Analyse zur IT-Sicherheit in Energieversorgungs-systemen

Forschungsarbeit

Robin Jüllig

9. Mai 2013

Fachhochschule Köln

Deckblatt

Name, Vorname:	Jüllig, Robin
Kurs:	Master Communication Systems and Networks
Matrikelnummer:	11087125
Betreuer der Arbeit:	Herr Prof.Dr. Waffenschmidt

Ehrenwörtliche Erklärung

Hiermit versichere ich, die vorliegende Studienarbeit selbstständig und ohne Hilfe Dritter angefertigt und nur die angegebenen Quellen verwendet zu haben. Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Unterschrift Student Ort / Datum

Inhaltsverzeichnis

Abstract

Seit dem Angriff von Stuxnet[1] auf Industrieanlagen wurden weltweit immer mehr und immer komplexere Angriffe auf die IT-Systeme und -netzwerke der für die alltägliche Versorgung nötigen, kritischen Infrastrukturen (KRIS) öffentlichkeits-wirksam verzeichnet[2]. Bedingt durch die zunehmende Vernetzung von IT- und Versorgungsinfrastrukturen, die wachsende Bedeutung von (Kleinst-) Rechnern bei der Verwaltung und Steuerung von Infrastrukturen und die Entwicklung von Next Generation Networks wie dem Smart Grid können Angriffe, die früher einst nur einzelnen Rechnern oder Rechnergruppen galten, heute verheerende Schäden über die Rechnergrenzen hinaus anrichten. Die Symbiose von Energieversorgung und IT-Systemen stellt dabei eine der größten Schwierigkeiten dar. Diese Forschungsarbeit untersucht mögliche Risiken und Gefahren für Energieversorgungssysteme. Umfassenden Schutz leistet ins Besondere die Verwendung von Informationssicherheits-Management-Systemen[3] unter Beachtung des IT-Grundschutzes[4], die ausgehend von einer umfangreichen Risikoanalyse mögliche Maßnahmen zur Vermeidung von Gefahren bereitstellen. Die Aktualität der Sicherheitsmaßnahmen wird jedoch durch Cyber-Sicherheitsstrategien[5] gewährleistet. Dadurch kann die breite Masse an Kritischen Infrastrukturen effizient gegen IT-Angriffe abgesichert werden.

Key Words:

Energieversorgungssysteme, IT-Security-Management-System, IT-Grundschutz, Cyber-Sicherheit, Notfallmanagement, Datensicherheit, Risikoanalyse

---

1 Stuxnet, auch bekannt als RootkitTmphider: Speziell für das SCADA-System *Simantic S7* der Firma Siemens entwickelter Computerwurm, entdeckt im Juni 2010. Schäden unter anderem an Zentrifugen zur Urananreicherung in iranischen Kernkraftwerken

2 http://ibmexperts.computerwoche.de/commerce/artikel/cyber-angriffe-auf-deutsche-organisationen-werden-immer-komplexer, Stand 16.06.2013 vom 04.04.2013

3 Informationssicherheits-Management-System, kurz ISMS: „Ein Managementsystem für Informationssicherheit legt fest, mit welchen Instrumenten und Methoden die Leitungsebene einer Institution die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt.“ [BSI 1]

4 IT-Grundschutz: Methodik zur Identifizierung von Risiken in der IT-Umgebung sowie Umsetzung von Sicherheitsmaßnahmen zur Gewährleistung eines Mindestsicherheitstandes

5 Cyber-Sicherheit: Identifizierung und Behebung von kurzlebigen IT-Sicherheitsrisiken bedingt durch Angriffe aus dem virtuellen Raum (Cyber-Realm). http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/cybersicherheitsstrategie_node.html

Einführung

Der Wandel von analog gesteuerten Infrastrukturen im Bereich Energie, Gas und Wasserversorgung zu digital Verwalteten ist im vollen Gange [SPC]. Nur noch in einigen Nischen existieren weiterhin Felddienste, bei denen Mitarbeiter im Außenbereich manuell nach Fehler suchen und diese beheben. Der deutlich höhere Anteil an IT-Systemen und -netzen in der Verwaltung und Steuerung von Infrastrukturen macht sich bemerkbar: geringere Personalkosten, schnellere Reaktionszeiten, stärkere Unterstützung von Entscheidungsprozessen durch bessere Datenanalyse. Teilweise werden ganze Bereiche der öffentlichen Versorgung teil- oder vollautomatisch betrieben. Doch dadurch steigt auch die Bedrohung solcher Bereiche durch sogenannte „Cyber-Angriffe“, wie eine aktuelle Studie der OSZE zeigt[6]. Angriffe also, die über das Internet auf die IT-Systeme und -netze von Firmen, Versorgern und Behörden ausgeführt werden und deren Täter am anderen Ende der Welt sitzen können [COLLIER][CYBER]. Deutschland ist dabei durch seine viele forschenden Unternehmen, die Aufteilung der Versorgungsdienstleister und seine hohen immateriellen Ressourcen ein lohnendes Ziel, da die vielen (kleinen) Mittelständischen Unternehmen, Kommunen und Länder oftmals nicht ausreichend in ihre IT-Sicherheit investieren [WDR] [KRITIS]. Und die Bedrohungsszenarien sind vielfältig. Betrachtet man die vom Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Bundesbehörde für Katastrophenschutz (BBK) erarbeiteten Übersicht über die Branchen und Sektoren von Kritischen Infrastrukturen, so findet man nahezu jeden Bereich des öffentlichen Lebens wieder.

Sektoren Kritischer Infrastrukturen	
Energie	Transport und Verkehr
Informationstechnik & Telekommunikation	Finanz- und Versicherungswesen
Gesundheit	Staat und Verwaltung
Wasser	Medien und Kultur
Ernährung	

Sektorenübersicht der Kritischen Infrastruktur[7]

6 http://www.golem.de/news/osze-cyberangriffe-koennen-energieversorgung-gefaehrden-1307-100366.html

7 Nach http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html

Das ein Bewusstsein für Cyber-Angriffe in der öffentlichen Meinung entstanden ist, zeigen nicht nur Bücher wie „Black Out“ von Marc Elsberg oder Hollywood Blockbuster wie „Stirb Langsam 4.0“, in denen IT-Systeme erfolgreich angegriffen werden und das alltägliche Leben lahm legen. Auch die Suchanfragen zum Thema „Cyber War“, „Cyber crime“ oder „Cyber Warfare“ sind seit 2004 gestiegen und verdeutlichen das öffentliche Interesse[8]. Seit 2009 ist der „virtuelle Krieg“ sogar offizieller Bestandteil im „United States Cyber Command Asset“ der Vereinigten Staaten von Amerika[9]. Man geht sogar davon aus, dass „cyber war“ eine höhere Schadenswirkung auf Zivilisten haben kann, als die Bombardements während des Zweiten Weltkrieg. Dieses Bewusstsein für Bedrohungen aus dem Cyber-Space wurde in den USA zuletzt auch immer wieder durch Angriffe auf das veralte Energieversorgungsnetz geschärft. Schließlich stellt ein Stromausfall das Worst-Case-Szenario dar, denn nichts funktioniert mehr ohne Strom [LORENZ]. Die wirtschaftlichen und sozialen Schäden eines langanhaltenden Stromausfalles sind enorm [FASE]. Gerade in einem sehr dicht besiedelten Gebiet wie Deutschland stellen Stromausfällen nationale Katastrophen dar und erfordern entsprechende Sicherheitsmaßnahmen – auch in der IT [TAB2].

In Gesprächen mit Vertretern der Firmen IVU, SecuNet und dem TÜV Rheinland zeigte sich, dass dieses Bewusstsein für Cyber-Angriffe und ihre Schäden auch im deutschen Mittelstand angekommen ist. Die Umsetzung der notwendigen Investition in Techniken zum Schutz ihrer IT-Systeme werden jedoch noch von einem kleinen Teil getätigt. Es stellen sich zudem regionale und nationale Unterschiede im Umgang mit IT-Sicherheit heraus. Während man in London beispielsweise durch mehrere Sicherheitsschleusen muss, um an die kritische IT-Systeme heranzukommen, kommt man in vielen deutschen Städten oftmals ungehindert an Zugriff zu kritischen Systemen [COLLIER]. Verschärfend kommt hinzu, dass es in Deutschland oftmals zu einer „Schweigespirale“ kommt und sich betroffene Firmen „schämen“, die Angriffe zu melden[10]. Notwendige nationale Strukturen zur Hilfe vor und bei Angriffen stehen dabei jedoch zur Verfügung (Cyber-Lagezentrum in Bonn oder Cyber-Kompetenzzentrum NRW), es fehlt jedoch an der notwendigen Meldekultur bei Schadensfällen. Ebenso herrscht eine postventive Mentalität. Man wartet häufig erst bis zum Ernstfall und beseitigt die dabei entstandenen Schäden. Kosten-Risiko-Analysen zur Ergreifung von präventiven IT-

8 Von Google Trends, Suche nach „cyber war“ und „cyber warfare“ http://www.google.com/trends/explore?q=cyber+war%2C+cyber+warfare#q=cyber%20war%2C%20cyber%20warfare&cmpt=q

9 http://en.wikipedia.org/wiki/United_States_Cyber_Command

10 http://www.ftd.de/it-medien/computer-technik/:cyberkriminalitaet-unternehmen-erschweren-schutz-vor-hacker-attacken/70044299.html

Grundschutzmaßnahmen werden seltenst angewendet [FASE][EIAS]. Die Notwendigkeit zur Wertschätzung der IT-Sicherheit in Netzen ist jedoch gegeben[11].

Um das notwendige Bewusstsein zu schärfen und Lösungen anzubieten, werden in dieser Arbeit die Rolle von Energieversorgungssystemen in der Bundesrepublik als Teil der Kritischen Infrastrukturen betrachtet. Während andere Branchen wie Finanzdienstleistung oder Ernährung ebenfalls eine hohe Rolle spielen, so stellt der Energie- und vor allem der Stromversorgung durch ihre gegenseitige Abhängigkeit von und zu der IT/Telekommunikationsbranche eine Besonderheit dar. Ohne die Stromversorgung fallen die notwendigen Steuerungs- und Verwaltungsrechner aus, welche die Stromversorgung herstellen. Im Schlimmsten Fall führt dies zu einem gegenseitigen „Dead Lock“ - einer Pattsituation in der beide Systeme sich gegenseitig blockieren und nicht weiter arbeiten können [SCEI].

Im weiteren Verlauf der Forschungsarbeit wird der Aufbau der Energieversorgung in Deutschland anhand der Stromversorgung erläutert, elementare Schwachstellen der IT-Systeme dargestellt und eine Strategie erarbeitet, in wie weit die vom Bund bereitgestellten IT-Grundschutz- und Cyber-Sicherheitsstrategien eine grundlegende Schutz vor Angriffen auf Energieversorgungssysteme gewährleisten können.

In dieser Arbeit wird der Begriff „Energie“ mit „Strom“ gleichgesetzt, auch wenn dies Energieträger wie Kohle, Öl und Gas ausschließt.

