HWZ Hochschule für Wirtschaft Zürich

CAS DIGITAL RISK MANAGEMENT

ZERTIFIKATSARBEIT

VON FLORIN JAEGER

WESENTLICHE SICHERHEITSASPEKTE BEIM EINSATZ VON SMART METERING

Florin Jaeger
Untere Gasse 54
CH - 7012 Felsberg
Schweiz
florin.jaeger@yahoo.com

Ralph Hutter
Studienleiter CAS Digital Risk Management

Zürich, Juni 2016

Was passieren könnte, wenn ein Angreifer die Fernsteuerung
über ein ganzes Stromnetz in die Hand bekommt,
möchte man sich lieber nicht ausmalen.

SANDRO GAYCKEN
Cyberwar – Das Wettrüsten hat längst begonnen

VORWORT

Im Frühjahr 2015 las ich den Bestseller „Blackout“ (Elsberg 2013) und war von den darin beschriebenen Folgen eines von langer Hand vorbereiteten Cyber Angriffes auf unsere moderne Gesellschaft beeindruckt. Der Roman zeigte mir mit erschreckender Realitätsnähe, wie unvorbereitet und machtlos wir einem grossflächigen Stromausfall ausgeliefert sind.

Als technikbegeisterter Mensch wusste ich um die gegenseitige Abhängigkeit und Verwundbarkeit unserer Kommunikations-, Energie- und Verkehrsinfrastruktur; die Darstellung der möglichen Konsequenzen im Falle eines von langer Hand vorbereiteten Angriffes auf kritische Infrastrukturen haben mich dann doch wachgerüttelt.

Etwas später bin ich dann auf das Buch „Cyberwar – Das Wettrüsten hat längst begonnen“ (Gaycken 2012) gestossen. Der Sicherheitsexperte stellt die Vor- und Nachteile des Einsatzes von Informationstechnik (IT) in einen grösseren Zusammenhang. Je grösser ein System ist, desto einfacher ist es für einen Angreifer eine Schwachstelle zu identifizieren und auszunutzen.

Im Rahmen dieser Zertifikatsarbeit habe mich mit dem zunehmenden Einsatz von IT in der Stromversorgung beschäftigt und bin der Frage nachgegangen, welche Sicherheitsaspekte beim Einsatz von Smart Metering zu beachten sind.

INHALTSVERZEICHNIS

1 SUMMARY

Der Einzug von Informationstechnologie in der Energiewirtschaft ist vollem Gange. Der Einsatz von intelligenten Stromzählern („Smart Meter“) wird als Voraussetzung für eine zukunftsfähige Energieversorgung gesehen. Unter Smart Meter Systemen werden elektronische Zähler mit mehreren Schnittstellen verstanden, die über eine bidirektionale Kommunikationsinfrastruktur mit einem zentralen Datenverarbeitungssystem verbunden sind.

Der Begriff „Smart Grid“ steht für intelligente Stromnetze, die mittels Informations- und Kommunikationstechnologie (IKT) die komplexe Herausforderung vom Ausgleich vom Stromangebot und von Stromnachfrage meistern. Smart Meter (Systeme) sind in die IKT der Energieversorgungsunternehmen eingebunden, sind damit Bestandteil der Stromverteilungsnetze und müssen informationstechnisch abgesichert sein.

Diese digitale Vernetzung birgt Chancen aber auch Risiken. Smart Meter (Systeme) stehen unter dem Verdacht, anfällig für Angriffe auf sich selbst und das gesamte Stromnetz zu sein. Bei der Betrachtung der zukünftigen Durchdringung und Vernetzung mit Informations- und Kommunikationstechnologie wird klar, dass ein hohes Sicherheitsniveau nur durch eine Kombination von technischen und organisatorischen Massnahmen erreicht werden kann.

In Deutschland werden Netzbetreiber verpflichtet, einen angemessenen Schutz gegen Bedrohunen für die IKT im Bereich Netzsteuerung zu etablieren und ein Informationssicherheitsmanagementsystem (ISMS) einzuführen. Mit der Einführung von Smart Metering kommen nun aber weitere Akteure hinzu: die privaten Verbraucher werden auch zu Teilnehmern im Smart Grid und bieten damit zusätzliche Angriffsfläche für unerwünschte oder kriminelle Manipulationen im Stromnetz. Die Umsetzung von organisatorischen Sicherheitsmassnahmen beim Endkunden gestaltet sich ungleich schwieriger.

Vor diesem Hintergrund stellt sich die Frage: Ist es wirklich notwendig, diese neue Kommunikations- und IT-Infrastruktur bis zu jedem Endkunden auszurollen und damit die Angriffsfläche des Gesamtsystems Stromversorgung zu vergrössern? Kann die Weiterentwicklung der Stromnetze in Richtung intelligente Netze auch ohne einen umfangreichen Rollout intelligenter Stromzähler erfolgen? Offenbar führt auch ein gezielter Einsatz von Mess-, Kommunikations- und Steuerungspunkten im Verteilnetz zum gewünschten Effekt (Stichwort: „Messung in der Verteilstation“). Damit könnte man die Angriffsfläche, den Umfang der Vernetzung und die Komplexität und die damit verbundenen Risiken deutlich reduzieren.

Technische Schutzmassnahmen bei Smart Meter Systemen werden nicht ausreichen, die Sicherheit dieser vernetzten Systeme zu gewährleisten. Eine kritische Auseinandersetzung mit der Frage der Notwendigkeit und dem erwarteten Nutzen von intelligenten Stromzählern ist durchaus angebracht.

2 EINLEITUNG

2.1 PROBLEMSTELLUNG

Der zunehmende Einsatz von Informationstechnologie (IT) in der Stromversorgung – angefangen bei der Stromerzeugung, bei den Verteilnetzen und hin zu den Stromverbrauchern – rücken vermehrt Sicherheitsbedenken in den Vordergrund. Der verstärkte Einsatz von IT wird dabei oft als Konsequenz der Energiewende bzw. der zunehmenden Bedeutung von erneuerbaren Energiequellen (EE) dargestellt: die Stromnachfrage soll mittels IT Einsatz mit dem schwankenden Stromangebot aus EE in Einklang gebracht werden. Der Einsatz von intelligenten Stromzählern („Smart Meter“) wird als Voraussetzung für eine zukunftsfähige Energieversorgung (Stichwort: „Smart Grid“) gesehen. Der Ausbau von erneuerbarer Energieerzeugung, die dezentrale Erzeugung und die Steuerung von Verbrauchern sind die massgeblichen Treiber für den Einsatz von Smart Metering (Grandel 2012). Zusätzlich sollen Smart Meter zu mehr Transparenz führen und (zusätzliche) Anreize und Impulse zum Stromsparen geben, weil die Stromkunden sehen, wieviel sie im Moment verbrauchen.

