

# **Sicherheit und Datenschutz im Smart Grid**

**Bachelor-Thesis**  
im Studiengang Medieninformatik  
vorgelegt von

**Kristian Antic**  
**Matrikelnummer: 20177**

am 8. März 2012  
an der Hochschule der Medien Stuttgart

Erstprüfer: Prof. Dr. Joachim Charzinski  
Zweitprüfer: Christoph Lindenmüller

Bearbeitungszeitraum: 08. Dezember 2011 bis 8. März 2012

## Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig angefertigt habe. Es wurden nur die in der Arbeit ausdrücklich benannten Quellen und Hilfsmittel benutzt. Wörtlich oder sinngemäß übernommenes Gedankengut habe ich (mit Ausnahme dieser Erklärung) als solches kenntlich gemacht.<sup>1</sup>

---

Ort, Datum

---

Unterschrift

---

<sup>1</sup>Riekert: Eine Dokumentvorlage für Diplomarbeiten und andere wissenschaftliche Arbeiten (2002), [83], S. 42.

## Kurzfassung

Der vermehrte Einsatz von erneuerbaren Energien, welche nicht ständig verfügbar und nur begrenzt speicherbar sind, erschweren die Steuerung der Stromnetze. Zur Anpassung der Energieerzeugung an den tatsächlichen Bedarf werden Smart Grids („intelligente Stromnetze“) aufgebaut, die eine Steuerung des Energieverbrauchs in Abhängigkeit von der Verfügbarkeit ermöglichen. Die bereits vorhandenen Stromnetze werden hierzu um Kommunikationsnetze erweitert. Smart Meter („intelligente Stromzähler“) die beim Verbraucher eingesetzt werden, senden über die Kommunikationsnetze Messdaten zyklisch an die jeweiligen Stromnetzbetreiber. In Zukunft soll auch eine Steuerung von Haushaltsgeräten möglich werden. Daraus ergeben sich neue Herausforderungen in Bezug auf Sicherheit und Datenschutz.

Die hier vorliegende Arbeit bietet eine kurze Einführung in die Grundlagen zum Thema Smart Grid. Es wird eine Referenzarchitektur definiert und die einzelnen Bestandteile des Smart Grids werden vorgestellt. Eine Auseinandersetzung mit den rechtlichen und regulatorischen Rahmenbedingungen sowie ein Überblick über den Stand der Entwicklungen intelligenter Stromnetze, insbesondere der Verbreitung von Smart Metern, vervollständigt die Grundlagen. Zusätzlich werden wesentliche Aspekte von Sicherheit und Datenschutz angesprochen. Darauf aufbauend wird die Sicherheit in Smart Grids untersucht. Hierzu werden die Ursachen für Bedrohungen im Rahmen einer Bedrohungsanalyse anhand eines Szenarios analysiert. Abgeleitet von den Ergebnissen der Bedrohungsanalyse werden Risiken innerhalb einer Risikoanalyse evaluiert und Maßnahmen empfohlen, um die festgestellten Risiken zu bewältigen.

**Stichwörter:** Smart Grid, Sicherheit, Datenschutz, Risikoanalyse

## **Abstract**

The increased use of renewable energy sources, which are not constantly available and only limited storable complicate the management of power grids. Smart Grids allowing control of energy consumption depending on availability will be built up in order to adapt energy generation on the actual demand of energy. For this purpose existing power grids are extended by communications networks. Smart meters located at the customer are used to send data periodically to the respective power company via communication networks. For the future there are also plans to control household appliances. This results in new challenges in terms of security and privacy.

The following thesis provides a brief introduction to the basics of smart grids. A reference architecture will be defined and individual components of the Smart Grid are presented. A discussion of the legal and regulatory framework as well as an overview about the the current state of development with already installed smart meters completes the Smart Grid basics. In addition, key aspects of security and privacy are addressed. On this basis the security of smart grids is investigated. For this purpose the causes of threats will be analyzed in a threat analysis based on a scenario. Derived from the findings of the threat analysis, risks are evaluated within a risk analysis. Finally measures are recommended to address the identified risks.

**Keywords:** Smart Grid, security, privacy, risk analysis

# Inhaltsverzeichnis

<b>Abkürzungsverzeichnis</b>	<b>vii</b>
<b>Abbildungsverzeichnis</b>	<b>x</b>
<b>Tabellenverzeichnis</b>	<b>xi</b>
<b>1 Einleitung</b>	<b>1</b>
<b>2 Grundlagen</b>	<b>3</b>
2.1 Elektrizitätsversorgung	3
2.1.1 Heutige Elektrizitätsversorgung	3
2.1.2 Zukünftige Elektrizitätsversorgung	4
2.1.3 Rollen in der Elektrizitätswirtschaft	5
2.2 Smart Grid	6
2.2.1 Referenzarchitektur	6
2.2.2 Industrielle Steuerungssysteme und Feldgeräte	9
2.3 Smart Metering	10
2.3.1 Smart Meter	10
2.3.2 Smart Meter Gateway	11
2.3.3 Online-Dienste	12
2.4 Rechtliche und regulatorische Rahmenbedingungen	12
2.4.1 International	12
2.4.2 National	13
2.4.3 Standards und Normen	15
2.5 Realisierungsstand	16
2.5.1 International	17
2.5.2 National	19
<b>3 Sicherheit und Datenschutz</b>	<b>20</b>
3.1 Sicherheitsarten	20
3.1.1 Informationssicherheit	21
3.1.2 Datenschutz	21
3.2 Schutzziele	23
3.3 Schutzmaßnahmen	24
3.4 Bewertungskriterien von Sicherheit	25
3.4.1 Common Criteria	25
3.4.2 Schutzprofil	25
3.5 Risiko	27
3.6 Risikoentstehungsfaktoren	30
3.6.1 Schwachstelle und Verwundbarkeit	30

3.6.2	Bedrohung	30
3.6.3	Angriff	31
3.6.4	Angreifer	32
<b>4</b>	<b>Angriffe und Bedrohungsszenarien</b>	<b>34</b>
4.1	Mögliche Angreifer	34
4.2	Mögliche Angriffsziele und Bedrohungen	34
4.2.1	Szenario	36
4.2.2	Bedrohungsanalyse	37
4.2.3	Risikoanalyse	45
4.2.4	Maßnahmen	62
4.3	Überprüfung der Angriffsziele und Bedrohungen	69
4.3.1	Bedrohungsanalyse	69
4.3.2	Risikoanalyse	73
4.3.3	Maßnahmen	91
<b>5</b>	<b>Zusammenfassung und Ausblick</b>	<b>94</b>
	<b>Anhang</b>	<b>95</b>
<b>A</b>	<b>Smart Grid Referenzarchitektur</b>	<b>95</b>
A.1	Entities & Networks	95
A.2	Reference Points	97
<b>B</b>	<b>Angriffe und Bedrohungsszenarien</b>	<b>99</b>
B.1	Bedrohungsbäume	99
B.2	Bedrohungsanalyse	106
<b>C</b>	<b>Ausdruck von Quellen</b>	<b>119</b>
	<b>Quellenverzeichnis</b>	<b>120</b>
	<b>Danksagungen</b>	<b>137</b>

## Abkürzungsverzeichnis

<b>Abb.</b>	Abbildung
<b>AES</b>	Advanced Encryption Standard
<b>AG</b>	Aktiengesellschaft
<b>ALARP</b>	As Low As Reasonably Practicable
<b>AMI</b>	Advanced Metering Infrastructure
<b>Anm.</b>	Anmerkung
<b>ARP</b>	Address Resolution Protocol
<b>BDSG</b>	Bundesdatenschutzgesetz
<b>BfDI</b>	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
<b>BMU</b>	Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit
<b>BMWi</b>	Bundesministerium für Wirtschaft und Technologie
<b>BNetzA</b>	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
<b>BPL</b>	Broadband over power line
<b>BSI</b>	Bundesamt für Sicherheit in der Informationstechnik
<b>CC</b>	Common Criteria
<b>CEN</b>	Europäisches Komitee für Normung
<b>CENELEC</b>	Europäisches Komitee für elektrotechnische Normung
<b>CLS</b>	Controllable Local Systems
<b>CVE</b>	Common Vulnerabilities and Exposures
<b>DCS</b>	distributed control system, <b>dt.</b> verteiltes Prozessleitsystem
<b>DIN</b>	Deutsches Institut für Normung
<b>DKE</b>	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik
<b>DMS</b>	Distribution Management System, <b>dt.</b> Verteilungsmangementsystem
<b>DNP3</b>	Distributed Network Protocol
<b>DNS</b>	Domain Name System
<b>DoS</b>	Denial-of-Service
<b>DSL</b>	Digital Subscriber Line
<b>dt.</b>	Deutsch
<b>EAL</b>	Evaluation Assurance Level, <b>dt.</b> Evaluierungsstufen
<b>EEG</b>	Gesetz für den Vorrang Erneuerbarer Energien (Erneuerbare-Energien-Gesetz)
<b>EEX</b>	European Energy Exchange
<b>EMS</b>	Energiemanagementsystem
<b>EN</b>	Europäische Norm
<b>engl.</b>	Englisch
<b>EnWG</b>	Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz)

<b>ETSI</b>	European Telecommunications Standards Institute
<b>EU</b>	Europäische Union
<b>EVG</b>	Evaluierungsgegenstand
<b>EVU</b>	Elektrizitätsversorgungsunternehmen
<b>FAN</b>	Field Area Network
<b>FERC</b>	Federal Energy Regulatory Commission
<b>FIPS</b>	Federal Information Processing Standard
<b>Gateway PP</b>	Protection Profile for the Gateway of a Smart Metering System, <a href="#">dt.</a> Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen
<b>GmbH</b>	Gesellschaft mit beschränkter Haftung
<b>GPRS</b>	General Packet Radio Service
<b>HAN</b>	Home Area Network
<b>HGÜ</b>	Hochspannungs-Gleichstrom-Übertragung
<b>HMI</b>	Human Machine Interface, <a href="#">dt.</a> Mensch-Maschine-Schnittstelle
<b>HTML</b>	Hypertext Markup Language
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>ICS</b>	Industrial Control System, <a href="#">dt.</a> Industrielles Steuerungssystem
<b>IEC</b>	International Electrotechnical Commission
<b>IED</b>	Intelligent Electronic Device
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IKT</b>	Informations- und Telekommunikationstechnologie
<b>IP</b>	Internet Protocol
<b>ISO</b>	International Organization for Standardization
<b>k</b>	Kilo
<b>LMN</b>	Local Metrological Network
<b>MAC</b>	Message Authentication Code
<b>MAC-Adresse</b>	Media-Access-Control-Adresse
<b>MDMS</b>	Messdatenmanagementsystem
<b>MessZV</b>	Verordnung über Rahmenbedingungen für den Messstellenbetrieb und die Messung im Bereich der leitungsgebundenen Elektrizitäts- und Gasversorgung (Messzugangsverordnung)
<b>MUC</b>	Multi Utility Communication
<b>NAN</b>	Neighborhood Area Network
<b>NIST</b>	National Institute of Standards and Technology
<b>PCS</b>	Process Control System, <a href="#">dt.</a> Prozessleitsystem
<b>PLC</b>	Powerline Communication
<b>PP</b>	Protection Profile, <a href="#">dt.</a> Schutzprofil
<b>PTB</b>	Physikalisch-Technische Bundesanstalt
<b>RFC</b>	Request for Comments