11 http://www.thueringer-allgemeine.de/web/zgt/leben/detail/-/specific/Netzbetreiber-sollen-staerker-auf-IT-Sicherheit-achten-1355871530 Stand 16.06.2013 vom 1.6.2013

Aufbau der Energieversorgungssysteme in Deutschland

Das Energieversorgungsnetz in der Bundesrepublik Deutschland lässt sich in vier Spannungsbereiche einteilen (siehe Illustration 1):

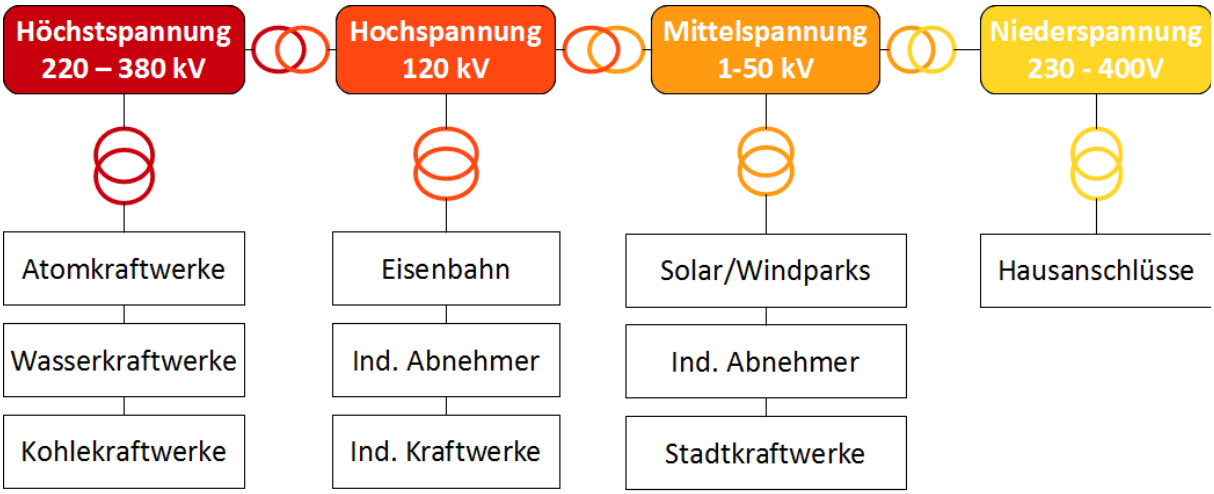

Illustration 1: Aufteilung des Energieversorgungsnetzes in

1. Höchstspannung
   Der Höchstspannungsbereich beherbergt mit den Atom-, Kohle- und Wasserkraftwerken und Höchstspannungsleitungen die Hauptversorgungselemente. Sie stellen die Aorta und Basis der Energieversorgung dar. Das An- oder Abschalten der Kraftwerke oder -blöcke in diesem Bereich ist sehr langsam und kostenaufwendig. Es besteht daher das Interesse diese Kraftwerke möglichst lange am Netz zu lassen. Verbraucher in diesem Bereich sind vor allem Pumpspeicherkraftwerke und Energiespeichersysteme, welche die Überschüsse in der Energiebereitstellung auffangen und bei Gelegenheit langsam in das Netz zurückspeisen können. Potentielle Angriffe auf Anlagen im Höchstspannungsbereich können zu enormen Kosten und Schäden führen.
2. Hochspannung
   Im Hochspannungsbereich befinden sich mit der Eisenbahn und industriellen Großabnehmern energiehungrige Verbraucher. Deren An- und Abschalten kann zu enormen Spitzen im Energieverbrauch und somit hohen Engpässen/Überschüssen führen. Industrielle Kraftwerke, die Strom für den Eigenbedarf der Fabriken produzieren, können bei Unterlast hohe Mengen an Strom in das Netz einspeisen. Schwankungen in der Netzlast können jedoch mit hohem Verlauf vorausgesagt werden.

3. Mittelspannung
   Der Mittelspannungsbereich umfasst neben den Wind- und Solaranlagen auch die städtischen Kraftwerke beispielsweise Müllverbrennungsanlagen oder geothermal Anlagen. Der enorme Zuwachs solcher Techniken in den letzten Jahren führt zu einer deutlichen Dezentralisierung der Energieversorgung und der unabhängig einiger Städte von den großen Energieversorgern. Die hohe Menge dezentraler Einrichtungen führt jedoch zu starken regionalen und nationalen Schwankungen in der Energieversorgung. So können unter optimalen Bedingungen mehr als 50% des nationalen Verbrauches der Bundesrepublik durch regenerative Kraftwerke im Mittelspannungsbereich gewonnen werden[12]. Da die hier verwendeten Anlagen für die Erzeugung von Energie von einigen wenigen Herstellern sind, stellt dieser Bereich auf Grund seiner Größe und Beschränkung verwendeter Techniken einen potentiell lohnendes Ziel dar.
4. Niederspannung
   Im Niederspannungsbereiche sind vor allem die Hausanschlüsse für Wohnungen und Büroräume wieder zu finden. Es gibt in diesem Bereiche viele, kleine Abnehmer und im Vergleich wenige Kleinerzeuger. Angriffe auf Anlagen in dem Niederspannungssektor können sich gegen Stadtteile und Orte wenden, um Dominoeffekte zu erzeugen, oder richten sich konkret gegen einzelne Firmen oder Haushalte. Die verwendeten Systeme können auf Grund weiter Verbreitung zu lohnenden Angriffszielen werden.

Zwischen den einzelnen Spannungsbereichen befinden sich Umspannwerke (auch Trafo-Stationen genannt), welche die Spannungen umwandeln (gekennzeichnet durch ineinander verschlungene Kreise).

Die zunehmende Produktion von Energie durch Wind- und Solaranlagen in den Nieder- und Mittelspannungsnetzen führt zudem zu einer Wandlung einstiger Verbraucherbereiche in Erzeugerbereiche. Hierdurch entstehen neue Daten- und Energieflüsse aus diesen Bereichen in die darüber liegenden (Bottom-Up) [TAB]. Sowohl das Energie- als auch das Datennetz werden bidirektional, wodurch die Netzelemente reaktive Komponenten besitzen müssen. Dies heißt konkret, dass die Energieerzeugung im Stadtbereich durch städtische Solaranlagen zur Einspeisung von Strom in den Hochspannungsbereich führen kann. Die Information zur Einspeisemenge muss in den Höchstspannungsbereich weitergeleitet werden, um gegebenenfalls die Abschaltung eines Kraftwerkes oder die Aktivierung von Energiespeichern auszulösen. Eine feindselige Manipulation der in den IT-Systemen und -netzen verarbeiteten Daten

12 http://www.focus.de/immobilien/energiesparen/kraft-von-26-atomkraftwerken-deutschland-produziert-so-viel-oekostrom-wie-nie_aid_965083.html

kann somit zu Schäden und Kosten jenseits der Netzgrenzen führen, wenn Bauteile beschädigt werden oder Kraftwerke ineffizient arbeiten [FASE].

Durch die neue Dynamik des Energieversorgungsnetzwerkes steigt die Bedeutung der erhobenen Daten. Anhand dieser können effektive Vorhersagen getroffen werden, beispielsweise wie wahrscheinlich es ist, dass diverse Verbraucher an- oder Kraftwerke abgeschaltet werden können [FORECAST]. Die höheren Datenmengen stellen die vorhandenen IT-Systeme und -netze jedoch vor neue Herausforderungen, da sie zu erhöhtem Datenverkehr, schnellerer und präziserer Datenverarbeitung und der Verbesserung der Vorhersagetechniken zu dem Verhalten der Informationsflusses führen.

Bei der Verteilung von Systemen zur Energieversorgung und Datenerhebung wird zudem folgendes Phänomen festgestellt: Je mehr Anwender es in einem Bereich gibt, umso allgemeiner sind die Systeme. Häufig gibt es nur ein paar wenige Dutzend unterschiedliche Hersteller für Haus- und Büroanwendungen. Je weniger Anwender es gibt, umso spezifischer werden jedoch die Anlagen und umso spezifischer werden auch die Angriffe. Für wenige spezielle Anlagen wird also Expertenwissen benötigt [EIAS]. So ist Stuxnet beispielsweise maßgeschneidert auf Anlagen der Firma Siemens angesetzt worden[13]. Dadurch ergibt sich nicht nur ein Schaden für die befallenen Systeme sondern auch für die Herstellerfirmen. Mittels eines Angriffes können somit auch gezielt mehrere verschiedene Branchen angegriffen und geschädigt werden.

Datenquellen in Energieversorgungssystemen

Cyber-Angriffe auf IT-Systeme und -netze verfolgen stets eines von zwei Zielen: Einerseits versucht man durch das Gewinnen von Informationen über das Opfers mittels Datendiebstahl, Kombinatorik oder Beobachtung des Opferverhaltens die eigene Organisation in eine vorteilhafte Lage zu bringen. Andererseits besteht durch das Stören, Unterbrechen, Einspielen fehlerhafter Informationen oder Zerstörung von Daten und Geräten die Möglichkeit, das Opfer nachhaltig zu schädigen [CYBER]. Durch eine subtile, langanhaltenden Schädigung kann ein Angriff zudem sehr gut vertuscht werden, da oftmals andere Ursachen (Materialermüdung o.Ä.) zuerst untersucht werden[14].

Dabei ist es von besonderem Interesse die Daten zu ermitteln, die ein Angreifer für seine Zwecke verwenden kann. Hierbei sollte zwischen **Verwaltungsinformationen** und **Steuerdaten** in dem **Energieversorgungsnetz** und dem **IT-Netz** unterschieden werden.

13 http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/slides.pdf

14 http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

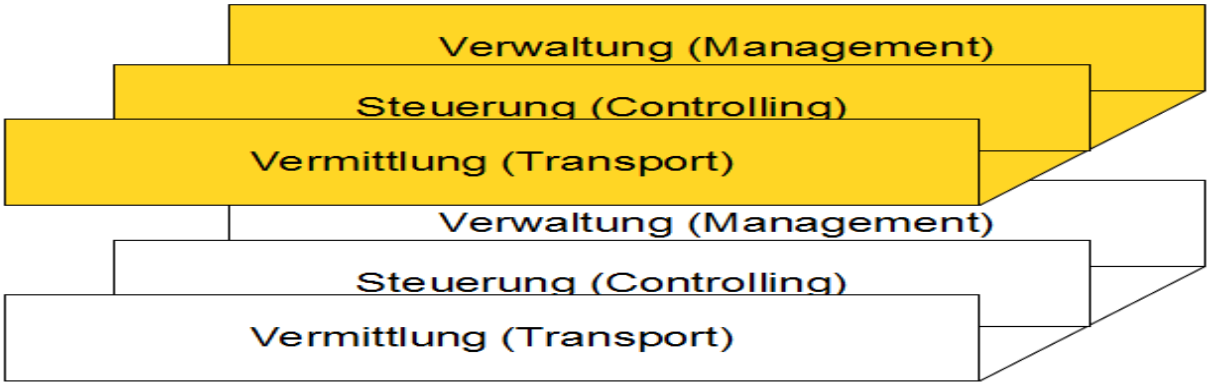

Illustration 2: Illustration 2: Die Datenebenen in Energieversorgungs- (gelb) und IT-Netzwerken (weiß)

Steuerdaten	Energieversorgungsnetz	IT-Netz
Nutzen	Steuerdaten erlauben es, einzelne Netzkomponenten effizient anzusprechen und zu steuern. Dabei können mechanische Elemente beispielsweise Schließventile angesprochen oder Transformatoren ans Netz angeschlossen werden.	Mittels Steuerdaten wird der Informationsfluss im Netz gewährleistet. Komponenten können hinzugefügt, entfernt oder geändert werden.
Risiko	Sofern Steuerdaten nicht richtig, gar nicht oder mehrfach angekommen, wird ein falscher Effekt erzeugt, das Element reagiert gar nicht oder reagiert mehrfach. Dadurch wird es unsachgemäß bedient, es kann zu Schäden an der Komponente und angeschlossenen Elementen kommen. Ausgefallene Komponenten können zum Ausfall der IT-Systeme zur Steuerung des Energienetzes führen.	Fehlerhafte Befehle können zu einer unsachgemäßen Bedienung führen. Im schlimmsten Fall werden Einstellungen gelöscht, sodass die über das IT-Netz vermittelten Steuerdaten für das Energieversorgungsnetz nicht mehr bei deren Komponente angekommen.

Verwal-tungs-information en	Energieversorgungsnetz	IT-Netz
Nutzen	Die Erhebung und Verarbeitung von Verwaltungsdaten kann in Optimierungsprozessen zur Steigerung der Effizienz sowie für ein genaueres Vorhersagemodell verwendet werden. Somit können Steuerdaten bestmöglich konfiguriert werden. Zudem können wichtige Informationen über den Zustand der Geräte, des Energieflusses und für die Abrechnung gewon-nen werden. Es besteht die Möglichkeit zur Fernwartung und Fehlersuche /-behebung.	Zur optimalen Verwendung des Netzwerkes und der Routingverfahren werden Verwaltungsinformationen benötigt. Mittels einfacher Protokolle können dabei der Stand und die Auslastung des Netzwerkes erfasst werden. Zudem können wichtige Informationen über den Zustand der Geräte, des Energieflusses und für die Abrechnung ge-wonnen werden. Es besteht die Möglichkeit zur Fernwartung und Fehlersuche /-behebung.
Risiko	Fehlende Daten bei der Abrechnung können zu Verlusten in der Bilanz führen. Ineffiziente Prozesse bei Optimierung und Vorhersage von Nutzerverhalten resultieren in einem nicht optimalen Netz und können gegebenenfalls in einer Unterver-sorgung enden.	Fehlerhafte Daten beim Management des Netzes resultieren oftmals in einem schlechteren Netzverhalten und verringerte Qualität der Dienstleistungen. Diese können in darüber liegenden Anwen-dungen zu Problemen führen (Datenverlust, Fehlerhafte Daten).

In der folgende Grafik werden exemplarisch die Daten dargestellt, die in mittelgroßen Hausanschlüssen (Mehrfamilienhaushalt, Bürogebäude) anfallen. Diese Daten können abstrahiert auf alle anderen Bereiche angewendet werden, da es sich hierbei um einfach Verbraucher beziehungsweise Erzeugerdaten handelt. So kann die „Heizung“ im Einfamilienhaushalt auch für ein elektrisch gesteuertes Lagerverwaltungssystem in einem kleinen mittelständischen Unternehmen stehen. Die Grafik dient vor allem der Trennung von Daten, die der Energieversorger, der Eigentümer der Immobilie und der Kunde benötigen.