2.2 ZIELSETZUNG UND AUFBAU

Diese Arbeit beleuchtet die aktuellen Veränderungen im Bereich der Elektrizitätsversorgung, namentlich die Einführung von Smart Metering und die damit verbundenen Risiken. Im Kapitel 3 „Grundlagen“ werden die Begriffe „Smart Meter“ und „Smart Grid“ erläutert und in den Kontext des zunehmenden Einsatzes von Informationstechnologie gestellt. Im Kapitel 4 „Risiken“ erfolgt ein Blick auf die Themen Komplexität und Vernetzung im modernen Stromnetz und die damit verbundenen Risiken. Im Kapitel 5 „Schlussfolgerungen“ werden die Erkenntnisse zusammengefasst. Das Kapitel 6 „Fazit und Ausblick“ rundet die Arbeit ab.

2.3 ABGRENZUNG

Der Bericht fokusiert auf intelligente Zähler und intelligente Messsysteme im Stromnetz. Die Einbindung bzw. Anbindung vergleichbarer Zähler aus dem Bereich der Wärme- und Wasserversorgung sind nicht Gegenstand der Arbeit.

Es wird nicht auf die technischen Details der intelligenten Messsysteme eingegangen. Zudem erfolgt kein Vergleich der unterschiedlichen Kommunikationstechnologien bei der Anbindung von Smart Meter Systemen (siehe dazu Raquet & Liotta 2013).

Das Thema Sicherheit ist sehr umfangreich; auf der einen Seiten steht die Betriebssicherheit („safety“), auf der anderen Seite die Datensicherheit („security“). Datensicherheit hat das Ziel, Daten jeglicher Art in ausreichendem Maße gegen Verlust, Manipulationen und andere Bedrohungen zu sichern. Diese Arbeit fokussiert auf die Datensicherheit und die Konsequenzen von möglichen

Sicherheitslücken; Fragen der Betriebssicherheit und des Datenschutzes (Schutz von personenbezogenen Daten) im Zusammenhang mit Smart Metering werden hier ausgeklammert.

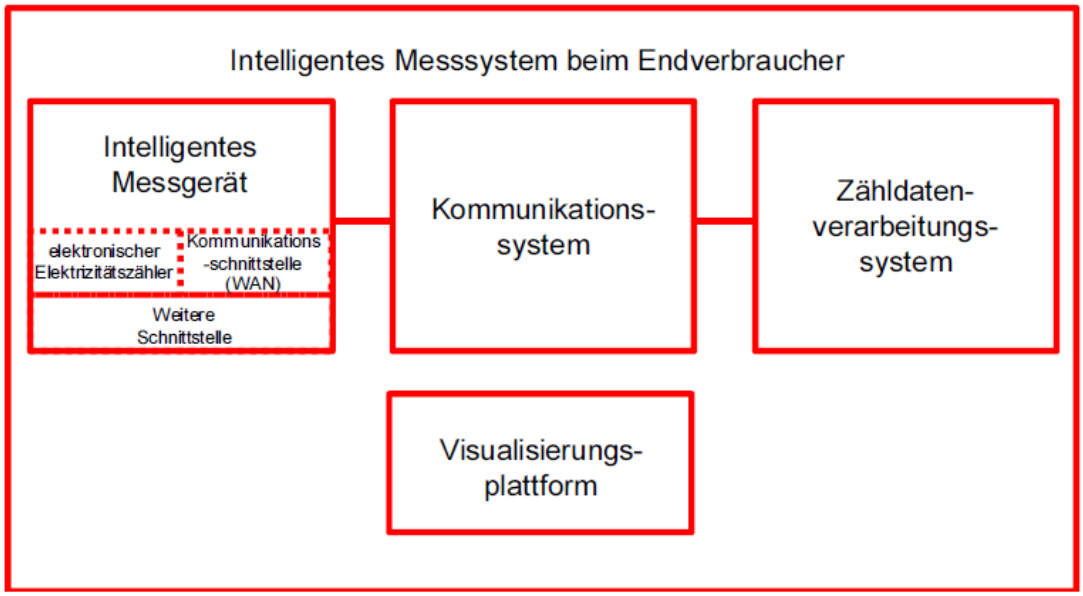
Abschliessend halte ich an dieser Stelle fest, dass ich keine abschliessende Erfassung von allen Risiken vornehme, die mit der Einführung von Smart Metering Systemen zusammenhängen. Das würde den für diese Arbeit gesteckten Rahmen überschreiten.

3 GRUNDLAGEN

3.1 SMART METER

Unter „Smart Meter“ wird ein intelligenter Zähler zur Erfassung des Stromverbrauchs verstanden. Dieser intelligenten Zähler verfügt strenggenommen noch keine Kommunikationsverbindung. Der Smart Meter ist jedoch Teil eines intelligenten Messsystems und dieses Messsystem ermöglicht eine 2-Weg Kommunikation zwischen Verbraucher und Versorger. Ein intelligentes Messgerät verfügt also über eine Schnittstelle, die es ihm ermöglicht, eine bidirektionale Kommunikation aufzubauen. Die Kommunikationsschnittstelle kann physisch im Gehäuse des Smart Meters integriert sein oder auch nicht. Die Abbildung 1 zeigt den modularen Aufbau von einem intelligenten Messsystemen (Smart Metering System).

Abbildung 1: Intelligentes Messsystem beim Endverbraucher und seine Hauptkomponenten



Quelle: BFE (2014, S. 6)

Smart Meter verfügen also über Schnittstellen und sind in ein Kommunikationssystem eingebunden.

