CYBER SECURITY AUSTRIA

Smart Metering

und mögliche Auswirkungen auf die nationale Sicherheit

www.cybersecurityaustria.at

res publica

Vorwort

Der Verein „Cyber Security Austria“ hat sich die Förderung der IT Sicherheit Österreichs strategischer Infrastruktur zum Ziel gesetzt.

Durch das Erfassen, Vernetzen, Vermitteln und Publizieren der vorhandenen Kompetenzen aus den unterschiedlichen Informationssicherheitsbereichen soll das Sicherheitsbewusstseins in Österreich gefördert werden.

Als erstes Kernthema wurde die Smart Metering Sicherheit definiert.

„Smart Metering und mögliche Auswirkungen auf die nationale Sicherheit“ ist im Rahmen des Master-Studiengangs „Defence Economics“ als Seminararbeit von Herbert Saurugg entstanden. Aufgrund der hohen Aktualität und wahrscheinlich auch Brisanz, wird sie von ihm unter der Creative Commons Lizenz (by-nc-sa)[1] allgemein, zur generellen Sensibilisierung, bereit gestellt.

Der Verein „Cyber Security Austria“ nimmt dies zum Anlass, seine erste Publikation diesem Thema zu widmen. Weitere Bearbeitungen und Vertiefungen sind geplant.

Wien, Juli 2011

Sprachliche Gleichbehandlung: In weiterer Folge beziehen sich, um die Lesbarkeit zu erleichtern, soweit auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, diese auf Frauen und Männer in gleicher Weise.

1 URL: https://secure.wikimedia.org/wikipedia/de/wiki/Creative_Commons [28.06.11]; by: Namensnennung, nc: nicht kommerziell, sa: Weitergabe unter gleichen Bedingungen.

Inhaltsverzeichnis

1 Einleitung

In der ersten Seminararbeit *„Der Cyberspace und die Auswirkungen auf die nationale Sicherheit“*[2] wurden mehrere Beispiele zur Darstellung des Gefährdungspotentials aus dem Cyberspace, mit möglichen Auswirkungen auf die nationale Sicherheit, behandelt. Dem wurden kurz derzeit verfügbare nationale Instrumente zur Krisenbewältigung gegenübergestellt.

> **Nationale Sicherheit:** „Die Fähigkeit einer Nation, ihre inneren Werte vor äußerer Bedrohung zu schützen.“[3]

Aufgrund der aktuellen Entwicklungen soll mit der zweiten Seminararbeit das Thema „Smart Metering“[4] detaillierter behandelt werden. Ein erster Überblick wurde bereits in der ersten Seminararbeit im Abschnitt 4.3, Intelligentes Stromnetz (Smart Grid)[5], gegeben.

Öffentliche Stromnetze stellen einen wesentlichen Bestandteil der Strategischen Infrastruktur[6] dar. Durch die zunehmende dezentrale Einspeisung von Energie aus erneuerbaren Energiequellen über z.B. Wind-, Photovoltaik oder Biomassekraftwerke, dem zu erwartenden Anstieg der Elektromobilität und der Forderung nach mehr Energieeffizienz, wird eine umfassende Einbindung von Informations- und Kommunikationstechnologien (IKT) zur Netzwerksteuerung unentbehrlich. Erst durch den Informationsaustausch zwischen den Erzeugungsanlagen, den Netzkomponenten, den Speichern und den Verbrauchern kann eine flexible Reaktion auf komplexe Veränderungen im Netz gewährleistet werden. Die Komplexität ergibt sich u.a. aufgrund der Eigenheiten von dezentralen, von exemplarisch Sonnen- oder Windenergie abhängigen, Erzeugungsanlagen, welche naturbedingt keine konstante Energieerzeugung gewährleisten können. Für diese informationstechnische Vernetzung und Steuerung wird der Begriff intelligentes Stromnetz oder Smart Grid verwendet.

Grundvoraussetzung für intelligente Stromnetze ist das sogenannte Smart Metering. Beim Smart Metering wird der traditionell mechanische oder elektronische Drehstromzähler des Endkunden durch einen intelligenten Zähler (Smart Meter) ersetzt, der regelmäßig über elektronische Übertragungsmedien wichtige (Verbrauchs-)Daten an den Netzbetreiber übermittelt. Durch diesen Informationsaustausch wird eine bessere Netzsteuerung ermöglicht. Zusätzlich soll für den Endkunden eine Verbrauchstransparenz geschaffen werden, die auch zu besseren Stromsparmaßnahmen führen soll.

2 Vgl. Saurugg, 2011.
3 Woyke 2006, S. 288.
4 „intelligentes Messwesen“, siehe Kapitel 2.
5 Vgl. Saurugg, 2011, S. 22ff.
6 In Österreich wird häufig der Begriff Strategische statt Kritische Infrastrukturen verwendet. Darunter sind gem. Österreichischem Programm zum Schutz kritischer Infrastrukturen (APCIP) Infrastrukturen aus den Sektoren Verfassungsmäßige Einrichtungen, Energie, IKT, Wasser, Lebensmittel, Gesundheit und Soziales, Finanzen, Transport- und Verteilungssysteme, Chemische Industrie, Forschungseinrichtungen, Hilfs- und Einsatzkräfte mit gesamtstaatlicher Relevanz zu verstehen.

Wie die bisherige Geschichte der IKT gezeigt hat, entsteht durch eine weitreichende, ständig verfügbare Vernetzung von Systemen immer auch ein Missbrauchspotential. Die möglichen Bedrohungen reichen von Abrechnungsbetrug bis hin zu gravierenden Angriffen, die Stromnetzausfälle oder permanente Netzschäden verursachen können.

Die **forschungsleitende Frage** in dieser Arbeit lautet, wie ist es um das Thema Sicherheit im Bereich von Smart Metering bestellt und welche möglichen Folgen könnten sich daraus für die nationale Sicherheit ergeben.

Primäres Ziel ist dabei, die Grundlagen auf allgemein verständlicher Basis aufzubereiten und so zu einer generellen Sensibilisierung beizutragen. Aufgrund der Komplexität besteht jedoch kein Anspruch auf Vollständigkeit, wenngleich versucht wird, ein möglichst umfangreiches Bild zu vermitteln, welches sich nicht nur auf technische Details beschränkt. Dies vor allem auch deshalb, da dieses Thema sehr euphorisch verfolgt wird, mögliche Risiken aber so gut wie nie angesprochen werden.

Wie sich aber im Laufe dieser Arbeit zeigen wird, sind die mit der Einführung dieser neuen Technologien verbundenen Risiken ganz erheblich. Dies beginnt mit möglichen finanziellen Schäden, da von zu positiven Annahmen für den volkswirtschaftlichen Nutzen ausgegangen wird, bzw. Berechnungsgrundlagen nicht plausibel sind und führt bis zu einer erheblichen Steigerung der Verwundbarkeit der Strategischen Infrastrukturen.[7]

Das zweite Kapitel soll einen Überblick über das Gesamtsystem verschaffen. Dieser Überblick ist für die weitere Gefährdungsanalyse erforderlich. Zusätzlich werden die derzeit gültigen rechtlichen Grundlagen (EU und national) beleuchtet.

Das dritte Kapitel beschäftigt sich mit dem Thema Sicherheit, insbesondere der Angriffssicherheit (security). Es werden mögliche Angriffspunkte und Schwachstellen im Bereich von Smart Metering angesprochen. Darüber hinaus werden weitere Bereiche, welche für die nationale Sicherheit von Bedeutung sein könnten, angerissen.

Das vierte Kapitel beschäftigt sich mit möglichen Folgen einer versagenden (Energie-)Infrastruktur – bis hin zum Blackout. Hier wird herausgearbeitet, dass ein länger andauernder Blackout eine katastrophale Auswirkung auf das Staatsgefüge und das soziale Leben nach sich ziehen wird. Dies ist besonders für die tatsächliche Gefährdungseinschätzung sehr wichtig.

Im fünften Kapitel erfolgt eine Zusammenfassung und die Ableitung von einigen Folgerungen, die zu einer besseren Widerstandsfähigkeit der Strategischen Infrastrukturen führen und somit auch einen Beitrag für die nationale und soziale Sicherheit darstellen könnten.

"Hope for the Best. Expect the worst.

Life is a play. We're unrehearsed."

Mel Brooks

7 Vgl. PwC Österreich, 2010.

2 Die Stromversorgung

2.1 Die Stromversorgung von heute

Die bisherige in der Industriegesellschaft übliche Stromversorgung basiert vorwiegend auf einer zentralen Struktur und der Energieerzeugung in Großkraftwerken. Die elektrische Energie wird von diesen Erzeugungsanlagen über Stromnetze an die Stromverbraucher geliefert (siehe Abbildung 1). Der Vorteil einer zentralen Struktur ist ein verringerter Koordinierungsaufwand, welche aber wiederum zu Lasten der Flexibilität geht.

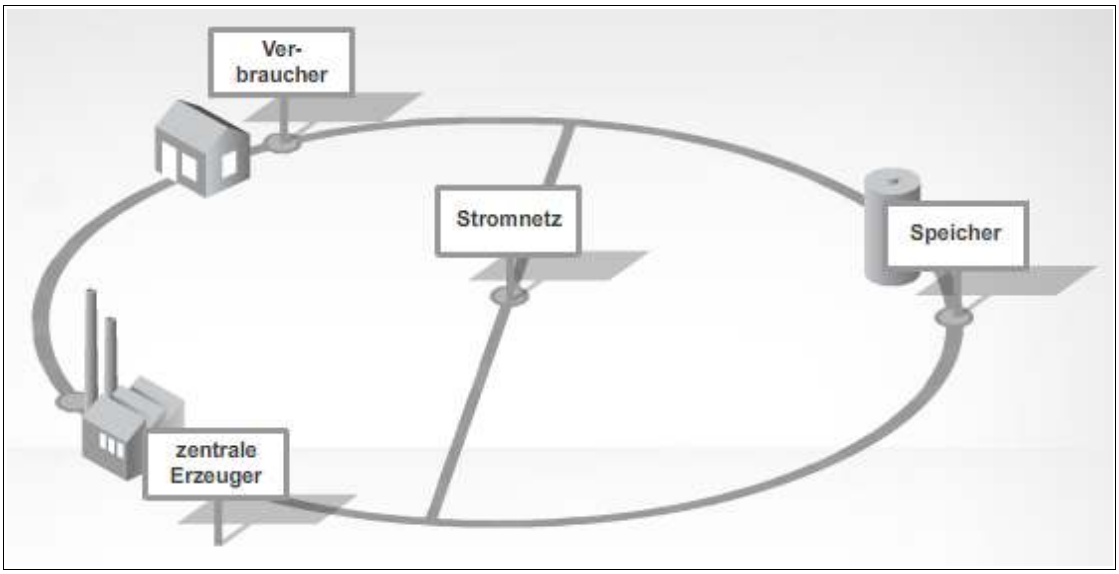

Abbildung 1: Bisherige Stromversorgung - Quelle: www.smartgrids.at

In den bisherigen Industriegesellschaften sind viele Bereiche des Lebens auf die Konzentration von Ressourcen ausgerichtet. Beispielsweise die Arbeit in Fabriken, die zentrale Energieerzeugung, die Konzentration der Bevölkerung in Städten, die standardisierte Ausbildung für die breite Masse. Viele westliche Gesellschaften sind derzeit im Übergang zur Wissensgesellschaft, welche im Wesentlichen durch Personalisierung/Individualisierung, Vielfältigkeit, Asynchronisation, Verteilung/Dezentralisierung und Miniaturisierung gekennzeichnet ist.[8] [9]

2.2 Die Stromversorgung in der Zukunft

Diese sich veränderten Rahmenbedingungen und der verstärkte Einsatz von erneuerbaren Energieformen und der damit einhergehenden Dezentralisierung der Energieerzeugung führen die bisherigen Systeme an die Grenze ihrer Leistungsfähigkeit.

> *„Die für die Regelung des Stromnetzes notwendige Kommunikationsinfrastruktur (Anbindung von Kraftwerken und Netzanlagen) ist bisher schwerpunktmäßig nur in Hochspannungsnetzen vorhanden. Die bisher zentral überwachten und gesteuerten*

8 Vgl. Toffler, 1997.
9 Vgl. Toffler, 2006.

Stromnetze können die angeführten großen Herausforderungen in Zukunft immer weniger beherrschen, da sie dafür nicht konzipiert wurden."[10]

Abhilfe sollen sogenannte intelligente Netzinfrastrukturen oder Smart Grids schaffen, die als wichtiger Beitrag zu dieser, sich veränderten Welt, gesehen werden. Wie lange dieser Übergang dauern wird, weiß niemand. Das er bereits begonnen hat, ist in vielen Lebensbereichen zu erkennen.

Auch im Bereich der Energieversorgung, nicht zuletzt auch durch die Atomkatastrophe von Fukushima, geht die Tendenz verstärkt zu einer dezentralen, auf erneuerbaren Ressourcen basierende Energieerzeugung, wenngleich es dazu auch ganz gegenteilige Projekte, wie etwa das DESERTEC gibt (siehe Abbildung 2). Dieses sieht die zentrale Erzeugung von Strom mittels solarthermischer Kraftwerke in Wüsten (z.B. Sahara) und den langen Transport in die Bedarfsregionen (z.B. Europa) vor[11].

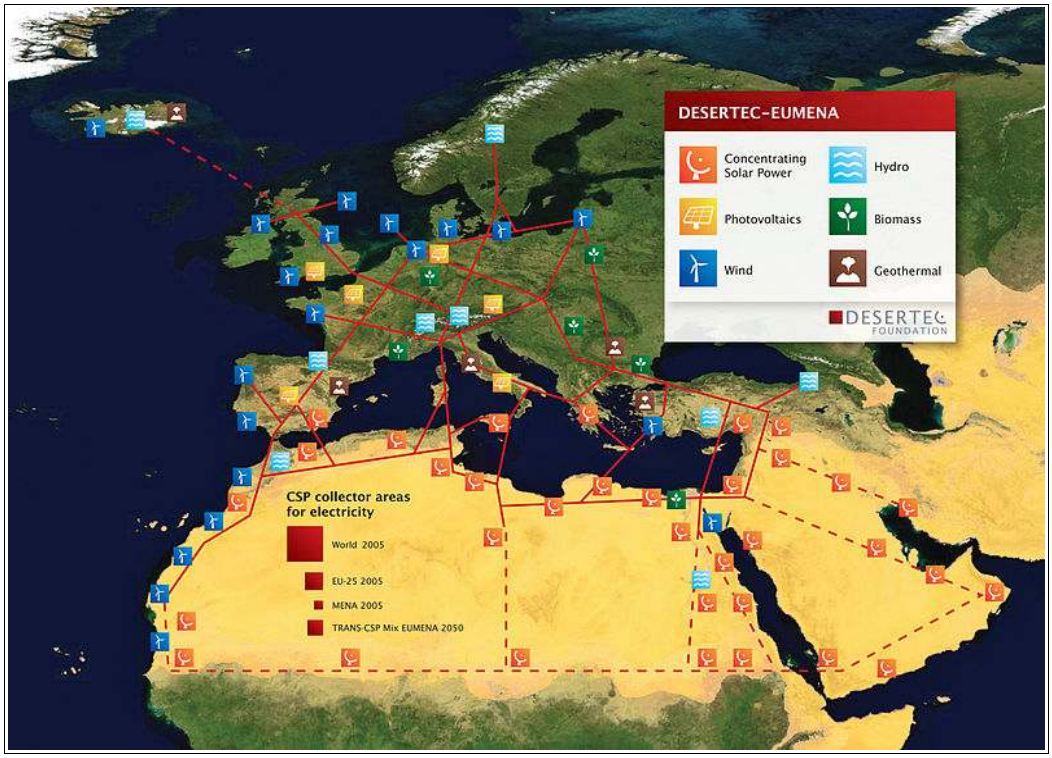

Abbildung 2: Projekt DESERTEC - Quelle: www.desertec.org

Die Zunahme des Energiebedarfes[12], die Dezentralisierung und Individualisierung der Erzeugung, führen zu einer steigenden Komplexität des Gesamtsystems (siehe Abbildung 3). Dies erfordert auf der einen Seite innovative Lösungsansätze führt aber gleichzeitig auch zu einer erhöhten Anfälligkeit gegenüber Störungen jeglicher Art. Diese Anfälligkeit wird aber auch durch andere gesellschaftspolitische Rahmenbedingungen verstärkt wie etwa

10 URL: http://www.smartgrids.at/smart-grids/ [06.06.2011].
11 Vgl. URL: http://www.desertec.org [26.05.2011].
12 dzt. rund 2% pro Jahr in Österreich. Quelle: URL: http://oesterreichsenergie.at/stromverbrauch-in-oesterreich.html [26.05.2011].

- der wirtschaftliche- bzw. Innovations-druck führen zu einer verstärkten Vereinheitlichung von Netztechnologien und Netzen.
- die stetig zunehmende Vernetzung in allen möglichen Lebensbereichen und die beinahe vollständige Abhängigkeit von der Verfügbarkeit der Kommunikationsinfrastruktur.
- unüberschaubare und nicht mehr nachvollziehbare Abhängigkeiten.

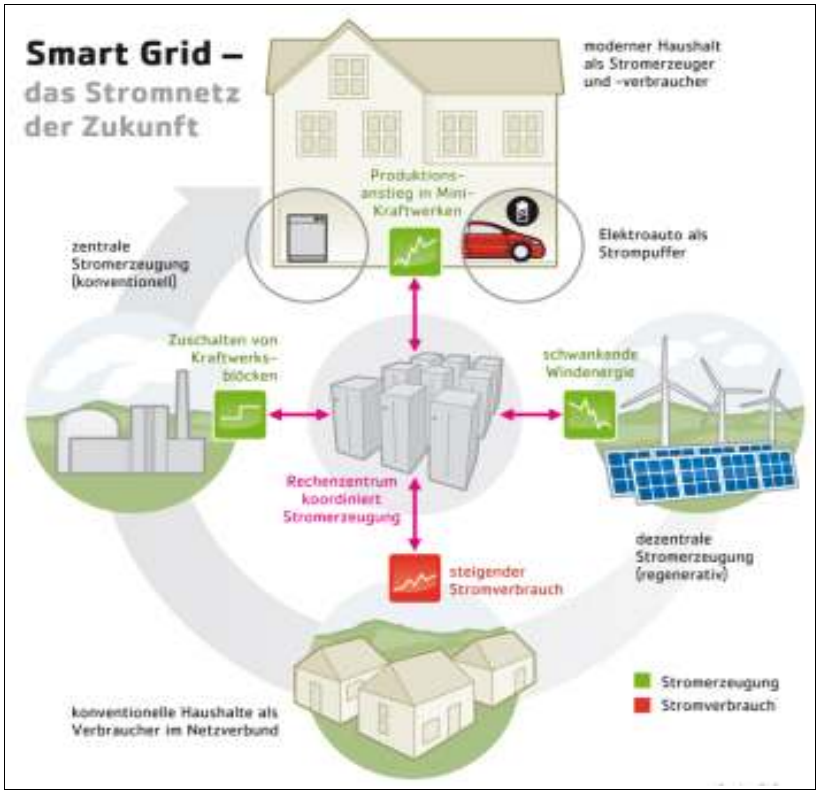

Abbildung 3: Zukünftige Stromversorgung - Quelle: T-Systems

Die Versorgung mit Strom als Basis für alle anderen Versorgungsbereiche des täglichen Lebens (exemplarisch Wasser Ver- und Entsorgung, Kommunikation, medizinische Versorgung, Transport, Beleuchtung, Ernährung) spielt eine ganz zentrale Rolle. Ohne funktionierende Stromversorgung bricht unser heutiges Gesellschaftsleben innerhalb kürzester Zeit völlig zusammen, vor allem in Ballungszentren.[13] In der öffentlichen Wahrnehmung spiegelt sich dies aber kaum wieder. Dies ist wohl auch auf die in Österreich sehr hohe Versorgungssicherheit zurückzuführen. 2009 lag

> *„die durchschnittliche, ungeplante Nichtverfügbarkeit von Elektrizität im österreichischen Stromnetz bei 36,65 Minuten pro Kunde, womit eine Versorgungssicherheit von 99,99 Prozent gewährleistet war. Im internationalen Vergleich weist Österreich damit eine überdurchschnittlich hohe Versorgungssicherheit auf."*[14]

13 Vgl. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011.

14 URL: http://oesterreichsenergie.at/die-versorgungssicherheit-in-oesterreich-ist-gewaehrleistet.html [26.05.2011].

Im Rahmen dieser Arbeit kann leider nicht überprüft werden, ob diese hohe Versorgungssicherheit auf derart gute Notfallmaßnahmen und einer detaillierten Risikoanalyse, inkl. der erforderlichen Vorsorgemaßnahmen beruht. In Deutschland besteht auf jeden Fall die Befürchtung, dass eine hohe Versorgungssicherheit wahrscheinlich zu einer gewissen Nachlässigkeit bei den Notfallmaßnahmen, bzw. bei der Risikoanalyse eines möglichen längeren Stromausfalles führt.[15]

2.3 Die Messung des Stromverbrauchs

Seit rund 100 Jahren werden die heute am weitest verbreiteten, sogenannten Ferrariszähler, als Stromzähler verwendet (siehe Abbildung 4). Es handelt sich hierbei um ein elektromechanisches Messgerät für elektrische Energie und dient zur Anzeige der konsumierten, oder auch der eingespeisten, elektrischen Energie.[16]

Der Ferrariszähler misst und speichert den Energieverbrauch lokal. Damit der Endkunde seinen Energieverbrauch feststellen kann, muss er in den Zählerraum gehen und den Zählerstand ablesen. Diese Selbstkontrolle des Endverbrauchers erfolgt aufgrund des Aufwandes und der geringen Aussagekraft – es kann nur der momentane Gesamtstand abgelesen werden – nur in Ausnahmefällen. Auch für die Verrechnung ist es erforderlich, dass ein Mitarbeiter des Energieversorgungsunternehmens zu jedem einzelnen Zähler geht und diesen manuell abliest. Daher wird in der Regel der tatsächliche Stromverbrauch nur alle paar Jahre abgelesen und dazwischen ein Mittelwert verrechnet.