Dadurch entstehen Schnittstellen, die im späteren Verlauf der Arbeit betrachtet werden.

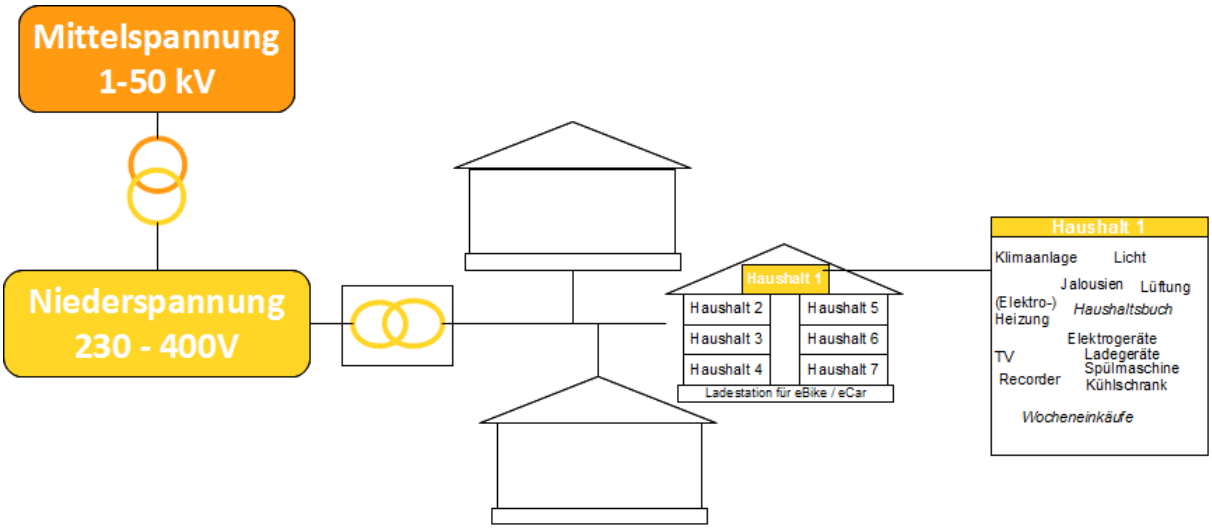

Illustration 3: Datenaufkommen in den Spannungsbereichen (exemplarisch im Niederspannungsbereich)

Wie in Illustration 3 zu erkennen, treten im Niederspannungsbereich bereits etliche Datenquellen auf, welche für den Energieversorger, Netzbetreiber und Kunden von unterschiedlicher Bedeutung sind. Deutlich zu erkennen sind einzelne Haushalte (beispielsweise Haushalt 1) mit verschiedenen Verbrauchern sowie *Prozessen*, die sich aus den Verbrauchern ableiten lassen. Diese Prozesse können für Angreifer von Interesse sein. Sofern der Angreifer beispielsweise feststellt, dass das Licht im Wohnzimmer über lange Zeit nicht mehr verwendet wurde, kann er auf einen Leerstand der Wohnung schließen und gegebenenfalls einbrechen. Die Geräte und Prozesse in Illustration 3 sind exemplarisch. So kann der Kühlschrank im Haushalt 1 auch für eine Dampfturbine in einem Kohlekraft der Höchstspannungsebene stehen und der Prozess *Haushaltsbuch* für eine Produktionsprozess bei einem industriellen Großabnehmer.

Ein Großteil wichtiger Geschäftsprozesse in Familien oder Firmen wirkt sich indirekt auf den Stromverbrauch aus. Die Überwachung der Energieversorgung kann somit zu Rückschlüssen auf laufende Prozesse führen[15]. Für den Angreifer sind in diesem Fall die **Verwaltungsinformationen** von Interesse, die aber auch dem Kunden zur Verfügung gestellt werden. Die folgende Tabelle vergleicht den Nutzen und das Risiko erhobener Verwaltungsdaten für den Kunden:

15 Seitenkanalangriff: Bei einem Seitenkanalangriff auf elektrische Komponenten versucht man beispielsweise über den Energieverbrauch oder Wärmentwicklung herauszufinden, welche Komponente aktiv sind und wie man auf einen Prozess zurückschließen kann.

Verwaltungs-informationen	Messhäufigkeit	Nutzen für den Kunden	Risiko bei Angriff
Erzeugter Strom	Echtzeit (3-5min) ergibt sich aus Summierung: Stündlich, Täglich, wöchentlich, Monatlich, jährlich, ...	+ Der Kunde weiß, wie viel Strom er erzeugt + er kann ermitteln wie viel CO2 er spart oder wie viele Zertifikate er verkaufen kann + er kann ermitteln, wie viele Kosten er spart, wenn er hätte Strom zukaufen müssen	- Der Angreifer weiß, wie viel Strom erzeugt wird - er kann gegebenenfalls CO2 Käufe manipulieren - er kann ermitteln, wie wichtig das potentielle Opfer für die Stromversorgung auf dieser Schicht ist
Verbrauchter Strom	Echtzeit (3-5min) ergibt sich aus Summierung: Stündlich, Täglich, wöchentlich, Monatlich, Jährlich, ...	+ Der Kunde weiß, wie viel Strom er verbraucht + er kann ermitteln wie viel CO2 er erzeugt oder wie viele Zertifikate er kaufen muss + er kann ermitteln, wie viele Kosten er spart, wenn er hätte Strom selbst erzeugen würde + er kann seinen Verbrauch abschätzen und Prozesse entsprechend auslegen	- Der Angreifer weiß, wie viel Strom verbraucht wird - er kann gegebenenfalls CO2 Käufe manipulieren - er kann ermitteln, welche Rolle das Opfer für den Stromverbrauch dieser Schicht spielt - er kann den Verbrauch und laufende Prozesse abschätzen
Eigenbedarfsdeckung	Vergleichend: Erzeugung/Verbrauch	+ Der Kunde kann seine Abhängigkeit vom Strommarkt abschätzen + Er kann seine Kosten bzw. Erträge durch Verbrauch bzw. Erzeugung abschätzen	- Der Angreifer kann die Abhängigkeit des Opfers von seinen eigenen Erzeugern ermitteln - Sabotage der Erzeuger und Leistungsminderung dieser kann zu hohen Schäden für das Unternehmen führen i.B. bei hoher Eigenbedarfsdeckung
Durchfluss	Echtzeit	+ Der Kunde kennt den Energiefluss in seinem Unternehmen + Er kann ermitteln welche Komponenten zu- oder abgeschaltet werden können/müssen	- Der Angreifer kennt den Energiefluss in dem Unternehmen - Er kann kritische Komponenten ermitteln und schädigen

Daten für die Vorhersage		+ Der Kunde kann seine eigenen Prozesse beobachten und daraus Rückschlüsse auf den Strommarkt entwickeln. Anhand dieser kann er sein Verhalten anpassen + Kurzfristige Schwankungen können vorhergesagt und präventiv angegangen werden	- Der Angreifer kann das Verhalten des Opfers beobachten und es in gefährliche Situationen zwingen (bspw .durch Fehlinformationen) - Kurzfristige Schwankungen können vorgetäuscht werden
Daten für die Optimierung		+ Der Kunde kann aus seinem Verbrauch/Erzeugung ermitteln, wann er Strom billig kaufen/ teuer verkaufen kann + er kann seine Prozesse an den Strommarkt anpassen	- Der Angreifer kann aus dem Verbrauch/Erzeugung ermitteln, wann Strom billig gekauft/ teuer verkauft werden muss. Eine Störung des Stromhandels führt zu hohen Kosten bei dem Opfer. - er kann die Abhängigkeit der Prozesse von dem Strommarkt ermitteln und ausnutzen, um sie ineffizient zu machen
Aufwand/ Ertrag		+ Der Kunde kann Echtzeitdaten ermitteln und diese in seine Bilanz / Haushaltsplanung übernehmen	- Der Angreifer kennt die genaue Marktposition seines Opfers - Er kann Haushaltsplanung und Bilanz in Echtzeit negativ beeinflussen

Um dem potentiellen Opfer direkte Schäden beizufügen oder um Kontrolle über Netzelemente des Energieversorgungs- oder des IT-Netzwerkes zu erhalten, benötigt der Angreifer die **Steuerdaten**. Die folgende Tabelle vergleicht den allgemeinen Nutzen und das Risiko verwendeter Steuerdaten für das Energie- und IT-Netz aus Sicht des Kunden:

Steuerdaten	Messhäufigkeit	Nutzen für Kunden	Risiko bei Angriff
Zustand der Komponenten	Echtzeit	+ Der Kunde weiß jederzeit, welche Netzkomponente sich in welchem Zustand befindet + Der Zustand beschreibt dabei neben dem Status (aktiv, inaktiv, warte auf Antwort usw.) auch die auf der Transportebene anliegende Daten bspw. den Energiedurchsatz / Stunde + Durch Fernzugriff können Fernwartungen durchgeführt werden	- Der Angreifer kommt in den Besitz wichtiger Informationen für den Betrieb des Netzwerkes - Er kann zudem den Zustand des Transportnetzes ermitteln und die Wegführung (Routing) im Transportnetz verändern - Durch das Einspeisen von Fehlinformationen kann er zu Kritischen Gefährdungen für das Netz führen
Instandhaltungstermine /Intervalle	Bei Bedarf, auf Abfrage	+ Der Kunde kennt den Wartungszustand seiner Komponenten + Er weiss, welche Komponenten welchen Verschleiß aufweisen und kann Ersatz vorbestellen + Er kann Komponenten maximal ausnutzen, in dem er sie optimal betreibt	- Der Angreifer kann den Wartungszustand der Geräte manipulieren - Er weiss, welche Komponenten verschleißanfällig sind und kann teure oder für das Netz neurale Komponenten gezielt schädigen - Durch Fehlinformationen kann er zur Über-/ Unterlastung von Komponenten führen und damit Schäden hervorrufen
Probleme / Fehlermeldungen	Echtzeit, reaktiv	+ Der Kunde kann Probleme in seinem Netzwerk ermitteln und darauf reagieren + Er kann den Fehlerstatus von Komponenten einsehen und diese austauschen + Häufige Probleme und Fehler können effektiver	- Der Angreifer kann Fehler und Meldungen ermitteln, diese duplizieren und erneut einspielen - Er kann Fehlerstatus von Komponenten einsehen und verändern - Durch die Analyse der Fehler können Dominoeffekte festgestellt

		behoben werden + Man kann bereits aus der Ferne potentielle Fehlerquellen ermitteln + Die Fehlersuche im Netz kann per remote erfolgen	und ausgelöst werden - Potentielle Fehlerquellen können virtuell erzeugt werden
Fehler in Steuerdaten	Bei Bedarf, auf Abfrage	+ Der Kunde kann erkennen, ob seine Steuerdaten unverfälscht bei der Komponente angekommen + Er kann erkennen, was fehlerhafte Steuerdaten auf den Komponenten für Fehler anrichten.	- der Angreifer kann Angriffe in Steuerdaten tarnen oder Steuerdaten einfach manipulieren, so-dass Kommandos nicht ankommen.
Netzwerk-qualität	Bei Bedarf, auf Abfrage	+ Der Kunde kennt den Status seines Netzwerkes + Er kann Aussagen darüber treffen, wie gut sein Netzwerk funktioniert + Er kann anhand der vorhandenen Daten sein Netzwerk hinsichtlich Ausfallsicherheit, Risiken und Effizienz optimieren + Wichtige Informationen wie Durchsatz, temporäre Spitzen, Verzögerungen und Durchsatzstärke können ermittelt werden	- Der Angreifer kennt den Status des Netzwerkes - Er kann kritische Stellen im Netzwerk finden und gezielt angreifen - Wichtige Informationen über das Netzwerk und seine Effizienz können gestohlen oder miss-braucht werden
Routing-/ Traffic informationen		+ Der Kunde erhält wichtige Informationen über die Wegführung (Routing) und den Verkehr (Traffic) in seinem Netzwerk + Er kann den Durchfluss in seinem Netz über andere Wege umleiten	- Der Angreifer erhält wichtige Informationen über die Wegführung und den Verkehr im Netzwerk des potentiellen Opfers - Er kann den Durchfluss über schlechtere Wege umleiten und dort zu Verstopfungen und Eng-

		+ Optimale Wege führen zu einer Verbesserung des Netzwerkes + Schwankungen im Netzdurchsatz können erkannt und behoben werden + Störeffekte können lokal eingegrenzt und dort behoben werden + Im Netzwerk kann das Wegführungsverhalten vorhergesagt und optimiert werden	pässen führen - Schwankungen im Netzdurchsatz können erzeugt werden und zu Störungen führen - Das Wegführungsverhalten kann durch fehlerhafte Daten negativ beeinflusst werden und zu Störeffekten führen.
Anzahl und Art von IT-Angriffen	Bei Bedarf, auf Abfrage Echtzeit, reaktiv	+ Der Kunde kann sein Netzwerk überwachen und Angriffe kategorisieren + Dadurch können IT-Sicherheitsmaßnahmen angemessen eingesetzt werden	

Die oben beschriebenen Vor- und Nachteile gelten in den jeweiligen Netzwerken für eine Vielzahl an Komponenten. Durch die hohe Anzahl dieser entsteht ein größerer Verwaltungsaufwand, der jedoch teilautomatisch verwendet werden kann. Da ähnliche Komponenten häufig über das gesamte Netzwerk verwendet werden, steigt die Angriffsfläche und damit die Erfolgsaussicht eines Angreifers. Es bietet sich daher an, ein ganzheitliches Informations-Sicherheits-Management-System (ISMS) zu verwenden, dass beiden Netzwerke – IT- und Energieversorgungsnetz- umfassend abbildet und sichert.