> „Die Smart Metering Systeme bestehen aus mehreren Komponenten. Hierzu zählen das intelligente Messgerät, d.h. der eigentliche Smart Meter, eine bidirektionale Kommunikationsinfrastruktur, ein zentrales Datenverarbeitungssystem sowie eine Visualisierungsplattform. Die intelligenten Messgeräte umfassen elektronische Elektrizitätszähler, eine Kommunikationsschnittstelle (WAN) zur bidirektionalen Kommunikationsinfrastruktur sowie weitere Schnittstellen“ (BFE 2015c, S. 7).

Im vorliegenden Bericht gehen wir davon aus, dass der Einsatz von Smart Metern mit der die Einführung von Smart Metern Systemen einhergeht. Erst bei einer Fernauslesbarkeit des intelligenten Zählers, d.h. einer Anbindung an ein Kommunikationsnetz zur automatischen Übertragung der Messda-

ten an das Energieversorgungsunternehmen (EVU), spricht man vom „Smart Metering“ (Haberler et. al., 2013). Oder anders formuliert: der Smart Meter steht für die Einführung von intelligenten Messsystemen mit Schnittstellen zu Vorgängen im Verbrauchserfassungs-, Abrechnungs- und Verwaltungssystem sowie für neue Möglichkeiten im Betrieb und in der Steuerung der Stromnetze.

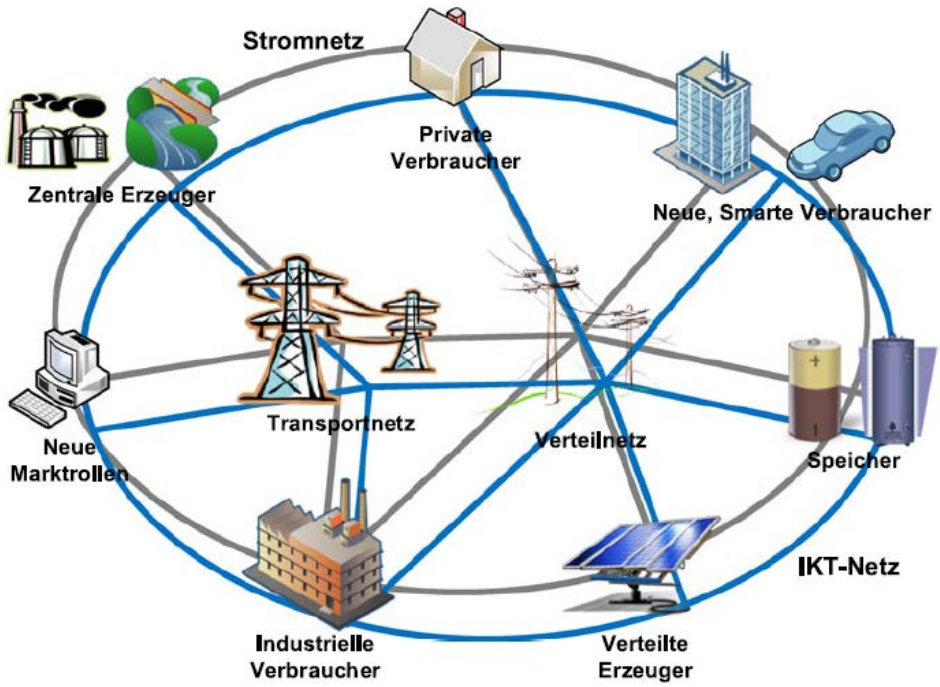
3.2 SMART GRID

Der Begriff „Smart Grid“ steht für intelligente Stromnetze, die mittels Informations- und Kommunikationstechnologie (IKT) die komplexe Herausforderung vom Ausgleich vom Stromangebot und von Stromnachfrage meistern.

> „Ein Smart Grid ist ein System, das den Austausch elektrischer Energie aus verschiedenartigen Quellen mit Konsumenten verschiedener Verbrauchsprofilen intelligent sicherstellt, d.h. unter Einbezug von Messtechnologien sowie Informations- und Kommunikationstechnologien (IKT)“ (BFE 2015a, S. 1).

Gemäss Bleier (2013) entsteht parallel zum elektrischen Netz ein IKT-Netz und die resultierende Kombination wird Smart Grid genannt. In Abbildung 2 werden die verschiedenen Komponenten eines Smart Grid dargestellt.

Abbildung 2: Strom- und IKT-Netz im Smart Grid



Quelle: Bleier (2013, S. 110)

Ein Smart Grid charakterisiert sich durch:

- breiten Einsatz von IKT
- zunehmende Vernetzung
- bidirektionale Kommunikation

und den Einsatz bzw. das Zusammenspiel von verschiedenen Technologien.

3.3 SICHERHEIT

Der vermehrte Einsatz von Informations- und Kommunikationstechnologien (IKT) in den Energieversorgungsunternehmen stellt höchste Anforderungen an die Sicherheit. Smart Meter (Systeme) sind in die IKT der Energieversorgungsunternehmen eingebunden, sind damit Bestandteil der Stromverteilungsnetze und müssen informationstechnisch abgesichert sein.

> „Eine Sicherung der für Smart Metering Systeme verwendeten Infrastruktur ist sinnvoll, da sie entweder ein Eingangstor zu nachgelagerten Systemen oder durch direkte Manipulation eine Gefahr für den stabilen Netzbetrieb bilden können“ (BFE 2015c, S. 52)

> „Die Anforderungen hinsichtlich Sicherheit und Zuverlässigkeit an die informations- und kommunikationstechnischen Komponenten und Systeme im Smart Grid sind aus den hohen Ansprüchen an die Versorgungssicherheit abzuleiten, die üblicherweise an das Stromnetz gestellt werden. Daher sind diese sehr spezifisch und mit den allgemeinen üblichen Betrachtungen aus der IT- und Internetsicherheit nicht gleichzusetzen“ (TAB 2014, S. 144)

> „Das Stromnetz stellt eine kritische Infrastruktur dar, von deren Funktionieren das Wohlergehen von Gesellschaft und Wirtschaft empfindlich abhängt. (…) Um das zuverlässige Funktionieren dieser vitalen kritischen Infrastruktur zu sichern, ist es zwingende erforderlich, höchste Anforderungen an die IT-Sicherheit (…) zu stellen“ (BMWi 2014, S. 18-19).