<b>RTU</b>	Remote Terminal Unit, <a href="#">dt.</a> Fernbedienungsterminal
<b>SCADA</b>	Supervisory Control and Data Acquisition
<b>Security Module PP</b>	Protection Profile for the Security Module of a Smart Metering System, <a href="#">dt.</a> Schutzprofil für das Sicherheitsmodul eines intelligenten Messsystems
<b>SHA</b>	Secure Hash Algorithm
<b>SM-GW</b>	Smart Meter Gateway
<b>SPS</b>	Speicherprogrammierbare Steuerung
<b>StGB</b>	Strafgesetzbuch
<b>StromNZV</b>	Verordnung über den Zugang zu Elektrizitätsversorgungsnetzen (Stromnetzzugangsverordnung)
<b>TCP</b>	Transmission Control Protocol
<b>TLS</b>	Transport Layer Security
<b>ugs.</b>	umgangssprachlich
<b>UMTS</b>	Universal Mobile Telecommunications System
<b>URL</b>	Uniform Resource Locator
<b>USA</b>	United States of America, <a href="#">dt.</a> Vereinigte Staaten von Amerika
<b>V</b>	Volt
<b>VDE</b>	VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V
<b>WAN</b>	Wide Area Network
<b>WLAN</b>	Wireless Local Area Network

## Abbildungsverzeichnis

2.1	Rollen und Vertragsbeziehungen in der Elektrizitätswirtschaft	6
2.2	Smart Grid Referenzarchitektur	7
2.3	Smart Metering in der EU	18
2.4	Übersicht Smart Metering Projekte in Deutschland	19
3.1	Aspekte der Sicherheit	20
3.2	Risikokarte	29
4.1	Risikokarte aus Sicht des Netzbetreibers/Messstellenbetreibers	61
4.2	Risikokarte aus Sicht des Nutzers/Verbrauchers	62
4.3	Übersicht Maßnahmen Netzbetreibers/Messstellenbetreiber	63
4.4	Übersicht Maßnahmen Nutzer/Verbraucher	67
4.5	Risikokarte aus Sicht des Netzbetreibers/Messstellenbetreibers	90
4.6	Risikokarte aus Sicht des Nutzers/Verbrauchers	91
4.7	Übersicht Maßnahmen Netzbetreibers/Messstellenbetreiber	91
B.1	Allgemeiner Bedrohungsbaum-Betrug bei der Einspeisung von elektrischer Energie	100
B.2	Allgemeiner Bedrohungsbaum-Entziehung elektrischer Energie	101
B.3	Allgemeiner Bedrohungsbaum-Entziehung elektrischer Energie beim Einsatz von Prepaid Smart Metern mit lokalem Guthaben Abrechnungssystem	102
B.4	Allgemeiner Bedrohungsbaum-Entziehung elektrischer Energie beim Einsatz von Prepaid Smart Metern mit zentralisiertem Abrechnungssystem	103
B.5	Allgemeiner Bedrohungsbaum-Ausfall/Störung der Stromversorgung in den Bereichen Erzeugung, Übertragung, Verteilung und Verbraucher, Teil 1	104
B.6	Allgemeiner Bedrohungsbaum-Ausfall/Störung der Stromversorgung in den Bereichen Erzeugung, Übertragung, Verteilung und Verbraucher, Teil 2	105
B.7	Discovery Smart Meter/SM-GW mit geöffnetem SM-GW Gehäuse	106
B.8	Discovery Smart Meter/SM-GW mit geschlossenem SM-GW Gehäuse	106
B.9	Zertifikatsfehler beim Aufruf von <a href="https://discovery.com">https://discovery.com</a>	107
B.10	Zertifikat-Status der Adresse <a href="https://discovery.com">https://discovery.com</a>	108
B.11	Informationen zum Zertifikat der Adresse <a href="https://discovery.com">https://discovery.com</a>	108
B.12	Diensterkennung mit dem Portscanner Nmap für das Ziel <a href="https://discovery.com">discovery.com</a>	109

## Tabellenverzeichnis

2.1	Spannungsebenen in Deutschland . . . . .	3
2.2	Übersicht ausgewählter Smart Grid Standards . . . . .	16
3.1	Übersicht Schutzmaßnahmen . . . . .	25
3.2	Übersicht Eintrittswahrscheinlichkeit . . . . .	28
3.3	Übersicht Schadensausmaß . . . . .	28
4.1	Bedrohungsanalyse-Abhören einzelner Nutzer . . . . .	40
4.2	Bedrohungsanalyse-Abhören vieler Nutzer . . . . .	41
4.3	Bedrohungsanalyse-Manipulation von Messdaten einzelner Nutzer . . . . .	42
4.4	Bedrohungsanalyse-Manipulation von Messdaten vieler Nutzer . . . . .	42
4.5	Bedrohungsanalyse-Einschränkung der Verfügbarkeit der Abrechnung für einzelne Nutzer . . . . .	43
4.6	Bedrohungsanalyse-Einschränkung der Verfügbarkeit der Abrechnung für viele Nutzer . . . . .	43
4.7	Bedrohungsanalyse-Einschränkung der Verfügbarkeit der Stromversorgung für einzelne Nutzer . . . . .	44
4.8	Bedrohungsanalyse-Einschränkung der Verfügbarkeit der Stromversorgung für viele Nutzer . . . . .	44
4.9	Normierung des Schadensausmaß der Hautbedrohungen/Hauptschutzzielverletzungen . . . . .	45
4.10	Risikoanalyse 1, Teil 1 . . . . .	47
4.11	Risikoanalyse 1, Teil 2 . . . . .	48
4.12	Risikoanalyse 1, Teil 3 . . . . .	49
4.13	Risikoanalyse 1, Teil 4 . . . . .	50
4.14	Risikoanalyse 1, Teil 5 . . . . .	51
4.15	Risikoanalyse 1, Teil 6 . . . . .	52
4.16	Risikoanalyse 1, Teil 7 . . . . .	53
4.17	Risikoanalyse 1, Teil 8 . . . . .	54
4.18	Risikoanalyse 1, Teil 9 . . . . .	55
4.19	Risikoanalyse 1, Teil 10 . . . . .	56
4.20	Risikoanalyse 1, Teil 11 . . . . .	57
4.21	Risikoanalyse 1, Teil 12 . . . . .	58
4.22	Risikoanalyse 1, Teil 13 . . . . .	59
4.23	Risikoanalyse 1, Teil 14 . . . . .	60
4.24	Risikoanalyse 2, Teil 1 . . . . .	73
4.25	Risikoanalyse 2, Teil 2 . . . . .	74
4.26	Risikoanalyse 2, Teil 3 . . . . .	75
4.27	Risikoanalyse 2, Teil 4 . . . . .	76
4.28	Risikoanalyse 2, Teil 5 . . . . .	77
4.29	Risikoanalyse 2, Teil 6 . . . . .	78
4.30	Risikoanalyse 2, Teil 7 . . . . .	79
4.31	Risikoanalyse 2, Teil 8 . . . . .	80

4.32 Risikoanalyse 2, Teil 9 . . . . .	81
4.33 Risikoanalyse 2, Teil 10 . . . . .	82
4.34 Risikoanalyse 2, Teil 11 . . . . .	83
4.35 Risikoanalyse 2, Teil 12 . . . . .	84
4.36 Risikoanalyse 2, Teil 13 . . . . .	85
4.37 Risikoanalyse 2, Teil 14 . . . . .	86
4.38 Risikoanalyse 2, Teil 15 . . . . .	87
4.39 Risikoanalyse 2, Teil 16 . . . . .	88
4.40 Risikoanalyse 2, Teil 17 . . . . .	89
A.1 Referenzarchitektur - Entities & Networks Teil 1 . . . . .	95
A.2 Referenzarchitektur - Entities & Networks Teil 2 . . . . .	96
A.3 Referenzarchitektur - Reference Points, Teil 1 . . . . .	97
A.4 Referenzarchitektur - Reference Points, Teil 2 . . . . .	98
B.1 Detaillierte Bedrohungsanalyse, Teil 1 . . . . .	110
B.2 Detaillierte Bedrohungsanalyse, Teil 2 . . . . .	111
B.3 Detaillierte Bedrohungsanalyse, Teil 3 . . . . .	112
B.4 Detaillierte Bedrohungsanalyse, Teil 4 . . . . .	113
B.5 Detaillierte Bedrohungsanalyse, Teil 5 . . . . .	114
B.6 Detaillierte Bedrohungsanalyse, Teil 6 . . . . .	115
B.7 Detaillierte Bedrohungsanalyse, Teil 7 . . . . .	116
B.8 Detaillierte Bedrohungsanalyse, Teil 8 . . . . .	117
B.9 Detaillierte Bedrohungsanalyse, Teil 9 . . . . .	118

### 1 Einleitung

Elektrische Energie stellt eine wichtige Energie-Ressource dar. Diese lässt sich bisher allerdings nur in begrenzten Mengen zu vertretbaren Kosten speichern. Das Angebot an aktuell eingespeister Energie und deren Nachfrage in Form des aktuellen Verbrauchs müssen sich jederzeit entsprechen, um einen stabilen Betrieb zu gewährleisten.

Bisher zeichnet sich die Energieerzeugung in Deutschland durch Zentralisierung in Großkraftwerken aus. Zukünftig soll ein Wandel in Richtung einer ökologischen und dezentralen Energieerzeugung erfolgen. Der Anteil an erneuerbaren, teilweise aber nur temporär verfügbaren, volatilen Energiequellen soll bei gleichzeitigem Verzicht auf Kernkraftwerke stark steigen. Zugleich soll es zu einem Anstieg der Elektromobilität kommen.

Die derzeitige nicht leistungsfähige Steuerung der Energieeinspeisung soll durch eine Verbrauchssteuerung abgelöst werden. Lastspitzen sollen in Zeiten, in denen viel Energie in das Netz eingespeist wird, verschoben werden. Mit Hilfe eines neuen Kommunikations- und Stauernetzes für die Verteilnetze soll diese Flexibilisierung des Energienetzes erreicht werden.

Oft wird dieses vollautomatisierte Stromnetz zusammen mit den Stauernetzen als Smart Grid bezeichnet. Beim Verbraucher sollen die klassischen Stromzähler durch intelligente Energiezähler, welche die aktuellen Verbrauchswerte elektronisch an den Netzbetreiber übermitteln, ersetzt werden. Auf Endkundenseite soll dies zu mehr Transparenz führen, um damit Stromsparmaßnahmen zu unterstützen. Netzseitig soll so eine bessere Netzsteuerung ermöglicht werden. Als kritische Infrastruktur unterliegt ein mit [Informations- und Telekommunikationstechnologies \(IKTs\)](#) vernetztes Energienetz neben traditionellen physischen Problemen für die Energieversorgung zusätzlich Problemen aus der Cyber-Sicherheit. Mit der Massenverarbeitung personenbezogener Verbrauchsdaten ergeben sich hier zusätzlich datenschutzrechtliche Probleme. Die Spanne der möglichen Bedrohungen reicht dabei von einfachem Abrechnungsbetrug bis hin zu schwerwiegenden Angriffen, die Stromnetzausfälle oder permanente Netzschäden nach sich ziehen können.