Abbildung 4: Smart Meter (links), Ferrariszähler (rechts) - Quelle: http://e-control.at

Um dieses aufwändige Verfahren stark zu vereinfachen, bzw. dem Kunden auch die Möglichkeit zu geben, seinen unmittelbaren Stromverbrauch direkt, etwa über Internet oder einer Applikation am Smartphone, zu übermitteln und somit auch sein Energieverbrauchsprofil aktiv beeinflussen zu können, sollen zukünftig intelligente Strom-

15 Vgl. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011.

16 Vgl. URL: http://e-control.at/de/industrie/strom/smart-meter [05.06.2011].

zähler (engl. Smart Meter) zum Einsatz kommen (siehe Abbildung 4). Darüber hinaus würde ein solcher intelligenter Stromzähler auch einen direkten Rückkanal in das Stromnetzmanagement bieten und damit die bedarfsorientierte Stromnetzsteuerung erst ermöglichen.

Der Begriff *Smart Meter* wird zur Zeit häufig, sofern er überhaupt bekannt ist, mit einem intelligenten Stromzähler in Verbindung gebracht. Der Begriff bzw. der mögliche Anwendungsbereich beschränkt sich jedoch nicht nur auf elektrische Energie, sondern soll zukünftig in möglichst allen Bereichen, wo der tatsächlichen Energieverbrauch bzw. die Nutzungsdauer oder -menge erfasst wird, z.B. Wasser-, Gas-, oder Wärmeverbrauch, zum Einsatz kommen.

2.4 Die Intelligenz des Systems

Der Zähler alleine reicht natürlich nicht aus. Ganz wesentlich für die Kommunikation zwischen Endverbraucher und dem Netz sind weitere Netzwerkkomponenten und Kommunikationskanäle, welche die entsprechenden Werte an das Netzwerkmanagementsystem übermitteln und andererseits auch wieder mögliche Steuersignale zurück transportieren. Für dieses System wird der Begriff *Smart Metering* oder intelligentes Messwesen verwendet. Darin sind die digitalen Zählgeräte (Smart Meter), Datenübertragungseinrichtungen bis hin zu Auswertungen und Anwendungen in den so genannten „Messdatenmanagementsystemen" enthalten. Der Begriff Smart Meter bezieht sich hingegen nur auf den Sensor beim Endkunden. Jedoch erst durch das Zusammenwirken aller Komponenten ergibt sich die „Intelligenz".[17]

Der Begriff Smart Grid oder intelligentes Netz beschreibt daher das Gesamtsystem.

> *„Smart Grids ermöglichen es, energie- und kosteneffizient zwischen einer Vielzahl von Stromverbrauchern, Stromerzeugern und in Zukunft auch verstärkt Stromspeichern ein Gleichgewicht herzustellen. Dieses Gleichgewicht wird durch optimiertes Management von Energieerzeugung, Energiespeicherung, Energieverbrauch und dem Stromnetz selbst erreicht. Eine durchgängige Kommunikationsfähigkeit vom Kraftwerk bis hin zu den Verbrauchern ist notwendig.*
>
> *Einzeltechnologien für Smart Grids existieren bereits. Das Management von Stromübertragungsnetzen ist automatisiert, das ferngelenkte Steuern von großen Kraftwerken ist seit langer Zeit Routine. Es gilt nun, diese Konzepte ins Stromverteilernetz einzubringen, durch neue Elemente zu ergänzen und die einzelnen Elemente systematisch zu kombinieren. Dabei existieren große technische, organisatorische und nicht zuletzt wirtschaftliche Herausforderungen."*[18]

Die offizielle Definition von Smart Grids durch die nationale Technologieplattform Smart Grids Austria lautet:

> *„Smart Grids sind Stromnetze, welche durch ein abgestimmtes Management mittels zeitnaher und bidirektionaler Kommunikation zwischen*
> - *Netzkomponenten,*
> - *Erzeugern,*

17 Vgl. PwC Österreich, 2010, S. 14.

18 URL: http://www.smartgrids.at/smart-grids/ [12.06.2011].

- *Speichern und*
- *Verbrauchern*

einen energie- und kosteneffizienten Systembetrieb für zukünftige Anforderungen unterstützen."[19]

2.5 Die Komponenten von Smart Metering

Smart Metering ist derzeit noch nicht standardisiert. Daher kommen im Rahmen der in Österreich laufenden Pilotprojekte unterschiedliche Lösungen verschiedenster Hersteller zum Einsatz.[20] Im Wesentlichen müssen aber durch Smart Metering folgende Aufgaben erfüllt werden:[21]

- Messen
- Datensammeln, -speichern und Steuern (Zählen, Datenlogging, Tarifregister, u.ä.)
- Kommunizieren
- Mehrwertfunktionen (optional, wie etwa Manipulationssicherung, Web-Service/Feedbacksystem, Energiemanagement))

2.5.1 Smart Meter (Messung; Mehrwertfunktionen)

Smart Meter stellen den Sensor beim Kunden dar und befinden sich zu ca. 40% in Haushalten (Einfamilienhäuser) und zu ca. 60% in zentralen Zählerräumen oder Zählernischen (Mehrparteienhäuser). Diese zeichnen den aktuellen Stromverbrauch der Endkunden auf und leiten die entsprechenden Daten in periodischen Abständen (beispielhaft 15 Minutentakt) über unterschiedliche Übertragungskanäle (siehe weiter unten) an einen Konzentrator weiter.

2.5.2 Konzentrator (Datensammlung)

Der Konzentrator ist die Schnittstelle zum Datennetz des Netzbetreibers. Er verwendet zwei unterschiedliche Kommunikationsschnittstellen. Einerseits zu den Smart Meter (siehe vorher) und andererseits zum Netzbetreiber via WAN[22]-Technologie (z.B. Glasfaser oder GSM).

2.5.3 Netzwerkkommunikation (Kommunikation)

Für de Kommunikation zwischen den einzelnen Netzwerkkomponenten können unterschiedliche Kanäle und Verfahren zum Einsatz kommen (siehe Abbildung 5 und 6). Für die Nahkommunikation können dies beispielhaft M-Bus[23] (Draht/Funk), ZigBee[24]

19 Ebenda.
20 Vgl. IKARUS Security Software GmbH, 2011.
21 Vgl. URL: http://www.kine-ev.de/download/vortraege/20080716_Dr.M.Buettner_SmartMetering.pdf [12.06.2011].
22 Wide Area Network.
23 Meter-Bus; Europäische Norm zur Zählerfernauslesung / Verbrauchsdatenerfassung; Bei der Verwendung der M-Bus-Technologie für die Kommunikation mit den Smart Meter ist die Anzahl aufgrund des eingeschränkten primären Adressraumes von M-Bus auf 249 Smart Meter pro Konzentrator beschränkt. Es gibt aber Erweiterungsmöglichkeiten (sekundäre Adressierung), die aber entsprechend aufwendiger ist und durch die Endgeräte unterstützt werden muss.
24 Funknetz-Standard zur Verbindung von Haushaltsgeräte, Sensoren, uvm. auf Kurzstrecken (10 bis 100 Meter)

(Funk), Ethernet[25] (Draht) sein. Zusätzlich ist es möglich, dass keine Nahkommunikation verwendet wird, sondern die Fernkommunikation direkt im Zähler integriert ist.

Für die Fernkommunikation können dies z.B. Modemverbindungen, DSL[26], PLC[27], POTS[28], ISDN[29], GSM (Funk) sein. Im WAN Bereich kommen gängige IT-Übertragungsprotokolle, wie etwa TCP/IP[30], zum Einsatz.

Zusätzlich ist die Implementierung eines Feedback-Systems über z.B. ein Display im Haushalt, ein Internetportal oder einer Mobiltelefonapplikation vorgesehen. Dieses soll dem Kunden eine zeitnahe Übersicht über sein aktuelles Verbraucherverhalten liefern und damit, in Kombination mit entsprechenden Tarifmodellen, das Energieverbrauchsverhalten beeinflussen. Dadurch werden Energieeinsparungen im einstelligen Prozentbereich erwartet.[31] [32]

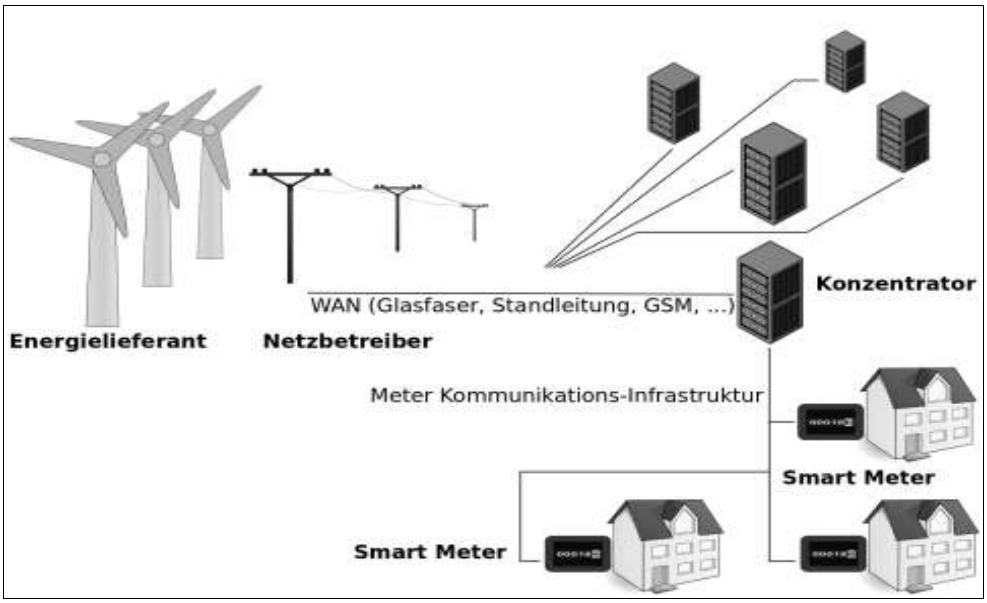

Abbildung 5: Bidirektionale Kommunikationsverlauf im Bereich Smart Metering - Quelle: IKARUS Security Software GmbH

Der Netzbetreiber verwendet entsprechend IT-gestützte Netzwerkmanagementwerkzeuge. Zum Beispiel, um mit den übermittelten Daten die automatische Abrechnung oder ein Internetportal zur Verbrauchsanalyse für die Kunden zu betreiben. Der Netzbetreiber kann aber auch mit den Smart Meter kommunizieren und diese etwa aus der Ferne abschalten, wenn diese Funktion implementiert ist. Damit sollen zahlungsunfähige Kunden rascher vom Netz genommen werden können, oder ein einfacheres Umzugsmanagement ermöglicht werden.

25 Eine Netzwerktechnikfamilie, die ursprünglich für lokale Netzwerkkommunikation entwickelt wurde, aber mittlerweile auch zur Verbindung großer Netzwerke zum Einsatz kommt.

26 Digital Subscriber Line; vgl. z.B. ADSL für Breitbandinternetanbindungen.

27 Powerline Communication – direkte Kommunikation über die Stromleitung; vgl. Internet aus der Steckdose.

28 Plain old telephone service; In der Fachsprache die Bezeichnung für den analogen Telefondienst.

29 Integrated Services Digital Network; Ein internationaler Standard für ein digitales Telekommunikationsnetz.

30 Transmission Control Protocol/Internet Protocol.

31 Vgl. URL: http://www.energyagency.at/energiewirtschaft/aktuelle-projekte/smart-metering.html [15.06.2011]

32 In wie weit hier der Rebound Effekt berücksichtigt wird, kann nicht gesagt werden. Mit Rebound wird in der Energieökonomie der Umstand bezeichnet, dass das Einsparpotenzial von Effizienzsteigerungen nicht oder nur teilweise verwirklicht wird.

Der Energielieferant bekommt vom Netzbetreiber die erforderlichen Daten, um auf Schwankungen im Netz rascher und flexibler reagieren zu können. Er hat aber keine direkte Anbindung an die Smart Metering-Infrastruktur. Durch die genauen Verbrauchsdaten kann der Energielieferant für den Verbraucher attraktivere Tarifmodelle zur Verfügung stellen (Stichwort: Steigerung der Energieeffizienz).

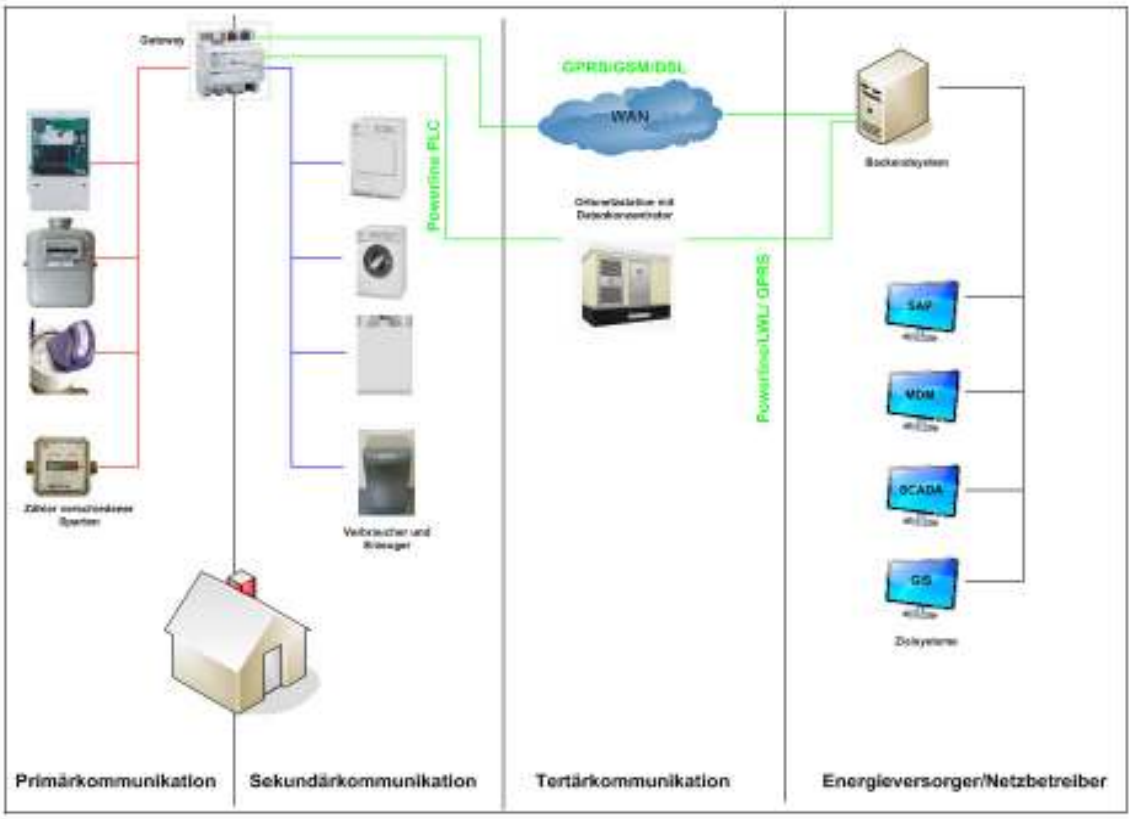

Abbildung 6: Kommunikationsnetzaufbau - Quelle: http://winfwiki.wi-fom.de/index.php/Smart_Metering_als_Grundstein_für_Smart_Grids [12.06.2011]

2.6 Internationale Grundlagen (EU)

Die europäische Kommission hat 2009 das dritte Energiebinnenmarktpaket verabschiedet. Die Richtlinie 2009/72/EG (für Strom) und 2009/73/EG (für Gas) fordern eine Einführung von „intelligenten Zählersystemen".[33]

Dazu ist im Anhang I, Maßnahmen zum Schutz der Kunden, (2), angeführt:

> *„Die Mitgliedstaaten gewährleisten, dass intelligente Messsysteme eingeführt werden, durch die die aktive Beteiligung der Verbraucher am Stromversorgungsmarkt unterstützt wird. Die Einführung dieser Messsysteme kann einer wirtschaftlichen Bewertung unterliegen, bei der alle langfristigen Kosten und Vorteile für den Markt und die einzelnen Verbraucher geprüft werden sowie untersucht wird, welche Art des intelligenten Messens wirtschaftlich vertretbar und kostengünstig ist und in welchem zeitlichen Rahmen die Einführung praktisch möglich ist.*
>
> *Entsprechende Bewertungen finden bis 3. September 2012 statt.*
>
> *Anhand dieser Bewertung erstellen die Mitgliedstaaten oder eine von ihnen benannte zuständige Behörde einen Zeitplan mit einem Planungsziel von 10 Jahren für die Einführung der intelligenten Messsysteme. Wird die Einführung intelligenter Zähler positiv bewertet, so werden mindestens 80% der Verbraucher bis 2020 mit intelligenten Messsystemen ausgestattet."*[34]

In dieser Richtlinie wird im Wesentlichen nicht auf die Sicherheit, wie etwa in Form von Risiko, Risikoabschätzung, Verwundbarkeit (engl. vulnerability) eingegangen, ausgenommen mit

> *„Die Sicherheit der Energieversorgung ist ein Kernelement der öffentlichen Sicherheit und daher bereits von Natur aus direkt verbunden mit dem effizienten Funktionieren des Elektrizitätsbinnenmarktes und der Integration der isolierten Strommärkte der Mitgliedstaaten."*

Sicherheit wird primär im Sinne der Wirtschaftlichkeit (Ökonomie) behandelt. Konkrete Hinweise auf mögliche Gefährdungen durch mangelnde technische Sicherheit sind nicht enthalten.