An die Hardware und an die Software der Smart Meter (Systeme) sowie an die Einbindung in Kommunikationsnetze werden also höchste Ansprüche in Bezug auf Sicherheit gestellt. Es stellt sich aber die Frage, ob technische Massnahmen alleine die Sicherheit in Smart Metering Systemen gewährleisten können.

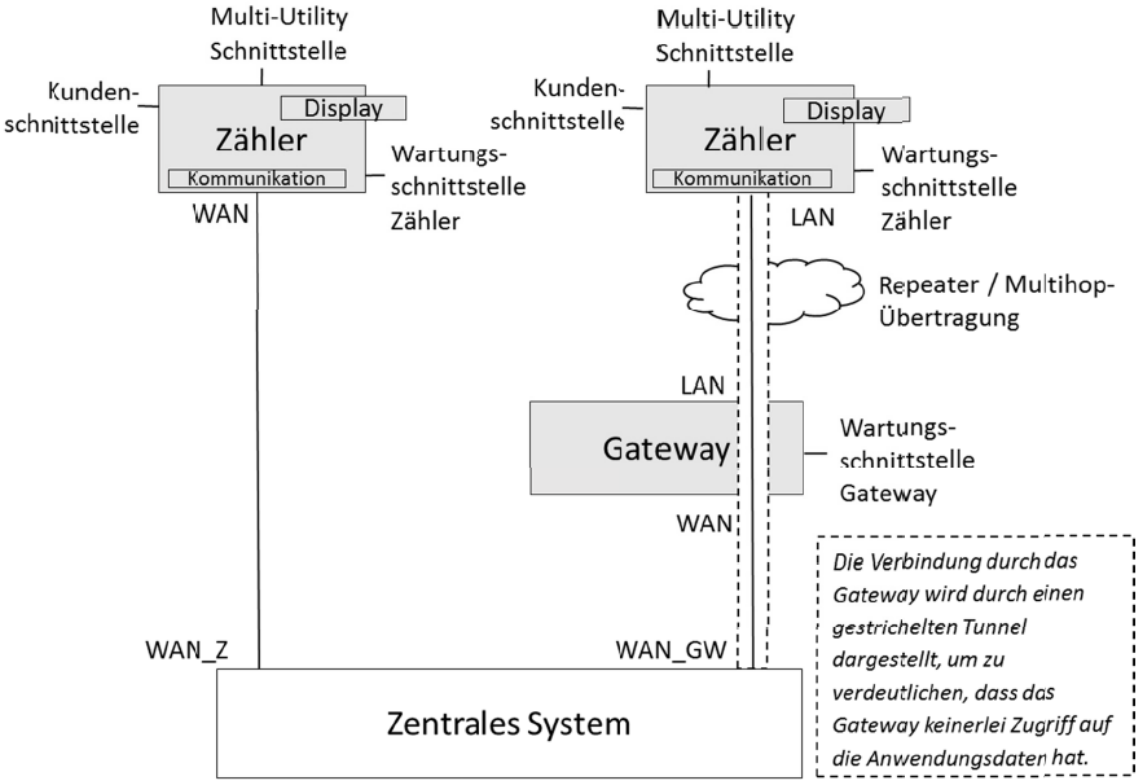
Im Kapitel 3 „Grundlagen“ wurden die Begriffe Smart Meter und Smart Grid eingeführt. Zusätzlich wurde der Zusammenhang zwischen der Weiterentwicklung der Stromnetze in Richtung intelligente Netze und der Einführung von intelligenten Messsystemen dargestellt. Im nächsten Kapitel 4 „Risiken“ werden die Konsequenzen des vermehrten Einsatzes von Informations- und Kommunikationstechnologie im modernen Stromnetz und die damit verbundenen Risiken näher betrachtet.

4 RISIKEN

4.1 TECHNISCHE RISIKEN

Der Einsatz von Smart Metering ist mit Risiken verbunden. Smart Meter (Systeme) stehen unter dem Verdacht, anfällig für Angriffe auf sich selbst und das gesamte Stromnetz zu sein (Politik-Digital, 2015). Internationale Studien haben das Gefahrenpotential und die Gefährdung für das Stromversorgungssystems analysiert. In Deutschland und Österreich wurden umfangreiche Risiko- und Schutzbedarfsanalysen durchgeführt, um anschließend die (technischen) Sicherheitsanforderungen für Smart Meter Systeme im Detail festzulegen. Stellvertretend dafür wird an dieser Stelle der vom European Network for Cyber Security (ENCS) für Österreich erstellte Anforderungskatalog erwähnt (ENCS 2014). Mit diesem Katalog werden die Maßnahme aus der Risikoanalyse umgesetzt und Mindestanforderungen an die IKT-Sicherheit der Smart Meter Komponenten festgelegt. Abbildung 3 zeigt die im Anforderungskatalog definierte Smart Meter Architektur.

Abbildung 3: Ende-zu-Ende gesicherte Smart Meter Architektur



Quelle: ENCS (2014, S. 9)

Es werden (sehr) hohe Anforderungen an die Hard- und Software der Smart Meter Systeme gestellt, um die technischen Risiken zu minimieren. Die Einhaltung von technischen Mindestanforderungen soll den unerlaubten Zugriff auf die IKT Infrastruktur verhindern. Es dürfen ausschließlich Geräte