Viele grundsätzliche Themen, wie Sicherheit und Datenschutz, hinsichtlich Smart Grids müssen noch geklärt werden. Trotzdem hat der Umbau der Stromnetze bereits begonnen und in einigen Haushalten sind bereits Smart Meter im Einsatz. Anhand eines Szenarios wird analysiert welche Bedrohungen sich für den Messstellenbetreiber Discovergy GmbH und einen typischen Verbraucher in einem Mehrfamilienhaus ergeben. Ferner wird untersucht welche Risiken daraus resultieren und mit welchen Maßnahmen man diese bewältigen kann.

Der mögliche Anwendungsbereich von Smart Metern bzw. Smart Metering als wichtiger Bestandteil des Smart Grids beschäftigt sich mit der Verbrauchsmessung für verschiedene Versorgungsbereiche wie Energie, Wasser und Gas. In dieser Arbeit soll dabei allerdings nur der Aspekt der Energie betrachtet werden. Bei Steuerung von Verbrauchern und Erzeugern greift das Smart Grid auch in den Bereich des Smart Homes ein. An entsprechenden Stellen wird das Smart Home zwar erwähnt, es wird in dieser Arbeit allerdings nicht näher betrachtet.

Die Arbeit gliedert sich in fünf aufeinander aufbauende Kapitel. Da die Themen der verschiedenen Kapitel ineinander greifen, wird an den entsprechenden Stellen auf Vorwärts- und Rückwärtsverweise zurückgegriffen. Die Einleitung zeigt die Motivation für die Einführung von Smart Grids und die Herausforderungen, die sich aus Sicherheitssicht daraus ergeben. Smart Grids stehen in Verbindung mit anderen Technologien, deshalb erfolgt in der Einleitung eine Abgrenzung. Mit der Beschreibung des Aufbaus der Arbeit schließt die Einleitung ab. Kapitel 2 zeigt nach einer Einführung in den Bereich der Elektrizitätsversorgung einen Überblick über die Bestandteile von Smart Grids. Hierzu werden die einzelnen Komponenten mit Hilfe einer Referenzarchitektur in Bezug zueinander gestellt. Nach einer Erläuterung der einzelnen Komponenten folgt eine Auseinandersetzung mit den rechtlichen Rahmenbedingungen, die für das Smart Grid gelten. Ein weiterer Teil widmet sich der bisherigen Standardisierungsktivistäten. Zum Ende des Kapitels wird der bisherige Stand der Umsetzung von Smart Grids an Hand einiger Beispiele aufgezeigt. In Kapitel 3 werden grundlegende Begriffe aus den Bereichen Sicherheit und Datenschutz eingeführt. Dies umfasst neben verschiedenen Sicherheitsarten, Schutzziele und Schutzmaßnahmen. Daneben werden die vom [Bundesamt für Sicherheit in der Informationstechnik](#) erstellten Schutzprofile kurz vorgestellt. Ein weitere Teil befasst sich mit Risiken und Faktoren die zur Entstehung von Risiken beitragen. Im darauf folgenden Kapitel 4 wird das Szenario erläutert, das innerhalb einer Bedrohungsanalyse und einer anschließenden Risikoanalyse untersucht wird. Zusätzlich werden Maßnahmen beschrieben, die zu treffen sind, um die Sicherheit zu erhöhen. Das abschließende Kapitel 5 fasst wichtige Aspekte dieser Arbeit zusammen und liefert einen Ausblick auf die Zukunft des Themas.

Im Anschluss der Kapitel folgt der Anhang. Anhang A beinhaltet die Auflistung aller Bereiche der Referenzarchitektur und der einzelnen Referenzpunkte. Im darauf folgenden Anhang B befinden sich allgemeine Bedrohungsbäume für Bedrohungen, die nicht Teil des in der Bedrohungsanalyse untersuchten Szenarios sind. Anschließend sind einige Abbildungen und einzelne Bedrohungen in einer detaillierten Bedrohungsanalyse gelistet. Anhang C verweist auf die dieser Arbeit beiliegende CD auf der sich komplette Screenshots von Internetquellen und einigen ausgewählten Quellen im Portable Document Format befinden.

## 2 Grundlagen

### 2.1 Elektrizitätsversorgung

#### 2.1.1 Heutige Elektrizitätsversorgung

Die Elektrizitätsversorgung in Deutschland wird über ein nationales Verbundnetz sichergestellt. Es ist derzeit in vier überregionale Stromnetze aufgeteilt, die jeweils von unterschiedlichen Unternehmen, den sogenannten Übertragungsnetzbetreibern ([engl. transmission system operator](#)) betrieben werden. Sie sind für Betrieb, Ausbau sowie Wartung der überregionalen Transportnetze verantwortlich und sorgen für die überregionale Netzstabilität. Das elektrische Energieversorgungsnetz lässt sich in vier verschiedene Spannungsebenen aufteilen (siehe Tabelle 2.1) Verbraucher und Industriebetriebe werden durch die Nieder- und Mittelspannungsebene mit Energie versorgt. Die Hoch- und Höchstspannungsebenen dienen vor allem dem Transport von elektrischer Energie über weite Strecken. Zwischen den verschiedenen Ebenen wird der Strom mit Hilfe von Transformatoren umgewandelt und anschließend in andere Spannungsebenen eingespeist.<sup>2</sup>

Bezeichnung der Ebene	Nennspannung $U_N$	Beschreibung
Höchstspannung	220kV oder 380kV	Überregionale Transportnetze zur Verbindung der nationalen Stromnetze
Hochspannung	60kV bis 220kV	Regionale Verteilnetze zur Verbindung von Ballungszentren oder großen Industriebetrieben
Mittelspannung	6kV bis 60kV	Verteilnetze zur Versorgung von regionalen Transformatorstationen und spezieller Teilnehmer (z. B. Stadtwerke)
Niedrigspannung	230V oder 400V	Verteilnetze zur Anbindung von Haushalten und kleineren Industriebetrieben

Tabelle 2.1: Spannungsebenen in Deutschland<sup>3</sup>

Neben der Wechselstromübertragung wird die [Hochspannungs-Gleichstrom-Übertragung \(HGÜ\)](#) für die Fernübertragung in Seekabeln eingesetzt. Bisher wird Strom hauptsächlich in zentralisierten Großkraftwerken aus fossilen oder atomaren Primärenergieträgern erzeugt. Dieser wird dann in der in die Höchstspannungsebene eingespeist. Kleinere Kraftwerke speisen zusätzlich in die Hoch- und Mittelspannungsebene. Die Stromverteilung in den Verteilnetzen erfolgt dabei immer in eine Richtung, vom Kraftwerk bis zum Verbraucher.<sup>4</sup> Für einen stabilen Netzbetrieb müssen sich Einspeisung und Verbrauch entsprechen. Ein Überangebot bzw. Unterangebot führt zu einer veränderten Netzfrequenz. Sind die Unterschiede zwischen Einspeisung und Verbrauch zu groß, kann es zu größeren Stromausfällen kommen.<sup>5</sup>

<sup>2</sup>Vgl. [BMW](#)i, Referat Öffentlichkeitsarbeit: [BMW](#)i - Stromnetze (2011), [100].

<sup>3</sup>Angelehnt an: [ebd.](#), Allelein u. a.: [Energietechnik](#) (2010), [1], S. 380.

<sup>4</sup>Vgl. [ebd.](#), S. 380f.

<sup>5</sup>Vgl. [Kästner und Kießling](#): [Energie in 60 Minuten](#) (2009), [25], S. 62.

Um das Angebot an die Nachfrage möglichst genau anzupassen werden Lastprognosen erstellt. Diese Prognosen werden anhand der Lastgänge der Verbraucher erstellt. Dabei kommen je nach Höhe der jährlichen Entnahme unterschiedliche Verfahren zum Einsatz. Bei Verbrauchern mit einer jährlichen Entnahme von bis zu 100.000 Kilowattstunden werden repräsentative Lastprofile, die Standardlastprofile genannt werden, verwendet. In einem Standardlastprofil wird das Verbrauchsverhalten von Endverbrauchern unterschiedlichen normierten Kundengruppen (Gewerbe, Haushalt, Landwirtschaft) zugeordnet.<sup>6</sup> Mit Hilfe der jährlichen Abrechnung wird das Lastprofil schließlich angenähert. Bei Großabnehmern dient als Datenbasis „eine viertelstündige registrierende Leistungsmessung“<sup>7,8</sup>

Die vier überregionalen Netze werden auch als Regelzonen bezeichnet. Jede Regelzone ist wiederum in 100-200 Bilanzkreise eingeteilt, dem die Netznutzer zugeordnet sind. Für die einzelnen Bilanzkreise erstellt der Bilanzkreisverantwortliche eine Abschätzung über den Verbrauch in 15 Minuten Intervallen anhand der Lastprognosen. Aus den gewonnenen Daten werden daraus viertelstündliche Kraftwerksfahrpläne erstellt. Kommt es zu einer Abweichung des tatsächlichen Verbrauch von dem geplanten Verbrauch, greifen die Übertragungsnetzbetreiber auf Regelenenergie zurück. Diese wird im Energiehandel von anderen Energieerzeugern zu höheren Preisen als die im voraus geplante Energie angeboten. Die Mehrkosten für Regelenenergie werden dem Bilanzkreisverantwortlichen in Rechnung gestellt. Reicht auch die Regelenenergie nicht aus um ein Leistungsgleichgewicht herzustellen, kommt es im Notfall zur Trennung von einzelnen Kraftwerken bzw. zu einer Aufspaltung in Teilnetze.<sup>9</sup>

### 2.1.2 Zukünftige Elektrizitätsversorgung

Am 30. Juni 2011 hat die deutsche Bundesregierung beschlossen die letzten Kernkraftwerke Deutschlands spätestens im Jahr 2022 abzuschalten.<sup>10</sup> Gleichzeitig wurden mit der Novellierung des „Erneuerbare-Energien-Gesetz“<sup>11</sup> die Ziele festgelegt bis 2020 den Anteil erneuerbarer Energien an der Stromversorgung von derzeit 17 Prozent<sup>12</sup> auf einen Anteil von mindestens 30 Prozent zu erhöhen.<sup>13</sup> Die Tendenz geht in Richtung einer dezentralen, auf erneuerbaren Ressourcen basierende, Energieerzeugung. So sind große Offshore-Windparks an Küsten oder Solarkraftwerke in Wüsten mit Übertragung zu weiter entfernten Verbrauchszentren geplant.<sup>14</sup> Hierfür ist der Ausbau der Netze auf internationaler Ebene mit neuen Leitungen wie beispielsweise HGÜ-Leitungen geplant.

Regenerative Energien haben die Eigenschaft sehr volatil zu sein. Als Folge wird die Stromerzeugung ungleichmäßiger. Diese Schwankungen können auch Auswirkungen auf die Netzstabilität haben. Eine Möglichkeit die Auswirkungen in den Griff zu bekommen ist den Stromhandel

---

<sup>6</sup>Vgl. StromNZV (2011), [191], § 12.

<sup>7</sup>Ebd., § 18.

<sup>8</sup>Vgl. ebd., § 18.

<sup>9</sup>Vgl. Höfer-Zygan, Oswald und Heidrich: Smart Grid Communications 2020 (2011), [69], S. 10.

<sup>10</sup>Vgl. Renneberg: Bundestag beschließt Atomausstieg und Energiewende, [118].