2.7 Nationale Grundlagen

Mit der Novellierung des Elektrizitätswirtschafts- und Organisationsgesetz (ElWOG) im Winter 2010 wurden die Vorgaben der EU-Richtlinie in nationales Recht umgesetzt und die Voraussetzungen für den Einsatz von intelligenten Stromzählern in Österreich geschaffen.

> *„Intelligente Messgeräte*
>
> *§ 83. (1) Der Bundesminister für Wirtschaft, Familie und Jugend kann nach Durchführung einer Kosten/Nutzanalyse die Einführung intelligenter Messseinrichtungen festlegen. Dies hat nach Anhörung der Regulierungsbehörde und der Vertreter des Konsumentenschutzes durch Verordnung zu erfolgen. Die Netzbetreiber sind im Fall*

33 Vgl. Amtsblatt der Europäischen Union, 2009.

34 Ebenda, S. 37.

> *der Erlassung dieser Verordnung zu verpflichten, jene Endverbraucher, deren Verbrauch nicht über einen Lastprofilzähler gemessen wird, mit intelligenten Messgeräten auszustatten."*[35]

Die Energie Control Austria GmbH (ECG)[36], der behördliche Regulator des österreichischen Strommarktes, hat bereits im Vorfeld der Gesetzesnovellierung das Beratungsunternehmen PricewaterhouseCoopers (PwC) mit der Durchführung einer volkswirtschaftlichen Kosten-Nutzen-Analyse beauftragt. Untersucht wurden die möglichen Auswirkungen einer Implementierung von intelligenten Zählern für Strom und Gas in Österreich.[37]

Diese Analyse spricht sich klar für eine rasche und umfassende Einführung von Smart Meter in Österreich aus.

> *„Die Ergebnisse der Kosten-Nutzen-Analyse für die Einführung von Smart Meter in Österreich zeigen, dass ein positiver Gesamteffekt (Nettoeffekt) (...) erzielt werden kann. (...) Die Kunden werden nach der Einführung von Smart Meter von einem geringeren Energieverbrauch (im Durchschnitt 3,5% im Strombereich und 7,0% im Gasbereich) sowie geringere Kosten durch effizientere Netzbetreiber, den größten Nutzen erzielen. Durch die elektronische und zeitnahe Ablesung werden die Kunden nun erstmals die Möglichkeit haben, den Energieverbrauch regelmäßig zu kontrollieren."*[38]

Dieses Ergebnis beruht im Wesentlichen auf die Analyse folgender Parameter[39]:

- Energieverbrauchsanalysen für die Kunden und damit verbundene Möglichkeiten im Bereich Energieeffizienz und -sparen.
- Neue und kundenspezifische Angebote der Stromlieferanten.
- Vorteile durch rasche Messwertübertragung und damit zeitnahe Verbrauchsinformation (Echtzeitmessungen, keine Verbrauchsschätzungen mehr für die Rechnung notwendig, etc.).
- Effizientere Prozesse der Netzbetreiber und Lieferanten, die zu geringeren Kosten für die Kunden führen (weniger fehleranfälliger Wechselprozesse, direkte Ablesung, etc.).

Weder im Bundesgesetz noch in der Analyse kommen Sicherheit, wie etwa in Form von Risiko, Risikoabschätzung, Verwundbarkeit vor. Ob daher der Anspruch, mit „dieser Studie eine umfangreiche volkswirtschaftliche Kosten-Nutzen-Analyse zu erstellen", erfüllt wurde, muss bezweifelt und damit noch im Rahmen dieser Arbeit behandelt werden.

35 BGBl. I Nr. 110/2010, S. 48.

36 „Aufgabe des Regulators ist es, den Wettbewerb zu stärken und sicherzustellen, dass dieser unter Berücksichtigung der Vorgaben der Versorgungssicherheit und Nachhaltigkeit funktionieren kann. Um im Interesse aller Marktteilnehmer handeln zu können, muss der Regulator politisch und finanziell unabhängig sein." Vgl. URL: http://e-control.at/de/econtrol/unternehmen [26.05.2011].

37 Vgl. PwC Österreich, 2010, S. 16.

38 Vgl. ebenda, S. 13.

39 Vgl. ebenda, S. 16.

2.8 Der aktuelle Status in Österreich

Derzeit sind in Österreich rund 70.000 Stromkunden im Rahmen von diversen Pilotprojekten mit Smart Meter ausgestattet. Im Generellen gilt Österreich jedoch noch als „unentschlossen". Nicht zuletzt auch wegen der ungenau definierten rechtlichen Anforderungen im ElWOG.[40] Die EnergieAG Oberösterreich hat derzeit rund 10.000 Smart Meter ausgerollt und plant eine weitere Ausrollung auf 100.000 Kunden in naher Zukunft.[41] LinzStrom hat rund 60.000 Smart Meter in Verwendung und betreibt die weitere Ausrollung von rund 200.000 Smart Meter.[42] Einige andere Energieversorgungsunternehmen (EVU) haben kleinere Pilotprojekte in Betrieb. Derzeit gibt es jedoch noch keine offiziellen Pläne für ein vollständiges Rollout.[43]

2.9 Der aktuelle Status in der EU

Die Österreichische Energieagentur veröffentlichte im Februar 2011 eine umfassende Studie über den Stand der Einführung intelligenter Zähler in allen EU-Staaten und Norwegen (siehe Abbildung 7). Einige EU-Staaten wie Finnland, Spanien oder Schweden haben bereits mit dem Zählertausch begonnen.

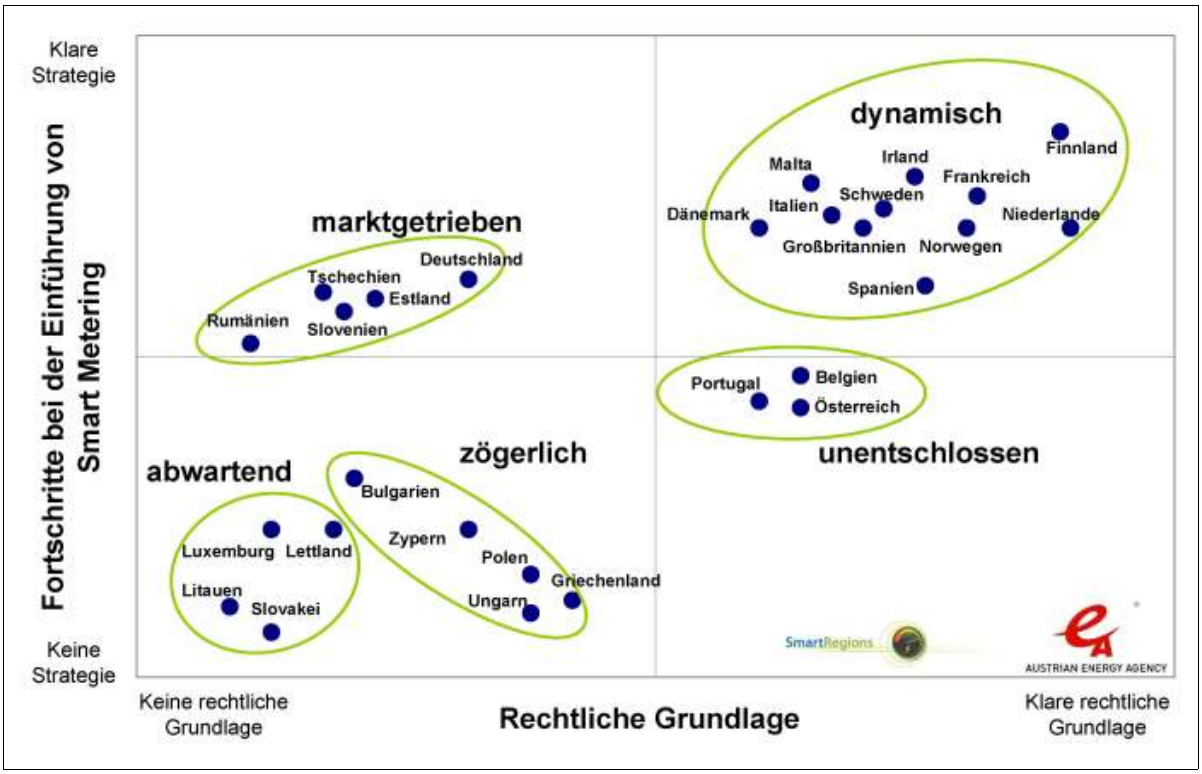

Abbildung 7: Status Smart Metering in der EU - Quelle: Österreichische Energieagentur

40 Vgl. URL: http://www.energyagency.at/presse/aktuelle-presseaussendungen-2011/presseaussendungen-detail/article/1224/chancen-und-gefahren-von-smart-metering-im-energiemarkt.html [06.06.2011].
41 Vgl. URL: http://www.e-control.at/de/konsumenten/strom/smart-meter [06.06.2011].
42 Vgl. URL: www.oecd.org/dataoecd/25/47/46137453.pdf [06.06.2011] und URL: http://www.linzag.at/portal/portal/linzag/linzag/linzag_1/presse_1/pressemeldungen_4_p_17152;jsessionid=324DA05B4D923720F0FE2A4D87F356DB.node2 [06.06.2011].
43 Vgl. Österreichische Energieagentur, 2011, S. 11.

3 Sicherheit

Sofern bisher das Thema Sicherheit im Rahmen der Smart Metering Diskussion in Österreich angesprochen wird, bezieht sich dieses in der Regel auf den Datenschutz. Das geht sogar soweit, dass damit suggeriert wird, dass damit alles abgedeckt und auch sicher ist.

> *„Datenschutzkommission hat System der Energie AG als sicher eingestuft*
>
> *Selbstverständlich stehen bei der Einführung von Smart Metering der Datenschutz und die Datensicherheit an oberster Stelle. Entsprechend den gesetzlichen Bestimmungen zum Schutz personenbezogener Daten hat die Energie AG den gesamten Datenverarbeitungsprozess im intelligenten Stromnetz - von den Smart Meters über die Datenkonzentratoren bis in das Rechenzentrum der Energie AG - von der Datenschutzkommission prüfen lassen.“*[44]

Sonstige Sicherheitsthemen in Zusammenhang mit Smart Metering existieren, abgesehen von einzelnen Ausnahmen, in der öffentlichen Wahrnehmung derzeit de-facto nicht. Eine Ausnahme stellt das Interview mit dem Sprecher des Vereins „Cyber Security Austria“[45], Paul Karrer, in der Ö1 Sendung Matrix vom 05.06.2011 dar, der u.a. besonders auf das Sicherheitsrisiko im Zusammenhang mit der Fernabschaltung hinweist.[46]

3.1 Welche Sicherheit?

Für Sicherheit gibt es je nach Anwendungsbereich unterschiedliche Definitionen. Im Bereich der IKT-Sicherheit handelt es sich eher um eine subjektive und nur sehr schwer messbare Sicherheit.

im Wesentlichen kann Sicherheit als ein Zustand gesehen werden, der frei von nicht vertretbaren Risiken oder Beeinträchtigungen ist und im technischen Bereich eine wahrscheinlich störungsfreie und gefahrlose Funktion gewährleistet.

Sicherheit ist ein dynamischer Prozess. D.h. zur Gewährleistung der Sicherheit müssen ständig die Rahmenbedingungen überprüft und bei Bedarf die Parameter angepasst werden. Dabei ist es hilfreich, folgende Grundsätze zu berücksichtigen:[47]

- Es gibt keine 100%ige Sicherheit.
- Sicherheit kann nie bewiesen werden, sondern nur Unsicherheit.
- Sicherheit ist nicht das Ziel, sondern der Weg.
- Sicherheit ist kein Eigenzweck.
- Schutzmaßnahmen sind eine Kosten-/Nutzenrechnung: Gegen wen sollen oder müssen eigene Informationen geschützt werden und was sind sie dem Eigentümer aber auch einem möglichen Angreifer Wert?
- IKT-Sicherheit wird durch Menschen, Prozesse und Technologien beeinflusst.

44 URL: http://www.energieag.at/eag_at/page/257501226587649392_0_719227280749388605,de.html [12.06.2011].
45 URL: www.cybersecurityaustria.at [12.06.2011].
46 URL: http://oe1.orf.at/programm/276276 [12.06.2011].
47 Vgl. URL: http://www.educa.ch/de/definition-sicherheit [13.06.2011].

- Aber auch, dass Schutzmaßnahmen nicht mehr kosten sollen, als der Wert des zu schützenden Gutes ist. Dabei sind aber auch subjektive und immaterielle Werte zu berücksichtigen, da der rein materielle Wert deutlich unter dem eigentlichen Wert liegen kann.

Im Gegensatz zum angloamerikanischen Raum gibt es im Deutschen so gut wie keine Unterscheidung zwischen den beiden Themen

- Angriffssicherheit (Security) und
- Betriebssicherheit (Safety).

Dies führt dazu, dass eigentlich immer wieder von unterschiedlichen Themen gesprochen, bzw. das eine oder andere vernachlässigt wird. Grundsätzlich gibt es bei den Anforderungen und Annahmen bei beiden Themen große Ähnlichkeiten. Safety-Anforderungen sind in der Regel auch Security-Anforderungen und umgekehrt. Jedoch gibt es in der Umsetzung häufig wesentliche Unterschiede. Es sind jeweils andere Konzepte gefragt. Zur besseren Verständlichkeit folgendes Beispiel. Redundanzen, beispielhaft in Form eines zweiten und dritten Steuerrechners in Flugzeugen sind elementare Instrumente in der Safety, um Ausfälle des Gesamtsystem Flugzeug zu verhindern und die Verfügbarkeit sicher zu stellen. Für die Security reicht das aber nicht aus, da damit die Integrität der übertragenen Daten nicht überprüft werden kann. Die Daten könnten während der Übertragung gefälscht oder gestört worden sein und so zu einem falschen Ergebnis führen. Daher stellen kryptographische Verfahren, wie Verschlüsselung oder Hashfunktionen, in der Security einen zentralen Mechanismus für die Integrität dar. Nur wenn die Integrität gewährleistet ist, ist auch die zuverlässige Verfügbarkeit des Systems sichergestellt.[48]

In dieser Arbeit wird generell auf die Angriffssicherheit, sprich dem Schutz vor absichtlicher Manipulation durch Menschen eingegangen, da diese häufig zu wenig berücksichtigt wird. Die Betriebssicherheit ist im generellen sehr gut etabliert und stellt häufig einen wichtigen Qualitätsfaktor dar.

3.1.1 Betriebssicherheit (Safety)

Betriebssicherheit wird oft als technische Sicherheit gesehen und mit Stichworten wie beispielsweise, Zuverlässigkeit, Ausfallwahrscheinlichkeit, Schutz von Leben und Umwelt, fehlertolerante Systeme, (Hoch)Verfügbarkeit, redundante Systeme, in Verbindung gebracht.

Betriebssicherheit konzentriert sich auf den Schutz der Umgebung vor Systemfehlern. Im Wesentlichen wird nicht von einem gezielten Angriff, sondern von zufälligen Ereignissen / Fehlern ausgegangen.[49]

3.1.2 Angriffssicherheit (Security)

Angriffssicherheit wird häufig auch mit IKT- oder Informationssicherheit ausgedrückt und mit Stichworten wie beispielsweise, Angriffe, Vertraulichkeit, Integrität, Verfügbarkeit, Spionage, Schadsoftware, Cyber-Crime, Programmierfehler, Passwörtern, Schutzprogramme in Verbindung gebracht.

48 Vgl. Freiling, 2010.
49 Ebenda.

In der Angriffssicherheit ist der Fokus auf den Schutz von Informationen und technischen Systemen vor gezielten und böswilligen Angriffen gerichtet.[50]

3.2 Sicherheit im Bereich des Ferrariszählers

Bevor aber auf die aktuellen Sicherheitsproblematiken eingegangen wird, erfolgt noch ein historischer Rückblick. Auch bei den bisher verwendeten Ferrariszähler gibt es verschiedene Angriffsmöglichkeiten, die auch ausgenutzt werden.

Methode	Lösung	Risiko	Erkennung
Zähler überbrücken	Plomben & Spezialschrauben	Abrechnungsbetrug	Siegelbruch
Gleichstrom / Kapazitive Rückspeisung	Rücklaufschutz	Abrechnungsbetrug	nicht möglich; indirekt über Statistik
Zähler überlaufen lassen	Zähler stoppt bei Maximalwert	Abrechnungsbetrug	Zähler steht; indirekt über Statistik
Magnet anlegen	Bauform, Design	Abrechnungsbetrug	verliert Kalibrierung

Tabelle 1: Angriffsvektoren auf Ferrariszähler - Quelle: IKARUS Security Software GmbH

Auch bei den Lösungsansätzen gibt es Schwachstellen, z.B. kann das entsprechende Plombenwerkzeug heute über Internet (etwa auf eBay) bezogen werden. Zu erkennen ist aber auch, dass es sich hier um reine Hardwaremanipulationen handelt und so gut wie immer Abrechnungsbetrug im Vordergrund steht. Die Manipulation wirkt sich immer nur auf den unmittelbar angegriffenen Zähler bzw. dessen Nutzer aus.

3.3 Sicherheit im Bereich von Smart Metering

Mit der Einführung von Smart Metering-Technologien entstehen im Gegensatz zu den bisher verwendeten Ferrariszählern völlig neue Risiken für die Energiewirtschaft, die Netzbetreiber und die Endkunden. Beispielsweise soll nur der Netzbetreiber beim Smart Meter des Endkunden Steueraufgaben vornehmen können. Oder der Netzbetreiber und in weiterer Folge der Energielieferant müssen davon ausgehen können, das nur gültige Daten von den Smart Metern der Endkunden gesendet werden. Einerseits, um eine richtige Abrechnung stellen und andererseits, um die richtigen Netzsteuerungsentscheidungen treffen zu können.

Von besonderer Bedeutung sind hierbei die Grundwerte der IKT- und Informationssicherheit[51], Vertraulichkeit, Integrität, Verfügbarkeit, sowie zusätzlich Authentizität und Aktualität. Die Integration von IKT in das Stromnetz ermöglicht, bisher in diesem System nicht, oder nur in eingeschränkten Bereichen mögliche, Manipulationen. Durch die bidirektionale Kommunikation sind de-facto an allen Stellen (z.B. Smart Meter, Konzentrator, Kommunikationssysteme) Eingriffe möglich. Als potentielle Angriffsziele kommen alle Bestandteile der Smart Metering Infrastruktur, d.h. die gesamte Wir-

50 Vgl. ebenda.

51 Vgl. Saurugg, 2011. S. 10.

kungskette vom Steuerungssystem beim Energielieferant, über die Netzwerkmanagementebene beim Netzbetreiber bis hin zum Smart Meter beim Endkunden in Frage.

Wie bereits im Kapitel 2 teilweise angeführt wurde, gibt es mehrere Hinweise, dass bei den Beurteilungen, welche zur Einführung und Forcierung von Smart Meter führen, nicht alle Aspekte, vor allem hinsichtlich möglicher Risiken und der Verwundbarkeit, berücksichtigt wurden. Im allgemeinen wird das Thema Smart Metering äußerst positiv und euphorisch betrachtet, Risiken jedoch so gut wie nirgends angesprochen.