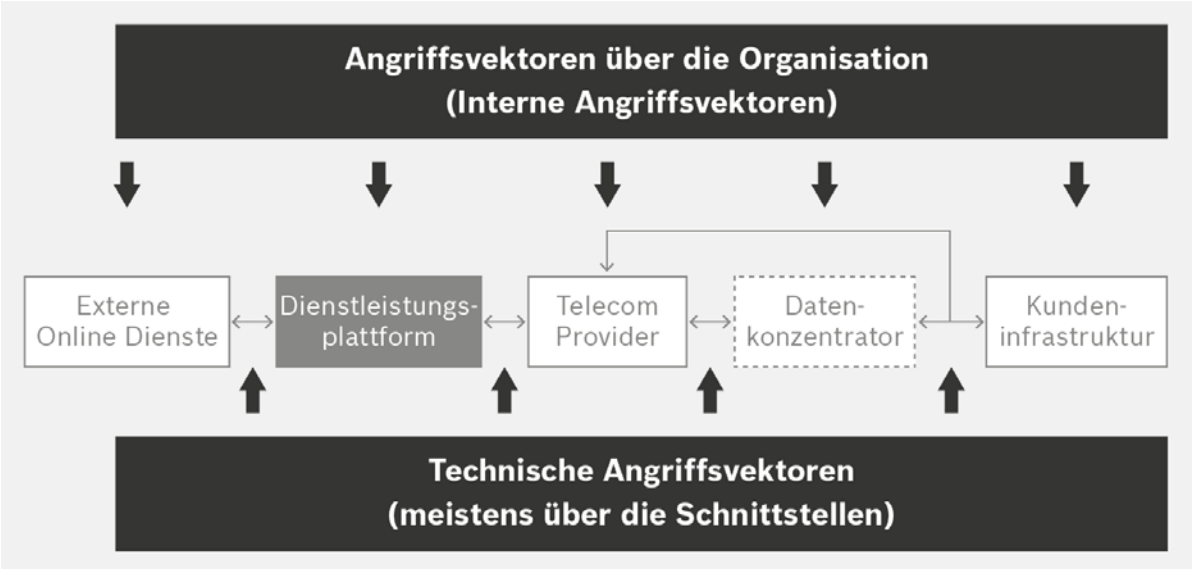
zum Einsatz kommen, die den notwendigen Anforderungen an Datenschutz und Datensicherheit genügen.

Eine 100% Sicherheit ist aber illusorisch; ein erfolgreicher Angriff ist meist nur eine Frage des Aufwandes. Bei vielen Technologien hat sich gezeigt, dass unter Umständen sehr viel Aufwand in das „Knacken" bzw. Umgehen von Sicherheitssystemen gesteckt wird und diese Sicherheitssysteme diesen „Angriffen" nur selten wirklich standhalten können; man muss davon ausgehen, dass einzelne Sicherheitsmechanismen über kurz oder lang überwunden werden (Bleier 2013, S. 112). Ein Rückblick auf die vergangenen 30 Jahre zeigt: es gibt keine massentaugliche Hardware, deren Schutzeinrichtung nicht umgangen werden konnte. Unerwünschte oder kriminelle Manipulationen der Smart Meter Systeme bzw. der IT-basierten Betriebs der Stromnetze können nicht vollständig ausgeschlossen werden.

4.2 ORGANISATORISCHE RISIKEN

Bei der Betrachtung der Risiken beim Einsatz von Smart Metering müssen auch organisatorische Risiken betrachtet werden. Die Angriffsflächen liegen sowohl entlang der Kommunikationsstrecke als auch bei den mit Smart Metering eingesetzten Informatik Plattformen. Abbildung 4 zeigt die organisatorischen Angriffsvektoren:

Abbildung 4: Technische und Organisatorische Angriffsvektoren



Quelle: Maluenda, W., Wagner, S. & Schulze, X. (2015, S. 92).

Energieunternehmen sind in der Regel grosse Organisationen mit vielen Mitarbeitern und komplexen Geschäftsprozessen. Der „Faktor Mensch" stellt immer ein Risiko dar; fehlende Kontrollmechanismen oder unklare Verantwortlichkeiten in den Geschäftsprozessen können zu Sicherheitslücken führen. In den vergangenen Jahren war bei den Energieversorgungsunternehmen und Netzbetrei-

bern das Bewusstsein für organisatorische Risiken beim Einsatz von Informationstechnologie noch nicht allzu hoch. Das hat sicherlich auch mit den unterschiedlichen Unternehmenskulturen von Stromversorgern und IT-Unternehmen zu tun (TAB 2014, S. 13). Daher werden die Netzbetreiber in Deutschland nun verpflichtet, einen Verantwortlichen für IT-Security zu benennen und bis spätestens 2018 ein Informationssicherheitsmanagementsystem (ISMS) einzuführen (BFE 2015c, S. 13). Denn nur die systematische Erhebung und Behandlung von Unternehmensrisiken wird einen angemessenen Schutz vor organisatorischen Risiken bieten.

Mit der Einführung von Smart Metering kommen nun aber weitere Akteure hinzu: die privaten Verbraucher werden auch zu Teilnehmern im Smart Grid und bieten damit zusätzliche Angriffsfläche für unerwünschte oder kriminelle Manipulationen im Stromnetz. Die Umsetzung von organisatorischen Sicherheitsmaßnahmen beim Endkunden gestaltet sich ungleich schwieriger.

> „Smart Meter befinden sich beim Endkunden in einer weitgehend ungesicherten Umgebung. Durch die Fernablesung fällt auch die periodische Kontrolle durch ein Ableseorgan weg. Daher bleibt die Entdeckungswahrscheinlichkeit einer Hardwaremanipulation mehr oder weniger dem Zufall überlassen. (…) Smart Meter stellen einen wichtigen Eintrittspunkt für Angreifer in die gesamte Smart Metering aber auch Smart Grid Infrastruktur dar und sind daher einer entsprechend hohen Gefährdung ausgesetzt.“ (Saurugg 2011, S. 24-25).

Vor diesem Hintergrund stellt sich die Frage: Ist es wirklich notwendig, diese neue Kommunikations- und IT-Infrastruktur bis zu jedem Endkunden auszurollen? Könnte die Weiterentwicklung der Stromnetze in Richtung intelligente Netze auch ohne einen umfangreichen Rollout von Smart Metering erfolgen?

4.3 RISIKO KOMPLEXITÄT

Das Stromnetz ist ein komplexes System. Die Zunahme des Energiebedarfes, die Dezentralisierung und Individualisierung der Erzeugung, führen zu einer steigenden Komplexität des Gesamtsystems (Saurugg 2013, S. 8). Die Vernetzung der Energie- und IKT-Netze erhöht die Komplexität des Systems nun weiter. Oft fehlt aber das Bewusstsein, dass sich komplexe Systeme anders als mechanische Systeme verhalten und sich nicht im klassischen Sinne managen lassen. An und für sich vernachlässigbare Störungen können sich über das System, oder im schlimmsten Fall über Systemgrenzen hinaus, ausbreiten. Die Erhöhung der Komplexität trägt auf keinen Fall zur Erhöhung der Sicherheit bei (Saurugg & Pichelmayr 2013, S. 105-106).