<sup>11</sup>Vgl. EEG (2011), [183], § 1.

<sup>12</sup>Vgl. BMWi, Referat Öffentlichkeitsarbeit: BMWi - Stromnetze (2011), [100].

<sup>13</sup>Vgl. EEG (2011), [183], § 1 (2).

<sup>14</sup>Vgl. Knies, Möller und Straub: Clean Power from Deserts (2007), [72], S. 35.



innerhalb Europas zu verstärken.

Eine weitere existiert in der Einbindung von Energiespeichern. Besteht eine geringe Energienachfrage wird überschüssige Energie mit Hilfe von Speichertechnologien zwischengespeichert. Bei steigender Nachfrage kann diese dann wieder zugänglich gemacht werden. Neben der Speicherung in Pump- und Druckluftspeicherkraftwerken bieten sich Elektrofahrzeuge als zukünftige Energiespeicher an. So plant die Nationale Plattform Elektromobilität eine Million zugelassene Elektrofahrzeuge im Jahr 2020.<sup>15</sup> Diese werden neben der Speichermöglichkeit und damit der Unterstützung des Lastmanagements auch zusätzliche Spitzenlasten erzeugen.

Darüber hinaus sollen Endverbraucher Energie ihrer Kleinst- bzw. Mikrokraftwerke wie z.B. Photovoltaikanlagen in das Netz einspeisen. Mehrere kleinere Kraftwerke sollen sich als virtuelle Kraftwerke in einem Verbund zusammenschließen, die netzseitig wie ein größeres Kraftwerk behandelt werden können. Mit der Einspeisung der Verbraucher soll sich damit auch das Paradigma des einseitigen Stromflusses vom Verteilnetz zum Verbraucher ändern. Der Verbraucher wird damit zum Produzenten.

### 2.1.3 Rollen in der Elektrizitätswirtschaft

Auf Grund von gesetzlichen Änderungen im [Energiewirtschaftsgesetz \(EnWG\)](#) (siehe Abschnitt [2.4.2](#)) kam es zu einer Liberalisierung im Elektroenergiemarkt. Bestehende staatliche Gebietsmonopole wurden abgeschafft, sodass einzelne Lieferanten (Stromanbieter) nicht mehr nur regional, sondern national auftreten können. Der Wettbewerb wurde angekurbelt, indem die vertikal integrierten Energieversorger aufgesplittet und die bestehende Infrastruktur für unterschiedliche vom Gesetzgeber vorgegebene Marktrollen freigegeben wurde. Dem Netzkunde (Verbraucher) wurde dabei insbesondere die Möglichkeit gegeben den Lieferanten zu wählen und für die Messung des Stromverbrauchs einen unabhängigen Messstellenbetreiber bzw. Messdienstleister zu beauftragen. Der Messstellenbetreiber ist dabei für Einbau, Betrieb und Wartung von Messeinrichtungen und der Messdienstleister für die Messung der Verbrauchsdaten zuständig.<sup>16</sup> Im Fall von elektronischen Messsystemen, wie es Smart Meter sind, (siehe Abschnitt [2.3.1](#)) ist der Messstellenbetreiber zugleich zwingend auch der Messdienstleister.<sup>17</sup>

[Abbildung 2.1](#) zeigt einen Überblick über die verschiedenen Marktrollen in der Elektrizitätswirtschaft und die dabei bestehenden vertraglichen Beziehungen.<sup>18</sup>

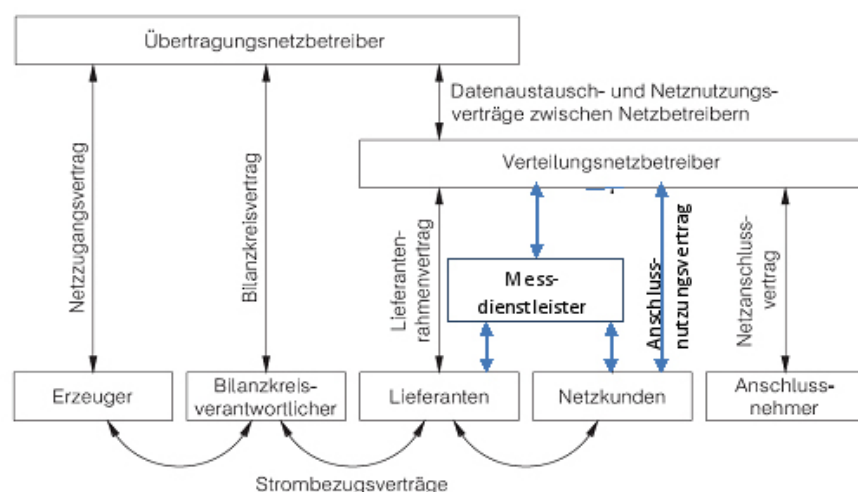
---

<sup>15</sup>Vgl. BMWi, Referat Öffentlichkeitsarbeit: BMWi - Elektromobilität, [97].

<sup>16</sup>Vgl. Köhler-Schute: Smart Metering (2009), [20], S. 65.

<sup>17</sup>Vgl. MessZV (2010), [190], § 9 (2).

<sup>18</sup>Vgl. Höfer-Zygan, Oswald und Heidrich: Smart Grid Communications 2020 (2011), [69], S. 16.

Abbildung 2.1: Rollen und Vertragsbeziehungen in der Elektrizitätswirtschaft<sup>19</sup>

## 2.2 Smart Grid

Unter dem Begriff Smart Grid (dt. intelligentes Stromnetz) versteht man eine mit Hilfe von **IKT** unterstützte Vernetzung und Steuerung der unterschiedlichen Teilnehmer zukünftiger Energieversorgungssysteme. Dies beinhaltet Teilnehmer aus den Bereichen Erzeugung, Speicherung, Transport, Verteilung und Verbrauch von Energie.<sup>20</sup> Im Smart Grid wird das bereits vorhandene Leitungsnetz für die Energieübertragung weiterhin genutzt und durch ein Datennetz zur Übertragung von Informationen ergänzt. Diese Informationen können Messdaten, Preisinformationen, Steuersignale, Netzzustandsinformationen und weitere sein, die zwischen den beteiligten Teilnehmern ausgetauscht werden.

### 2.2.1 Referenzarchitektur

Die Ausgestaltung eines Smart Grid kann unterschiedliche Formen annehmen. Eine Referenzarchitektur abstrahiert die Systemarchitektur, die hinter diesen unterschiedlichen Realisierungsformen steht und dient als Kommunikations- bzw. Diskussionsgrundlage. Von verschiedenen Parteien wurden für das Smart Grid unterschiedliche Referenzarchitekturen definiert, die sich im Detaillierungsgrad (von abstrakt<sup>21</sup> bis sehr detailliert<sup>22</sup>) oder im Fokus unterscheiden.<sup>23</sup> Für diese

<sup>19</sup>Quelle: Höfer-Zygan, Oswald und Heidrich: Smart Grid Communications 2020 (2011), [69], S. 16

<sup>20</sup>Vgl. BMWi, Referat Öffentlichkeitsarbeit: Intelligente Netze und intelligente Zähler - Smart Grids/Smart Meter (2011), [99]; VDE: Die deutsche Normungsroadmap E-Energy / Smart Grid (2010), [93], S. 13.

<sup>21</sup>Vgl. ebd., S. 34; NIST: NISTIR 7628 Vol. 1 (2010), [170], S. 15; Benze, Hübner und Kießling: Das intelligente Energiesystem als zukünftige Basis für ein nachhaltiges Energiemanagement (2011), [48], S. 6.

<sup>22</sup>Vgl. IEEE 2030-2011 (2011), [167]; NIST: NIST SP 1108 (2010), [92], S. 35; Beenken: Schutz sicherheitsrelevanter Informationen in verteilten Energieinformationssystemen (2010), [5], S. 20; Cisco Systems: Cisco Grid Blocks Reference Model (2011), [56].

<sup>23</sup>Vgl. IEC Smart Grid Standardization Roadmap (2010), [70], S. 24; Coyne u. a.: Systems Architecture for Smart Grids (2010), [57], S. 9; Microsoft: Smart Energy Reference Architecture (2009), [77]; SCE-Cisco-IBM SGRA Team: Smart Grid Reference Architecture Volume 1 (2011), [85].

Arbeit soll deshalb die in [Abbildung 2.2](#) dargestellte Referenzarchitektur festgelegt werden, in der die Kommunikationsbeziehungen zwischen den einzelnen Bestandteilen dargestellt sind.