Hierfür bietet sich jedoch zunächst eine Schwachstellenanalyse an.

Schwachstellenanalyse

In heutigen Netzwerken spielen ins Besondere drei Datentypen eine entscheidende Rolle. Ihr Verlust oder ihre Manipulation können zu einem enormen Vertrauensverlust, zu hohen Schäden an Mensch, Material und Maschine sowie diversen Kosten führen.

1. Personenbeziehbare Daten

Unter Personenbeziehbaren Daten versteht man die kleinste, disjunkte Datenmenge, welche eineindeutig einer juristischen oder reell existierenden Person zugeordnet werden kann[16]. Die Korrelation von Eigentümer und Daten führt zu einem genauen Abbild des Verhaltens. Neben persönlichen Daten wie Adresse und Geburtstag gelten auch Kontodaten und IP-Adressdaten als personenbeziehbaren Daten. Der Verlust solcher Datensätze führt zu einem hohen Misstrauen und folglich zu einem Ansehensverlust der Firma. Die Erhebung, Verarbeitung und Verwendung von personenbeziehbare Daten unterliegt dem Datenschutzgesetz .In Energieversorgungsnetzen können mehrere Bereiche klar abgetrennt werden:

1. „Heim“- Ebene

Auf der Heimebene wird der kleinsten Bereich der Datenerhebung dargestellt. Hier sind Privat- und Firmenkunden zu finden, die in ihren Haushalten, Büros oder Fabriken verschiedenste, für sie immens bedeutsame Informationen erzeugen. Diese können für sie von besonderem Interesse sein und sollten in der Regel nicht die „eigenen vier Wände“ verlassen. Diese Abschottung des Privathaushaltes wird in letzter Zeit durch einheitliche „Smart Home“ / „Smart Office“ Lösung großer Energiekonzerne aufgeweicht. So ist bei „Lösungen aus einer Hand“ beispielsweise von RWE oder Siemens fraglich, welche Daten diese zusätzlich erheben und an ihre Firmenzentralen weiterleiten. Es bietet sich an, den „Heim“-Bereich getrennt zu betreiben und eine klare Schnittstelle nach oben zu definieren.

2. Gebäudeebene

In einem Gebäude treffen ein oder mehrere Heimebene aufeinander. Während für den Gebäudebetreiber der Verbrauch einzelner Untermieter interessant ist, müssen für die höheren Netzebenen solche Informationen nicht von besonderem Interesse sein. Die Verwaltung des Gebäudes selber kann als weiterer Heimbereich modelliert werden. Erste Lokale Schwankungen können auf dieser Ebene geglättet werden, indem der Gesamtverbrauch des Gebäudes zu Spitzenzeiten ermittelt wird.

16 Nach http://www.gesetze-im-internet.de/bdsg_1990/__3.html

3. Block-/Orts-/Stadtteilebene

In diesem Bereich sind die Informationen bereits so grob granular, dass man nicht mehr auf einzelne Personen schließen kann. Jedoch können noch gezielt einzelne Gebäude oder Fabrikstandorte überwacht und angegriffen werden. Hauptverbraucher und Spitzenzeiten lassen sich in diesem Bereich bereits sehr gut

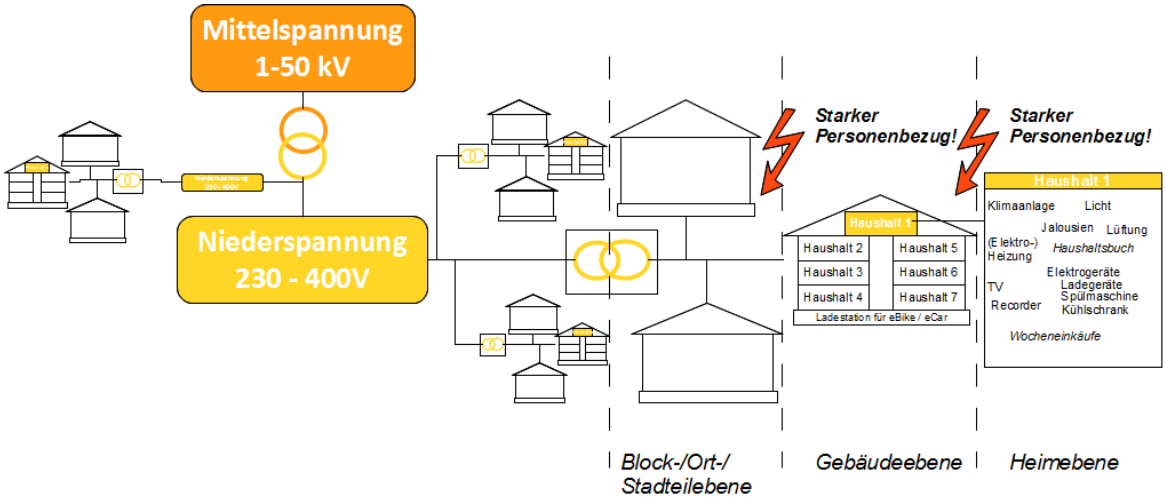

Illustration 4: Personenbeziehbare Daten

ermitteln.

Es bietet sich an, auf den verschiedenen Ebenen bereits zu anonymisieren und Personen- von Verwaltungs- und Steuerdaten getrennt zu halten. Die benötigten Daten zur Abrechnung liegen dann beim Dienstleister vor und fallen in seinen Schutzbedarf.

2. Neurale Daten des Unternehmens

Unter „neuralen“ Daten eines Unternehmens werden sämtliche Informationen verstanden, die für den täglichen Geschäftsbetrieb von Nöten sind. Ebenso werden all jene Daten als „neural“ gewertet, die kritisch für laufende Geschäftsprozesse sind und deren Entwendung im schlimmsten Fall zur Insolvenz oder sofortigen Schließung führt. Darunter fallen beispielsweise die Dokumentation der Geschäftsprozesse, sämtliche Daten zur korrekten Kostenerhebung und -abrechnung, Wartungsstechnische Informationen, Sicherheitsrelevante Daten und natürlich Kundendaten. Ein Großteil dieser Daten läuft in den jeweiligen Schaltelementen der Energieversorgungs- und IT-Netze sowie den Netzwarten zusammen.

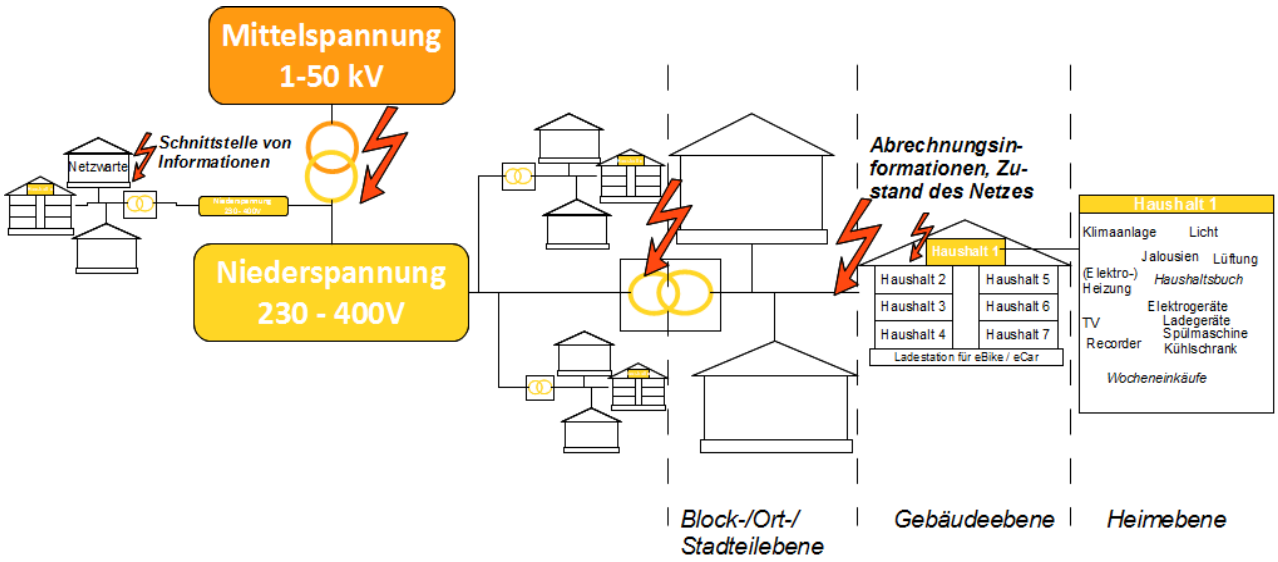

Illustration 5: Neurale Informationen in einem Energieversorgungsnetzwerk

3. Erweiterte Datensätze

   Erweiterte Datensätze dienen in Unternehmen dazu, Prozesse zu analysieren, das Verhalten einzelner Komponenten vorherzusagen und den gesamten Geschäftsprozess zu optimieren. Die Datenbasis, welche die Organisation gesammelt hat, gilt es daher vor Fehlern zu schützen. Jedoch werden auch solche Informationen zu den erweiterten Datensätzen gezählt, welche eine Aussage über die Autarkie oder die Abhängigkeit des Unternehmens von anderen machen. Hierzu zählen beispielsweise Lieferketten, Engpässe und das Business Continuity Management. Daher wird unterscheiden zwischen:

   1. Datenbasis
   2. Güte der Algorithmen zur Datenanalyse und zur Vorhersage von Verhalten
   3. Art und Anzahl von Fehlern
      1. im Energieversorgungsnetz
      2. im IT-Netzwerk
      3. in den Algorithmen und der Datenbasis
   4. Grad der Autarkie
      1. Unabhängigkeit von Lieferanten
      2. Grad Deckung von verbrauchten und erzeugtem Strom
      3. Redundanzen im Netzaufbau

Diese Daten werden in den Schaltzentralen und Netzwarten erhoben. Auch einzelne Trafostationen können diese Daten erfassen, senden sie aber zeitnah an die Zentralen weiter.

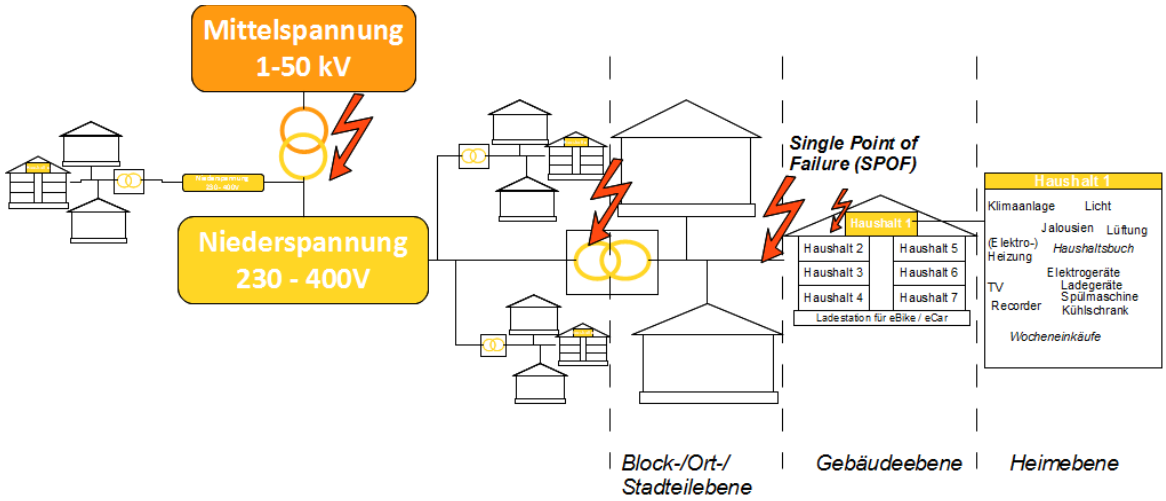

Illustration 6: Übergangselemente und ihre Bedeutung als Single Points of

Übergangselemente zwischen einzelnen Netzwerken werden in der Regel beiden Bereichen zugerechnet. Ein Transformator unterliegt als Schnittstellenelement somit sowohl Regelungen für den Nieder- als auch Mittelspannungsbereich. Die Rolle von Übergangselemente sollte im Rahmen der Schwachstellenanalyse gesondert betrachtet werden, da sie einen ***Single Point of Failure*** (SPOF) darstellen. Hierunter fallen Haushaltsanschlüsse, Hausanschlüsse und Transformatoren sowie entsprechende Elemente im IT-Netzwerk.