Sicherheitsforscher gehen dabei sogar noch einen Schritt weiter und bezeichnen die heute verfügbare und im Einsatz befindliche Informationstechnologie (IT) per se als unsicher. Gaycken (2012, S.47) ist der Auffassung, dass „(…) die enorme Komplexität von IT und die daraus resultierende Unbeherrschbarkeit ein Sicherheitsproblem auf drei verschiedenen Ebenen darstellt: die unsichere Technik, ihre unsichere Produktion und ihr unsicherer Gebrauch.“

4.4 RISIKO VERNETZUNG

Im Rahmen der Umsetzung der EU Richtlinien 2009/72/EG und 2009/73/EG werden in Europa Smart Meter beim Endverbraucher installiert. Bisher endete die Kommunikationsinfrastruktur der Netzbetreiber typischerweise in Umspannwerken und Verteilstationen, mit dem Smart Meter wird aber eine neue Kommunikationsinfrastruktur bis in jeden einzelnen Haushalt ausgerollt (Bleier 2013, S. 112). Dadurch ergeben sich deutlich mehr Angriffspunkte und es besteht das Risiko, dass Smart Meter ein Einfallstor zu nachgelagerten Systemen bilden.

> „Durch die weiter fortschreitende informationstechnische Vernetzung steigt die Zahl der möglichen Einstiegspunkte und ausnutzbaren Schwachstellen. (…) Dabei können unsicher konfigurierte Remotezugänge für die Fernwartung von Netzen ausgenutzt, (…) die Protokolle drahtloser Kommunikation über Funk manipuliert werden und weiteres mehr“ (TAB 2014, S. 144).

> Der stark ansteigende Umfang der Nutzung von IT auf allen Ebenen – von der Steuerung von Stromerzeugungsanlagen und des Netzbetriebs (v. a. auf der Verteilnetzebene), bei gewerblichen und Haushaltskunden (Smart Home, Smart Meter) bis zur zunehmenden Vernetzung von Komponenten und (Sub-)Systemen lässt die Zahl der möglichen Eintrittspunkte für Cyberangriffe in die Höhe schnellen (TAB 2014, S. 150).

Moderne Stromnetze kommen nicht mehr ohne IKT aus. Umgekehrt ist aber die gesamte IKT vollumfänglich von einem funktionierendem Energienetz abhängig. Ein grosser Ausfall der IKT Infrastruktur hätte daher wahrscheinlich ebenso weitreichende und folgenschwere Konsequenzen wie ein Stromausfall. Da die permanente Verfügbarkeit der Stromversorgung nun aber massgeblich von eben dieser Informations- und Kommunikationstechnologien abhängt, wird die wechselseitige Abhängigkeit von Energie und IKT-Netz um Faktoren weiter anwachsen.

Natürlich waren auch bisher Angriffe auf die Energieversorgungsinfrastruktur möglich. Nun möchte man die IKT-Infrastruktur mit dem Stromnetz verbinden; diese Vernetzung führt zu einer neuen Dimension und vor allem Dynamik. Die massive Erhöhung der Vernetzung führt zu einer unkalkulierbaren Erhöhung der Verwundbarkeit“ (Saurugg & Pichelmayr 2013, S. 105-106).

Ein Grund für diese Erhöhung der Verwundbarkeit liegt in der gegenseitigen Abhängigkeit. Bei einem Stromausfall funktioniert auch die gesamte Kommunikations- und Steuerungstechnik nicht. Das geordnete „Hochfahren“ der verschiedenen Komponenten nach einem Stromausfall stellt eine grosse Herausforderunge dar. „Was im Normalfall kein Problem darstellt, wird nach einem Blackout zu einem Henne-Ei-Problem. Dies lässt sich nur durch sorgfältige Planung und Vorbereitung solcher Fälle lösen (…)“ (Bleier 2013, S. 113).

5 SCHLUSSFOLGERUNGEN

Beim Einsatz von Smart Meter bzw. Smart Meter Systeme rücken vermehrt Sicherheitsaspekte in den Vordergrund. Smart Meter sind ein Teil der Stromnetze und damit Bestandteil der kritischen Infrastruktur und können ein Eingangstor zu nachgelagerten Systemen darstellen. Unerwünschte oder kriminelle Manipulationen der Smart Meter können trotz umfangreichen Sicherheits- und Technikeinsatz nicht vollständig ausgeschlossen werden. Eine umfassende Einführung von Smart Meter steigert die Komplexität und vergrössert damit die Angriffsfläche des Gesamtsystems Stromversorgung.

Intelligente Messsysteme sind Bausteine der intelligenten Netze. Der Einsatz von Smart Meter bzw. von Smart Meter Systemen sind aber offenbar keine grundlegende Voraussetzung für die Schaffung eines Smart Grid:

> „Die wesentlichen aus der Sicht eines Netzbetreibers gewünschten Effekte könnten nämlich durchaus auch mit einer Messung in der Verteilerstation sozusagen am ersten Transformator erreicht werden“ (Vest 2012, S. 209).

In diesem Zusammenhang wurde in der Schweiz ein Pilot durchgeführt. Verschiedene Partner prüften im Auftrag des Bundesamt für Energie BFE das Potential eines Echtzeit-Management-Systems für das Verteilnetz. Im Rahmen des Projekts „GridBox Pilotnetz“ wurde einerseits die technologische Plattform aufgebaut. Andererseits wurden Algorithmen zur Netzzustandsbestimmung, zur Gewährleistung der Netzstabilität sowie zur Spannungshaltung entwickelt und in Kampagnen demonstriert (BFE 2016, S. 3). Der am Pilot beteiligte Netzbetreiber EWZ bezeichnet das Vorhaben als „einen Meilenstein zu einem intelligenten Stromnetz“ (EWZ 2016).

> „Die GridBox Plattform ist eine flexible und erweiterbare Mess-, Kommunikations- und Regelplattform für verschiedenste künftige Netzapplikationen und ermöglicht die Umsetzung neuer Business Modelle. So ermöglicht die GridBox Plattform Anwendungen wie z.B. Fehlererkennung und -lokalisierung, erweitertes Netzmonitoring, (…)“ (SCS 2016)

Vor diesem Hintergrund stellt sich die Frage, ob die Entwicklung hin zu einem Smart Grid auch ohne einen umfangreichen Rollout von Smart Metering erfolgen kann. Offenbar führt auch ein gezielter Einsatz von Mess-, Kommunikations- und Steuerungspunkten im Verteilnetz zum gewünschten Effekt. Das Büro für Technologiefolgen Abschätzung beim Deutschen Bundestag (TAB) hält fest, dass „(…) technologisch zwischen Smart Meter und Smart Grid kein zwingender Zusammenhang gesehen wird, da beide Konzepte ohne das jeweils andere implementiert werden können. (TAB 2014, S.44). Damit könnte man die Angriffsfläche, den Umfang der Vernetzung und die Komplexität und die damit verbundenen Risiken deutlich reduzieren.