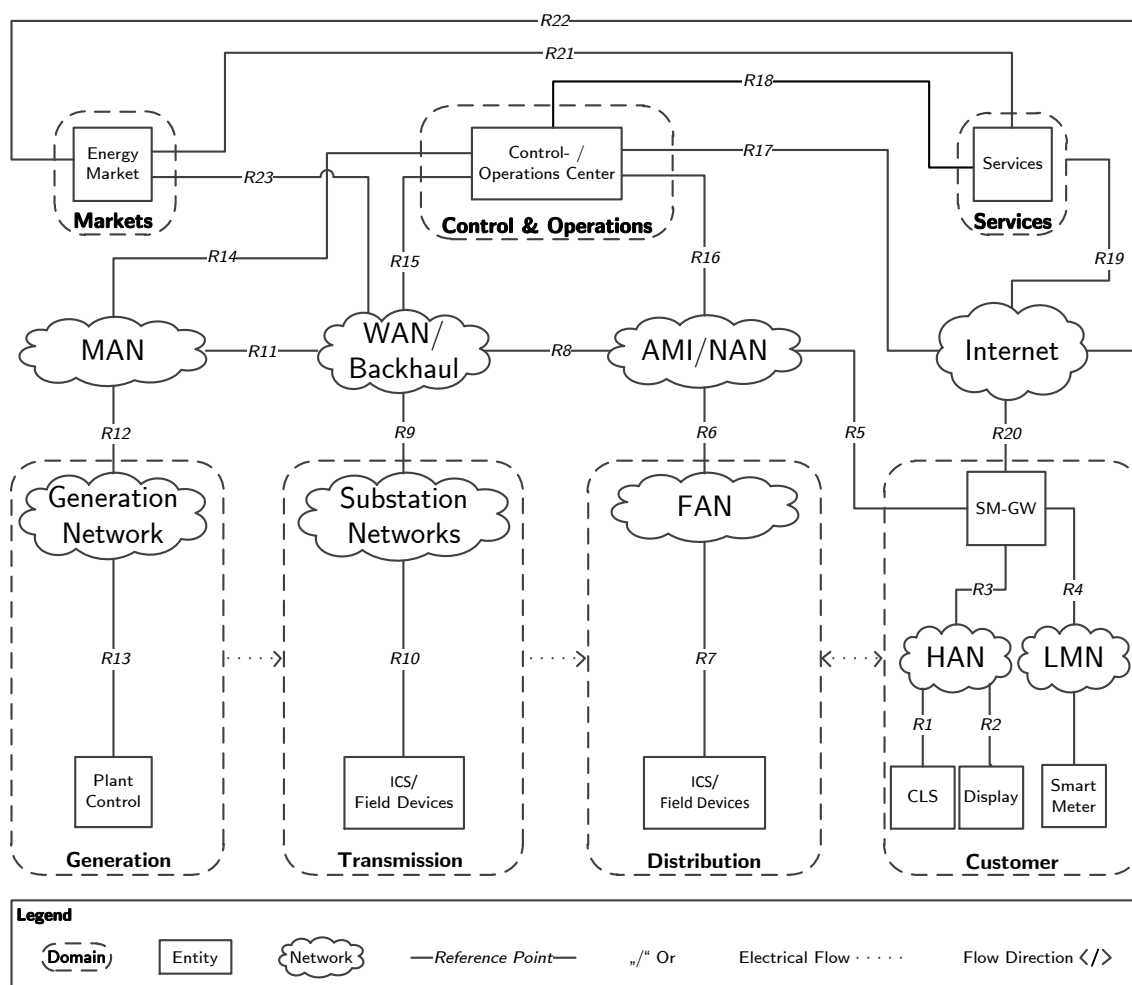


Abbildung 2.2: Smart Grid Referenzarchitektur<sup>24</sup>

Zusätzlich ist der Energiefluss zwischen den Bereichen ([engl. domain](#)) Erzeugung ([engl. generation](#)), Übertragung ([engl. transmission](#)) und Verteilung ([engl. distribution](#)) in Richtung der Verbraucher ([engl. customer](#)) durch Pfeile skizziert. Dezentrale Energieerzeugung beim Verbraucher ([engl. customer](#)) kann zu einem Energiefluss in Gegenrichtung (als Doppelpfeil in [Abbildung 2.2](#) dargestellt) führen. Der Bereich des Verbrauchers umfasst neben privaten auch kommerzielle und industrielle Kunden. Bei den letztgenannten und größeren kommerziellen Kunden werden ebenso Smart Meter und [Smart Meter Gateways \(SM-GWs\)](#) eingesetzt. Allerdings kann sich der dortige Aufbau der Architektur von der hier gezeigten, die ihren Fokus im Bereich des Verbrauchers auf private bzw. kleinere kommerzielle Kunden legt, unterscheiden.

Neben den bereits erwähnten Bereichen sind auch die Märkte ([engl. markets](#)), Dienstleistungen ([engl. services](#)) und die Leittechnik ([engl. control & operations](#)), welche mit den anderen

<sup>24</sup>Angelehnt an: [IEEE 2030-2011 \(2011\)](#), [167], S. 30, 43, 45, 66; [NIST: NIST SP 1108 \(2010\)](#), [92], S. 35; [Becken: Schutz sicherheitsrelevanter Informationen in verteilten Energieinformationssystemen \(2010\)](#), [5], S. 20; Bereich des Verbrauchers: [Kreutzmann u. a.: BSI-CC-PP-0073 \(2011\)](#), [150], S. 11.

Bereichen in Verbindung stehen, in der Referenzarchitektur eingezeichnet.

Die wichtigsten Bestandteile der Referenzarchitektur werden in den folgenden Abschnitten näher beschrieben. In Anhang A findet sich eine Aufschlüsselung aller Bestandteile.

Im Bereich der Erzeugung wird mit Hilfe von Generatoren Energie umgewandelt. Die Kontrolle innerhalb eines Kraftwerks wird dabei über die Kraftwerkssteuerung (*engl.* plant control) durchgeführt welche an ein Netzwerk innerhalb des Kraftwerks angeschlossen ist (*engl.* generation network).<sup>25</sup> Industrielle Steuerungssysteme (ICS, *engl.* industrial control systems, siehe Abschnitt 2.2.2) und Feldgeräte (*engl.* field devices) sind an Umspannnetzwerke (*engl.* substation networks) innerhalb des Übertragungsbereichs bzw. an Feldgerätenetzwerke (FAN) im Verteilnetzbereich angeschlossen. Sie werden zur Überwachung der Energieübertragung eingesetzt.

SM-GW und Smart Meter sind wichtige Geräte des Smart Grids im Bereich des Verbrauchers (für eine Beschreibung siehe Abschnitt 2.3.1 und 2.3.2). Das SM-GW ist dabei mit dem AMI/NAN-Netz (üblicherweise in den *United States of America (USA)*) oder mit dem Internet (z. B. in Deutschland) verbunden. AMI (Advanced Metering Infrastructure) bzw. NAN (Neighborhood Area Network) stellen dabei eine Netzwerkstruktur zur Zählerfernauslesung dar. Dabei werden die Messdaten von mehreren Haushalten z. B. per *Wireless Local Area Network (WLAN)*<sup>26</sup> oder *Powerline Communication (PLC)*<sup>27</sup> an Zwischenstationen übertragen und gesammelt weitergeleitet. Die Anbindung an das Internet erfolgt z. B. per *Digital Subscriber Line (DSL)*<sup>28</sup>, Breitband Kabelanschluss<sup>29</sup> oder *Universal Mobile Telecommunications System (UMTS)*<sup>30</sup>

Die Verbraucher beziehen neben Energiedienstleistungen wie Strom auch weitere Dienstleistungen auf die sie über das Internet Zugriff erhalten (siehe Abschnitt 2.3.3). Beim Einsatz von dynamischen Tarifen werden den Kunden Preisinformationen zur Verfügung gestellt. Dazu greifen Dienstleister auf den aktuellen Strompreis, der sich im Energiehandel ergibt, zurück und leiten davon die übermittelten Preisinformationen ab, denn Strom wird im Bereich der Märkte an Börsen wie in Deutschland am *European Energy Exchange (EEX)*<sup>31</sup> gehandelt.

Der Bereich der Leittechnik umfasst neben industriellen Steuerungssystemen, die im nächsten Abschnitt beschrieben werden, folgende unterschiedliche Managementsysteme:

- Energiemanagementsystem (EMS): System, das zur Optimierung oder Kontrolle von Energiesystemen eingesetzt wird indem z. B. Lastprognosen erstellt werden.
- Verteilungsmangementsysteme (DMS, *engl.* distribution management system): Besondere Ausführung eines Energiemanagementsystems, welches zur Steuerung und Planung der Energieverteilung im Niederspannungsnetz eingesetzt wird.

---

<sup>25</sup> *Anm.*: Zur Kraftwerkssteuerung werden industrielle Steuerungssysteme verwendet. Der Name Kraftwerkssteuerung soll verdeutlichen, dass es sich um besondere industrielle Steuerungssysteme handelt.

<sup>26</sup> Siehe Sauter: Grundkurs Mobile Kommunikationssysteme (2011), [37], S. 337ff.

<sup>27</sup> *Anm.*: Datenübertragung über vorhandene Stromnetze; siehe Carcelle: Power Line Communications in Practice (2009), [8].

<sup>28</sup> *Anm.*: Verschiedene Arten von DSL-Techniken werden unter diesem Begriff zusammengefasst. In Deutschland hauptsächlich in der Variante ADSL (Asymmetric Digital Subscriber Line). Siehe Bluschke, Matthews und Badach: XDSL-Fibel (2001), [7].

<sup>29</sup> Siehe Laubach, Farber und Dukes: Delivering Internet Connections over Cable (2001), [26].

<sup>30</sup> Siehe Sauter: Grundkurs Mobile Kommunikationssysteme (2011), [37], S. 155ff.

<sup>31</sup> Siehe <http://www.eex.com>.

- Messdatenmanagementsystem (MDMS): System, das zur Verwaltung gesammelter Messdaten verwendet wird.

Informationen zur Planung und Steuerung der Energielieferung werden dabei nicht nur innerhalb des Energieversorgungsunternehmens, sondern auch mit anderen Unternehmen über das Internet ausgetauscht (siehe [Abb. 2.2 R17](#)).<sup>32</sup>

### 2.2.2 Industrielle Steuerungssysteme und Feldgeräte

Innerhalb von Energieversorgungsnetzen werden industrielle Steuerungssysteme und Feldgeräte im Bereich der Übertragung und Verteilung bzw. in der Leittechnik zur Automatisierung, Überwachung, Steuerung und Regelung technischer Prozesse mit Hilfe von Computersystemen eingesetzt.<sup>33</sup> Dort sammeln sie Messdaten von entfernten Sensoren, welche Feldgeräte genannt werden. Das industrielle Steuerungssystem umfasst als allgemeiner Oberbegriff die verschiedenen Arten von Kontroll- und Steuerungssystemen. Neben Supervisory Control and Data Acquisition (SCADA)-Systemen gehören dazu Speicherprogrammierbare Steuerungen (SPS; engl. Programmable Logic Controller) und Prozessleitsysteme (PLS; engl. Process Control Systems) bzw. verteilte Prozessleitsysteme (DCS; engl. Distributed Control Systems).<sup>34</sup> Steuerung und Regelung in SCADA-Systemen erfolgen entweder automatisiert oder manuell. Ein SCADA-System besteht dabei aus folgenden Komponenten:

- Operator: Ein Operator bzw. ein Operatorteam überwacht von einem Leitstand aus die Systeme und greift gegebenenfalls in die automatisierte Steuerung ein.
- HMI: Zur manuellen Steuerung durch den Operator dienen Bedienungsfelder (engl. operator control panel) als Mensch-Maschine-Schnittstelle (HMI; engl. human machine interface).
- RTU: Fernbedienungsterminals (RTU, engl. Remote Terminal Unit) sind externe Steuereinheiten, die Befehle an von ihnen kontrollierte Geräte versenden. Zu diesen Geräten gehören Sensoren, Aktuatoren oder Steuergeräte, welche mit dem Begriff „intelligent electronic device“ (IED) zusammengefasst beschrieben werden.
- Netzwerke: Die verschiedenen Geräte sind über unterschiedliche Arten von Netzwerken verbunden. Die Datenkommunikation erfolgt dabei über unterschiedliche Protokolle wie Modbus oder DNP3.<sup>35</sup>

Bisher wurden SCADA-Systeme eher in isolierten Umgebungen betrieben. Im Smart Grid sollen sie verstärkt vernetzt und so mit anderen Systemen gekoppelt werden.<sup>36</sup>

---

<sup>32</sup>Vgl. Beenken: Schutz sicherheitsrelevanter Informationen in verteilten Energieinformationssystemen (2010), [5], S. 19-24.

<sup>33</sup>Vgl. Flick und Morehouse: Securing the Smart Grid (2011), [15], S. 54.

<sup>34</sup>Vgl. Stouffer, Falco und Scarfone: NIST SP 800-82 (2011), [158], S. 2-1.

<sup>35</sup>Vgl. Knapp: Industrial Network Security (2011), [22], S. 89-94.

<sup>36</sup>Vgl. Eckert und Krauß: Sicherheit im Smart Grid (2011), [13].