Diverse Forschungsprojekte, wie etwa im Rahmen des Programms „Neue Energien 2020" des Klima- und Energiefonds[52], beschäftigen sich einerseits intensiv mit der technischen Umsetzbarkeit der verschiedenen Konzepte und andererseits auch mit rechtlichen Aspekten (z.B. Datenschutz). Eine grundsätzliche und eingehende Betrachtung aus der Sicherheitsperspektive fehlt derzeit jedoch.[53]

Im September 2010 wurde das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Entwicklung eines Schutzprofils für Smart Meter beauftragt. Dabei sollen verbindliche Sicherheitsanforderungen für den Datenschutz und der Datensicherheit erstellt werden. Die Endversion ist für September 2011 geplant. Das Schutzprofil soll vor allem für Entwickler und Erzeuger von Smart Meter als Vorgabe dienen. Darüber hinaus stellt es eine entsprechende Handlungsempfehlung für EVUs dar, die nur entsprechende Geräte zum Einsatz bringen sollten.[54] Im derzeitigen Entwurf liegt das Schwergewicht auf dem kryptografischen Schutz von Daten. Dies stellt zumindest einen wichtigen Ansatz zur Erhöhung des Smart Metering Sicherheit dar, lässt aber auch noch einige wichtige Bereiche (z.B. Sabotageschutz) offen.

> *„It should be noted that this Protection Profile does not aim to imply any concrete system architecture or product design as long as the security requirements from this Protection Profile are fulfilled."*[55]

Bedenklich ist, wenn Hersteller vorgeben, ihre Geräte seien sicher aber sich gleichzeitig über Details bedeckt halten bzw. vorgeben, gegen alles sicher zu sein, ohne das spezifizieren zu können oder zu wollen. Wie mittlerweile aus der IKT-Welt belegt ist, hat diese Taktik noch nie funktioniert, vor allem, wenn entsprechende (finanzielle) Interessen an einer Kompromittierung damit verbunden sind.

3.3.1 Mögliche Angreifer

Das BSI unterscheidet grundsätzlich zwei Arten von Angreifern:[56]

- Der Lokale Angreifer, welcher physikalischen Zugriff auf die Infrastruktur hat, aber grundsätzlich nur im lokalen, eingeschränkten Bereich agieren kann. Dieser Angreifertyp umfasst auch den Endkunden, der mit einer Manipulation in der Regel eine Begünstigung herbeiführen möchte. Nicht berücksichtigt ist hier eine, zumindest theoretische mögliche, Einbringung von Schadsoftware, welche sich dann über das LAN/WAN in das gesamte System ausbreiten könn-

52 URL: http://www.ffg.at/neue-energien-2020-das-programm [05.06.2011].
53 Vgl. Klima- und Energiefonds, 2011.
54 Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2011.
55 Ebenda, S.12.
56 Vgl. ebenda, S. 31.

te. Dieser Angreifer lässt sich mit dem bisherigen Angreifer gleichsetzen, wenngleich es sich nicht mehr um reine Hardwaremanipulationen handelt.

- Der WAN Angreifer, welcher mit seinem Angriff aus der Ferne auf die Vertraulichkeit und/oder Integrität der übermittelten Daten abzielt und auf größeren Profit aus ist. Dieser Angreifer war de-facto in den bisherigen Bereichen nicht vorhanden und ist eigentlich nur aus der IKT-Welt bekannt.

3.3.2 Mögliche Ziele eines Angreifers

Derzeit können zwei wesentliche Ziele einer Manipulationen abgeleitet werden:

1. Abrechnungsbetrug (→ Betrug)
2. Eingriff in die Netzwerksteuerung (→ Sabotage, Erpressung)

Die Bedrohungen reichen von einfachen lokalen Manipulationen in der Datenkommunikation und gehen bis zur völligen Sabotage des Netzes durch Einbringung von destruktiver Schadsoftware. Die Datenmanipulation in größeren Netzsegmenten könnte durch einen Angriff auf die Integrität und Vertraulichkeit auch zu Erpressungsversuchen führen. Exemplarisch, wenn das Erpressungsgeld nicht bezahlt wird, dann werden die Daten bloßgestellt oder die Datenintegrität kompromittiert, was einen erheblichen wirtschaftlichen Schaden nach sich ziehen würde.

Die Manipulation kann im Wesentlichen durch

1. ändern,
2. löschen,
3. einspielen,
4. wiederholen oder
5. umleiten

von Daten erfolgen.

Der wesentliche Unterschied zu bisherigen Angriffen in der IKT stellt die enge Vernetzung zwischen physischer Infrastruktur und der IKT dar, welche vor allem erhebliche Folgen für die in allen Lebensbereichen unverzichtbare Energieversorgung nach sich ziehen könnte.

Nachdem durch Smart Meter eine Fernablesung erfolgt, ist eine Hardwaremanipulationen durch etwa ein Ableseorgan, nicht möglich. Derartige Manipulationen bleiben daher fast ausschließlich dem Zufall überlassen.

3.4 Mögliche Angriffsvektoren und Schwachstellen

Ein Angriffsvektor stellt einen Weg oder eine Technik dar, die zur Kompromittierung der verarbeiteten Daten in einem Zielsystems führen kann.

In diesem Abschnitt wird versucht, verschiedene Angriffsvektoren und Schwachstellen darzustellen. Dabei besteht kein Anspruch auf Vollständigkeit.

3.4.1 Generelle Herausforderungen

Im Vergleich zu den bisherigen einfachen, elektromechanischen Ferrariszähler, stellen Smart Meter, aufgrund der Architektur, enorme Herausforderungen an die Hersteller dar.

Darunter fallen[57]:

- Digitale Messsysteme sind kleine Computer. Daher muss von einer ähnlich hohen Verwundbarkeit, wie die derzeit im IKT Bereich eingesetzten System, ausgegangen werden.
- Durch Störungen und externe Einflüsse können Computer abstürzen. Diese können zufällig auftreten (z.B. größere Sonnenaktivitäten CME[58]), oder ganz gezielt durch Manipulation (z.B. mit EMP[59]) herbeigeführt werden. Entsprechende Geräte können über das Internet erworben werden.[60]
- Bei einem schwerwiegendem Hard- oder Softwarefehler muss unter Umständen die gesamte Hardware ausgetauscht werden, was erhebliche wirtschaftliche Folgen nach sich ziehen würde.

Zusätzlich kommen marktwirtschaftliche Parameter hinzu:

- Ein Smart Meter ist ein relativ einfaches Gerät. Der Verkauf kann daher im Wesentlichen nur durch die Preisgestaltung bzw. durch Einbindung in ein Gesamtsystem gesteuert werden. Das führt dazu, dass möglichst einfache und preisgünstige Komponenten verbaut und sich diese auf das unbedingt erforderliche Mindestmaß beschränken werden. Darüber hinaus muss eine starke Homogenisierung erfolgen, um möglichst billig produzieren zu können.
- Wie in der IKT-Welt muss zur Kostensenkung modulare Software eingesetzt werden, welche viel mehr Funktionen aufweist, als der jeweilige Betreiber benötigt. Die nicht benötigten oder bezahlten Funktionen werden softwaremäßig deaktiviert. Eine Aktivierung könnte durch einen Angreifer möglich sein.
- Die Vorgaben und Fokus ist primär auf ein geeichtes, korrekt zählendes System und auf den Datenschutz gerichtet.
- Immer wieder entsteht der Eindruck, dass in vielen, vor allem nicht technischen Bereichen, mangelndes Verständnis bzw. Interesse für das Gesamtsystem bzw. der Sicherheitsproblematiken im IKT-Bereich vorherrschen. Angriffe auf IKT-Hardware scheinen derzeit so gut wie nicht bekannt.[61]
- Häufig fehlt es an einem interdisziplinärem Verständnis zwischen Hard- und Softwareentwicklung. Die Auslagerung von einzelnen Prozessen verschärft zusätzlich die Situation.
- Dieser spezielle Anwendungsbereich ist noch relativ neu. Daher ist die Anzahl der Programmierer mit Erfahrung wahrscheinlich noch nicht sehr hoch.

57 Vgl. Vortrag „Smart Meter“ durch IKARUS Security Software GmbH am CERT.at IT-Security Stammtisch vom 11.05.11.

58 Coronal Mass Ejection.

59 Elektromagnetischer Puls; Ein einmaliger kurzzeitiger, hochenergetischer, breitbandiger elektromagnetischer Ausgleichsvorgang mit hoher Zerstörungswirkung bei elektrischen Anlagen durch Überspannung; vgl. NEMP bei einer Nuklearexplosion.

60 Vgl. URL: http://www.amazing1.com/emp.htm [19.06.2011].

61 Vgl. Angriffe auf SCADA (Supervisory Control and Data Acquisition) Systeme bzw. die Schadsoftware STUXNET; Saurugg, 2011, S. 13ff.

3.4.2 Smart Meter Hardware

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.

In einer amerikanischen Studie ist es gelungen, Daten aus dem Speicher von Smart Meter auszulesen und zur Einbringung von Schadsoftware zu manipulieren. Dabei wurden auch Schlüssel, welche zur Authentifizierung im Netzwerk verwendet wurden, ausgelesen.[62]

Z.T. sind Smart Meter bereits jetzt über Internet für jedermann beziehbar (siehe Abbildung 8) und ermöglichen dadurch eine ungestörte Analyse, zumindest der Geräte des jeweiligen Herstellers.

Abbildung 8: Smart Meter auf eBay zu erwerben - Quelle: Screenshot 11.06.11

Wenn derzeit auch nicht die Geräte vieler Hersteller verfügbar sind, durch eine reguläre Verbreitung wird aber auch der entsprechende Schwarzmarkt dazu steigen. Der Diebstahl von in Betrieb befindlichem Gerät fällt mit Sicherheit auf. Aber was ist bei Katastrophenszenarien, wie etwa nach einem Erdbeben oder einer Überschwemmung, wo möglicherweise haufenweise Smart Meter in zerstörten Regionen frei zugänglich werden?

Die bisherige eingeschränkte Analyse von Hardware hat zu Tage geführt, das Smart Meter fehlende oder nur unvollständige Sabotageeinrichtungen aufweisen. Darüber hinaus scheint es mehrere Angriffsverfahren zu geben, um den Smart Meter zu zerstören, den Stromfluss jedoch aufrecht zu erhalten. Beispielsweise Manipulation der Hardware mittels Einbringung eines Gegenstandes in den Card Slot für Chipkarten (für Pre-Paid Systeme), oder Bestrahlung mittels einer offenen Mikrowelle, um die Elektronik zu zerstören. Das Zählsystem muss geeicht sein, was auch vor der Ausrol-

62 Vgl. U.S. Department of Energy, 2009, S. 11.

lung überprüft wird. Jedoch erscheint nicht sichergestellt, dass danach keine Manipulationen erfolgen können.[63]

Wie aber auch aus der IKT-Welt bekannt ist, gibt es de-facto keine massentaugliche Hardware, deren Schutzeinrichtungen bisher nicht umgangen werden konnten. Als Beispiele seien hier nur das iPhone, digitale Tachometer, verschiedene Kopierschutzverfahren oder die Möglichkeit SIM-Karten zu duplizieren bzw. die Netzsperre aufzuheben, angeführt.

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.

3.4.3 Smart Meter Software

In der IKT-Welt gibt es keine fehlerfreie Soft- und Hardware. Je komplexer ein System wird, desto höher ist die Wahrscheinlichkeit, dass entsprechende Schwachstellen vorhanden sind. Daher rechnet man grundsätzlich damit, dass pro 1.000 Softwarecodezeilen (LOC) ein unkritischer und pro 10.000 Softwarecodezeilen ein kritischer Fehler enthalten ist.[64]

Besonders ist dabei zu berücksichtigen, dass eine Softwaremanipulation nur sehr schwer nachzuweisen ist. Darüber hinaus sind Softwareangriffe in der Regel nach einer aufwändigeren Entwicklung relativ einfach massentauglich zu machen und dann billig zu verbreiten. Ein Softwareupdate auf ausgerollten Smart Meter stellt wahrscheinlich eine erhebliche Herausforderung dar. Einerseits was den logistischen Aufwand betrifft und andererseits, was die Sicherheit betrifft. Sicherheit im Sinne von, dass es zu keinen Fehlfunktionen kommt oder, dass keine falschen Updates eingespielt werden können. Darüber hinaus könnte eine bereits vorhandene Schadsoftware verhindern, dass neue Softwareupdates eingespielt werden kann.

Eine der wahrscheinlich größten Risiken geht derzeit von der geplanten Abschaltfunktion aus der Ferne aus. Sollte es einem Angreifer gelingen, dieses Steuersignal unautorisiert zu senden oder mittels Schadsoftware zu verbreiten, so könnten innerhalb sehr kurzer Zeit sehr viele Smart Meter vom Netz genommen werden, was in der Folge, bei einer entsprechend hohen, gleichzeitigen Anzahl, auch zu einem Blackout[65] führen könnte.

Es ist ein Beispiel im Bereich digitale Zähler bekannt, wo dieser nach einer Datumsfehlberechnung irreversible abgestürzt ist und ein Hardwaretausch erfolgen musste. Sollte es gelingen, Smart Meter durch Manipulation oder Störungseinflüsse in eine ähnliche Situation zu bringen, dann könnte dies erhebliche Folgen nach sich ziehen. Bei einem gleichzeitigen Ausfall einer hohen Anzahl von Geräten würde dies eine erhebliche logistische Herausforderung darstellen. Einerseits, was die Bereitstellung von Ersatzgeräten betrifft und andererseits den Austausch der Geräte durch Fachkräfte vor Ort. Zusätzlich muss angenommen werden, dass Ersatzgeräte auch über

63 Vgl. Vortrag „Smart Meter“ durch IKARUS Security Software GmbH am CERT.at IT-Security Stammtisch vom 11.05.11.

64 Vgl. URL: http://www.dlr.de/fs/Portaldata/16/Resources/dokumente/vk/Vortrag_Hase_091203.pdf [22.06.2011].

65 Vgl. Kapitel *Mögliche Folgen eines plötzlichen, langandauernden und großflächigen Stromausfalls.*

die ausgenutzte Schwachstelle verfügen und sofort nach Installation ebenfalls betroffen oder infiziert und damit unbrauchbar werden. Die betroffenen Endkunden müssten sich wahrscheinlich auf einen längerfristigen Stromausfall und die Netzbetreiber auf erhebliche Kosten einstellen.[66]

3.4.4 Smart Meter Schnittstellen

Im Bereich von Smart Metering / Smart Meter sind zahlreiche Datenschnittstellen vorgesehen.[67] Vor allem mit den Funkschnittstellen (beispielsweise GSM, WLAN, M-Bus, ZigBee) soll eine einfachere und flexiblere Vernetzung ermöglicht werden.

> *„Every communication path that supports monitoring and control of the Smart Grid is a two-way communication path as shown in Figure 1. Each communication path is a potential attack path for a knowledgeable attacker. There are many potential entry points physically unprotected. Wireless networks can be easily monitored by attackers and may be susceptible to Man-in-the-Middle (MitM) attacks."*[68]

Diese Schnittstellen, sofern sie nicht mit kryptografischen Verfahren abgesichert werden, bieten zahlreiche Ansätze für eine Kompromittierung der Daten. Insbesondere die Funkschnittstellen ermöglichen einen Angriff, ohne dass der Angreifer unmittelbar Zugang zur Hardware haben muss. Eine Analyse des versendeten Datenstroms wird dadurch stark vereinfacht, was wiederum einen Angriff wesentlich erleichtert. Hinzukommt, dass mittels eines DoS-Angriffes[69] oder Jamming[70] die Verbindung jederzeit gestört werden kann.

Auch das Display am Smart Meter, wie auch die Fernanzeige in einem Internetportal, stellt eine Schnittstelle dar. Der Endkunde muss sich auf die Anzeige verlassen (können). Wie die Schadsoftware STUXNET gezeigt hat, ist die Manipulation der Anzeige durch Schadsoftware durchaus machbar, ohne das dies einfach erkannt werden kann.[71]

3.4.5 Kryptografische Verfahren

Kryptografische Verfahren, z.B. zur Verschlüsselung der Daten oder zur Authentifizierung der Netzwerkkomponenten oder des Wartungspersonals, sollten grundsätzlich einen erheblichen Sicherheitsgewinn für die Smart Metering Infrastruktur darstellen.

Jedoch darf dabei nicht übersehen werden, dass damit auch eine weitere Komplexität und dadurch zusätzliche Angriffsvektoren geschaffen werden. Kryptografische Verfahren erfordern ein entsprechendes Schlüsselmanagement, was bei einer unüberschaubaren Anzahl von Geräten in ungesicherten Bereichen eine enorme Herausforderung darstellt.[72] Eine mangelhafte Implementierung führt daher wahrscheinlich zu

66 Vgl. Vortrag „Smart Meter" durch IKARUS Security Software GmbH am CERT.at IT-Security Stammtisch vom 11.05.11.

67 Vgl. Abschnitt *Netzwerkkommunikation (Kommunikation).*

68 Vgl. U.S. Department of Energy, 2009, S. 12.

69 Denial of Service = Überlastung von Systemen durch eine massive Anzahl von parallelen Anfragen, welche das Zielobjekt massiv belasten, verlangsamen oder sogar zum Absturz bringen können.

70 Störung der Kommunikation mittels Störsignalen

71 Vgl. Saurugg, 2011, S. 15.

72 Vgl. U.S. Department of Energy, 2009, S. 11.

einem erheblichen Mehraufwand. Fragen wie, wie kann ein kompromittiertes Schlüsselmanagement wiederhergestellt werden, müssen bereits vor der Implementierung geklärt sein. Sonst kann das dazu führen, dass die gesamten Endgeräte im Anlassfall getauscht werden müssen, da sie beispielsweise keine vertrauenswürdigen Daten mehr liefern.

Auch direkte Angriffe auf Verschlüsselungsalgorithmen können nicht ausgeschlossen werden. Exemplarisch wurde auch der GSM-Verschlüsselungsalgorithmus A5/1 kompromittiert.[73]

> *„There are security mechanisms in place intended to prevent unauthorized use of these communication paths, but there are weaknesses in these mechanisms. The history of security in complex networks implies that more vulnerabilities exist and are yet to be discovered."*[74]

3.5 Sicherheit im Bereich Smart Grid

Um zu verdeutlichen, dass Sicherheitsproblematiken nicht nur im Bereich von Smart Metering zu finden sind, sollen in diesem Abschnitt ein paar Beispiele für die übergeordnete Ebene angeführt werden.

3.5.1 SCADA Systeme

Supervisory Control and Data Acquisition (SCADA) Systeme werden heute in sehr vielen Bereichen zur Automation, Überwachung und Steuerung von technischen Prozessen mittels Computer eingesetzt. Daher spielen sie eine wichtige Rolle bei der Verwirklichung von Smart Grids. Bisher galten SCADA Systeme als sicher, da sie im Wesentlichen in sicheren Umgebungen betrieben wurden. Angriffssicherheit (Security) spielte im Gegensatz zur Betriebssicherheit (Safety) bisher kaum eine Rolle. Durch das Zusammenwachsen von diesen Systemen mit hochgradig unsicheren IKT-Systemen ergibt sich aber eine völlig neue Situation. Ein besonders eindrucksvolles Beispiel wurde mit der Schadsoftware STUXNET geliefert.[75]

Es ist davon auszugehen, dass das nicht der einzige Vorfall bleiben wird und in naher Zukunft weitere Schwachstellen bekannt bzw. Vorfälle auftreten werden.[76]

SCADA Systeme kommen vor allem in der Netzwerksteuerung, wie etwa bei den Transformatorstationen oder Umspannwerken für die Automation zum Einsatz, aber auch beim Energieerzeuger (Kraftwerk).

> *„The level of automation in substations is increasing. Level of automation is indirectly related to security because increased automation implies increased computer-controlled electronics and software, which tends to increase the potential for cyber security weaknesses. Increased automation does not necessarily imply reduced security; however, the study identified many vulnerabilities associated with substation automation devices and described the potential consequences of exploitation of substation vulnerabilities. Potential consequences of successful sub-*

73 Vgl. URL: http://www.zdnet.de/news/41525048/t-print/26c3-deutscher-hacker-knackt-gsm-verschluesselung.htm [19.11.2011].