6 FAZIT UND AUSBLICK

Die Durchdringung aller Wirtschafts- und Lebensbereiche mit Informations- und Kommunikationstechnologien (IKT) setzt sich weiter fort. Der Einsatz von IKT für die Weiterentwicklung zu einem modernen und intelligenten Stromnetz (Smart Grid) scheint unabdingbar. Das European Network for Cyber Security (ENCS) beschäftigt sich intensiv mit den damit verbundenen Risiken. Die im Mai 2016 publizierte ENCS News Meldung mit dem Titel *„Cyber security climbs up the energy agenda"* fasst die Situation bei der Stromversorgung wie folgt zusammen:

> "(…) As Europe increasingly takes advantage of the huge benefits a smarter grid can bring, it also opens itself up to new types and vectors of attack. (…) A clearer understanding of the nature of cyber risk and mitigation measures for energy infrastructure is necessary, in an environment of increasing interconnectivity and emerging technologies" (ENCS 2016).

Die digitale Vernetzung und der Einsatz von neuen Technologien birgt Chancen aber auch Risiken. Im Stromnetz gibt es eine Menge Aspekte, die in Bezug auf die Zuverlässigkeit und die Sicherheit berücksichtigt werden müssen.

Zusammenfassend lässt sich festhalten, dass die zunehmende Vernetzung von verschiedenen Systemen und Infrastrukturen im Stromnetz ein Risiko darstellen. Rein technische Massnahmen werden nicht ausreichen, die Sicherheit der Smart Meter Systeme zu gewährleisten. Durch die umfangreiche Einführung von Smart Metering entstehen *per se* neue Risiken für das Gesamtsystem und daher ist eine kritische Auseinandersetzung mit der Frage der Notwendigkeit und dem erwarteten Nutzen von intelligenten Stromzählern durchaus angebracht.

A ABBILDUNGSVERZEICHNIS

B QUELLENVERZEICHNIS

BFE (Bundesamt für Energie) (2014). Grundlagen der Ausgestaltung einer Einführung intelligenter Messsysteme beim Endverbraucher in der Schweiz - Technische Mindestanforderungen und Einführungsmodalitäten. Bern, Schweiz. http://www.news.admin.ch/NSBSubscriber/message/attachments/37458.pdf

BFE (2015a). Faktenblatt Smart Grid Roadmap. Bern, Schweiz. http://www.bfe.admin.ch/smartgrids/index.html?lang=de&dossier_id=06309

BFE (2015b). Smart Grid Roadmap Schweiz - Wege in die Zukunft der Schweizer Elektrizitätsnetze. Bern, Schweiz. http://www.bfe.admin.ch/smartgrids/index.html?lang=de&dossier_id=06308

BFE (2015c). Ansätze zur Gewährleistung der IKT-Sicherheit von intelligenten Messsystemen bei Endverbrauchern. Untersuchung von aartesys & vZsecurITy im Auftrag des BFE. Bern, Schweiz. http://www.bfe.admin.ch/smartgrids/index.html?lang=de&dossier_id=06437

BFE (2016). GridBox Pilotnetz - Potential eines Echtzeit-Management-Systems für das Verteilnetz. Schlussbericht vom 31. März 2016. PDF unter http://www.bfe.admin.ch/forschungnetze/01246/03569/index.html?lang=de

Bleier T. (2013). Was braucht man für sichere IKT in Smart Grids. In OVE (Österr. Verband für Elektrontechnik (Hrsg.), Elektrotechnik und Informationstechnik (S. 109-114). Wien, Österreich: Springer Verlag.

BMWi (Bundesministerium für Wirtschaft und Energie). (2014). Gesetz zur Digitalisierung der Energiewende. Regierungsentwurf vom 04.11.2015 abrufbar unter http://www.bmwi.de/DE/Themen/Energie/Netze-und-Netzausbau/intelligente-messsysteme.html

BMWi (Bundesministerium für Wirtschaft und Energie). (2015). Faktenblatt Energiewende. Intelligente Messsysteme als wichtiger Baustein der Energiewende. PDF abrufbar unter http://www.bmwi.de/BMWi/Redaktion/PDF/F/faktenblatt-digitalisierung-energiewende,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

Elsberg, M. (2013). BLACKOUT - Morgen ist es zu spät. München, Deutschland: Blanvalet.

ENCS (European Network for Cyber Security. (2014). Anforderungskatalog Ende-zu-Ende Sicherheit Smart Metering. Studie im Auftrag der Österreich Energie. Wien, Österreich.

ENCS (European Network for Cyber Security) (2016). World Energy Council: Cyber security climbs up the energy agenda. Abgerufen 15.05.2016, von https://www.encs.eu/2016/05/04/world-energy-council-cyber-security-climbs-up-the-energy-agenda

EWZ (Elektrizitätswerk der Stadt Zürich). (2016, April 13). Ein Meilenstein zu einem intelligenten Stromnetz. Medienmitteilung. Abgerufen am 15.04.16, von https://www.ewz.ch/de/ueber-ewz/medien/medienmitteilungen/2016/gridbox.html

Gaycken, S. (2012). Cyberwar - Das Wettrüsten hat längst begonnen. Vom digitalen Angriff zum realen Ausnahmezustand. München, Deutschland: Goldmann.

Grandel, M. (2012). Das „Smart Metering Dilemma“ – Strategische Überlegungen zum flächendeckenden Einsatz von Smart Metering. In H.-G. Servatius & U. Schneidewind & D. Rohlfing (Hrsg.), Smart Energy. Wandel zu einem nachhaltigen Energiesystem (S. 221-231). Heidelberg, Deutschland: Springer.