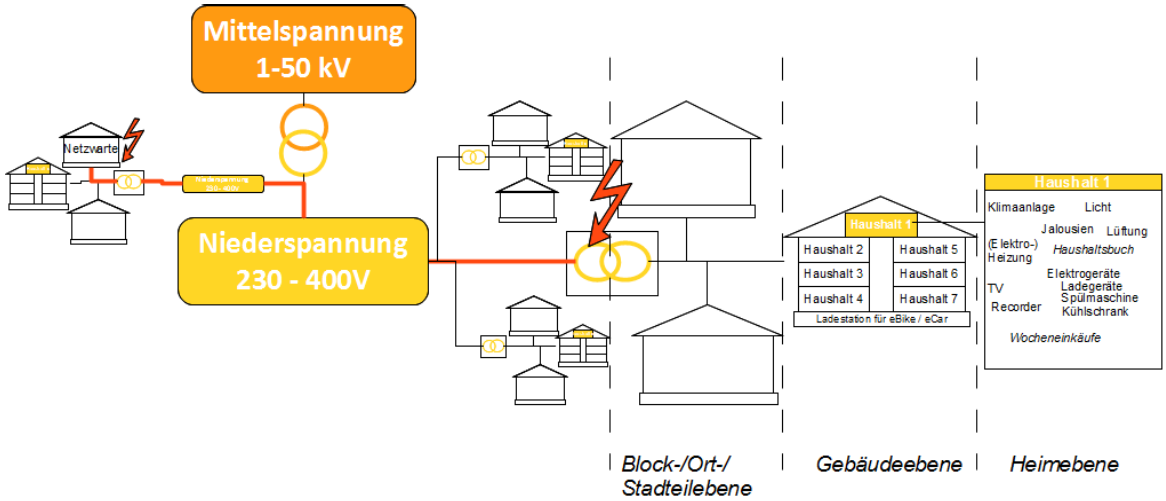

Illustration 7: Schwachstelle Tunneling

In einigen Fällen ist es von Nutzen, auf die Daten per Fernzugriff (Remote Access) zuzugreifen. Darunter fällt im Endkundenbereich vor allem die Möglichkeit die zentrale Heimsteuerung anzusprechen, um Licht, Jalousien, Heizung oder Endgeräte via Handy oder vom Arbeitsplatz aus zu steuern. Im Bereich der Energieversorgungssysteme kommt zudem hinzu, dass durch Fernwartung und Abfrage von Verwaltungsdaten verschiedene Geschäftsprozesse vereinfacht werden, die von einer oder mehreren Netzwarten aus der Ferne ausgeführt werden können. Für diese Verbindungen ist zu beachten, dass die verschiedenen Systeme über das Internet oder ein eigenes IT-Netz weiterhin ansprechbar bleiben und somit auch für Angriffe anfällig sind. Hier können diverse Techniken zum **Tunneln** des Verkehrs von Steuer- und Verwaltungsdaten angewendet werden, um den Kommunikationskanal zu sichern. Diese Kanäle stellen dennoch Schwachstellen dar, da eine unsachgemäße Konfiguration leicht zu Einbrüchen in das gesamte IT-Netz führen kann[17] .

Somit sind nicht nur Endsysteme als Schwachstellen im Netzwerk zu betrachten, sondern auch die Verbindungskanäle. Während die Energieversorgungssysteme diesbezüglich mit wenigen Lösungen für rein physische Probleme auskommen, bieten IT-Netze ein Vielzahl unterschiedlicher Techniken zur Datenkommunikation an [SMCS], welche kurz hinsichtlich ihrer Vor- und Nachteile, sowie den Anwendungsszenarien betrachtet werden:

Funkübertragung	Vorteil	Nachteil	Anwendungsszenario
868 Mhz	+ vielfältige Lösungen, da 868Mhz Band nicht reguliert ist und somit für Open Source Anwendungen verwendet wird + breite Community bei Lösungen wie ZigBee ([WALLRAFF]) Funk	- geringe Bandbreite und Durchsatz zur Datenübertragung, schlecht geeignet für IPv6 Lösungen, da starker Overhead des IP Headers - Interferenzen mit anderen Anwendungen im 868Mhz Bereich - kurze Reichweite	Heimanwendung (RWE Smart Home,), Kurzstreckenfunk, Hausvernetzung
GSM	+ Mobilfunktechnik + ausreichender Durchsatz für kleinere Abfragen + billige Implementierung	- Übertragung von IP Paketen sehr schwer, dh. Übersetzung von Befehlen in „IP“ - angreifbar, Daten können bereits mit wenig	Vernetzung von mobilen Stationen und Ad Hoc Netzwerken, Implementierun

17 http://www.heise.de/security/artikel/Einbruch-ins-VPN-270592.html

	+ wird in Smart Metern und einigen Trafo-Stationen im Außenbereich bereits eingesetzt	Ausrüstung ermittelt werden[18] - Kosten der Rahmenverträge mit Mobilfunkprovidern	g in Smart Metern der ersten Ge-neration
UMTS / LTE	+ Mobilfunktechnik + Durchsatz für Umfangreiche, gebündelte Abfragen + Übertragung von IP Paketen möglich, können somit getunnelt und an die Module einfach weitergeleitet werden. + Sicherer gegen Angriffe + Fernwartung und Aufspielen von Software Updates möglich	- teurer - wenige Implementierungen bekannt - Deckung, dh. nicht überall unbedingt einsetzbar - Starke Abhängigkeit von Mobilfunkprovidern	Vernetzung mobiler Stationen und Ad Hoc Netzwerken in Siedlungsdichten Gebieten
WLAN	+ Sehr hoher Datendurchsatz (bis 600Mbit/s) + billig	- Setzt DSL Anschluss voraus - nur sicher unter WPA - in Firmennetzwerken wird von Verwendung meist abgesehen - größtmögliche Einstiegsstelle für unbemerkte Angriffe	Heim- und Hausvernetzung

Man kann deutliche Unterschiede zwischen einer lokalen und einer überregionalen Verwendungen von Funkübertragungstechniken erkennen. Techniken im Bereich der Heimebene (auch Home Area Network, HAN gennant, [WALLRAFF]) verwenden das 868MHz Band beziehungsweise das 2,4GHz / 5GHz Band und bieten sich für lokale Dienste wie ZigBee oder WLAN an. Sofern die Entfernung größer werden, kommen meist GSM Techniken zum Einsatz, die zwar billiger, aber für Angreifer auch leichter zu attackieren sind als UMTS/LTE.

18 http://myassgeek.wordpress.com/2011/07/31/how-hackers-hack-gsm-phones/

Übertra-gung via Kabel	Vorteile	Nachteile	Anwendungsszenarien
Power Line Communication	+ verwendet die vorhandene Stromversorgung + wird in Heimanwendungen und einigen Smart Meter Techniken bereits verwendet	- Reichweite - unbekannte Auswirkung der Spannungsschwankungen auf empfindliche Komponenten - keine Ausfallsicherheit	Hausanwendung bis Blockebene
Ethernet	+ Günstige im Nahbereich + Gutes Preis/Leistungsverhältnis + Power via Ethernet zur Versorgung kleiner Komponenten möglich	- Ziel auch für Kupferdiebe - begrenzte Reichweite	Heim- und Nahbereich
Glasfaser	+ sehr hoher Datendurchsatz	- sehr teuer	Stadtbereich aufwärts

Die Datenübertragung über Kabel besitzt den Vorteil, dass im Vergleich zu Funktechniken, deutlich mehr Daten übertragen werden können. Dadurch ist es den Netzbetreibern möglich deutlich mehr Verwaltungsdaten zur Optimierung ihrer Netzwerke zu sammeln. Zudem können Fernwartungs- und Fernsteuerungsmethoden sicher verwendet werden, weil Netzausfälle sehr selten sind. Problematisch ist lediglich die gegenseitige Abhängigkeit von Strom- und Kabelübertragungsnetz. Verstärker in den IT-Netzen benötigen notwendigerweise Strom. Sollte dieser von dem Stromnetz geliefert werden, dass sie steuern, kann der Ausfall des einen Netzes den Ausfall des anderen Netzes bedeuten.

Um die Kosten niedrig und das IT-Netzwerk dennoch funktional zu halten, lassen sich meist vorhandene IT-Netzwerke großer IT-Betreiber verwenden. Notfalltechniken basierend auf UMTS und GSM können beim Ausfall des Stromnetzes die notwendigen Daten übermitteln. Große Energieversorger und Netzbetreiber können es sich zudem leisten, eigene IT-Netze aufzubauen, die einzig für ihre Versorgung dienen und somit unabhängig vom Internet sind. Im Wide Area Network Bereich (Stadtbereich) können zudem Kooperationen mit den IT-Dienstleistern oder Hausbesitzern eingegangen werden, um vorhandene Netze zu verwenden. Dafür gilt es jedoch rechtliche Aspekte zu klären. Andernfalls können Power Line Communication Techniken die notwendige Datenübertragung im Stadtbereich zur Verfügung stellen, sofern die Ausfallsicherheit des Daten- und Energienetzes gegeben ist [SCMS].

Umsetzung der IT-Sicherheit in Energieversorgungsnetzen

Nachdem ausführlich dargelegt wurde, welche Bedenken es bei dem Betrieb eines Kommunikationsnetzes für Energieversorger zu beachten gilt, können mögliche Lösungsszenarien entwickelt werden.

Da mit der Verabschiedung des Energie-Wirtschafts-Gesetz (EnWG) auch rechtliche Aspekte hinsichtlich IT-Sicherheit und Datenschutz benannt wurden, stehen zunächst die Rechtlichen Rahmenbedingungen im Mittelpunkt. Anschließend folgt die Erläuterung verschiedener Schutzszenarien und (inter-)nationale Standards sowie die Unterscheidung zwischen IT-Grundschutz und Cyber-Sicherheit [CYBER]. Mögliche Unterstützende Werkzeuge zur Modellierung und Überprüfung der IT-Sicherheit werden unter dem Punkt „ISMS“ zusammengefasst, ehe der Markt hinsichtlich verwendbarer Software analysiert wird.

Rechtlicher Rahmenbedingungen

Das Energiewirtschaftsgesetz (EnWG) wurde mit in Kraft treten zum 07. Juli 2005 eingeführt, um eine „möglichst effiziente und umweltverträgliche leistungsgebundene Versorgung der Allgemeinheit mit Elektrizität [..], die zunehmend auf erneuerbaren Energien beruht [zu sichern]“ [ENWG]. Die aktuellste Version stammt vom 21.2.2013 und dient als Grundlage. Es stechen hierbei vor allem zwei Punkte heraus:

1. Erfassung, Verarbeitung und Übertragung sensibler Daten

In den Paragraphen „§ 6a Verwendung von Informationen“ und ins Besondere den Paragraphen „§ 21c Einbau von Messsystemen“, „§ 21d Messsysteme“, „§ 21e Allgemeine Anforderungen an Messsysteme zur Erfassung elektrischer Energie“ und „§ 21g Erhebung, Verarbeitung und Nutzung personenbezogener Daten“ wird die Bedeutung der „„Vertraulichkeit wirtschaftlich sensibler Informationen“ ([ENWG], §6a) und personenbezogener Daten erwähnt. Für die genaue Ausgestaltung und Umsetzung wird jedoch auf Rechtsverordnungen nach §21i verwiesen. Durch eine mangelnde Aktualität dieser Rechtsverordnungen kann es zu Lücken in der Umsetzung der Maßnahmen und Gewährleistung der IT-Sicherheit kommen. Zudem wird dem Netzbetreiber durch „technische und wirtschaftliche“ Machbarkeit die Möglichkeit offenbart, fehlende Sicherheit und Sorgfalt mit wirtschaftlichem Interesse zu begründen. Mit Einhaltung des §11 Bundesdatenschutzgesetz und Beachtung des §43 BDSG (nach [ENWG] §21g (4)) kann die Erhebung und Verarbeitung personenbezogener Daten zudem an Drittdienstleister. weitergegeben werden. Mit diesen Einschränkungen im Hinterkopf wird das Thema Datenschutz ausgelagert. Der Gesetzgeber behält sich Änderungen vor.