74 Vgl. U.S. Department of Energy, 2009, S. 12.

75 Vgl. Saurugg, 2011, S. 13ff.

76 Vgl. U.S. Department of Energy, 2009, S. 2.

station cyber attacks include the destruction of generators, power outages, and grid instability."[77]

3.5.2 Kommunikations- und Steuersysteme

Für die Datenkommunikation zwischen den verschiedenen Einrichtungen werden häufig, die aus der IKT-Welt stammenden Protokolle wie beispielsweise, das Transmission Control Protocol (TCP)/Internet Protocol (IP), Hypertext Transfer Protocol (HTTP), oder File Transfer Protocol (FTP) eingesetzt. Viele Sicherheitsprobleme aus der IKT-Welt sind direkt oder indirekt mit diesen Protokollen in Verbindung zu bringen.

Durch die zunehmende Verbindung verschiedener, bisher in der Regel offline betriebener Systeme mit dem Internet, werden die Risiken erheblich gesteigert. Durch die massiven Auswirkungen werden diese Angriffsziele auch erst für Angreifer interessant und wahrscheinlich in absehbarer Zukunft ausgenützt werden.[78]

3.6 Manipulationsmöglichkeiten auf den Finanzmärkten

Dass es beim Thema Smart Metering Sicherheit nicht zwangsläufig nur um technische Themen gehen muss, sollen nachfolgende Abschnitte verdeutlichen.

Bei Angriffen auf Strategische Infrastrukturen, insbesondere im Bereich der Energieversorgung, könnten Finanzmärkte eine ganz zentrale Rolle spielen.

Nach dem Zusammenbruch der Immobilienblase in den USA, 2008, und der damit ausgelösten weltweiten Wirtschaftskrise wurde durch viele Regierungen versprochen, eine derartige Situation zukünftig verhindern zu wollen und entsprechende Maßnahmen für die Finanzmärkte zu beschließen.[79] Drei Jahre nach dem Beginn der Krise gibt es nach wie vor keine entsprechenden Abkommen und ganz im Gegenteil, es gibt bereits wieder Anzeichen von neu entstehenden Börsenblasen.[80]

Eine ganz besondere Rolle spielen dabei die sogenannten Verkaufsoptionsschein (Put) auf fallende Kurse.

„Hier erwirbt der Käufer das Recht, einen Basiswert – etwa eine Aktie, einen Index oder eine Währung– zu einem vorher festgelegten Preis (Basispreis) während der Laufzeit (amerikanischer Optionstyp) oder bei Fälligkeit (europäischer Optionstyp) zu verkaufen. Dafür zahlt er dem Verkäufer, i.d.R. dem Emittenten, vorab eine Prämie. Der Anleger wird sein Verkaufsrecht natürlich nur solange in Anspruch nehmen, wie er den Basiswert über seinen Optionsschein teurer verkaufen kann, als über die Börse. Andernfalls verzichtet er auf die Wahrnehmung seines Optionsrechts. Auch die Verkaufsoption ist somit ein Recht, aber keine Verpflichtung.

Put-Inhaber profitieren also von einem Kursverfall des Basiswertes.

77 Vgl. ebenda.
78 Vgl. ebenda, S. 2f.
79 Vgl. URL: http://www.welt.de/politik/article3253020/Merkels-Krisenstrategie-ueberzeugt-Europa.html [21.06.2011].
80 Vgl. URL: http://www.handelsblatt.com/finanzen/boerse-maerkte/anlagestrategie/das-finanzsystem-hat-krebs/v_detail_tab_print,3340418.html [21.06.2011].

Beispiel: Angenommen die Aktie der Muster AG notiert bei 100 Euro. Der Put auf die Aktie der Muster AG soll einen Basispreis von ebenfalls 100 Euro haben und 10 Euro kosten. Am Laufzeitende hat der Put einen positiven Wert, sollte die Aktie unter 100 Euro notieren. Einen Gewinn erzielt der Put-Inhaber aber erst, wenn die Aktie unterhalb von 90 Euro schließt. Wie beim Call ist der Verlust auf die gezahlte Optionsprämie begrenzt. Ein Totalverlust entsteht am Laufzeitende bei Kursen oberhalb von 100 Euro (siehe nachfolgende Grafik / Abbildung 9).

Die Hebelwirkung entsteht auch hier durch den geringeren Kapitaleinsatz im Vergleich zu einem Leerverkauf der Aktie. Fällt die Aktie der Muster AG bis zum Laufzeitende von 100 auf 80 Euro, verliert der Titel 20%. Bei einem solchen Kursverfall legt der Put-Optionsschein von 10 auf 20 Euro zu, was einen Gewinn von 100% bedeutet."[81]

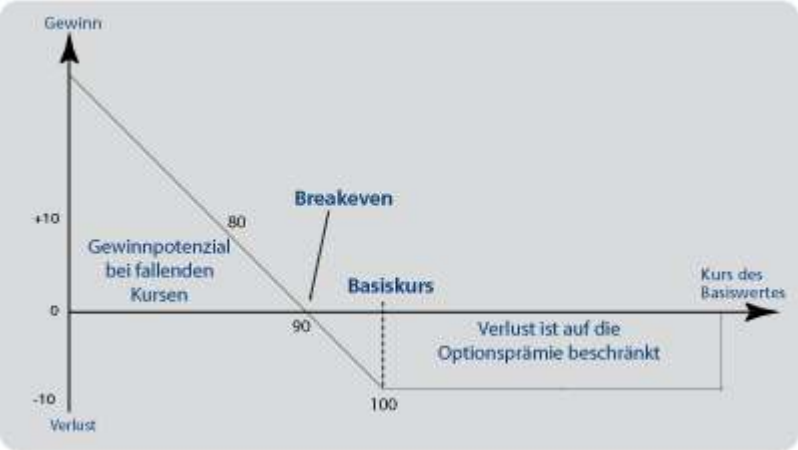

Abbildung 9: Beispiel für einen Verkaufsoptionsschein (Put) - Quelle: https://www.boerse-stuttgart.de

Mit dieser Börsenoption kann in sehr kurzer Zeit sehr viel Geld „erwirtschaftet" werden. Derartige Praktiken wurden bereits in Zusammenhang mit großen Terroranschlägen kolportiert.[82]

Wird ein aktuelles Beispiel, wie der Angriff auf das Sony PlayStation Network herangezogen, kann sehr gut das Gewinnpotential dargestellt werden. Am 27.April 2011 wurde offiziell von Sony bekannt gegeben, dass es einen groß anlegten Angriff auf das Spielkonsolennetzwerk von Sony gegeben hat. In weiterer Folge wurde davon ausgegangen, dass wahrscheinlich weit über 100 Millionen Kundendaten gestohlen wurden. In der Folge kam es zu massiven Kurseinbrüchen bei den Sony Aktien (siehe Abbildung 10).

81 URL: https://www.boerse-stuttgart.de/de/marktundkurse/hebelprodukte/optionsscheine/basiswissen/grundlagen.html [21.06.2011].

82 Vgl. Dr. Johann König. Die Finanzen des Osama Bin Laden, in: Frankfurter Rundschau, 26.03.2004, S. 4. *„Bin Laden griff neben den Investition im Sudan auch zu anderen Mitteln der Finanzierung. So spekulierten zahlreiche Banken in seinem Auftrag an den Börsen, z.T. mit Insiderinformationen hinsichtlich bevorstehender Anschläge und damit der sicheren Aussicht auf fallende Kurse. Mit Hilfe von Put-Optionen konnten so immense Gewinne erzielt werden."* .

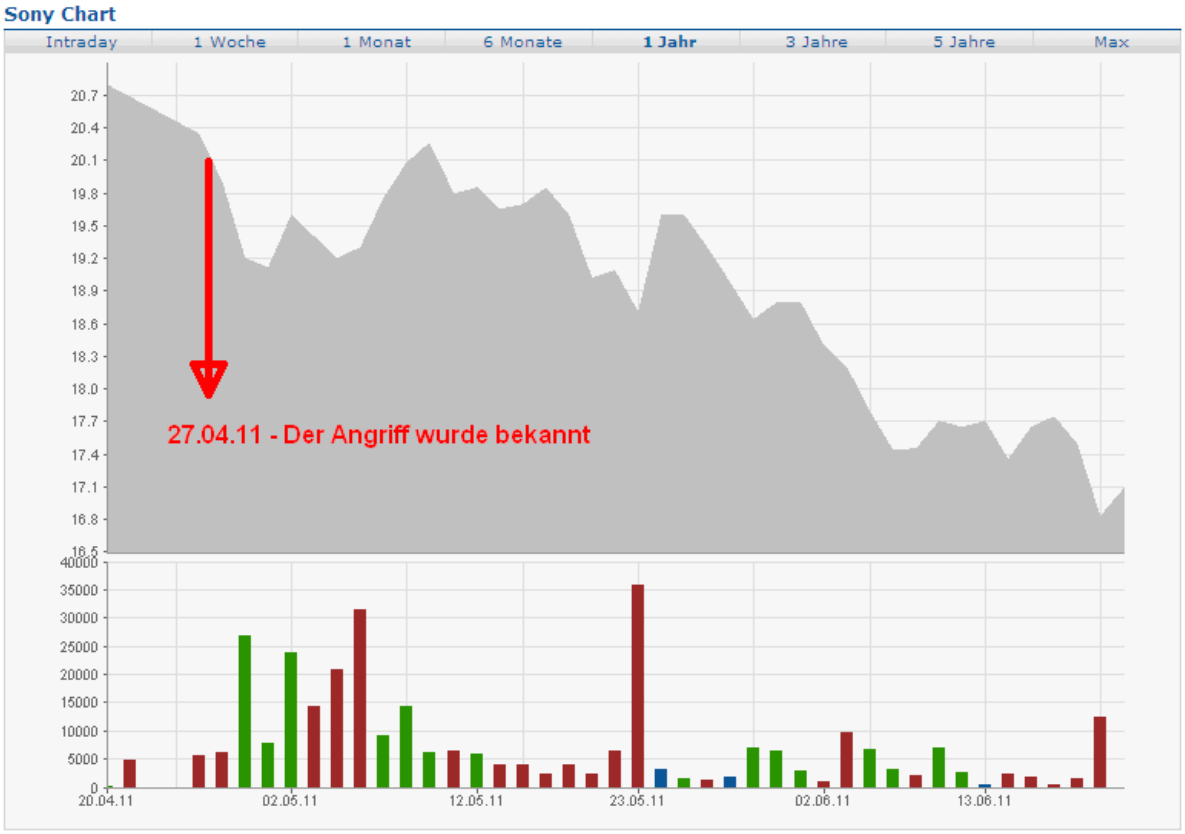

Abbildung 10: Kursentwicklung der Sony Aktien im Zeitraum 20.04.11 - 21.06.11 - Quelle: http://www.finanzen.net/chart/Sony

Derartige Szenarien sind daher auch für den gegenständlichen Sachverhalt nicht aus der Luft gegriffen. Die Hersteller und Netzbetreiber der Smart Grid / Metering Infrastrukturen sollten sich dieser Bedrohungen bewusst sein. Aber auch Staaten, denn letztendlich bezahlen schwerwiegenden Folgen so gut wie immer die Bürger, wie das aktuell nach der Atomkatastrophe von Japan, bei den diversen Bankenrettungspaketen oder im Fall von Griechenland zu beobachten ist, sollten sich mit dieser Bedrohung auseinandersetzen..

3.7 Erpressungsversuche

Ein anderes, mögliches Szenario stellen Erpressungsversuche dar. Sollte ein Netzbetreiber vor die Wahl gestellt werden, entweder er bezahlt einen bestimmten, verschmerzbaren Betrag oder die Daten von Smart Meter werden z.B. manipuliert und unbrauchbar gemacht (siehe Abbildung 11), beginnt der Teufelskreis. Wenn das ganze Szenario mit Beispielen untermauert werden kann, werden wahrscheinlich viele Netzbetreiber bereit sein, zu zahlen. Damit entsteht eine noch größere Abhängigkeit und die Opfer können nur mehr verlieren.

Die besondere Schwierigkeit wird auch darin liegen, Behauptungen in sehr kurzer Zeit auf Plausibilität zu prüfen. Es könnte sich natürlich auch um eine Täuschungsaktion handeln.

Nicht ausgeschlossen werden kann, dass derartige Praktiken auch zur öffentlichen Diffamierung von bestimmten marktführenden Herstellern ausgenutzt werden.

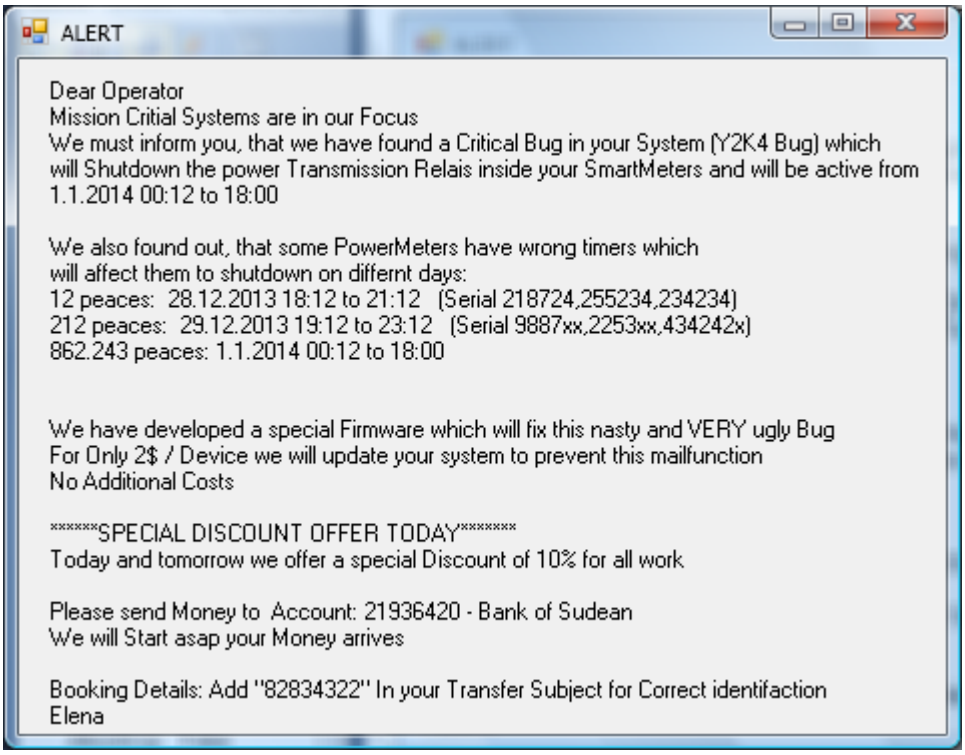

Abbildung 11: Beispiel für eine mögliches Erpressungsszenario - Quelle: Ikarus Security Software GmbH

Daher sollten sich Hersteller und Netzbetreiber ebenfalls im Vorfeld mit derartigen Szenarien auseinandersetzen und auf mögliche Erpressungsversuche vorbereiten.

3.8 Wirtschaftliche Zwänge

Natürlich muss davon ausgegangen werden, dass kein Hersteller oder Netzbetreiber daran interessiert ist, ein leicht verwundbares System bereit zu stellen. Dabei darf aber nicht vergessen werden, dass es einen enormen wirtschaftlichen Druck und entsprechende Zwänge (Gesetze) zur Umsetzung gibt.

Dadurch werden leicht Sicherheitsanforderungen übersehen bzw. bekommen nicht die entsprechende Priorität. In der Geschichte der IKT gibt es dafür unzählige Beispiele (SMTP[83], VoIP[84], WLAN, u.v.m).

Darüber hinaus handelt es sich um hochkomplexe Zusammenhänge, die wahrscheinlich nur in einem interdisziplinären Ansatz erfassbar sind. Viele Auswirkungen können erst in der Zusammenschau erkannt werden, bzw. wirken sich diese erst im Gesamtsystem aus.

3.9 Internationaler Terrorismus

Grundsätzlich hat Smart Metering mit Terrorismus nichts zu tun. In der Gesamtbedrohungsanalyse sollte aber auch dieses Thema nicht ausgeschlossen werden. Der heute verbreitete internationale Terrorismus strebt öffentlichkeitswirksame Aktionen an, in der Regel durch spektakuläre Tötung von Menschen. Vielfach wird daher angenom-

83 Simple Mail Transfer Protocol.
84 Voice over Internet Protokoll.

men, dass Cyber-Terrorismus derzeit noch kein Thema ist, da diese Bilder mit Cyber-Angriffen schwer zu erzeugen sind.

Zumindest in der aktuellen Medienberichterstattung wird aber immer häufiger davor gewarnt.[85] Wie seriös diese Aussagen sind, kann derzeit nicht beurteilt werden.

Zu bedenken ist, dass aufgrund der vielschichtigen Verwundbar- und Abhängigkeit einer modernen Gesellschaft, mit einem Angriff auf die Stromversorgung wahrscheinlich erhebliches Aufsehen erregt werden könnte. Besonders hervorzuheben ist die Breitenwirkung. Bei einem konventionellen Terroranschlag bleiben die Primärfolgen meist lokal begrenzt. Bei einem erfolgreichen Angriff auf die Stromversorgung könnte eine wesentlich höhere Betroffenheit erzielt werden.

3.10 Koronaler Massenauswurf (KMA/CME)

Zum Schluss dieses Kapitels wird noch ein Sonderbereich, welcher sich sowohl auf die Betriebs- als auch auf die Angriffssicherheit auswirken kann, angerissen, der Koronale Massenauswurf (KMA) oder engl. Coronal Mass Ejection (CME). Hierbei handelt es sich um eine Sonneneruptionen, bei der Plasma ausgestoßen wird. Dabei werden auch große Mengen an Energie freigesetzt, welche z.B. Schäden an Satelliten, Störungen im Funkverkehr (inkl. GPS Navigation) oder im schlimmsten Fall Blackouts verursachen können. Die letzte große Sonneneruption erfolgte am 07.Juni 2011. Die Erde wurde jedoch nicht direkt von der ausgestoßenen Energie getroffen, daher kam es zu keinen nennenswerten Zwischenfällen.[86]

Am 14.März 1989 war dies anders. Der Sonnensturm verursachte in Kanada ein 9 stündiges Blackout, von dem 6 Millionen Menschen betroffen waren. Dabei wurden Stromnetze und elektrische Geräte zerstört.[87]

Die NASA erwartet in den nächsten Jahren erhöhte Sonnenaktivitäten.

> *„As the sun becomes more active, these storms become much more frequent. Most of the time they completely miss the Earth. But once and a while, the Earth happens to be in the wrong place at the wrong time. And when that happens, you wind up with communications difficulties with satellites, you wind up with blackouts on the ground, and you can even wind up with health problems if you happen to be an astronaut orbiting in space."*[88]

Die Wirkung des CME im Kleinen kann durch EMP verursacht werden. Im Bereich Betriebssicherheit ist vor allem der Schutz vor unbeabsichtigten Störstrahlungen anzuführen.

3.11 In dieser Arbeit nicht berücksichtigt

In dieser Arbeit wurde der Fokus auf mögliche Auswirkungen auf die nationale Sicherheit gelegt, daher sind einige, vor allem für die EVUs relevante Bereiche, nicht näher

85 Vgl. URL: http://www.gulli.com/news/cyber-terrorismus-bundesinnenminister-f-rchtet-virtuelle-bomben-2011-05-23 [23.06.2011].

86 Vgl. URL: http://www.welt.de/wissenschaft/article13418284/Sonnensturm-droht-weltweit-Stromnetze-lahmzulegen.html [19.06.2011].

87 Vgl. URL: http://sunearth.gsfc.nasa.gov/podcasts/media/Blackout_part1.htm [19.06.2011].

88 Vgl. ebenda.

beleuchtet worden. Für eine Gesamt- bzw. vor allem wirtschaftliche Betrachtung dürfen diese Bereiche aber nicht außer Acht gelassen werden.