Speicherprogrammierbare Steuerungen übernehmen als spezielle Computersysteme die Steuerung bzw. Regelung von Maschinen, indem sie mehrere Ein-/Ausgabekanäle verwalten.<sup>37</sup> Prozessleitsysteme bzw. verteilte Prozessleitsysteme stellen komplexe Prozesse übersichtlich dar und unterstützen oder ermöglichen damit überhaupt erst die Steuerung durch den Menschen.<sup>38</sup> Korrekterweise sollte zwischen den in diesem Abschnitt beschriebenen Systemen unterschieden werden.<sup>39</sup> Allerdings kommt es zu Überschneidungen der Begriffe. So ist eine SPS oft Teil eines SCADA oder DCS Systems.<sup>40</sup> Dies führt dazu, dass diese Begriffe zum Teil als Synonym verwendet werden. Da eine feingranulare Betrachtung den Rahmen dieser Arbeit sprengen würde, werden die Systeme unter dem Begriff industrielle Steuerungssysteme wissentlich zusammengefasst betrachtet.<sup>41</sup>

### 2.3 Smart Metering

Smart Metering beinhaltet die automatische Erfassung und Verarbeitung von Messdaten über aktuellen Verbrauch bzw. aktuelle Einspeisung, eine bidirektionale Kommunikation und Fernauslesung von Zählern sowie zusätzlich weitere Mehrwertfunktionen wie Fernabschaltung bzw. Zuschaltung intelligenter Geräte, Energieberatung und Energiemanagement über Feedbacksysteme. Mit seinen Eigenschaften bildet das Smart Metering damit eine Basistechnologie für das Smart Grid.<sup>42</sup> Für eine optimale Steuerung des Energieverbrauchs der Geräte innerhalb eines Haushaltes muss das Smart Metering um Konzepte des Smart Home erweitert werden. Das Ziel dabei ist, dass die Geräte die Stromnachfrage an das schwankende Angebot aus erneuerbaren Energiequellen anpassen. Allerdings gelingt dies nur mit neuen, intelligenten Endgeräten, die an das Heimnetzwerk angeschlossen werden. Dies ist nicht Teil der vorliegenden Arbeit und wird deshalb nicht weiter betrachtet.

#### 2.3.1 Smart Meter

Ein Smart Meter oder [dt.](#) intelligenter Stromzähler<sup>43</sup> ist ein Messgerät, das den aktuellen Bedarf an elektrischer Energie, [ugs.](#) Stromverbrauch, in kurzen Zeitintervallen, wie z. B. alle 2 Sekunden aufzeichnet. Die Ergebnisse werden dabei in digitaler Form im Zähler verarbeitet und elektronisch beispielsweise per D0-Schnittstelle<sup>44</sup>, [PLC](#), [M-Bus](#)<sup>45</sup>, [Wireless M-Bus](#)<sup>46</sup> oder [ZigBee](#)<sup>47</sup> weitergeleitet. Als Messgeräte unterliegen Smart Meter in Deutschland damit

<sup>37</sup>Vgl. Knapp: Industrial Network Security (2011), [\[22\]](#), S. 90.

<sup>38</sup>Vgl. Bolch und Zahner: Was heißt Prozessautomatisierung? (2004), [\[51\]](#), S. 20.

<sup>39</sup>Vgl. Knapp: Industrial Network Security (2011), [\[22\]](#), S. 7.

<sup>40</sup>Vgl. Stouffer, Falco und Scarfone: [NIST SP 800-82](#) (2011), [\[158\]](#), S. 2-1.

<sup>41</sup>[Anm.](#): Für eine genauere Beschreibung von Industriellen Steuerungssystemen und den dort verwendeten Protokollen siehe Knapp: Industrial Network Security (2011), [\[22\]](#).

<sup>42</sup>Vgl. Koponen u. a.: Definition von Smart Metering, Anwendungen und Identifikation der Vorteile (2008), [\[73\]](#), S. 4.

<sup>43</sup>[Anm.](#): Im allgemeinen Sprachgebrauch wird die technisch falsche Bezeichnung Stromzähler verwendet. Die physikalisch korrekte Bezeichnung lautet Elektrizitätszähler. Gemessen wird die elektrische Arbeit.

<sup>44</sup>Siehe [DIN EN 62056-21](#) (2003), [\[143\]](#).

<sup>45</sup>Siehe [DIN EN 13757-2](#) (2005), [\[134\]](#); [DIN EN 13757-3](#) (2005), [\[135\]](#).

<sup>46</sup>Siehe [DIN EN 13757-4](#) (2005), [\[136\]](#).

<sup>47</sup>Siehe [ZigBee Standards Organization: ZigBee-2007 specification](#) (2008), [\[161\]](#); [IEEE 802.15.4-2006](#) (2006), [\[169\]](#).

dem Eichgesetz (siehe Abschnitt 2.4.2). Das übliche Geschäftsmodell für den Strombezug in Deutschland sieht ein festes Vertragsverhältnis mit nachträglicher Rechnungslegung des Stromkunden mit seinem Lieferanten vor. In anderen Ländern wie z. B. Großbritannien sind dagegen Modelle mit Vorausbezahlung (engl. prepaid) verbreitet<sup>48</sup>, bei denen nach Ablauf des Guthabens die Stromzufuhr komplett abgestellt wird bzw. nur noch der Notbetrieb möglich ist. Hierfür werden sogenannte Prepaid Smart Meter eingesetzt. Die Aufladung des Guthabens erfolgt dabei entweder über Guthabentoken wie z. B. Magnetkarten, Smart Cards oder über die Eingabe von Vouchercodes wie man es von Prepaid-Mobilfunktarifen kennt. Das Abrechnungssystem kann dabei lokal im Smart Meter arbeiten oder zentralisiert wie es im Mobilfunk üblich ist.<sup>49</sup> Optional können heutige Smart Meter mit einer Fernabschaltfunktion ausgestattet sein, die dem Energieversorger eine Trennung der Stromzufuhr aus der Ferne ermöglicht.<sup>50</sup> Einsatzgebiete umfassen dabei beispielsweise die weiter oben beschriebenen Prepaid Smart Meter oder die Abschaltung von Smart Metern in leer stehenden Häusern. Die detaillierte Aufzeichnung ermöglicht eine genaue Lastbestimmung, woraus sich datenschutzrechtliche Probleme ergeben können. Hierauf wird in Abschnitt 3.1.2 näher eingegangen.

### 2.3.2 Smart Meter Gateway

Das **Smart Meter Gateway (SM-GW)**, oft auch als **Multi Utility Communication (MUC)**-Controller oder Konzentrator bezeichnet stellt eine zentrale Kommunikationseinheit im Smart Metering System dar.<sup>51</sup> Hier werden die vom Smart Meter empfangenen Messwerte erfasst, verarbeitet und gespeichert. Als Schnittstelle verbindet es das Heimnetz, engl. **Home Area Network (HAN)**, eines Anschlussnutzers mit dem lokalen Messeinrichtungsnetz, engl. **Local Metrological Network (LMN)**, und verschiedene Marktteilnehmer über ein Weitverkehrsnetz, engl. **Wide Area Network (WAN)**.

Im **HAN** können über zwei logische Schnittstellen Anzeigeeinheiten und dezentral steuerbare Verbraucher- oder Erzeugersysteme, engl. **Controllable Local Systems (CLS)**, wie z. B. Kleinstkraftwerke oder intelligente Endgeräte angesprochen werden. Mit der Anzeigeeinheit in Form eines separaten Displays oder Personal Computers werden feingranulare Verbrauchswerte, eichrechtlich relevante Daten wie Verbrauchs- bzw. Einspeisungswerte in geringerer Auflösung, und weitere Informationen wie protokollierte Zugriffe auf das **SM-GW** abrufbar.

Über das **LMN** empfängt das **SM-GW** in regelmäßigen Abständen, beispielsweise alle 2 Sekunden Messwerte, von allen Smart Metern eines Anschlussnutzers. Diese werden mit einem Zeitstempel versehen und bei der Nutzung von zeitvariablen (Strompreis variiert je nach Uhrzeit) bzw. dynamischen Tarifen (der Strompreis hängt von externen Größen wie Gesamtlast, Saison oder

---

<sup>48</sup>Vgl. Köhler-Schute: Smart Metering (2009), [20], S. 60.

<sup>49</sup>Siehe Anderson und Bezuidenhout: On the Reliability of Electronic Payment Systems (1996), [3]; Talbot: Prepayment meters, [120].

<sup>50</sup>Vgl. Anderson und Fuloria: Who controls the off switch? (2010), [43], S. 1.

<sup>51</sup>Anm.: In VDE-Lastenheft MUC (2011), [74] wird das Konzept eines MUC und in Kreuzmann u. a.: BSI-CC-PP-0073 (2011), [150] das eines zukünftig verbindlichen SM-GW besprochen. Der Hauptunterschied zwischen den beiden ist der unterschiedliche Fokus. Beim MUC-Konzept geht es hauptsächlich um die wirtschaftliche Umsetzung der gesetzlichen Anforderungen (siehe Abschnitt 2.4.2). Das SM-GW-Konzept des BSI zielt hingegen auf den Schwerpunkt der Sicherheit der Kommunikationseinheit ab.



Preis an der Strombörse ab) dem zu dieser Zeit gültigen Tarif zugeordnet. Anschließend werden die Messwerte für die weitere Verarbeitung gespeichert. Die Datenübertragung im WAN erfolgt unter Verwendung unterschiedlicher Übertragungsstandards wie DSL, UMTS, GPRS<sup>52</sup> oder PLC. Dabei werden Messwerte übertragen und Administrations- und Konfigurationsinformationen ausgetauscht.<sup>53</sup>

Sicherheitsfunktionen sollten im SM-GW bereitgestellt werden, allerdings unterstützen oder nutzen diese nicht alle derzeit auf dem Markt erhältlichen SM-GW-Implementierungen. In Abschnitt 3.4.2 werden Sicherheitsfunktionen, welche zukünftige SM-GW umsetzen sollen erläutert. Smart Meter und Smart Meter Gateway sind voneinander getrennte Funktionen. Diese zu trennen ist insbesondere wichtig im Hinblick darauf, dass sich die Technologie der Kommunikationstechnik im Vergleich zur Messtechnik schneller verändert. Es gibt allerdings auch Bauformen in denen die getrennten Funktionen in einem Gerät integriert sind.<sup>54</sup>

### 2.3.3 Online-Dienste

Im Energiebereich gibt es Online-Dienste, die den Verbrauchern helfen sollen ihren Energieverbrauch zu visualisieren, um ihn danach zu optimieren. Als Datenquelle dienen heute hauptsächlich manuell eingegebene Daten,<sup>55</sup> die zukünftig automatisch ausgelesen werden sollen. Netzbetreiber, Messstellenbetreiber bzw. Messdienstleister oder externe Dienstleister stellen die gesammelten Verbrauchsinformationen in Webanwendungen<sup>56</sup> z. B. innerhalb des Kundenportals zur Verfügung. Darüber hinaus können auch Applikationen innerhalb von sozialen Netzwerken oder dort verfügbare Nachrichtenfunktionen aktuelle Verbrauchswerte visualisieren.<sup>57</sup>

In den Webanwendungen werden dabei z.B. neben Verbrauchsdaten und Lastgängen über definierbare Zeitintervalle auch Tarifsysteme visualisiert oder Trendanalysen für unterschiedliche Zeitintervalle ermöglicht. Daneben sind Energiespartipps bis hin zu einer Energieberatung, bei der den Verbrauchern Angebote über stromsparendere Haushaltsgeräte unterbreitet werden, denkbar. Zukünftig soll auch eine Steuerung von Geräten ermöglicht werden.<sup>58</sup>

## 2.4 Rechtliche und regulatorische Rahmenbedingungen

### 2.4.1 International

In den USA wurde mit dem „Energy Independence and Security Act of 2007“ eine Richtlinie verfasst, die eine Modernisierung des Stromnetzes, insbesondere der Transport- und Verteil-

---

<sup>52</sup>Siehe Sauter: Grundkurs Mobile Kommunikationssysteme (2011), [37], S. 93ff.