2. Technischer Betrieb des Energieversorgungsnetzes

Paragraph § 11 „Betrieb von Energieversorgungsnetzen“, Absatz 1 definiert, dass Betreiber von Energieversorgungsnetzen „ein sicheres, zuverlässiges und leistungsfähiges Energieversorgungsnetz diskriminierungsfrei zu betreiben, zu warten und bedarfsgerecht zu optimieren, zu verstärken und auszubauen“ haben, „soweit es wirtschaftlich zumutbar ist.“ „(1a) Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die der Netzsteuerung dienen. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen [KS] und veröffentlicht diesen“. Jedoch wird auch hier nur ein angemessener Schutz „vermutet“. Die Schutzziele werden ebenfalls durch den Wirtschaftlichkeit-Aspekt relativiert. So entstehen bereits im Gesetz technische Probleme zum Beispiel bei der verwendeten Verschlüsselung von Daten. Ziel ist es, dass nur der Sender und der Empfänger die Daten lesen können. Während für Messsysteme und die Übertragung von personenbezogenen Daten in allgemeinen Kommunikationsnetzen eine Verschlüsselung nach Stand heutiger Technik verbindlich vorgeschrieben ist (Paragraph § 21e (3)) gilt das nicht für den Betrieb eigener Kommunikationsnetze oder die Übertragung von Daten außerhalb der Messsysteme. Die genauen Vorgehensweisen müssen aus Sicherheitskatalogen entnommen werden, deren Aktualität nicht immer gegeben ist.

Es stellt sich allgemein das Problem heraus, dass die Notwendigkeit von IT-Sicherheit bekannt ist, aber weiterhin an andere Stellen abgetreten wird. Der „Katalog von Sicherheitsanforderungen nach § 109 Absatz 6 Telekommunikationsgesetz (TKG)“ der Bundesnetzagentur ist mit der Veröffentlichung im Amtsblatt Nr. 8 am 08.05.2013 in Kraft getreten. Die Planung und Umsetzung der technischen Vorkehrungen und sonstigen Maßnahmen zur Erfüllung der Verpflichtungen nach § 109 Absatz 1 und 2 und die Erstellung des Sicherheitskonzeptes gemäß § 109 Absatz 4 Satz 1 kann auch auf der Basis anderer geeigneter Standards, Normen (z.B. -Standards, -Grundschutzkataloge, DIN ISO/-Normen) erfolgen. Die Einhaltung der Verpflichtungen nach § 109 Absatz 1 bis 4 ist hierbei jedoch sicherzustellen.[BNA]

Da die ISO Norm 27001 und die IT-Grundschutz des BSI umfangreicher sind und auch Aspekte des Datenschutzes beachten, sollte ein BSI konformes ISMS verwendet werden. Der Sicherheitskatalog umfasst die elementaren Gefährdungen für die Telekommunikationsnetze.

Technische Probleme

Neben den Rechtlichen Rahmenbedingungen gilt es aber auch den aktuellen Stand der Technik zu berücksichtigen. Starke Veränderungen ins Besondere im Bereich der Übertragungstechniken führen häufig zu unsicheren Systemen. Eine fehlerhafte Konfiguration zwischen Übertragung und Anwendungen kann zudem weitere Schwachstellen offenbaren. Die Auswirkungen technischer Änderungen werden anhand der Smart Meter, die stellvertretend für weitere Sensoren im Außendienst herangezogen werden können, deutlich.

Smart Metering

Die Umsetzung des EnWG und der Übergang von analoger zu digitaler Messtechnik begünstigt den Einsatz sogenannter „intelligenter Zähler“ (Smart Meter). Sie ermitteln den Energieverbrauch und die Nutzungszeit in Intervallen und melden mindestens einmal täglich die Daten einer Institution zur Erfassung und Abrechnung des Energieverbrauches. Während die digitalen Zählgeräte der ersten Generation eine Einwegkommunikation zur Zentrale aufbauten, besitzen die Smart Meter heutzutage die Möglichkeit einer bidirektionalen Kommunikation und können somit auch Befehle der Zentrale umsetzen. Sie stellen somit ein „Messsystem“ nach EnWG §21 dar.

Da es für die Verwendung und den Einsatz von Smart Metern bisher keine gesetzlich vorgeschriebenen Standards oder Rahmenbedingungen gibt, herrscht eine gewisse Unsicherheit unter den Energieversorgern. Während Standards wie der IEC 62056-31 “Euridis“ aus den 90er Jahren veraltet sind, weisen auf das Global Mobile System (GSM) aufbauende Standards das Problem auf, dass die Übertragungstechnik nicht mehr als sicher gilt[19]. Smart Meter, die auf UMTS oder gar LTE[20] basieren sind dato noch nicht weitgehend entwickelt. Damit ist auch das Aufspielen von Software Updates auf die Smart Meter weiterhin nicht ohne Umstände möglich. Viele Hersteller neigen außerdem zu proprietären Standards, die auf ihre Geräte zugeschnitten sind. Ein einheitlicher, technisch aktueller Standard für Smart Meter ist in naher Zukunft nicht absehbar. Die fehlende Standardisierung und Verwendung proprietärer Lösungen ist ein Risiko, da die Anwendungen anfällig werden für Cyber Angriffe. Es fehlt zudem die Unabhängige Prüfung des Standards gegen IT-Sicherheitsrisiken[21].

---

19 http://securityaffairs.co/wordpress/1086/cyber-crime/gsm-mobile-the-insecure-network.html

20 LTE: 4G Mobilfunktechnik, Datenraten von bis zu 300Mbit/s, Authentifizierung und Verschlüsselung möglich

21 Nach „Linus Law“ http://en.wikipedia.org/wiki/Linus%27s_law „Genügend Tester finden alle Fehler.“ Mit ausreichend vielen Testern können bei offenen Standards und Systemen entsprechend viele Hintertüren gefunden und beseitigt werden, die als

1. Smart Meter als Teil von Smart Home Techniken

   Die steigende Verwendung sogenannter Smart Home Techniken, die eine Vernetzung des gesamten Haushaltes vorsehen (KNX, RWE) wird häufig von einer Verknüpfung mit den Smart Metern begleitet, welche die Daten der „Heimzentrale“ auslesen können. Es ist jedoch darauf zu achten, dass die im EnWG und BDSG gesetzten Richtlinien eingehalten werden. Ins Besondere bei Lösungen aus „einer Hand“, bei denen der Energieversorger auch die Technik des Smart Home stellt (bspw. RWE) muss die Schnittstelle Haushalt-Haus konkret abgegrenzt werden. Angriffe gegen die Heimtechnik oder das Smart Meter könnten sich sonst negativ auf eine weitere Ebene niederschlagen [DEFCON] [SMHT]. Entsprechende Anforderungen an die Sicherheit neuer Smart Meter wurden daher vom BSI ausgegeben und sollen in der neuen Generation von Smart Metern in Sicherheitsmodulen berücksichtigt werden [SSM] [BSI TR] [PP].

   Das gilt im gleichen Umfang auch für industrielle Lösungen, bei denen Anlagensteuerung und Energieversorgungssysteme vom selben Hersteller geliefert werden. Der Schutz der Heimebene unterliegt jedoch dem Letztverbraucher.

2. Kommunikationsnetze und -techniken für Energieversorgungssysteme

   1. Funk

      Bei den verwendeten Mess- und Steuersystemen mittels Funkverbindungen musste festgestellt werden, dass eine umfangreiche Abhörsicherheit in den seltensten Fällen gegeben ist. Gerade GSM oder veralteten WLAN Modulen können seit Jahren erfolgreich angegriffen und entschlüsselt werden. Aber auch neueren Installationen, die über keine oder nur eine begrenzte Verschlüsselung verfügen, sind für Angriffe anfällig. Hier sollte dringend über ausreichende Verschlüsselung auf Datenübertragungsebene nachgedacht werden, die sowohl die Integrität der Daten als auch ihre Ursprung absichert. Andernfalls können erfolgreich Replay Attacken durchgeführt werden, bei denen Steuerbefehle vom Angreifer abgefangen und erneut eingespielt werden. Solche Attacken können in Mobilfunknetzwerken, die bereits unter starker Auslastung stehen (siehe Innenstadtbereich) zu einer Überlastung und gegebenenfalls zu einem Netzzusammenbruch führen.

      Im Hinblick auf Software Updates und umfangreichen Datenverkehr zur Messung und Steuerung der Netze sollten hier neuere Techniken wie LTE genauer betrachtet werden.

Einstiegsmöglichkeiten dienen könnten.

2. Power Line

   Unter Power Line Communication wird die Modulation von Nutzdaten auf das Stromnetz verstanden. Die im Heimbereich eingesetzte PowerLAN Technik wird zunehmend auf die Datenübertragung im Niederspannungsnetz angepasst und weiterentwickelt. Hierfür werden sogenannte Konzentratoren im Ortsnetz installiert, welche die Daten zusammenfassen und an die Zentrale schicken. Dadurch wird die Abhängigkeit des Kommunikationsnetzes vom Energienetz und vice versa zwingend. Der Ausfall eines Netzes führt unweigerlich zum Ausfall des anderen, was sich gerade für die Netzsteuerung als kritisch erweist. Die redundante Auslegung der Technik im Ortsbereich ist wirtschaftlich jedoch schwer realisierbar [NERC]. Da es zudem keine Informationen über die Datenauf- und verarbeitung in den Konzentratoren gibt, können keine Aussage über die Sicherheit dieser Komponenten getroffen werden. Die Installation eines Gerätes im Konzentrator, dass die Daten ausliest (Sniffer genannt), ist mit Fachwissen möglich. Die Geräte sind öffentlich zugänglich. Eine umfassende Abhörsicherheit kann zudem nur über getrennte Stromkreise erzeugt werden. Andernfalls können auch Daten von Unbefugten ähnlich wie bei der PowerLAN Technik daheim ausgelesen werden. Wie sich die hochfrequenten Spannungsschwankungen bei hohem Datenaufkommen auf Endkomponenten auswirken, ist bisher Stand der Forschung [HFPLC].

3. Zusammenarbeit Kommunikationsnetz- und Energieversorgungsnetzbetreiber

   Während der Erstellung der Arbeit stellte sich zudem immer öfter heraus, dass viele kleine und mittelgroße Energieversorger zwingend auf die Verwendung der Kommunikationsnetze Dritter angewiesen sind, aber die Schnittstelle bei der Analyse und Meldung von Angriffen beidseitig kaum bis wenig beachtet wird. Zwar halten die Kommunikations- und Energienetzbetreiber Netzwarten am Laufen, die den Zustand ihrer Netze betrachtet und bei Ausfällen auch an die Kunden meldet, im seltensten Fall sind dabei aber die Art und Anzahl von Cyber-Angriffen bekannt.

   Es fiel darüber hinaus auf, dass nur einige wenige Energieversorger effektiv die vom Bund und den Regulierungsbehörden zur Verfügung gestellten Mittel zur Umsetzung von IT-Grundschutz und Cyber-Angriffen verwenden und dementsprechend zertifiziert sind. IT-Grundschutz behandelt vor allem die elementaren Bedrohung und liefert somit eine umfassend Grundlage zum Schutz vor Bedrohungen der Infrastruktur (auch jenseits der IT). In Kombination mit dem Schutz vor Cyber-Angriffen deckt er damit einen Großteil grundlegender Bedrohungen zeitnah und aktuell ab. Da auch weiter oben genannte Probleme mit diesen beiden Techniken abgedeckt werden, empfiehlt sich hier ein weitere Analyse.

Schutz durch Information-Security-Management-Systeme

Um einen umfassenden Schutz der Energieversorgungssysteme vor Cyber-Angriffe zu gewährleisten, werden Schutzmaßnahmen durch IT-Sicherheitskonzepte zwingend notwendig. Hierfür gilt es Verfahren, Regeln und Managementkonzepten in einem Unternehmen zu definieren. Dieses Regelwerk wird als Information Security Management System (ISMS) bezeichnet.

Ein Information Security Management System (ISMS, Managementsysteme für Informationssicherheit) ist eine nach ISO/IEC 27001 normierte Sammlung von Regeln und Richtlinien zum Umgang mit der Informationssicherheit in einem Unternehmen. Es dient einer dauerhaften Definition, Steuerung, Kontrolle, Aufrechterhaltung und Verbesserung der Sicherheitsmaßnahmen [ISO-27001]. Da diese Regeln sehr generisch sind, können sie auf beliebige Geschäftsbereiche und somit auch auf Energieversorgungsnetzen angewandt werden. Zur Unterstützung der Unternehmen wird seit 2006 ein an den ISO 27001 angepasster IT-Grundschutz-Katalog vom Bundesamt für Sicherheit in der Informationstechnik ausgegeben, der besonderen Wert auf die Themen Vertraulichkeit, Integrität und Verfügbarkeit legt.

Die Ziele eines ISMS für Energieversorgungsnetze sind somit:

- eine umfassende Modellierung der IT-Umgebung des Geschäftsbetriebes, in das auch Themen der Gebäudesicherheit und des Notfallmanagements (Business Continuity Management) integriert werden und das auf Datenschutz besonderen Wert legt
- eine standardisierte, national anerkannte Durchführung, um Schnittstellen zu Drittanbietern bedienen zu können und um das Vertrauen in die Sicherheit zu steigern
- die Analyse der IT-Sicherheit anhand diese Modells und nötige Maßnahme gegen mögliche Schwachstellen zu finden
- eine Abdeckung der rechtlichen Aspekte hinsichtlich dem Betrieb eines Energieversorgungsnetzes
- eine mögliche (inter-)nationale Zertifizierung des Netzes.