Die betrifft insbesondere die Themenbereiche

- Risikiobewertung und Bilanz Rückstellungen
- Abrechnungsbetrug bei Pre-Paid Systemen
- Abrechnungsbetrug generell
- Stromdiebstahl[89]
- Softwarezulassungen[90]

89 Vgl. „Energy Theft in the Advanced Metering Infrastructure“ - URL: http://www.patrickmcdaniel.org/pubs/critis09.pdf [29.06.2011] .

90 Vgl. URL: http://www.welmec.org/latest/guides/72.html [29.06.2011].

4 Blackout

Ein plötzlicher, langandauernder und großflächiger Stromausfall wird häufig auch mit dem englischen Begriff „Blackout“ beschrieben. Besonders bekannt wurde der Begriff mit den großen Stromausfällen in den USA (2003) und in Europa (2006), wo davon Millionen Menschen betroffen waren.

Das Elbe- und Oderhochwasser 2002/2005, das Schneechaos im Münsterland 2005 sowie der Orkan Kyrill 2007 führten dazu, dass in Deutschland das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) mit der Erstellung einer Studie[91] beauftragt wurde. Ziel war die Feststellung, wie sich ein langandauernder und großflächiger Stromausfall auf besonders kritische Infrastrukturen wie z. B. Trinkwasser, Abwasser, IKT-Systeme, Finanz- und Gesundheitsdienstleistungen auswirken könnte, insbesondere im Fall eines Kaskadeneffekts über Länder und nationale Grenzen hinweg, wie es u.a. beim großen europäischen Blackout 2006 der Fall war. In diesem Fall war die Ursache eine falsche Berechnung der Netztechniker. Dabei wurde eine Höchstspannungsleitung über den Fluss Ems abgeschaltet, um einem Kreuzfahrtschiff die Durchfahrt zu ermöglichen. Dabei wurde das Netz ungeplant so stark überlastet, dass schließlich in halb Europa das Stromnetz für z.T. mehrere Stunden zusammenbrach.[92]

Fast alle Strategischen Infrastrukturen[93] hängen wesentlich von einer funktionierenden Stromversorgung ab. Großflächige und längerfristige Stromausfälle würden daher massive Auswirkung auf diese herbeiführen und schwerwiegende Folgen für das gesellschaftliche Leben nach sich ziehen. Die Studie kommt sogar zum Schluss, dass „Betroffen wären alle Kritischen Infrastrukturen, und ein Kollaps der gesamten Gesellschaft wäre kaum zu verhindern.“[94]

Auch in Österreich liegt seit Anfang 2010 eine regionale Studie[95] für Niederösterreich vor, welche zu einem ähnlichen, wenn nicht noch bedrohlicherem Ergebnis kommt.

> *„Bei einem großen, überregionalen Stromausfall ist nach ca. 6 - 8 Stunden nach Ereigniseintritt mit einer zunehmenden Absenz der helfenden und ordnenden staatlichen Macht zu rechnen. Nach ca. 24 Stunden tritt sukzessive eine Situation ein, die zu Chaos und Anarchie und somit zu einem Zusammenbruch unseres Gemeinwesens und unserer Gesellschaftsform führen kann. Zur Abwendung dieser Gefahren kommt der Aufrechterhaltung der Treibstoffversorgung (Benzin, Diesel) zumindest im Notbetrieb die zentrale Bedeutung zu.“*[96]

Bisher gibt es, im Sinne von Risikoabschätzung und Präventivmaßnahmen, kaum Vorkehrungen, welche einer derart massiven Bedrohung für eine moderne, von der Stromver-

91 Vgl. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011.

92 Vgl. URL: http://www.stromvergleich.de/stromnachrichten/3573-system-gegen-strom-blackouts-geplant-1-3-2011 [02.06.2011].

93 Gem. Österreichischem Programm zum Schutz kritischer Infrastrukturen (APCIP) setzen sich diese aus Infrastrukturen mit gesamtstaatlicher Relevanz der Sektoren Verfassungsmäßige Einrichtungen, Energie, IKT, Wasser, Lebensmittel, Gesundheit und Soziales, Finanzen, Transport- und Verteilungssysteme, Chemische Industrie, Forschungseinrichtungen, Hilfs- und Einsatzkräfte zusammen.

94 Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 4.

95 Vgl. Ladinig, 2010.

96 Vgl. ebenda, S. 2.

sorgung abhängigen, Gesellschaft entgegenwirken würden. Eine Unterstützung bei diesem zu etablierenden Prozess könnte der aktuelle Bericht der Europäische Agentur für Netz- und Informationssicherheit (ENISA)[97] über die Bereitschaft zum nationalen Risikomanagement (National Risk Management, NRM) liefern. Dieser Bericht[98] legt die grundlegenden Elemente in Form eines Leitfadens zur Steuerung des NRM hinsichtlich der strategischen Informationsinfrastruktur (CII[99]) eines Staates fest. Weiter soll damit bei der Entwicklung und Implementierung eines NRM-Prozesses unterstützt werden.

Der Bericht soll nationalen Regierungen dienen, um:

- Stärken und Schwächen bei der Implementierung des NRM im eigenen Staat zu identifizieren,
- bei der Entwicklung eines Rahmenwerks zur Steuerung des NRM zu unterstützen,
- der Regierung zu helfen, CII-Stakeholder-Organisationen[100] bei der Entwicklung ihrer eigenen Risikomanagementprozesse zu unterstützen, und die NRM-Bereitschaft des Staates mit Hilfe eines definierten Testverfahrens einzuschätzen.

4.1 Verletzlichkeitsparadoxon

In diesem Zusammenhang muss besonders das „Verletzlichkeitsparadoxon“[101] berücksichtigt werden, welches den Widerspruch zwischen Risikowahrnehmung und Realität beschreibt. Die meisten technisch entwickelten Staaten weisen eine relativ zuverlässige, über lange Zeiträume funktionierende Stromversorgung auf. Darüber hinaus bauen nahezu alle technischen Systeme und sozialen Handlungen auf dieser relativen Verlässlichkeit auf. Nicht oder nur unzureichend wird die damit einhergehende massive Verletzbarkeit berücksichtigt. Darüber hinaus führt dies dazu, dass Versorgungsleistungen zunehmend weniger störanfällig organisiert werden. Ein Blackout trifft daher eine unvorbereitete Gesellschaft umso härter.

4.2 Mögliche Ursachen für ein Blackout

Es gibt eine Vielzahl an Möglichkeiten, wie ein Blackout ausgelöst werden kann. Beispielsweise durch[102]

- Naturereignisse, wie Blitzschlag, Schneefall, Erdbeben, Klima, Sonneneruptionen (CME),
- Menschliches Versagen, wie Schaltfehler, Fehlreaktionen, Unaufmerksamkeit
- Technisches Versagen, wie Wartungsmängel, Überalterung von Anlagen, Fehldimensionierungen,
- Ausfall der Primärenergie, wie Mangel an Wasser, Öl, Gas, Kohle oder Brennstäben,
- Systemische, organisatorische Mängel, wie Netzaufsplitterung, übertriebenes Gewinnstreben,

97 URL: http://www.enisa.europa.eu [01.06.2011].
98 Vgl. ENISA, 2011.
99 Critical Information Infrastructure.
100 Ressourcenbesitzer/Interessengruppe von Kritischer Informationsinfrastruktur – die Eigentümer oder Betreiber.
101 Vgl. Forschungsforum Öffentliche Sicherheit, 2010, S. 17.
102 Vgl. URL: www.noezsv.at/noe/media/0_Dokumente/KKM_blackout.pdf [29.05.2011].

- Kriminelle Handlungen wie, Diebstahl, Betrug, Erpressung, Angriff auf Steuersysteme,
- Gezielte Anschläge wie, Zerstörungen von Anlagen durch Sprengstoff oder Waffenwirkung,
- EMP, Mikrowellen wie, Zerstörung von Elektronikbauteilen.

Die Auswertung von bisherigen Blackouts hat ergeben, dass diese in der Regel von ein bis zwei nicht verbundenen Ereignissen ausgelöst wurden, die dominoartig zu Abschaltungen von Kraftwerken, Übertragungsleitungen und Schaltanlagen führten. Vor allem Wetterbedingungen, menschliches Versagen und technische Mängel, oder eine Kombination dieser Faktoren, waren die häufigsten Ursachen.[103]

Der TAB-Bericht geht davon aus, dass aufgrund der zunehmenden Gefahr terroristischer Angriffe und klimabedingter Extremwetterereignisse die Wahrscheinlichkeit eines Netzzusammenbruchs zunehmen wird.[104]

> *„Aufgrund der Erfahrungen mit bisherigen nationalen und internationalen Stromausfällen sind erhebliche Schäden zu erwarten. Bisherige Stromausfälle dauerten höchstens einige Tage, einige verursachten jedoch geschätzte Kosten von mehreren Mrd. US-Dollar. Für den Fall eines mehrwöchigen Stromausfalls sind die Schäden zu erwarten, die um Größenordnungen höher liegen."*[105]

4.3 Beispiele für historische Blackouts

Datum	Land	Betroffene	Ursache	Schäden in der Wirtschaft[2]
Februar 2008	USA (Florida)	6,000,000		
Juli 2007	Deutschland (Düsseldorf)	150,000		
Juli 2007	Spanien (Barcelona)	350,000	Schaltanlagendefekt	
Juli 2007	Georgien (Tiflis)	1,100,000		
November 2006	Deutschland/ NW-Europa	10,000,000	Schaltungsfehler	
November 2005	Deutschland (Münsterland)	250,000	Mastenbruch/ -knick	
Juni 2005	Schweiz	200,000	Fehler im Bahnnetz	
Mai 2005	Russland (Moskau)	2,000,000		
November 2004	Spain	2,000,000	Transformatorfeuer	
September 2004	Deutschland (Rheinland)	1,000,000	Kurzschluss	
Dezember 2003	Deutschland (Gütersloh)	300,000	Sabotage	
September 2003	Schweden / Dänemark	4,000,000	Schaltungsfehler	
September 2003	Italien	56,000,000	Zusammenbruch der Hochvoltleitung	
August 2003	USA / Kanada	50,000,000	Computerfehler/ Netz überaltert	7-10 Mrd USD
August 2003	Großbritannien (London)	1,000,000	Falsche Sicherheitseinrichtung	
Juni 2003	Italien	6,000,000	Ungenügende Kraftwerkskapazität	151 Mio USD
Januar 2001	Indien (New Delhi)	200,000,000		
Dezember 1999	Frankreich	3,400,000	Hurricane "Lothar"	
Dezember 1995	USA (Oregon)	2,000,000	Sturm	
Juli 1977	USA (New York)		Blitzschlag	350 Mio USD
November 1965	USA / Kanada	30,000,000	defektes Relais	452 Mio USD

Abbildung 12: Historische Blackouts - Quelle: http://portal.wko.at/;
Anmerkung zu Schäden in der Wirtschaft: Expertenschätzungen, vornehmlich nur für USA vorhanden.

103 Vgl. Zeitung für kommunale Wirtschaft, 2003, S.1.
104 Vgl. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 5.
105 Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 5.

4.4 Auswirkung im Kleinen

Abbildung 13: Auswirkung im Kleinen - Quelle: URL:http://www.energyefficiency.at/web/artikel/liste.html [11.06.2011]

4.5 Primärauswirkungen in den einzelnen Sektoren

Nachfolgend werden die möglichen Auswirkungen auf einige Sektoren der Strategischen Infrastruktur aus dem TAB-Bericht zitiert.

4.5.1 Informationstechnik und Telekommunikation

> *„Telekommunikations- und Datendienste fallen teils sofort, spätestens aber nach wenigen Tagen aus."*[106]

Die meisten Mobiltelefone würden zwar noch für längere Zeit Akkukapazitäten aufweisen, es ist aber unwahrscheinlich, dass die dahinter liegende und notwendige Infrastruktur für längere Zeit einsatzbereit bleiben wird. Das Netz wird möglicherweise durch die Überlastung von unzähligen Anrufversuche zusammenbrechen. Auch im Festnetzbereich ist mit massiven Ausfällen zu rechnen, vor allem im digitalen Bereich.

Bei den Massenmedien wird nur der Hörfunk sinnvoll zur Verfügung stehen, da hier noch am ehesten durch akku- bzw. batteriebetriebene Endgeräte ein länger andauernder Empfang möglich sein wird.

Auch im Bereich der Einsatzorganisationen wird es relativ rasch zu Ausfällen, bis hin zu Totalausfällen, kommen.

> *„Die durch Bundeswehr, Technisches Hilfswerk (THW) oder Telekommunikationsunternehmen im Ereignisfall einsetzbaren mobilen notstromversorgten Funktechniken und leitungsgebundenen Kommunikationsmittel sind vermutlich in erster Linie für die eigenen Erfordernisse vorgesehen; für die Gewährleistung der Kommunikation von Behörden, Bevölkerung und Unternehmen in einem Großraum sind sie nicht ausgelegt."*[107]

Natürlich gibt es in vielen Bereichen eine „Unterbrechungsfreie Stromversorgung" (USV) und Netzersatzstromversorgung. Aber auch hier sehen die realistischen Aussichten äußerst düster aus.

> *„Die Vielzahl der strombetriebenen Netzwerkknoten, Vermittlungsstellen und Funkantennen der Festnetz- und Mobiltelefonie sowie des Internets macht deren flächendeckende Wiederinbetriebnahme praktisch unmöglich, da Tausende von Batteriespeichern geladen und Treibstofftanks versorgt werden müssten."*[108]

Dem entsprechend entgegenzuwirken ist aber völlig unrealistisch.

> *„Eine nachhaltige Absicherung der Kommunikationsnetze, die es ermöglicht, über Wochen ein umfassendes Angebot an Dienstleistungen für die Kunden stabil zu halten, dürfte zurzeit wirtschaftlich und technisch nicht zu realisieren sein. Konzepte, die im Fall eines länger andauernden Stromausfalls zumindest ein definiertes minimales Versorgungsniveau bieten, sind – soweit ersichtlich – noch nicht entwickelt."*[109]

106 Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 5.
107 Ebenda.
108 Ebenda.
109 Ebenda.

4.5.2 Transport und Verkehr

„Im Sektor „Transport und Verkehr" fallen die elektrisch betriebenen Elemente der Verkehrsträger Straße, Schiene, Luft und Wasser sofort oder nach wenigen Stunden aus. (…) Zu Brennpunkten werden der abrupte Stillstand des Schienenverkehrs und die Blockaden des motorisierten Individual- und öffentlichen Personennahverkehrs in dichtbesiedelten Gebieten. (…) Durch den Ausfall der meisten Tankstellen bleiben zunehmend Fahrzeuge liegen, der Motorisierte Individualverkehr (MIV) nimmt nach den ersten 24 Stunden stark ab. Der Öffentliche Personennahverkehr (ÖPNV) kann wegen knappen Treibstoffs allenfalls rudimentär aufrechterhalten werden. (…) Da alle Tankstellen ausgefallen sind, wird der Treibstoff für die Einsatzfahrzeuge knapp. Darüber hinaus drohen erhebliche Engpässe bei der Versorgung der Bevölkerung, beispielsweise mit Lebensmitteln oder medizinischen Bedarfsgütern."[110]

4.5.3 Wasserversorgung und Abwasserentsorgung

„Die Wasserinfrastruktursysteme können ohne Strom bereits nach kürzester Zeit nicht mehr betrieben werden. Die Folgen ihres Ausfalls, insbesondere für die Versorgung der Bevölkerung mit Trinkwasser, wären katastrophal. (…) Die reduzierte Wasserversorgung wirkt sich auch auf die Abwasserentsorgung aus: So sinkt die anfallende Schmutzwassermenge, und es ändert sich die Zusammensetzung des Schmutzwassers. Deshalb besteht die Gefahr, dass sich durch das stark konzentrierte Abwasser in der Kanalisation Ablagerungen bilden und zu Verstopfungen und Geruchsbildung führen. (…) die hygienischen Zustände werden prekär (…) Es wächst die Gefahr der Ausbreitung von Krankheiten. (…) Eine weitere, mittelbare Folge des Stromausfalls ist ein wachsendes Risiko von Bränden. (…) ein Großteil der in den Netzen und auf Anlagen vorhandenen Trink- und Abwasserspeicher sowie Notstromkapazitäten allenfalls auf die Überbrückung wenige Stunden dauernder Versorgungsstörungen ausgelegt ist. "[111]

4.5.4 Lebensmittel

„Als Folge des Stromausfalls ist die Versorgung mit Lebensmitteln erheblich gestört; deren bedarfsgerechte Bereitstellung und Verteilung unter der Bevölkerung werden vorrangige Aufgaben der Behörden. Von ihrer erfolgreichen Bewältigung hängt nicht nur das Überleben zahlreicher Menschen ab, sondern auch die Aufrechterhaltung der öffentlichen Ordnung. (…) Der Lebensmittelhandel erweist sich angesichts der erhöhten Nachfrage als das schwächste Glied der Lebensmittelversorgung. Schon nach wenigen Tagen ist mit ernsthaften Engpässen bei der Lebensmittelversorgung zu rechnen."[112]

4.5.5 Gesundheitswesen

„Nahezu alle Einrichtungen der medizinischen und pharmazeutischen Versorgung der Bevölkerung sind von Elektrizität unmittelbar abhängig. Das dezentral und hocharbeitsteilig organisierte Gesundheitswesen kann den Folgen eines Stromausfalls daher nur kurz widerstehen. Innerhalb einer Woche verschärft sich die Situati-

110 Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 6.
111 Ebenda, S. 7.
112 Ebenda, S. 8.

on derart, dass selbst bei einem intensiven Einsatz regionaler Hilfskapazitäten vom weitgehenden Zusammenbrechen der medizinischen und pharmazeutischen Versorgung auszugehen ist. (…) Spätestens am Ende der ersten Woche wäre eine Katastrophe zu erwarten, d. h. die gesundheitliche Schädigung bzw. der Tod sehr vieler Menschen sowie eine mit lokal bzw. regional verfügbaren Mitteln und personellen Kapazitäten nicht mehr zu bewältigende Problemlage. " [113]

4.5.6 Finanzdienstleistungen

„Selbst bei einem großflächigen und langandauernden Stromausfall zeigt sich das Finanzdienstleistungssystem in einzelnen Teilsektoren als relativ robust."[114]

„Da auch die Geldautomaten ausgefallen sind, droht die Bargeldversorgung der Bevölkerung zu kollabieren. Es ist anzunehmen, dass es hierdurch und durch den Ausfall elektronischer Zahlungsmöglichkeiten in Geschäften und Banken mit der Zeit zu Unmut und teils zu aggressiven Auseinandersetzungen kommt, da es für die Bevölkerung keine Bezahlmöglichkeiten mehr gibt."[115]

4.6 Auswirkungen nach 24 Stunden (Österreich)

Die Analyse des Militärkommandos Niederösterreich[116] kommt zum Schluss, dass nach 24 Stunden ein völliger Zusammenbruch der Versorgung zu erwarten ist, da auch die letzten verfügbaren und zugänglichen Treibstoffreserven aufgebraucht sind.