<sup>53</sup>Vgl. BSI: BSI TR-03109 (2011), [164]; Kreuzmann u. a.: BSI-CC-PP-0073 (2011), [150].

<sup>54</sup>Vgl. „One Box Solution“ ebd., S. 33.

<sup>55</sup>Siehe z. B. <http://www.ganz-einfach-energiesparen.de/>.

<sup>56</sup>Anm.: Außer proprietären Webanwendungen von Netzbetreibern wie z. B. dem EnBW Cockpit ( [http://www.enbw.com/content/de/privatkunden/produkte/zusatzinformationen/isz\\_cockpit/index.jsp](http://www.enbw.com/content/de/privatkunden/produkte/zusatzinformationen/isz_cockpit/index.jsp)) gibt es mit mySmartGrid (Fraunhofer-Gesellschaft: Überblick | mySmartGrid, [106]) und Flukso ( <https://www.flukso.net/>) auch Open Source Varianten.

<sup>57</sup>Siehe z. B. <http://www.google.de/search?q=kWh+usage+site%3Afacebook.com> bzw. <http://www.google.de/search?q=kWh+usage+site%3Atwitter.com>.

<sup>58</sup>Vgl. ebd.



netze, vorsieht.<sup>59</sup> Der „American Recovery and Reinvestment Act of 2009“ unterstützt die Finanzierung von Smart Grid Projekten.<sup>60</sup> Zusätzlich wurde 2009 eine Rechtsverordnung zur Unterstützung von Smart Grid Entwicklungen durch die [Federal Energy Regulatory Commission \(FERC\)](#) verfasst.<sup>61</sup> Die [Europäische Union \(EU\)](#) verabschiedete Mitte der neunziger Jahre erste Richtlinien zur Liberalisierung der Energiemärkte.<sup>62</sup> Die bisherigen hauptsächlich auf Monopolen aufbauenden Märkte sollten damit für Dritte Parteien geöffnet werden. Im Jahr 2003 folgte eine Novellierung der EU-Richtlinien, welche als zweites Energiebinnenmarktpaket bekannt ist. Mit Verabschiedung des dritten Energiebinnenmarktpakets wurde schließlich der Grundstein für Smart Metering innerhalb der EU gelegt. Laut der Richtlinie 2009/72/EG müssen die EU-Mitgliedsstaaten bis zum 3. September 2012 eine wirtschaftliche Bewertung der Einführung von Smart Metern durchgeführt haben. Fällt die Bewertung positiv aus, muss eine 80-prozentige Marktdurchdringung mit Smart Metern bis zum Jahr 2020 umgesetzt werden.<sup>63</sup>

In dieser Richtlinie wird Sicherheit (siehe Abschnitt 3) hauptsächlich hinsichtlich Versorgungssicherheit, also der Sicherstellung der Energieversorgung, angesprochen. Eine weitere Betrachtung wie z.B. Hinweise auf Bedrohungen erfolgt nicht.<sup>64</sup>

### 2.4.2 National

In Deutschland wurden die Vorgaben der Europäischen Richtlinien durch Änderungen im [Energiewirtschaftsgesetz \(EnWG\)](#) im Jahr 2005 sowie dem Erlass der Messzugangsverordnung (MessZV),<sup>65</sup> in der Voraussetzungen und Bedingungen für den Messstellenbetrieb bzw. für einzelne Messungen geregelt sind, umgesetzt.

Das [EnWG](#) wurde hierzu seit der Ausfertigung vom 7. Juli 2005<sup>66</sup> bis zur letzten Änderung vom 24. November 2011 ([EnWG 2011](#)), auf die sich die folgenden Ausführungen beziehen, mehrmals angepasst.<sup>67</sup> § 21b [EnWG](#) schreibt vor, dass der Messstellenbetrieb entweder vom Netzbetreiber oder auf Wunsch des Kunden von einem Dritten, beispielsweise einem Messdienstleister, erfolgen soll. Der Messstellenbetreiber ist zur Installation von Smart Metern<sup>68</sup> verpflichtet, wenn dem Anschlussnutzer dadurch keine Mehrkosten entstehen oder genügend gesetzeskonforme Messsysteme am Markt verfügbar sind. Auch wenn dabei Mehrkosten entstehen, gilt die Einbaupflicht für Neubauten und für Gebäude, die einer größeren Sanierung unterliegen,<sup>69</sup> bei Verbrauchern mit einem Jahresverbrauch größer als 6.000 Kilowattstunden

---

<sup>59</sup>Vgl. Energy Independence and Security Act of 2007 (2007), [177], 292ff.

<sup>60</sup>Vgl. American Recovery and Reinvestment Act of 2009 (2009), [172].

<sup>61</sup>Siehe [FERC: Smart Grid Policy \(2009\)](#), [192].

<sup>62</sup>Vgl. [EU-Richtlinie für den Elektrizitätsbinnenmarkt 96/92/EG \(1996\)](#), [187]; [EU-Richtlinie für den Erdgasbinnenmarkt 98/30/EG \(1998\)](#), [188].

<sup>63</sup>Vgl. [EU-Richtlinie für den Elektrizitätsbinnenmarkt 2009/72/EG \(2009\)](#), [185], S. 91f.

<sup>64</sup>Vgl. [ebd.](#), (25), S. 57f.

<sup>65</sup>Siehe [MessZV \(2010\)](#), [190].

<sup>66</sup>Siehe [EnWG 2005 \(2005\)](#), [182].

<sup>67</sup>Siehe [EnWG 2011 \(2011\)](#), [181]; [Anm.](#): Die während der Bearbeitung dieser Arbeit verfügbare Literatur bezieht sich hauptsächlich auf das [EnWG 2008 \(2008\)](#), [180], § 21b und § 40; wesentliche Unterschiede werden gegebenenfalls hervorgehoben. Für eine übersichtliche Darstellung der Änderungen siehe <http://www.buzer.de/gesetz/2151/l.htm>.

<sup>68</sup>Vgl. [EnWG 2011 \(2011\)](#), [181], § 21d.

<sup>69</sup>[Anm.](#): Befindet sich im [EnWG 2008 \(2008\)](#), [180], in § 21b (3a).

oder bei Anlagebetreibern von Neuanlagen, die in das Niederspannungsnetz einspeisen, soweit eine installierte Leistung größer als sieben Kilowatt vorliegt. Dem Anschlussnutzer wird es dabei untersagt den Einbau eines Smart Meters zu verhindern oder im Nachhinein abzuändern. Für an das Messsystem angebundene Erzeugungsanlagen gilt dabei die selbe Regelung.<sup>70</sup>

Eingesetzte Smart Meter und **SM-GW** müssen den Anforderungen von Schutzprofilen und technischen Richtlinien (siehe Abschnitt 3.4.2) entsprechen, um Interoperabilität, Datensicherheit und Datenschutz zu gewährleisten. Die Einhaltung dieser werden in einem Zertifizierungsverfahren geprüft.<sup>71</sup> Als Ausnahme dürfen bis Ende 2012 noch Smart Meter verbaut werden, die den Anforderungen nicht genügen. Bis zum Ablauf der Eichfrist (siehe am Ende des Abschnittes) wird diesen ein Bestandsschutz gewährt.<sup>72</sup>

§ 40 **EnWG** verpflichtet Energielieferanten zu einer Verkürzung der derzeit üblichen jährlichen Abrechnungsperiode. Die Abrechnung soll hierzu auf monatlicher, vierteljährlicher oder halbjährlicher Basis erfolgen. Außerdem müssen die Lieferanten mindestens einen lastvariablen oder tageszeitabhängigen Tarif anbieten der Anreize zur Energieeinsparung bzw. eine Steuerung des Energieverbrauchs bietet. Zusätzlich muss mindestens ein Tarif angeboten werden der Datensparsamkeit ermöglicht, indem nur die innerhalb eines Zeitraums verbrauchte Strommenge übertragen wird. Dabei gilt für die Tarifvarianten die Einschränkung, dass diese nur soweit es technisch möglich und wirtschaftlich tragbar ist angeboten werden müssen.<sup>73</sup>

Im **EnWG** werden beim Thema Sicherheit (siehe Abschnitt 3), ähnlich zu den **EU**-Richtlinien, hauptsächlich Aspekte der Versorgungssicherheit,<sup>74</sup> aber auch der technischen Sicherheit,<sup>75</sup> angesprochen. Bei der technischen Sicherheit bzw. Betriebssicherheit, wird zum Beispiel besonderes hervorgehoben, dass die **IKT**-Systeme, die als Steuerungssysteme des Energieversorgungsnetzes verwendet werden, vor Bedrohungen angemessen geschützt werden müssen. Um einen angemessenen Schutz sicherzustellen werden Sicherheitsanforderungen in Form eines Sicherheitskatalogs vom **Bundesamt für Sicherheit in der Informationstechnik (BSI)** zusammen mit der **Bundesnetzagentur (BNetzA)** vorgelegt. Einhaltung und anschließende Dokumentation der Sicherheitsanforderungen wird dabei als angemessener Schutz angesehen.<sup>76</sup>

Die klassischen Schutzziele der Angriffssicherheit, Vertraulichkeit und Integrität sowie die Authentifizierung (siehe Abschnitt 3.2) werden im Zusammenhang der Anforderungen an Smart Meter erwähnt. Diese sollen von allen bei der Datenübermittlung beteiligten Stellen durch Maßnahmen zur Sicherstellung von Datensicherheit und Datenschutz gewährleistet werden.<sup>77</sup> Auf den Datenschutz (siehe Abschnitt 3.1.2) wird hauptsächlich im Zusammenhang mit dem Messbetrieb eingegangen.<sup>78</sup> Dabei wird z. B. die Pseudonymisierung bzw. Anonymisierung (siehe Abschnitt 3.1.2) von personenbezogenen Daten als Maßnahmen des Datenschutz

---

<sup>70</sup>Vgl. EnWG 2011 (2011), [181], § 21c; neu in EnWG 2011.

<sup>71</sup>Vgl. *ebd.*, § 21e, § 21i.

<sup>72</sup>Vgl. *ebd.*, § 21e.

<sup>73</sup>Vgl. *ebd.*, § 40; Abschnitt zu datensparsamen Tarif ist neu in EnWG 2011.

<sup>74</sup>Vgl. *ebd.*, § 12, § 15, § 50-52.

<sup>75</sup>Vgl. *ebd.*, § 12, § 49.

<sup>76</sup>Vgl. *ebd.*, § 11 (1a).

<sup>77</sup>Vgl. *ebd.*, § 21e.