Auf internationaler Ebene liegen mit der ISO Standard Reihe 27000 eine Vielzahl an Normen zur grundlegenden Verwendung von ISMS vor. Von Bedeutung sind der IS027001, der die Begriffe und Definitionen genauer erläutert, der ISO27001 und ISO27002 mit den generische Schemata zur Umsetzungen von IT-Sicherheit sowie ISO27031 und ISO27032 bezüglich Business Continuity Management und Cyber Security.

IT-Grundschutz

Da die vom BSI ausgegeben Zertifikate ISO 27001 anhand IT-Grundschutz umfassender sind, als die ISO Normen fordern, werden im weiteren Verlauf daher die nationalen Pendants (BSI Standard 100-1 bis 100-4) sowie die IT-Grundschutz-Kataloge betrachtet. Durch den Wegfall einer initialen Risikoanalyse mit Unterteilung nach Schadenhöhe und Eintrittswahrscheinlichkeit und Verwendung eines 3-Klassen-Schutzbedarfschemata ist der IT-Grundschutz zudem für abstrakte Gefährdungen besser handhabbar. Dadurch sind IT-Sicherheitsmaßnahmen und die Risikoanalyse auch ohne Expertenwissen durchführbar. Jedoch reichen die in den Grundschutzkatalogen vorgeschlagenen Sicherheitsmaßnahmen nur für niedrigen und mittleren Schutzbedarf. Hoher und sehr hoher Schutzbedarf müssen durch weitere Sondermaßnahmen abgedeckt werden. Hierfür kann jedoch der BSI Standard 100-3 für eine weitreichende Risikoanalyse herangezogen werden.

Da die BSI Reihe 100-1 bis 100-4 de facto Standard für den Umgang mit IT-Sicherheit in Deutschland sind, ist eine umfassende Marktanalyse für verschiedene ISMS mit Blick auf die ISO 27001 mit keinem Mehrgewinn behaftet. Daher werden im Weiteren Verlauf nur verschiedene Tools betrachtet, mit denen Modelle entsprechend IT-Grundschutz erzeugt werden können.

Tools für IT-Grundschutz

Um das nach IT-Grundschutz vorgeschlagene ISMS zu modellieren, können verschiedene Hilfsmittel (eng. Tools) verwendete werden. Der möglichen Nutzen wird nach folgende Kriterien ermittelt:

1. Bedienbarkeit

   Da IT-Grundschutz auch ohne Fachwissen möglich ist, sollte die Bedienung des Tools für Laien möglich sein.

2. Interoperabilität zu anderen (Dritt-)Anbietern

   Das Audit des Netzes erfolgt durch lizenzierte Auditoren, daher sollte das Extrahieren des Modells, die Übergabe und das Kontrollieren auch mit anderen Tools möglich sein

3. Normierung

   Das Tool sollte die vorgegebenen Normierungsrichtlinien einhalten und sich an den IT-Grundschutz-Katalogen orientieren.

4. Marktdeckung

   Unterscheidung zwischen Nischenprodukten und marktgängigen Tools.

5. Kosten

6. Auswertbarkeit / Nutzen für das Management

   Der Nutzen für das Management durch die Analyse und Darstellung von Daten sollte gegeben sein, um den Einsatz der IT-Sicherheitsmaßnahmen rechtfertigen zu können.

7. Aktualität

8. Übersichtlichkeit

Produkt	Hersteller
DHC Vision Information Security Manager 5.0*	DHC Dr.Herterich&Consultants GmbH
DocSetMinder	GRC Partner GmbH
GRC Suite iRIS	Ibi research GmbH
GSTOOL 4.7	BSI
HiScout GRC Suite 2.0*	HiScout GmbH
I-doit pro	Synetics GmbH
Indart Professional	Contechnet Ltd.

Opus BSI-Grundschutz*	Kronsoft e.K.
SAVe	INFODAS GmbH
Security Audit	Secure IT Consult
Sidoc Sicherheitsmanagement 9.0	2Net Carsten Lang
Verinice 1.5.0*	SerNet GmbH
Verinice PRO 1.5.0*	SerNet GmbH

Die oben angeführte Tabelle zeigt einen Überblick über die im Moment am Markt vertretenen, zu den BSI Grundschutz Standards kompatiblen ISMS. Die durch (*) gekennzeichneten Systeme sind dabei zudem kompatibel zum ISO 27001 und könnten für die Unterstützung einer Multinorm-Zertifizierung herangezogen werden.

Besonders hervorzuheben ist jedoch das offizielle Grundschutz-Tool des BSI „GSTOOL“, welches zur Zeit in der Version 4.7 vorliegt. Es ist streng an die IT-Grundschutzkataloge angelehnt und ist mit einer Marktpräsenz von knapp 20.000Lizenzen das am weitesten verbreitete GSTOOL. Der Entwicklungsstand des GSTOOL 5 ist nach einer Abnahmeverweigerung[22] derzeit unklar. Neben dem GSTOOL bieten die anderen ISMS vor allem mehr Flexibilität und alternative Lösungsansätze, die gerade für Marktnischen geeignet sind. Eine hohe Dynamik in der Weiterentwicklung, ins Besondere in Richtung Webanwendung, ist hierbei zu bemerken. Dadurch ergeben sich auch Möglichkeiten zur modularisierten Einbindung in IT-gestützte Governance, Risk and Compliance (GRC) Systeme, welche der allgemeinen Unterstützung des Business Continuity Management dienen.

Eine weiterführende, auf die Webpräsenz der Hersteller fixierte Marktanalyse zeigte uns, dass der Vergleich der Tools und eine mögliche Kaufentscheidung nur schwer möglich ist. Ins Besondere ein Mangel an Demo Versionen machte den Vergleich schwer.

22 http://it-sibe.de/2013/04/das-gstool-5-kommt-sicher-nicht/

Produkt	Vorteile	Nachteile
DHC Vision Information Security Manager 5.0*	+ IT Strukturanalyse nach BSI + Asset Management + grafische Visualisierung der Infrastruktur + Schutzbedarfsfeststellung + Durchführung ergänzender Risikoanalysen + Feststellung IT-Grundschutzanforderungen + Festlegunng von Terminen und Verantwortlichkeiten + Verlinkung IT-Grundschutz und Geschäftsprozesse + modularer Aufbau + Demo	- keine Versionierung / Historie vorhanden
DocSetMinder	+ Verantwortlichkeiten werden erfasst + notwendige Dokumente werden überwacht + lückenlose Dokumentation + Umfangreiche Suchfunktion + Flexible und erweiterbare Vorlagen + Umfangreiche Integration nach IT-Grundschutz	- existiert nur als Windows Client -
GRC Suite iRIS	+ Vollständige Darstellung gängiger IT Standards (CobiT, ISO 27002, IT Grundschutz) + Best Practice Dokumentenmanagement + Verschiedene Sichten auf Datenbasis (GRC, IT Revision, Security Management)	- IT Grundschutzvorgehen wird nicht detailliert behandelt

	+ Individualisierte Auswertungen	
GSTOOL 4.9	BSI	
HiScout GRC Suite 2.0*	+ ISMS Prozesse sind umfangreich abgedeckt + Automatisierte Vererbung des Schutzbedarfs +Angepasste Templates für Management und Audit + Auswahl zwischen ISO 27001 und/oder IT Grundschutz +Integration des GSTOOL in GRC Suite +Demo	- Funktionen für IT-Management nicht immer gegeben (Netzpläne, Zugehörigkeiten...)
I-doit pro	+ Aufstellung der eingesetzten IT-Systeme und Anwendungen sowie deren Zuordnung + Netzplan + Risikobeschreibung	- keine Versionierung / Historie - keine Importfunktionalität
Indart Professional	+Notfallpläne +BSI 100-4 konform	- zielt zu stark auf Notfallmanagement ab und weniger auf IT-Grundschutz
Opus BSI-Grundschutz*	+ Erstellung Sicherheitskonzepte nach BSI Grundschutz auf ISO 27001 Basis + IT-Strukturanalyse + Modellierung der Verbundsobjekte + Kostenbearbeitung + Revisionsunterstützung +Automatische Maßnahmenzuordnung zu ISO 27001 und ISO 27002 + Arbeitsplan	- Windowsbasiert
SAVe	+ Erstellung von IT-Sicherheitskonzepten nach BSI-	- keine erkennbaren

	Grundschutz-Methodik + IT Strukturanalyse + erweiterte Risikoanalyse nach BSI 100-3 + aktive Audit Unterstützung + Abbildung der Ergebnisse auf 27001 + Kostenverfolgung Maßnahmenumsetzung + ...	
Security Audit	+ n.v, da rudimentäre Umsetzung	- Excel basiert - Grobe Analyse
Sidoc Sicherheitsmanagement 9.0	+ Integration des IT-Grundschutzkataloge + Demo Version	- keinerlei weitere Informationen möglich - veraltet (11.Ergänzungslieferung als Demo) - ungewohntes Handling
Verinice 1.5.0* Verinice PRO 1.5.0*	+ Import /Export Funktion + Relevante Standards	- nur bedingter Import von GSTOOL Datenbeständen

Aufbau eines ISMS

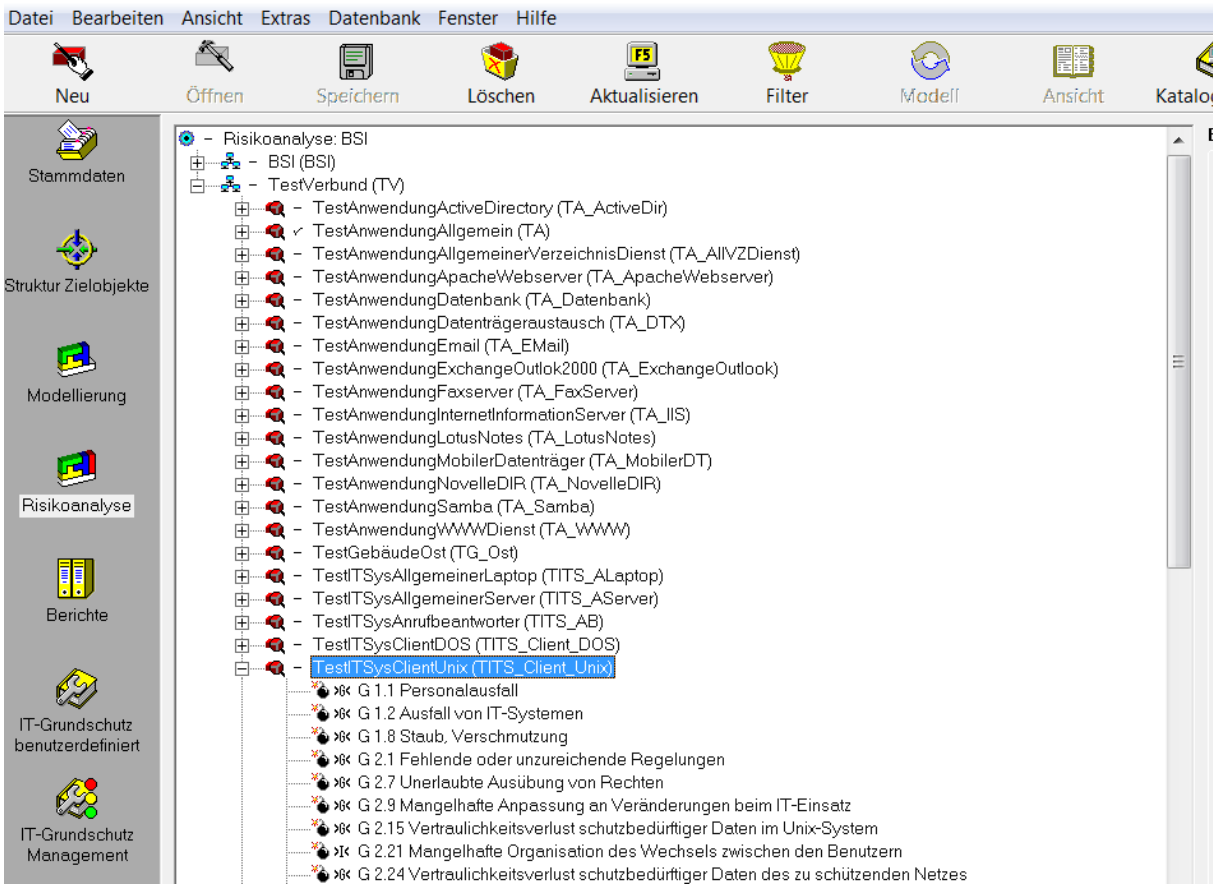

Illustration 8: Beispiel eines ISMS (hier GS Tool 4.7)

Die obige Abbildung zeigt einen Ausschnitt der Risikoanalyse des GSTOOL 4.7. Bei der Risikoanalyse werden mögliche Gefährdungen verschiedener Komponenten gelistet und hinsichtlich ihrer Auswirkungen bewertet. Am Baustein „TestTSysClientUnix“ lässt sich erkennen, dass es sich um einen Client Rechner mit Unix Betriebssystem handelt. Diese Komponente unterliegt Gefährdungen wie „G 1.1 Personalausfall“ oder „G 1.8 Staub, Verschmutzung“. Da diese Komponenten häufig verwendet werden, die Gefährdungen sich aber von Unix Client zu Unix Client nicht oder nur kaum ändern, spricht man im Rahmen des IT-Grundschutz auch von „Bausteinen“. Mehrere Bausteine werden zu einem „IT Verbund“ zusammengefasst. Dieser IT Verbund kann ein gesamtes Unternehmen oder nur einen Teilbereich wie einen Auslandsstandort umfassen. Bei der Modellierung der Gefährdungen greift das GSTOOL auf aktuelle Metadaten, die vom BSI gestellt werden, zurück. Dadurch ist die Aktualität des eigenen IT Verbundes mit den BSI Grundschutzkatalogen gegeben.