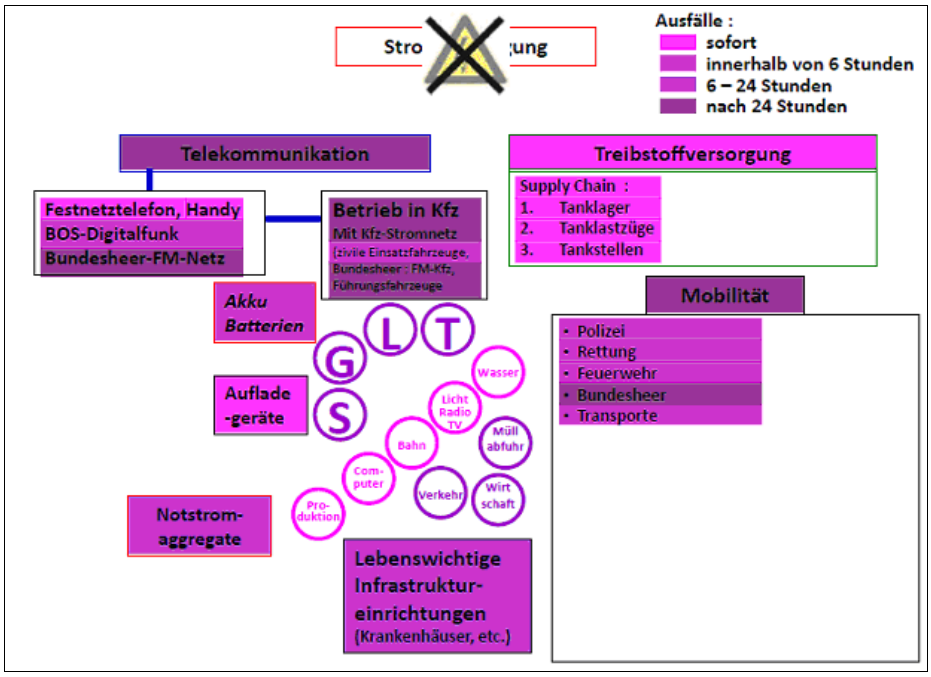

Abbildung 14: Situation in Österreich - 24 Stunden nach dem Beginn des Blackouts - Quelle: Ladinig, 2011, S. 21.
Legende: T: Versorgung mit Trinkwasser, L: Lebensmittel, G: Gesundheitswesen, S: Aufrechterhaltung von Ordnung und Sicherheit

113 Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 9f.
114 Ebenda, S. 10.
115 Ebenda.
116 Vgl. Ladinig, 2010.

Die Folgen der Abwesenheit von staatlicher Autorität und Hilfe lässt den Überlebenskampf der Individuen, Plünderungen, Faustrecht und anarchistische Zustände erwarten.

Eine ganz wesentliche Rolle spielt in dieser Analyse die Treibstoffversorgung der Einsatzkräfte. Unmittelbar nach dem Beginn des Blackouts bricht die Tankversorgung zusammen,

> *„damit besteht keine Möglichkeit mehr, Kfz-Tanks zu befüllen. Eine Notbetankung direkt aus Tanklastzügen ist nicht möglich, da an diese nur 4-Zoll-Schläuche angeschlossen werden können, für die Kfz-Betankung aber 2-Zoll-Schläuche erforderlich sind.*
>
> *Die Tanklager SCHWECHAT, LOBAU und St.VALENTIN verfügen über keine Notstromaggregate zur Befüllung von Tanklastzügen und Kesselwaggonen. Das OMV-eigene Kraftwerk in SCHWECHAT wird voraussichtlich bei einem BLACK OUT ebenfalls ausfallen. Somit fällt die Treibstoff-SUPPLY CHAIN ebenfalls von einer Sekunde auf die andere aus.*
>
> *In Österreich haben wir einen Krisenvorrat an Treibstoffen für 90 Tage, haben aber bei Stromausfall derzeit keine Möglichkeit, den Treibstoff in die Tanks der Kfz zu füllen. Auch ist die Anschlussversorgung mit Treibstoffen für Notstromaggregate nicht möglich.*
>
> *Die Kfz können je nach gerade aktuellem Tankinhalt noch unterschiedlich lange betrieben werden. Die Reichweite wird dabei von wenigen Km (fast leerer Tank) bis zu mehreren 100 Km (Tank fast noch voll) liegen."*[117]

Auch hier kommt erschwerend zu die zunehmende Automatisierung hinzu.

> *„Mechanische Zapfsäulen können mit handelsüblichen Notstromaggregaten in Betrieb gehalten werden. Ein Problem stellt die laufende Umstellung von mechanischen auf computergesteuerte Zapfsäulen dar, da letztere nur mit speziellen Notstromaggregaten (mit Kammfiltern ausgestattet) betrieben werden können. Handelsüblichen Aggregate würden durch die üblichen Spannungsschwankungen die Computer-Chips zerstören, und somit die Zapfsäulen insgesamt unbrauchbar machen."*[118]

Mit der Verfügbarkeit von Nottankstellen und Nottankeinrichtungen könnten die Auswirkungen erheblich gemildert werden.

117 Ladinig, 2010, S. 16.
118 Ebenda, S. 23.

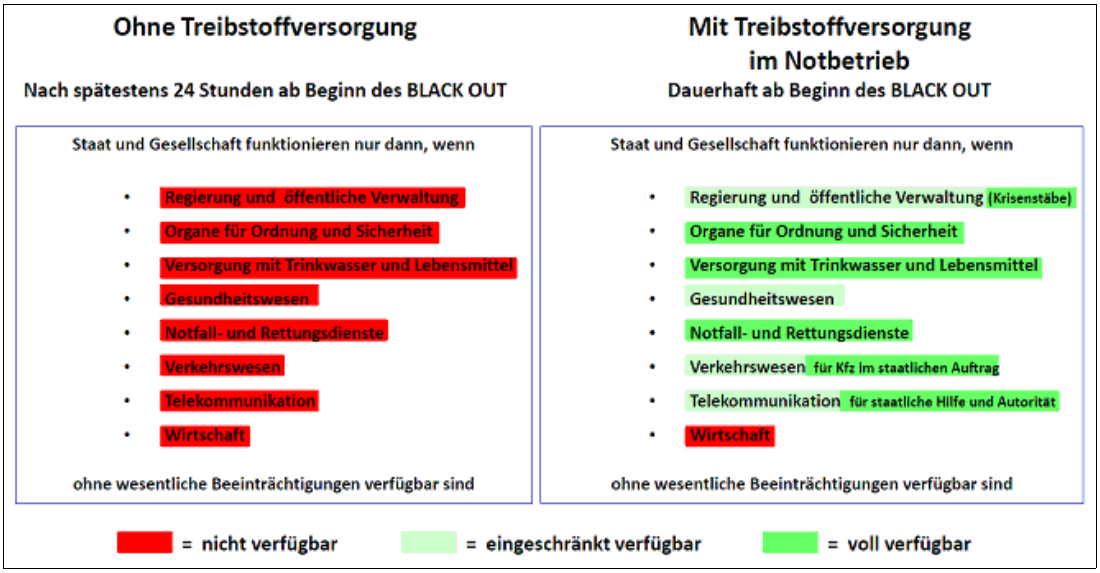

Abbildung 15: Situation in Österreich - 24 Stunden nach dem Beginn des Blackouts - mit verfügbarer Treibstoffversorgung - Quelle: Ladinig, 2011, S. 25.

4.7 Forschungsprojekt BlackÖ.I

Zusammenfassend kann gesagt werden, dass moderne Gesellschaften derzeit hochabhängig von nicht berechenbaren Infrastruktur-Systemen sind. Die derzeit verfügbaren Bewältigungskapazitäten der Staaten und der Bevölkerung sind mit hoher Wahrscheinlichkeit nicht darauf ausgelegt. Dieser Umstand stellt daher eine enorme Gefährdung für die davon abhängigen Gesellschaften dar.

Daher ist es umso wichtiger, dass verschiedene Ansätze gewählt werden, um das tatsächliche Gefährdungspotential besser einschätzen zu können und dass daraus ableitend entsprechende Maßnahmen gesetzt werden.

Derzeit läuft im Rahmen von KIRAS[119] das Forschungsprojekt *BlackÖ.I*[120], welches im August 2011 abgeschlossen wird und sich mit der Analyse der Schadenskosten, Betroffenenstruktur und Wahrscheinlichkeiten großflächiger Stromausfälle beschäftigt. Aber auch das bereits 2009 gestartete Projekt BlackÖ.I geht davon aus, dass

> *„Die zunehmende Belastung der Netze bei einem gleichzeitig zu geringen Ausbau der Infrastruktur lassen die Wahrscheinlichkeit großflächiger Ausfälle mit katastrophalen Auswirkungen für die heimische Wirtschaft und Bevölkerung jedoch immer stärker steigen.“*[121]

119 Österreichische Förderungsprogramm für Sicherheitsforschung; vgl. URL: http://www.kiras.at/ [11.06.2011].

120 Blackouts in Österreich Teil I – Analyse der Schadenskosten, Betroffenenstruktur und Wahrscheinlichkeiten großflächiger Stromausfälle.

121 URL: http://www.energyefficiency.at/web/projekte/blacko.html [11.06.2011].

5 Zusammenfassung und Folgerungen

Nach den bisherigen Ausführungen ist es hoffentlich gelungen, einen Einblick bzw. einen neuen Blickwinkel auf das Thema Smart Metering aber auch Smart Grid Sicherheit zu vermitteln. Dabei war es Absicht, den Fokus nicht auf technische Details zu beschränken, sondern auch weitere Einflussfaktoren zu beleuchten. Die beschränkte Betrachtung von Einzelkomponenten verleitet dazu, das Gesamtsystem aus den Augen zu verlieren. Für die Verfügbarkeit des Services ist aber das Gesamtsystem entscheidend.

Durch die derzeit allgemein sehr positive Berichterstattung führt die vorliegende Arbeit wohl zu einem sehr konträren und überwiegend negativem Bild. Dabei geht es nicht darum, eine neue und unbestritten notwendige Technologie für unsere zukünftige Stromversorgung zu verteufeln. Vielmehr soll damit ein Beitrag zur Bewusstseinsschärfung bei Verantwortungsträgern aller Ebenen erzielt werden, egal ob

- bei den Behörden, welche einerseits für die Spezifizierung der Geräte und damit auch der Sicherheitsvorgaben verantwortlich sind.
- in der Industrie, welche die Smart Meter herstellt.
- bei den Netzbetreibern, welche die Geräte einsetzen und das Gesamtsystem betreiben müssen.
- beim Endkunden, der von den negativen Folgen unmittelbar betroffen sein kann und in letzter Konsequenz auch
- das staatliche Krisenmanagement, welches laufend überprüfen muss, ob die aktuell vorgesehenen Krisenbewältigungsmaßnahmen ausreichend sind, oder eine Adaptierung erforderlich ist.

Durch die bisherige Trennung des Stromnetzes von sonstigen öffentlichen Netzen ist ein relativ hohes Sicherheitsniveau gegeben. Durch die nunmehrige Absicht, IKT-Netze mehr oder weniger direkt mit dem Stromnetz zu verbinden, zumindest aber bisher in der IKT-Welt als unsicher geltende Systeme im Bereich der Stromnetze einzusetzen, ergibt sich eine völlig neue Situation. Diese wird mit dem Wissen, dass es auch in den jetzigen Stromnetzen ausreichend Schwachstellen gibt, welche jedoch so gut wie nicht ausnützbar sind, noch erheblich erschwert. Als Höhepunkt wird mit dem Smart Meter eine neue, möglicherweise unsichere, Technologie in eine weitgehend ungesicherte Umgebung beim Endkunden, als Netzeintrittspunkt, eingebaut. Und soweit bisherige Untersuchungen vorliegen, scheinen zahlreiche Ansätze möglich, um dieses Endgerät zu manipulieren oder sogar zu zerstören.

> *„Because the cost of Smart Meters is low, there is no significant barrier to entry for hackers interested in attacking AMI[122]. (…) AMI security, as it currently stands, is insufficient to protect the national power grid from attack by malicious and knowledgeable groups. (…) Vendors of wireless AMI technology claim to provide security features, but in a rush to be first to market, security may not receive sufficient emphasis.“*[123]

122 Advanced Metering Infrastructure; AMR = Automatic Meter Reading.
123 Vgl. U.S. Department of Energy, 2009, S. 11.

Aufgrund der angeführten, öffentlich zugänglichen Informationen, muss davon ausgegangen werden, dass in so gut wie allen Bereichen Handlungsbedarf besteht und dass unsere Gesellschaft bereits jetzt, noch ohne flächendeckendem Einsatz von Smart Metering, einer ganz erheblichen Gefährdung durch Blackouts ausgesetzt sind und unsere Gesellschaft so gut wie nicht darauf vorbereitet ist. Wenn davon ausgegangen werden muss, dass je nach Jahreszeit, bereits nach wenigen Stunden eine nationale Katastrophe droht, dann sollte nichts dem Zufall überlassen werden.

Diese Situation ist nicht wirklich mit anderen Bereichen vergleichbar. Wenn in der IKT-Welt etwas schief läuft, dann können mittlerweile ebenfalls erhebliche Schäden eintreten. Wie Brisant das Thema ist, sollten mittlerweile die fast täglichen Beispiele für erfolgreiche Angriffe auf große Firmen und Einrichtungen verdeutlichen. Dennoch blieb der Schaden bisher eingrenzbar. Wenn es aber gelingen sollte, die Strominfrastruktur anzugreifen, dann besteht die Gefahr, dass wir dem derzeit keine geeigneten Gegenmaßnahmen gegenüberstellen können.

In den USA wurde dieses Risiko bereits 2009 ganz klar angesprochen und als Teil der Cyber Security definiert.[124] In Europa scheint es eine derartige Diskussion noch nicht zu geben.

Derzeit gibt es umfangreiche Diskussionen zur Zukunft der Elektromobilität, worin eine große ökonomische und ökologische Chance gesehen wird. Damit wird aber auch die Komplexität der Stromnetze und -versorgung aber auch die Abhängigkeit steigen. Daher sollten auch in diesem Bereich gesamtheitliche Betrachtungen bereits in die frühen Planungsphase einfließen und nicht der Fokus am Einzelsystem hängen bleiben. Komplexe Systeme zeichnen sich dadurch aus, dass ihr Ganzes immer mehr als die Summe ihrer Einzelteile ist.

Nachdem so gut wie immer finanzielle Rahmenbedingungen eine wesentliche Rolle spielen, muss hier auch noch dieser Aspekt angeführt werden.

> *„Der volkswirtschaftliche Schaden einer Stunde Stromausfall [Anm: in gesamt Österreich] ist beträchtlich und kann im schlimmsten Fall - bei Ausfall des Übertragungsnetzes - bis zu 40 Millionen Euro betragen. Die Auswirkungen auf die Industrie können gravierend ausfallen.“* [125]

Andere Berechnungen gehen von weit höheren Schäden aus.[126] Es ist wohl auch eine Frage, was alles dazu gezählt wird. Es ist aber davon auszugehen, dass der Schaden beträchtlich sein würde und präventive Vorkehrungen in vielen Bereichen wahrscheinlich nur einen Bruchteil davon ausmachen. An entsprechenden Vorkehrungen zu sparen wäre daher sehr fahrlässig.

5.1 Folgerungen generell

Die Betriebssicherheit von Smart Grids / Smart Metering hängt ganz wesentlich von der Angriffssicherheit ab. In der bisherigen Diskussion kommt die Angriffssicherheit und Risikobewertung weitgehend zu Kurz. Ein umdenken ist daher dringend erforder-

124 Vgl. U.S. Department of Energy, 2009.

125 URL: http://oesterreichsenergie.at/die-versorgungssicherheit-in-oesterreich-ist-gewaehrleistet.html [23.06.2011].

126 Ladinig, 2010, S. 13.

lich. Derzeit stehen viele Staaten und auch Österreich, noch am Beginn der Implementierung. Damit können derzeit noch kostengünstiger Änderungen und Verbesserungen vorgenommen werden. Je weiter Systeme ausgerollt werden, desto schwieriger und kostenintensiver wird die Implementierung von möglichen, nachträglich erforderlichen Sicherheitsmaßnahmen.[127]

Bei einer Risikoanalyse muss auch klar sein, dass die Verwundbarkeit mit dem Umfang der Ausrollungen steigt. Einerseits, weil damit die Komplexität des Gesamtsystems steigt und auf der anderen Seite, weil sich damit für mögliche Angreifer lohnendere Ziele ergeben.

„That's where the money is (Bank) crimes move beyond robbery to fraud"[128]

Die Risiken, die mit unserem modernen Lebensstil verbunden sind, sollten wieder stärker in unser Blickfeld gerückt werden, ohne jedoch gleich Panik zu erzeugen. Eine offene Kommunikation über Chancen und Risiken, sowie über akzeptierte Restrisiken wären ein wichtiger Beitrag zur Krisenprävention und Bewusstseinsschaffung.

Darüber hinaus muss es gelingen, Hersteller und Betreiber klar zu machen, dass Sicherheit als Qualitätsmerkmal zu sehen ist und auch dem entsprechend behandelt wird. Kein Hersteller wird sich nachsagen lassen wollen, dass sein Produkt eine schlechte Qualität aufweist. Diese muss aber auch Sicherheitsvorkehrungen betreffen und nicht nur am Gerät selbst, sondern im Gesamtsystem. Für Netzbetreiber und Kunden bedeutet dies, dass sich zusätzliche Sicherheit auch auf den Preis auswirkt. Einsparungen zum falschen Zeitpunkt könnten im Nachhinein ein Vielfaches an Kosten verursachen.

5.2 Folgerungen für Behörden

Behörden als staatliches Regulativ sollten sich in dieser Angelegenheit stärker aktiv und fachlich fundiert einbringen und vor allem kritisch Fragen stellen. Dieses Spielfeld darf auf keinem Fall dem freien Markt überlassen werden, da zu viel auf dem Spiel steht und letztendlich die Bürger für große Schäden aufkommen müssen.[129]

Der Staat als Vertreter der Bürger hat daher alle Möglichkeiten zum Schutz dieser zu unternehmen und muss im Bedarfsfall auch unpopuläre Maßnahmen setzen.

Als erster Schritt wären der tatsächliche volkswirtschaftliche Nutzen und die damit verbundenen Risiken neu zu berechnen. Unter anderem sollten auch mehrere Varianten errechnet werden, z.B. weit kürzere Betriebszeiten für Smart Meter. Die Annahme, dass Smart Meter eine Lebensdauer von 15 Jahren aufweisen[130], erscheint sehr hoch gegriffen. Darüber hinaus könnte damit ein möglicher, vorzeitiger und notwendiger Austausch von Endgeräten, beispielhaft wegen erheblicher Schwachstellen, simuliert werden.

Regulative Vorgaben im Bereich Smart Metering / Smart Grid dürfen sich nicht auf Einzelsysteme beschränken, sondern müssen immer im Verbund gesehen und getroffen werden. Darüber hinaus sind generelle IT-Sicherheitsstandards durch die Politik bzw.

127 Vgl. U.S. Department of Energy, 2009, S. iiiff.
128 URL: http://apps.americanbar.org/buslaw/blt/blt00may-money.html [21.06.2011].
129 Vgl. Atomkatastrophe in Japan, oder Bankenrettung in Europa.
130 Vgl. PwC, 2010, S. 8.

Gesetzgebung festzulegen. Diese Vorgaben erfordern natürlich auch entsprechende Kontrollen und Sanktionsmöglichkeiten. Sicherheit ist ein fortlaufender Prozess. Daher sind permanent Anpassungen erforderlich, vor allem, wenn sich die Rahmenbedingungen derart rasch ändern können, wie in der IKT.

5.3 Folgerungen für die Industrie / Hersteller

Durch die Industrie bzw. den Herstellern von Komponenten für die Smart Metering Infrastruktur muss eine umfassende Sicherheitsbetrachtung bereits in der Planungsphase seinen Niederschlag finden und vor allem darf sich diese nicht auf das Einzelsystem beschränken.

Wenn Sicherheit als Qualitätsmerkmal gesehen wird, dann kann damit bei entsprechender, plausibler Argumentation auch ein Wettbewerbsvorteil erzielt werden. Der Hinweis auf den möglichen Kostendruck sollte nicht als Argument dienen.

