz über das Messsystem umsetzen oder flexible Verbraucher (Speicher, Elektromobile, u.v.m.) in ein Demand-Side-Management integrieren. Darüber hinaus können intelligente Messsysteme netzdienlich eingesetzt werden. So können zum einen Netzzustandsdaten wie Ströme, Spannungen oder Leistungen zur Netzzustandsbewertung genutzt werden, aus der sich die Auslastung oder notwendige Eingriffe herleiten lassen. Netznutzer könnten dann für netzdienliches Verhalten belohnt werden. Zwei weitere zukünftige Bausteine wären die Integration der Messdaten in Smart Home oder Smart Building Anwendungen oder beispielsweise ein direkter Stromhandel (peer-to-peer) zwischen Erzeugungsanlage und Verbraucher.

Fazit:

- Die Sicherheitsanforderungen an Smart Meter sind in Deutschland sehr hoch.
- Das SMGW dient als standardisierte IKT-Plattform, auf dessen Basis sind attraktive Mehrwerte für den Endkunden möglich.
- Moderne Tarife für individuelle Kundenbedürfnisse sind umsetzbar.
- Smart-Grid Funktionalitäten können Netzausbau einsparen.

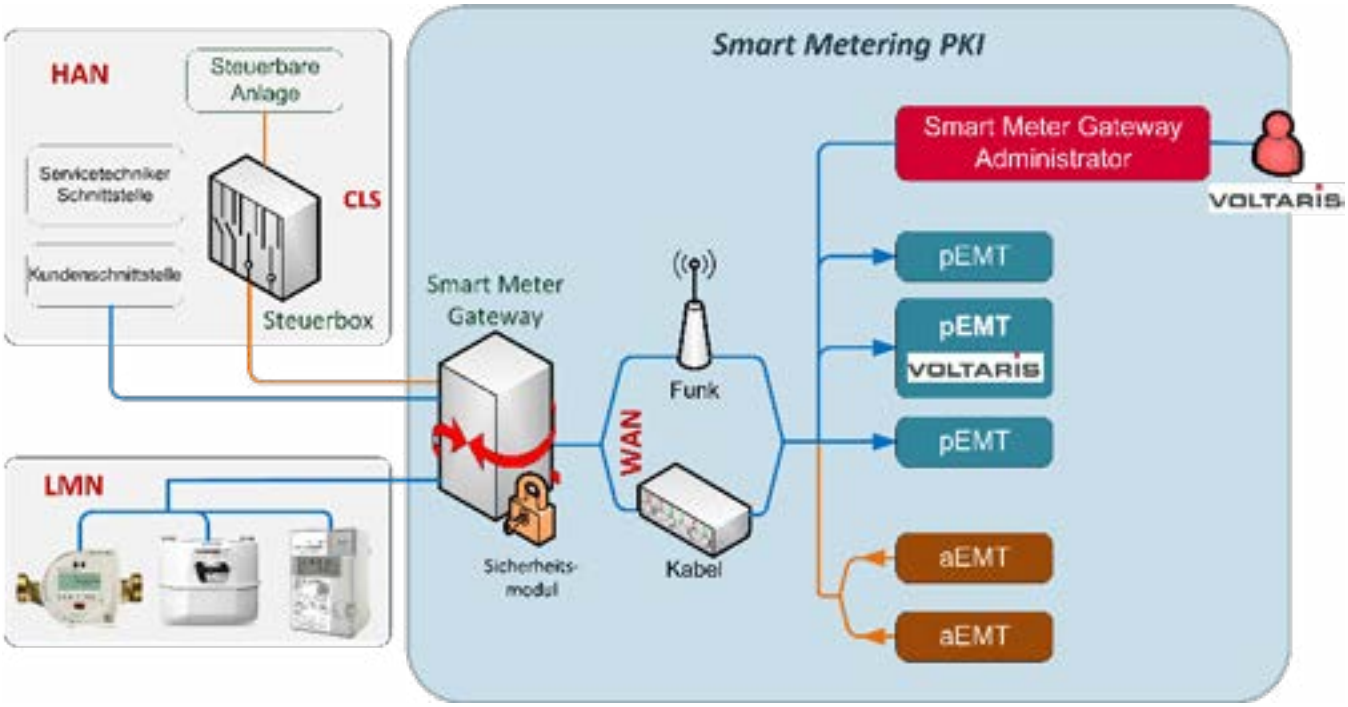

Abbildung 1: Systemumwelt von intelligenten Messsystemen und externen Marktteilnehmern im Zielmodell

Houses of Dialog: Die Energiewelt wird digital | Frankfurt am Main, 28.10.2018

Diskussion in Session 2 „IT-Sicherheit in der Energiewelt“

Wovor müssen wir uns beim Thema Cybersicherheit eigentlich fürchten – welche neuen Gefahren, die nicht zum „klassischen Handwerkszeug“ des IT-Sicherheits-Beauftragten gehören, sind derzeit relevant?

Beitrag Andreas Fuchs/FhG SIT

Grundsätzlich gilt, dass pauschal alles angreifbar ist. Primär natürlich technologische Systeme, genauso aber auch die Menschen, welche diese Systeme einrichten, warten, betreiben und nutzen. Die gesamte Betriebskette von Hersteller bis hin zum Endabnehmer ist potenzielles Einfalltor für Cyberangriffe. Dazu zählen derzeit auch Denial-of-Service-Angriffe (also das absichtliche Überlasten von Systemen, sodass diese ihre geplante Funktionalität nicht mehr erfüllen können), Fraud (Betrug mit dem Ziel, möglichst unauffällig zu sein) und ganz klassische Cyberweapons, deren technische Evolution derzeit schnell voranschreitet und stets neue Gegenmaßnahmen, aber insbesondere auch fachliches Bewusstsein, erfordert.

Wie ändert sich derzeit die Welt der IT-Sicherheit und sollen wir überhaupt alles digitalisieren und damit ein schwierig planbares Mehr IT-Sicherheit erforderlich machen?

Beitrag Thomas Blumenthal/QGroup

Cyberangriffe sind inzwischen hochgradig professionalisiert: Angreifer haben fast immer geschäftliche Interessen und sind mit aktuellem Fachwissen und umfangreichen finanziellen Mitteln ausgestattet. Auch Industriespionage funktioniert heute digital. Zudem wird weltweit der „Ton rauer“, die Angriffe gezielter, gefährlicher und zunehmend rücksichtslos.

Erschwerend kommt hinzu, dass derzeit viele Branchen Digitalisierung betreiben und IT-Sicherheit nicht von Anfang an mitdenken. Man erinnere sich nur an die Vielzahl von weltweiten Sicherheitsvorfällen im Bereich IoT und Smart Home.

Grundsätzlich muss attestiert werden, dass ein Cybersicherheitskonzept immer auch ein IT-OT-IoT-Sicherheitskonzept sein muss und nicht in Silos betrachtet oder gar angegangen werden darf.

Welche Wünsche hat die Energiewirtschaft an IT-Wirtschaft und Gesetzgeber?

Beitrag Julian Zimpel/Voltaris

Um mit einer digitalen Energiewende umgehen zu können, braucht es klare Vorgehensweisen, Richtlinien und Schutzprofile, die umfassend und einheitlich im Energienetz umgesetzt werden können. Das BSI geht hier erste Schritte in die richtige Richtung.

Aber auch hier ist ganz deutlich, dass solche Richtlinien keine reinen IT-Richtlinien sein dürfen, sondern das Thema IT-OT-IoT gesamtheitlich denken müssen.