Ebenfalls zu erkennen, sind die einzelnen Stufen des Grundschutzes. Die Risikoanalyse kann beispielsweise erst nach der „Modellierung“ erfolgen. In diesem Schritt wird der IT Verbund, die Zusammenhänge und

Abhängigkeiten unter Geräten sowie individuelle Eigenschaften des Betriebsumfeldes erfasst.

Der IT Grundschutz erlaubt zudem über den Reiter „Erweiterte Sicherheitsanalyse“ die Bewertung und Umsetzung von über den Grundschutz hinausreichenden Maßnahmen wie hochverfügbare Rechennetze bei Banken.

Ausgehend von den Gefährdungen und den Eintrittswahrscheinlichkeiten möglicher Risiken können verschiedene Maßnahmen durchgeführt werden, die der IT Grundschutz vorschlägt. Angefertigte Berichte ermöglichen eine Zertifizierung sowie die Unterstützung der Entscheidungsfindung im höheren Management.

Fazit

Nach Installation mehrere Demoversionen verschiedener Tools und mehrwöchigem Testen lassen sich die Ergebnisse wie folgt zusammenfassen:

Ein Großteil der hier vorgestellten Tools implementiert den gewünschten IT-Grundschutz und sind nach einer geringfügigen Einarbeitungszeit und Studium der Handbücher auch für Neulinge gut bedienbar. Durch Import/Exportkanälen stellen jedoch nur wenige Tools eine

Interoperabilität und Aktualität gerade zu dem vom BSI geführten GSTOOL her. Dadurch wird eine Konzentration auf der GSTOOL weiter fokussiert und der Markt stark segmentiert in GSTOOL, GRC kompatible Tools und Nischenprodukte. Einige Tools führen neben dem IT-Grundschutz auch weitere (inter-)nationale Standards in Feld und implementieren teilweise GRC-Strategien für umfassendere Sicherheitsmaßnahmen. Der Nutzen für das Management ist sowohl beim GSTOOL als auch den GRC kompatible Tools gegeben. Somit steht folgendes fest:

- Wenn ein umfangreiches, den nationalen Richtlinien zum IT-Grundschutz entsprechendes, in der Breite vertretenes Tool gewünscht ist, dass minimal angepasst werden muss und einen solide Sicherheitsstandard vertritt, dann fällt die Wahl auf das GSTOOL.
- Sofern ein höherer Umfang gewünscht ist, der auch weitere Standards implementiert und eine erweiterte Risikoanalyse zulässt, so kann auf DHC, SAVe oder OPUS zurückgegriffen werden. Diese bieten über verschiedene Views und Module etliche Anpassungsmöglichkeiten mit sich und können auf Energieversorger zugeschnitten werden

- Sollte jedoch ein GRC Ansatz gewählt werden, in dem IT-Grundschutz eine Rolle spielt, so sollte das HiScout Tool genauer betrachtet werden.

Nichtsdestotrotz kann die Implementierung von IT-Grundschutz den hohen Sicherheitsbedürfnissen in Energieversorgungssystemen nicht gerecht werden. Bei der Demonstration und Modellierung der Energienetze immer wieder festgestellt werden, dass das Modell an seine Grenzen kommt, wenn es um gegenseitige Abhängigkeiten ging oder wenn die zusätzliche Risikoanalyse sehr umfassend wurde. Selbst ähnliche Module (Solar- und Braunkohlekraftwerk) wiesen unterschiedliche Ausfallrisiken auf, deren Abhängigkeit nicht immer trivial zu modellieren ist. Was passiert beispielsweise, wenn jemand nicht das Braunkohlekraftwerk direkt, sondern die Zulieferwege wie das Stellwerk für eine Eisenbahntrasse angreift?

Zudem mussten festgestellt werden, dass IT-Grundschutz ein sehr langwierige, dafür aber sehr solider Sicherheitsprozess ist. Die Aktualität der Kataloge wird in fast jährlichen Zyklen gewährleistet, jedoch können Bausteine zu aktuellen Betriebssystemen oftmals 1 bis 1 ½ Jahre in Anspruch nehmen. Um also kurzfristige Sicherheit zu gewährleisten, muss neben dem IT-Grundschutz auch die Cyber-Sicherheitsstrategie [CYBER] und deren Papiere verwirklicht werden. Diese haben jedoch keine Modellierungsgrundlage im GSTOOL oder ähnlichen Werkzeugen.
Die Umsetzung des IT-Grundschutz nach BSI Standards ermöglicht jedoch eine grundlegenden Sicherung gegen IT-Angriffe in der Breite verschiedener Sektoren kritischer Infrastrukturen. Zudem können Schnittstellen zwischen Telekommunikations- und Energieversorgern sowie Notfallkonzepte verbessert werden. Es folgt somit eine klare Empfehlung einer Umsetzung des IT-Grundschutzkonzeptes in Kritischen Infrastrukturen, da elementaren, weit verbreiteten Gefährdungen entgegen gewirkt werden kann.

Schlusswort

In dieser Arbeit wurde gezeigt, dass Energieversorgungssysteme und ihre herausragende Rolle unter den Kritischen Infrastrukturen immer mehr zum potentiellen Angriffsziele im Cyber War werden. Dabei sind die grundlegende Struktur der Energieversorgungsnetze und ihrer Kommunikationsnetze aufgezeigt, Parallelen und Abhängigkeiten erklärt und mögliche Schwachstellen identifiziert worden. Es wurde dargestellt, welche Datenquellen in den verschiedenen Netzebenen welche Informationen liefern und was mit deren Missbrauch angerichtet werden kann. Anschließend wurde sich mit rechtlichen Richtlinien und technischen Herausforderungen bei der Umsetzung von Kommunikationskanälen in Energieversorgungsnetzen auseinandergesetzt. Aus diesen abgeleitet ergab sich der Bedarf des IT-Grundschutzes und die Frage, wie dieser modelliert werden kann. Es folgte eine Erläuterung des IT-Grundschutz ist, wie er gegen Gefährdungen eingesetzt werden kann, das Management unterstützt und welche Tools zur Modellierung offenstehen.

Zudem ist aufgefallen, dass es bereits eine Vielzahl an Analysen zur Lage der Gefährdung von Kritischen Infrastrukturen - ins Besondere von Energienetzen – gibt, aber die Rolle der IT-Sicherheit dort noch nicht ausreichend behandelt wird. Die wenigen Analysen, die sich mit IT-Sicherheit befassen, verweisen darüber hinaus auf die sehr generischen ISO Standards. Trotz der enormen Wichtigkeit werden kaum nationale Strukturen für das Notfallmanagement geschaffen und stattdessen auf die selbstregulierende Kraft des Marktes gesetzt. In Deutschland gibt es mit dem Nationalen Lagezentrum in Bonn und den IT-Grundschutz Katalogen sowie der Cyber-Sicherheitsstrategie zwar Hilfe von nationaler Seite. Diese wird jedoch nur in einem Bruchteil der Deutschen Wirtschaft auch umgesetzt.

Alles in allem wurde jedoch erkannt, dass mit der Umsetzung von IT-Grundschutz und den Cyber-Sicherheitsstrategie in Energieversorgungssystemen eine gemeinsame Basis gegen die Gefährdung durch Cyber-Angriffe geschaffen werden kann, auf die weiterführende Sicherheitsmaßnahmen auch betriebsübergreifend aufgesetzt werden können.

Quellen:

[BNA] http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/Sicherheitsanforderungen-node.html , Sicherheitsanforderungen der Bundesnetzagentur, vom 16.06.2013

[BSI1001] „Managementsysteme für Informationssicherheit (ISMS)“, BSI-Standard 100-1, Version 1.5, Mai 2008, www.bsi.bund.de

[BSI1002] „IT-Grundschutz-Vorgehensweise“, BSI-Standard 100-2, Version 2.0, Mai 2008, www.bsi.bund.de

[BSI1003] „Risikoanalyse auf der Basis von IT-Grundschutz“, BSI-Standard 100-3, Version 2.5, Mai 2008, www.bsi.bund.de

[BSI1004] „Notfallmanagement“ ,BSI-Standard 100-4, Version 1.0, Mai 2008, www.bsi.bund.de

[BSI TR] Technische Richtlinie des BSI für Kommunikationsmodule von Smart Metern, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/index_htm.html vom 16.06.2013

[COLLIER] „The Vulnerability of Vital Systems: How “Critical Infrastructure” Became a Security Problem“, Stephen J. Collier, Andrew Lakoff

[CYBER] „Cyber-Sicherheitsstrategie für Deutschland“, Bundesministerium des Innern

[DEFCON] Video, Thema Smart Meter Hacking, http://www.youtube.com/watch?v=HeoCOVXRX0w vom 16.06.2013

[EIAS] „ENERGY INFRASTRUCTURE AND SECURITY“, Alexander E. Farrell, Hisham Zerriffi,andHadi Dowlatabadi

[ENWG] EnergieWirtschaftsGesetz, www.gesetze-im-internet.de/enwg_2005/ vom 16.06.2013

[FASE] „The Financial Aspects of the Security of Assets and Infrastructure in the Energy Sector“, Harnser Group of European Commission
[FORECAST] „Intelligent Energy management of electrical power systems with distributed feeding on basis of forecasts of demand and generation“ , Chr. Meisenbach. M. Hable, G. Winkler and P. Meier

[HFPLC] „A transmission line model for High-Frequency Power Line Communication Channel“, H.Meng L.Guan, C.L.Law, P.L.So, E.Gunawan, T.T.Lie

[ISO-27001] „Information technology – Security techniques – Information security management systems – Requirements“

[KRITIS] „Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)“, Bundesministerium des Innern

[KS] „Katalog für Sicherheitsanforderungen an das Betreiben eines Telekommunikation- und Datennetzes sowie für die Verarbeitung personenbezogener Daten“, Bundesnetzagentur

[LORENZ] „Kritische Infrastrukturen aus Sicht der Bevölkerung“, Daniel F. Lorenz, M.A.

[NERC] „ Protection System Reliability Redundancy of Protection System Elements“, NERC Paper

[PP] „Protection Profile for the Gateway of a Smart Metering 1 System (Smart Meter Gateway PP)“, Bundesamt für Sicherheit in der Informationstechnik

[SCEI] „Security Challenges for the Electricity Infrastructure“, Massoud Amin

[SPC] „Security and Privacy Challenges in the Smart Grid“, Patrick McDaniel, Sean W. Smith,

[SSM] „Secure Smart Meters“, http://www.heise.de/newsticker/meldung/29C3-Hacker-erwarten-gespannt-die-neue-Smart-Meter-Generation-1775039.html

[SMCS] „Analysis of State-of-the-art Smart Metering Communication Standards“,Klaas De Craemer, Geert Deconinck

[SMHT] Smart Meter Hacking Tool http://www.smartplanet.com/blog/smart-takes/researcher-releases-smart-meter-hacking-tool/27954

[TAB] „Regenerative Energieträger zur Sicherung der Grundlast in der Stromversorgung“ ,Büro für Technikfolge-Abschätzungen beim Bundestag

[TAB2] „Was bei einem Blackout geschieht“, Thomas Petermann, Harald Bradke, Arne Lüllmann, Maik Poetzsch, Ulrich Riehm

[WALLRAFF] „Verfahren der Datenkommunikation für Smart Meter“, Sonja Wallraff

[WDR] Dokumentation zur IT-Sicherheit im Rahmen der Fernsehsendung „WDR Westpol“, Sendung vom Sonntag, 18.November 2012, http://www.wdr.de/tv/westpol/sendungsbeitraege/2012/1118/itsicherheit.jsp