Bei der Entwicklung von neuen Technologien sollte die Einbindung von Fachleuten aus verschiedenen Disziplinen angestrebt werden, um eine möglichst breite Betrachtung von eventuellen Problembereichen zu erhalten. Kritische Fragen und Herangehensweisen in der Planungs- und Entwicklungsphase ersparen wahrscheinlich hohe Kosten und Schwierigkeiten im Nachhinein.

Vor allem sollte rechtzeitig aus den Fehlern der IKT-Welt gelernt werden. Bei der Softwareentwicklung sind entsprechende hohe Qualitätsanforderungen zu stellen, um die Fehleranzahl so gering als möglich zu halten. Aber auch die Hardwareentwicklung muss auf die spätere Verwendung, wie zum Beispiel in einer unsicheren Umgebung, abgestimmt werden.

Die Hersteller tragen in diesem Bereich auch eine hohe soziale Verantwortung. Sollten die skizzierten Szenarien durch Mängel in den Produkten wirklich eintreten, wäre der volkswirtschaftliche und möglicherweise auch gesellschaftliche Schaden enorm.

5.4 Folgerungen für die Netzbetreiber

Energieversorger sind Dienstleister mit gesellschaftlichem Auftrag und Verantwortung, sie tragen daher nicht nur Firmenverantwortung. Auch sie müssen bei der Implementierung dieser neuen Technologie kritisch bleiben und bei Bedarf rechtzeitig die Notbremsen ziehen. Mögliche Angriffe oder das Versagen von Infrastrukturbereichen würden wahrscheinlich erhebliche wirtschaftliche Folgen für das betroffene Unternehmen nach sich ziehen.

Die Vernetzung ist heute wichtiger den je, dennoch sollten auch im Strombereich Vorkehrungen getroffen werden, damit im Worst-Case Fall auch ein Inselbetrieb von definierten Bereichen, vor allem für Betreiber von Strategischen Infrastrukturen möglich ist.

> *„Eine Inselnetztauglichkeit der dezentralen Stromerzeuger könnte einen Beitrag zu einer verbesserten Resilienz des Sektors nach dem Stromausfall leisten."*[131]

Die bisherigen hohen Standards im Bereich der Energieversorgung, insbesondere im Bereich Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit und Verbindlichkeit,

131 Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 8.

müssen, soweit irgendwie vertretbar, trotz enger Verbindung mit der IKT-Welt, aufrecht erhalten werden.

Derartige Anforderungen können nur durch laufende Überprüfungsmaßnahmen (Audits) und Nachtbesserungsmaßnahmen erreicht und gehalten werden. Eine wesentliche Rolle spielen dabei angemessene Notfall-, Krisen- und Business-Continuity-Konzepte und der Nachweis der Umsetzbarkeit dieser Konzepte.

> *„Dennoch bleibt die Energiewirtschaft gefordert, über die Krisenkommunikation hinaus PR für die Belange der Stromversorgung zu treiben. Mangelndes Bewusstsein über die Bedingungen einer sicheren Stromversorgung führt dazu, dass Verbraucher und Medien von den Folgen von Versorgungsausfällen unvorbereitet getroffen werden und Feindbilder aufbauen."*[132]

Für die Notfallplanung sind Fragen, wie

- Welche rechtlichen Folgen erwachsen, wenn Schwachstellen oder Angriffe auf Smart Metering Infrastrukturen bekannt werden? Vor allem für wen?
- Wer haftet in einem solchen Anlassfall?
- Welche Folgen könnten durch unberechtigte Fernabschaltungen von Smart Meter erwachsen?
- Welcher medialer bzw. öffentlicher Schaden könnte beim Bekanntwerden von Erpressungsversuchen, Schwachstellen oder Angriffen für das Unternehmen entstehen?
- Wie wird in einem Erpressungsfall vorgegangen?
- Steht eine entsprechend vorbereitetet Krisenkommunikation zur Verfügung?
- Welche Konsequenzen sind zu erwarten, wenn größere Kundenmanipulationen zum Abrechnungsbetrug bekannt werden?
- Verfügt der Systembetreiber auch über die erforderliche Autorität, um Systemsicherheit über kommerzielle Überlegungen zu stellen.[133]

  „In der Folge sind die Kooperationsanforderungen zwischen Netzbetreibern höher, als zwischen konkurrierenden Erzeugungs- und Vertriebsunternehmen. (…) Aufgabe der Netzbetreiber ist, das Netz sicher und effizient zu betreiben und diskriminierungsfrei allen Wettbewerbern zur Verfügung zu stellen. Ihre primäre Verantwortung ist also der Netzbetrieb, nicht die Bereitstellung ausreichender Erzeugungskapazitäten. (…) Die Sicherheit eines Versorgungsnetzes hängt nicht alleine vom Betrieb des eigenen Netzes, sondern immer stärker von der Funktionsfähigkeit des vermaschten Gesamtnetzes ab. Der Informationsbedarf moderner Systembetreiber endet daher nicht an der Grenze des eigenen Versorgungsgebietes, sondern setzt Informationen über benachbarte Systeme und ihren Status voraus."[134]

132 Zeitung für kommunale Wirtschaft, 2003, S. 2.
133 Vgl. Zeitung für kommunale Wirtschaft, 2003.
134 Ebenda, S. 3.

- Stehen für den Krisenfall ausreichende Personalressourcen mit entsprechender Ausbildung und Trainingserfahrung zur Verfügung?

zu stellen.

Wo immer möglich, sollte es zu einer Trennung von Netzen kommen. Dies verhindert am Besten die rasche Verbreitung von möglicher Schadsoftware bzw. schafft Übersichtlich- und Kontrollierbarkeit.

Es ist nicht möglich, alle denkbaren Szenarien vorauszuplanen oder eine hundertprozentige Ausfallgarantie zu gewährleisten. Generelle Annahmen ermöglichen jedoch entsprechende Vorbereitungsmaßnahmen und ein entsprechendes Krisenmanagement.

Smart Meter sind Teil der Netzinfrastruktur. Daher sollten Überlegungen angestellt werden, wie Smart Meter in der derzeit weitgehend ungesicherten Umgebung durch zusätzliche Maßnahmen abgesichert werden können.

5.5 Folgerungen für die Endkunden

Dem Endkunden bleiben nur wenige Möglichkeiten, diese zukünftigen Herausforderungen zu beeinflussen. Noch am ehesten über den Weg der Politik.

Ganz wesentlich wäre aber die Bereitschaft, sich mit Risiken der modernen Gesellschaft und möglichen Krisenszenarien auseinanderzusetzen und nicht in der Ignoranz zu verharren. Die Verleugnung von Realitäten verhindert nicht den Eintritt von negativen Ereignissen, ganz im Gegenteil. Die negative Überraschung wird wahrscheinlich umso schlimmer ausfallen, je weniger jemand darauf vorbereitet ist. Gleichzeitig muss aber auch zur Kenntnis genommen werden, dass Panik nicht angebracht ist und wiederum nur die Situation verschlimmern würde.

Ganz generell kann sich jeder Staatsbürger durch eine persönliche Krisenvorsorge das Leben im Anlassfall erheblich erleichtern. Hier wären entsprechende Vorschläge seitens des Zivilschutzes, wie es sie auch in anderen Bereichen gibt, sehr hilfreich. Einige Konserven, Trinkwasser in Flaschen, Batterien für Radioempfänger oder Taschenlampen, etwas Bargeld in Form von Münzen wären ein wichtiger Beitrag für die persönliche Krisenvorsorge.

5.6 Folgerungen für die Forschung und Lehre

In der derzeitigen österreichischen Bildungslandschaft stellt Angriffssicherheit weitgehend ein Randthema dar. Hier besteht erheblicher Nachholbedarf. Sicherheit ist kein Selbstzweck, sondern häufig ein wesentlicher Erfolgsfaktor. Daher muss die Sicherheitsausbildung nicht nur in einschlägigen technischen Richtungen seinen Niederschlag finden, sondern in vielen Bereichen mehr. Sicherheit muss vor allem als Querschnittmaterie und Qualitätsmerkmal ein Bestandteil der Führungs- und Managementausbildung, aber auch im Bereich von Marketing einfließen. Nur so kann gewährleistet werden, dass Fehler in der Planung und Führungsentscheidung frühzeitig verhindert werden.

5.7 Folgerungen für das staatliche Krisenmanagement

Wie auch in vielen anderen Bereichen, handelt es sich hier nicht um ein rein technisches Problem, sondern vorwiegend um ein organisatorisches und dies trifft ebenfalls für die Krisenvorsorge zu.

Die generelle Krisenvorsorge wurde nach dem Ende des Kalten Krieges in vielen Bereichen stark reduziert. Eine Ausnahme stellen dabei atomare Katastrophen dar. Im Sinne des Verletzlichkeitsparadoxon sollten Überlegungen angestellt werden, ob neue oder ergänzende Maßnahmen und Vorkehrungen erforderlich sind, wie wie Verhaltensregeln für den Fall eines größeren Blackouts für jeden Haushalt.

Es ist nicht möglich, alle Risiken auszuschalten. Aber nur ein entsprechend vorbereitetes Krisenmanagement ist in der Lage, die Folgen einer möglichen Krise bestmöglich zu lindern.

In der vergangenen Jahren wurden in vielen Ländern umfangreiche Maßnahmen zur Pandemieprävention gesetzt. Wie das aktuelle Beispiel zeigt, waren diese in Deutschland wahrscheinlich noch nicht ausreichend, um auch mit der aktuellen EHEC[135] Infektionswelle problemlos fertig zu werden. Auf der anderen Seite verdeutlicht dieses Beispiel, wie subjektiv Sicherheit sein kann. Im Straßenverkehr wird ein vielfaches an Todesopfer pro Jahr in Kauf genommen, ohne das ein derartiger Medienrummel entsteht.

Eine weitere Frage, die bereits im Vorfeld geklärt werden muss ist, ab wann das staatliche Krisenmanagement beginnt. Im klassischen Krisen- und Katastrophenmanagement ist dies in der Regel mit dem Eintritt der Krise oder Katastrophe. Dafür ist das Staatliches Krisen- und Katastrophenschutzmanagement (SKKM) beim Bundesministerium für Inneres (BMI) zuständig. Wie sieht es aber im Bereich von Smart Metering aus, wenn etwa bekannt wird, dass eine schwerwiegende Lücke entdeckt wurde, die jedoch noch nicht ausgenützt wird. Das wäre derzeit wahrscheinlich noch kein Anlassfall für das SKKM. Rasches und koordiniertes Handeln wird aber das Gebot der Stunde sein, um einer möglichen Katastrophe zuvorzukommen. Diese Frage muss bereits im Vorfeld eines möglichen Ereignisses geklärt sein, um im Anlassfall Zeit zu gewinnen. Bei diesen neuen Herausforderungen wird Zeit eine ganz wesentliche Rolle spielen, die über Erfolg oder Misserfolg entscheiden wird.

5.7.1 Sicherheitsforschung

Diese Arbeit stellt einen Ansatz für eine umfassende Betrachtung dieser Problematik dar. Darüber hinaus wird es erforderlich sein, weitere Aspekte und vor allem auch technische Details, wie die Smart Meter Sicherheit zu erforschen.

In der aktuellen Programmlinie 3.3 des Sicherheitsforschungsprogramms KIRAS wurde ein Antrag zur Erforschung der Smart Meter Security (SMS) durch die IKARUS Security Software GmbH eingebracht. Dabei konnten als Projektpartner

- die TU Wien, Institut für Rechnergestützte Automation,
- die TU Wien, Institut für Computertechnik,
- das Institut für Höhere Studien,

135 Enterohämorrhagische Escherichia Coli-Bakterien – vgl. URL: http://www.ehec-darminfekt.de [22.06.2011].

- die Wien Energie Stromnetz GmbH,
- die Österreichs E-Wirtschaft und
- die KELAG Netz GmbH

gewonnen werden.

Ob dieses Projekt gefördert wird, soll sich in den nächsten Wochen entscheiden.[136]

Es wäre ein wichtiger Beitrag zur Schaffung von weiteren Grundlagen und Präventionsmaßnahmen.

5.7.2 Krisenpläne

Im Bereich von atomaren Katastrophen gibt es umfangreiche Krisenvorkehrungsmaßnahmen. Hier ist eine entsprechende Sensibilität vorhanden. Daher sollte Seitens des staatlichen Krisenmanagements überprüft werden, ob die derzeit verfügbaren Krisenpläne auch auf derart komplexe Szenarien, wie vergleichsweise ein großer Blackout sein könnte, ausgerichtet sind.

Insbesondere wären Fragen wie,

- Sollte eine nationale Notfallfrequenz, analog zum Sirenensystem, für Rundfunkausstrahlungen etabliert und bekannt gegeben werden?
- Welche Krisenpläne müssen etabliert werden, damit vor allem die Sicherheit des betreuten Nachwuchses (Kindergärten, Schulen) gewährleistet werden kann? Damit können Panikreaktionen von besorgten Eltern minimiert und vielleicht für wichtige Krisenbewältigungstätigkeiten am Arbeitsplatz gehalten werden.
- Wie kann die Notfalltreibstoffversorgung für Einsatzkräfte und damit auch die Notfallkommunikationsfähigkeit aufrecht erhalten werden?
- u.v.m.

zu stellen.

5.7.3 Österreichisches Bundesheer

Dem Österreichischen Bundesheer obliegt gem. § 2. (1) c) des Wehrgesetzes „die Hilfeleistung bei Elementarereignissen und Unglücksfällen außergewöhnlichen Umfanges“, darüber hinaus gem. § 2 (1) b „der Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit und der demokratischen Freiheiten der Einwohner sowie die Aufrechterhaltung der Ordnung und Sicherheit im Inneren überhaupt“.[137]

Daher ist davon auszugehen, dass das Österreichische Bundesheer beim Eintritt eines großflächigen Blackouts, wie im Kapitel 4 beschriebenen, gem. dieser Paragrafen zum Einsatz kommen wird.

Entsprechende Planungen und Vorsorgemaßnahmen sind daher erforderlich, bzw. bei Bedarf zu ergänzen. Fähigkeiten werden wahrscheinlich im Bereich,

- Bereitstellung von entsprechender Transportlogistik,

136 IKARUS Security Software GmbH, 2011.

137 URL: http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001612 [23.06.2011].

- Bereitstellung von alternativen Verbindungsnetzen, inkl. Melder,
- Unterstützung der Exekutive im Rahmen eines sicherheitspolizeilichen Assistenzeinsatzes zur Aufrechterhaltung der Ordnung und Sicherheit,
- Unterstützung bei der Sanitätsversorgung,
- Bereitstellung von Hilfskräften jeglicher Art,

erforderlich sein.

Entsprechende Planspiele und Übungen im gesamtstaatlichen Kontext (Staatliches Krisenmanagement) sind erforderlich, um sich bestmöglich auf die Bewältigung derartiger Szenarien vorzubereiten und abzustimmen.

Insbesondere ist zu berücksichtigen, dass bei einem großflächigen Blackout wahrscheinlich die technische Kommunikation sehr rasch zusammenbricht, bzw. nicht mehr alle relevanten Stellen erreichbar sein werden. Daher müsste in den Notfallplanungen auch ein selbstständiges Handeln vorgesehen werden. D.h. wenn der Strom nach einer gewissen Zeit nicht wieder angegangen ist und es keine Verbindung zu Krisenstäben oder Einsatzzentralen gibt, müssen vordefinierte Abläufe automatisch anlaufen. Nur so kann gewährleistet werden, dass ein möglichst rasches Einschreiten und wiederherstellen der Ordnung und Sicherheit sichergestellt werden kann.

„Das Böse triumphiert allein dadurch,
dass gute Menschen nichts unternehmen“

(Edmund Burke, 1770)

6 Literaturverzeichnis

Amtsblatt der Europäischen Union: *Richtlinie 2009/72/EG über gemeinsame Vorschriften für den Elektrizitätsbinnenmark.* In: Internet, 2009, unter URL: http://www.e-control.at/portal/page/portal/medienbibliothek/recht/dokumente/pdfs/elektrizitaetsbinnenmarktrichtlinie-130709.pdf [30.05.2011].

Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.): *Protection Profile for the Gateway of a Smart Metering System*. In: Internet, 2011, unter URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf [07.06.2011].

Bundesgesetzblatt I: *110. Bundesgesetz: Elektrizitätswirtschafts- und –organisationsgesetz 2010 und Energie-Control-Gesetz.* In: Internet, 2010, unter URL: http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2010_I_110/BGBLA_2010_I_110.pdf [30.05.2011].

Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (Hrsg.): *Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung.* In: Internet, 2011, unter URL: http://dipbt.bundestag.de/dip21/btd/17/056/1705672.pdf [29.05.2011].

ENISA (Hrsg.): *National Risk Management Preparedness.* In: Internet, 2011, unter URL: http://www.enisa.europa.eu/act/rm/files/deliverables/WG%202010%20NRMP [01.06.2011].

Freiling, Felix: *Safety versus Security Gegenüberstellung und Einordnung.* In Internet, 2010, unter URL: http://pi1.informatik.uni-mannheim.de/filepool/presentations/siemens-vortrag-jul-2010.pdf [19.06.2011].

Forschungsforum Öffentliche Sicherheit (Hrsg.): *Kritische Infrastrukturen aus Sicht der Bevölkerung.* In: Internet, 2010, unter URL: http://www.sicherheit-forschung.de/publikationen/schriftenreihe/ [06.06.2011].

Forum Wissenschaft und Zukunft (Hrsg.): *Energiezukunft*. In: Internet, 2008, unter URL: http://www.fwu.at/wu_print/2008_11_energiezukunft.pdf [26.05.2011].

IKARUS Security Software GmbH: *Smart Meter Security – KIRAS Projektantrag PL 3.3. 2011.*

Klima- und Energiefonds: *Geförderte Projekte – Smart Grids Zusammenstellung ausgewählter Projekte Aktualisierte Fassung – 2011.* In: Internet, 2011, unter URL: http://www.ffg.at/sites/default/files/allgemeine_downloads/smart_grids_2011.pdf [05.06.2011].

Ladinig, Udo: *BLACK OUT/Maßnahmen des Militärkommando NIEDERÖSTERREICH bei BLACK OUT in der Stromversorgung*. Wien, 2010.

Österreichische Energieagentur (Hrsg.): *European Smart Metering Landscape Report*. In: Internet, 2011, unter URL: http://www.smartregions.net/default.asp?SivuID=26927 [06.06.2011].

PwC Österreich: *Studie zur Analyse der Kosten-Nutzen einer österreichweiten Einführung von Smart Metering.* In: Internet, 2010, unter URL: http://www.e-control.at/portal/page/portal/medienbibliothek/strom/dokumente/pdfs/pwc-austria-smart-metering-e-control-06-2010.pdf [26.05.2011].

Saurugg, Herbert: *Der Cyberspace und die Auswirkungen auf die nationale Sicherheit*. Corvinus Universität, Wien-Budapest, Seminararbeit, 2011.

Steven, John/Peterson, Gunnar/Frincke Deborah A.: *Smart-Grid Security Issues.* In: Internet, 2010, unter URL: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5403159 [10.06.2011]

Toffler, Alvin: *Die dritte Welle.* München: Goldmann Wilhelm GmbH, 1997

Toffler, Alvin/Toffler Heidi: *Revolutionary Wealth*. New York: Knopf, 2006

U.S. Department of Energy (Hrsg.): *Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues.* In: Internet, 2009, unter URL: http://www.inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf [11.06.2011].

Woyke, Wichard (Hrsg.): *Handwörterbuch internationale Politik.* Opladen: Barbara Budrich, 2006

Zeitung für kommunale Wirtschaft (Hrsg.): *Lehren aus den Blackouts/Hintergründe, Ursachen und Maßnahmen.* In: Internet, 2003, unter URL: http://www.zfk.de/zfk/knowhow/pdf.../hintergrund1203_03.pdf [11.06.2011]