Haberler et. al. (2013). Smart-Grid-Architekturen in Österreich: Eine Bewertung der IKT-Sicherheitsaspekte relevanter Pilotprojekte. In OVE (Österr. Verband für Elektrontechnik (Hrsg.), Elektrotechnik und Informationstechnik (S. 109-114). Wien, Österreich: Springer Verlag.

Maluenda, W., Wagner, S. & Schulze, X. (2015). Security and Safety im Smart Metering. In Chr. Köhler-Schute (Hrsg.), Smart Metering. Geschäftsmodelle und Handlungsoptionen, Prozesse und Technologien, Rollout, Rechtsgrundlagen (S. 85-100). Berlin, Deutschland: KS-Energy-Verlag.

Politik-Digital (2015). Intelligente Stromzähler: Einfallstor für Hacker. Beitrag von R. Meyer. Abgerufen am 24.04.2016, von http://politik-digital.de/news/smart-meter-einfallstor-hacker-147655

Raquet, Chr. & Liotta, G. (2013). Datenübertragungstechnologien in Smart Metering und Smart Grids. In Aichele, Chr. & Doleski O. D. (Hrsg.), Smart Meter Rollout. Praxisleitfaden zur Ausbringung intelligenter Zähler (S. 389-402). Wiesbaden, Deutschland: Springer Vieweg.

Saurugg, H. (2011). Smart Metering und mögliche Auswirkungen auf die nationale Sicherheit. Seminararbeit im Rahmen des Master-Studiengangs „Defence Economics“. Wien, Österreich. Download unter https://www.cybersecurityaustria.at/index.php/publikationen

Saurugg, H. & Pichlmayr, J. (2013). „Smart“, Vernetzung und Komplexität – Ein Plädoyer für einen kritischeren Umgang mit dem Thema Vernetzung. In OVE (Österr. Verband für Elektrontechnik (Hrsg.), Elektrotechnik und Informationstechnik (S. 109-114). Wien, Österreich: Springer Verlag.

SCS (Super Computing Systems) (2016). Pressemitteilung vom 20.05.2016: „GridBox Projekt: Erfolgreiche Beendigung der Mess- und Demonstrationskampagnen“ - Stephan Moser, Department Head „Energy Systems“ Abgerufen 31.05.16, von https://www.scs.ch/blog/2016/04/projekt-gridbox-erfolgreiche-kampagnen bzw. https://www.scs.ch/blog/wp-content/uploads/2016/04/Pressemitteilung_20160520.pdf

TAB (Büro für Technologiefolgenabschätzung beim Deutschen Bundestag). (2014). Moderne Stromnetze als Schlüsselelement einer nachhaltigen Energieversorgung. TAB-Arbeitsbericht Nr. 162, Berlin, Deutschland.

Vest, P. (2012). Intelligente Zähler, der Markt für Energieeffizienz und sein Dilemma. In H.-G. Servatius & U. Schneidewind & D. Rohlfing (Hrsg.), Smart Energy. Wandel zu einem nachhaltigen Energiesystem (S. 209-220). Heidelberg, Deutschland: Springer.

C WEITERE LITERATUR

- Adam, R. (2012). Die Zukunft der Energieversorgung ist digital. In H.-G. Servatius & U. Schneidewind & D. Rohlfing (Hrsg.), Smart Energy. Wandel zu einem nachhaltigen Energiesystem (S. 355-362). Heidelberg, Deutschland: Springer.
- Black Hat Conference (2014). Lights Off! The Darkness of the Smart Meters. Presentation by Alberto Garcia Illera and Javier Vazquez Vidal. Video abgerufen am 19.04.2016 von https://www.youtube.com/watch?v=Z_y_vjYtAWM
- BSI (Bundesamt für Sicherheit in der Informationstechnik). (2014) Das Smart Meter Gateway – Sicherheit für intelligente Netze. Bonn, Deutschland.
- Bosch. (2015). Security und Safety für Smart Metering in Deutschland: Der Umgang aus IT-Sicht mit relevanten Bedrohungen. Medienmitteilung. Abgerufen 16.05.16, von https://www.bosch-si.com/de/newsroom/news/veroeffentlichungen/veroeffentlichungen-63808.html
- Bundeskriminalamt. (2014) Bundeslagebild Cybercrime 2014. http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2014,templateId=raw,property=publicationFile.pdf/cybercrimeBundeslagebild2014.pdf
- Computerwoche. (2015, September 21) Wenn Hacker den Verkehr lahmlegen. Abgerufen 29.03.16, von http://www.computerwoche.de/a/wenn-hacker-den-verkehr-lahmlegen,3109960
- Computing. (2016) GCHQ forced to intervene to prevent catastrophically insecure smart metering plan http://www.computing.co.uk/ctg/news/2451772/gchq-forced-to-intervene-to-prevent-catastrophically-insecure-smart-metering-plan
- EBV Blog. (2016, April 21) The Smart Meter Security Dilemma. Abgerufen 16.05.16, von http://blog.ebv.com/smart-meter-security-dilemma/
- Die Zeit. (2013, November 19) Stromkunden sollen sich überwachen lassen – und dafür zahlen. Abgerufen 26.03.16, von http://www.zeit.de/digital/datenschutz/2013-11/smart-meter-teuer-daten-vermarkten
- Die Zeit. (2010, September 16) Attacke im Sicherungskasten. Abgerufen 26.03.16, von http://www.zeit.de/2010/38/Smart-Grid-Hacker
- MobileGeeks (2015). Virus im Kernkraftwerk – Conficker-Wurm in Gundremmingen. Abgerufen 02.05.2016, von http://www.mobilegeeks.de/news/conficker-wurm-kernkraftwerk-grundremmingen
- Smart Grid Awareness. (2014). Smart Meters Can Be Hacked to Order a Power Blackout. Abgerufen 19.04.16, von https://smartgridawareness.org/2014/10/04/smart-meters-can-be-hacked
- Symantec. (2014). Dragon Fly: Western Energy Companies Under Sabotage Threat. Abgerufen 29.03.16, von http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat
- Symantec. (2014). Dragonfly: Cyberespionage Attacks Against Energy Suppliers. Whitepaper. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
- Tech Insider. (2016). Watch hackers break into the US power grid - A power company in the Midwest hired a group of white hat hackers known as RedTeam Security to test its defenses. Video abgerufen am 20.05.2016 von https://www.youtube.com/watch?v=pL9q2lOZ1Fw