<sup>78</sup>Vgl. *ebd.*, § 21b, § 21e, § 21g, § 21h.

vorgeschlagen.<sup>79</sup>

Messsysteme müssen eichrechtlichen Vorgaben entsprechen.<sup>80</sup> Sie unterliegen dem deutschen Eichgesetz.<sup>81</sup> Die Eichgültigkeitsdauer für elektrisch betriebene Zähler beträgt acht Jahre.<sup>82</sup> Zusätzlich besteht die Möglichkeit einer Nacheichung vor Ablauf der Eichgültigkeitsdauer per Stichprobenprüfung. Damit verlängert sich die Eichgültigkeitsdauer um weitere fünf Jahre.<sup>83</sup> Statt einer amtlichen Eichung kann auch eine Eichung durch den Hersteller vorgenommen werden.<sup>84</sup>

### 2.4.3 Standards und Normen

Standards stellen eine Vereinheitlichung eines Verfahrens oder einer Technik dar. Normen sind in einem festgelegtem Normierungsverfahren definierte Standards.<sup>85</sup> Es gibt keinen direkten Zwang zur Unterstützung von Standards, allerdings kann die Verwendung vertraglich festgelegt werden<sup>86</sup> oder Teil von Zulassungsbestimmungen des Gesetzgebers sein.<sup>87</sup>

Unterschiedliche Organisationen sind für die Erarbeitung von Standards verantwortlich. In folgenden sollen einige Standardisierungsgremien, die im Bereich Smart Grid aktiv sind, vorgestellt werden. Global gültige Standards werden vom [Institute of Electrical and Electronics Engineers \(IEEE\)](#), dem weltweiten Berufsverband von Ingenieuren aus den Bereichen Elektrotechnik und Informationstechnik oder durch die [International Electrotechnical Commission \(IEC\)](#) verabschiedet. Auf europäischer Ebene werden Standards durch das Europäische Komitee für Normung ([CEN](#)), das Europäische Komitee für elektrotechnische Normung ([CENELEC](#)) und das [European Telecommunications Standards Institute \(ETSI\)](#) in Form von Europäischen Normen ([EN](#)) ratifiziert. In Deutschland werden Standards bevorzugt vom Deutschen Institut für Normung ([DIN](#)) als Deutsche Industrie Normen verabschiedet. Standards in elektro- und informationstechnischen Bereichen werden durch die [Deutsche Kommission Elektrotechnik Elektronik Informationstechnik \(DKE\)](#), einer Kooperation des [DIN](#) mit dem deutschen Verband der Elektrotechnik Elektronik Informationstechnik ([VDE](#)), bearbeitet. Tabelle 2.2 (siehe nächste Seite) zeigt eine Übersicht einiger für Smart Grids relevanter Standards. Diese beinhaltet die in den USA wichtigen Standards [IEEE 1547](#)<sup>88</sup> und [IEEE 2030](#), die von der [IEC](#) identifizierten Smart Grid Kernstandards<sup>89</sup>, welche teilweise als deutsche bzw. europäische Normen übernommen wurden sowie die innerhalb der [EU](#) relevanten Standards, [DIN EN 13757](#) und [DIN EN 50438](#).<sup>90</sup>

---

<sup>79</sup>Vgl. EnWG 2011 (2011), [181], § 21g.

<sup>80</sup>Vgl. ebd., § 21e.

<sup>81</sup>Vgl. EichG 2011 (2011), [179], § 2.

<sup>82</sup>Anm.: Die Eichgültigkeit mechanischer Elektrizitätszähler beträgt 16 Jahre.

<sup>83</sup>Vgl. Eichordnung, [176], Anhang B, Ordnungsnummer 20.3.

<sup>84</sup>Vgl. EichG 2011 (2011), [179], § 2 (4).

<sup>85</sup>Anm.: Im weiteren Verlauf wird nicht mehr streng zwischen Standards und Normen unterschieden, die beiden Begriffe werden unter dem Begriff Standards zusammengefasst.

<sup>86</sup>Vgl. IHK Würzburg-Schweinfurt - Unterschied Normen und Standards (2011), [124].

<sup>87</sup>Vgl. Barnert u. a.: Der Brockhaus - Computer und Informationstechnologie: Standard (2005), [47], „Standard“.

<sup>88</sup>Vgl. Energy Policy Act of 2005 (2005), [178], S. 377.

<sup>89</sup>Vgl. IEC Smart Grid Standardization Roadmap (2010), [70], S. 108.

<sup>90</sup>Anm.: Für weitere Informationen über Standardisierungsaktivitäten im Bereich Smart Grid siehe: [VDE](#): Die deutsche Normungsroadmap E-Energy / Smart Grid (2010), [93]; Standards for Smart Grids (2011), [63]; IEC Smart Grid Standardization Roadmap (2010), [70]; Uslar u. a.: Untersuchung des Normungsfeldes zum

Standard	Titel	Bereich	Kurzbeschreibung
IEEE 1547	Standard for Interconnecting Distributed Resources with Electric Power Systems	Dezentrale Energieerzeugung	Zusammenschaltung dezentraler Energieressourcen mit Elektrizitätssystemen
IEEE 2030	IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads	Interoperabilität; Referenzarchitektur	Interoperabilität in den Bereichen Elektrotechnik, Kommunikationstechnik und Informationstechnologie; Smart Grid Referenzmodell
IEC 61508 / DIN EN 61508	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme	Funktionale Sicherheit elektronischer Systeme	Sicherheitsanforderungen an industrielle Systeme werden hier definiert; Software Qualitätssicherung
IEC 61850 / DIN EN 61850	Kommunikationsnetze und -systeme in Stationen	Schaltanlagen-Automatisierung	Definiert ein Netzwerkprotokoll für die Leittechnik in elektrischen Schaltanlagen der Mittel- und Hochspannungstechnik
IEC 61968 / DIN EN 61968	Integration von Anwendungen in Anlagen der Elektrizitätsversorgung - Systemschnittstellen für Netzführung	Datenaustausch	Informationsaustausch zwischen Verteilnetzen; Schnittstellendefinition für die Integration von IT-Systemen im Verteilnetzmanagement-Umfeld; Common Information Model Erweiterungen für das Verteilnetzmanagement
IEC 61970 / DIN EN 61970	Schnittstelle für Anwendungsprogramme für Netzführungssysteme (EMS-API)	Datenaustausch	Im Standard wird eine Programmierschnittstelle für Energiemanagementsysteme beschrieben; Common Information Model (Definition von Objekten und Datenaustauschformaten)
IEC 62351	Power systems management and associated information exchange - Data and communications security	IT-Sicherheit	IT-Sicherheit von Netzleitsystemen
IEC TR 62357	Power system control and associated communications - Reference architecture for object models, services and protocols	Referenzarchitektur – elektrischen Energieversorgung	Setzt verschiedene Standards in Kontext zueinander; Seamless Integration Reference Architecture
DIN EN 13757	Kommunikationssysteme für Zähler und deren Fernablesung	LMN; Smart Meter	Fernablesung von Messgeräten mit Hilfe von Kommunikationssystemen (M-Bus, Wireless M-Bus)
DIN EN 50438/ VDE 0435-901: 2008-08	Anforderungen für den Anschluss von Klein-Generatoren an das öffentliche Niederspannungsnetz	Dezentrale Energieerzeugung, Niederspannungs-Verteilnetz	Anschluss von Kleinerzeugern an das öffentliche Niederspannungsnetz

Tabelle 2.2: Übersicht ausgewählter Smart Grid Standards

## 2.5 Realisierungsstand

Der folgende Abschnitt liefert einen Überblick über den Realisierungsstand von Smart Grids. Hauptsächlich wird dabei auf die Verbreitung von Smart Metern eingegangen, da diese sich beim Verbraucher befinden und damit den am deutlichsten sichtbaren Teil des Smart Grids darstellen.

BMW-Förderschwerpunkt „e-Energy - IKT-basiertes Energiesystem der Zukunft“ (2009), [89].

### 2.5.1 International

In den [USA](#) gibt es neben aktuell laufenden Projekten<sup>91</sup> bereits einige Energieversorgungsunternehmen, die ein Smart Grid aufgebaut haben. Austin Energy aus Texas baute das erste Smart Grid in den [USA](#).<sup>92</sup> Dieses als „Smart Grid 1.0“ bezeichnete Netz, bestehend aus einer zentralisierten Stromerzeugung, Transport- und Verteilnetzen sowie Smart Metern, wurde bereits im Oktober 2009 umgesetzt. Für das zukünftige „Smart Grid 2.0“ ist die Erweiterung um verteilte Stromerzeugungsanlagen, Elektrofahrzeuge, Energiespeicher und eine Kommunikation mit dem Smart Home der Kunden geplant. Abgesehen von Austin Energy mit 500.000 ausgelieferten Smart Metern<sup>93</sup> hat Oncor Electric Delivery, ebenfalls aus Texas, zwei Millionen<sup>94</sup> und die Pacific Gas and Electric Company aus Kalifornien bis Dezember 2011 mehr als 8,8 Millionen<sup>95</sup> solcher Geräte bei seinen Kunden installiert.

Im asiatischen Raum hat China bereits mit dem Ausbau seiner Transportnetze begonnen.<sup>96</sup> In den anderen asiatischen Ländern wie beispielsweise Japan gibt es Pläne für zukünftige Smart Grids<sup>97</sup> und bereits gestartete Pilotprojekte.<sup>98</sup> Die Japanische Regierung kooperiert zudem mit der US Regierung in einem Demonstrationsprojekt, das Ende 2012 beginnt und 2015 fertiggestellt sein soll.<sup>99</sup>

In Europa hatte Italien mit dem Enel Telegestore Projekt<sup>100</sup> Ende der neunziger Jahre als eines der ersten Länder damit begonnen eine Smart Metering-Infrastruktur aufzubauen. Bis 2012 sollen 36 Millionen Kunden mit Smart Metern ausgestattet sein.<sup>101</sup> Die Österreichische Energie Agentur veröffentlichte im Februar 2011 im Rahmen des SmartRegions Projekts, ein von der [EU](#) gefördertes Projekt um Smart Metering-Dienstleistungen voranzutreiben, den „European Smart Metering Landscape Report“. In dieser Studie wurde der Stand der Umsetzung bei der Einführung von einer Smart Metering-Infrastruktur inklusive zugehöriger Dienstleistungen sowie die rechtliche und regulatorische Situation in den [EU](#)-Mitgliedsstaaten und Norwegen bewertet. In die Bewertung floss dabei auch ein, ob Energiesparmaßnahmen, z. B. durch die Forderung von lastvariablen Tarifen, unterstützt werden. [Abbildung 2.3](#) zeigt eine grafische Übersicht der Ergebnisse aus der Studie in Form eines Matrixdiagramms.

Die Länder sind dabei in folgende fünf Gruppen eingeteilt:

- dynamisch (dynamic movers): Länder mit einer klaren Planung für den Aufbau einer Smart Metering-Infrastruktur, in denen größere Pilotprojekte bereits laufen oder die über eine große Installationsbasis verfügen.

---

<sup>91</sup>Anm.: Für weitere Informationen siehe „Current Major Projects“ unter [IEEE](#): United States - IEEE Smart Grid, [\[132\]](#).

<sup>92</sup>Vgl. Carvallo und Cooper: The Advanced smart grid (2011), [\[9\]](#), S. 84.

<sup>93</sup>Vgl. [ebd.](#), S. 35-38; Austin Energy Smart Grid Program, [\[96\]](#).

<sup>94</sup>Vgl. Cuellar: Oncor Installs Two Millionth Advanced Meter (2011), [\[102\]](#).

<sup>95</sup>Vgl. Pacific Gas and Electric Company - SmartMeter Installation Progress, [\[117\]](#).

<sup>96</sup>Vgl. Li: From Strong to Smart (2009), [\[76\]](#); [IEEE](#): China - IEEE Smart Grid, [\[130\]](#).

<sup>97</sup>Vgl. Rehn: Viel Bewegung bei neuen Stromnetzen in Japan (2011), [\[81\]](#); METI Japan (2010), [\[94\]](#).

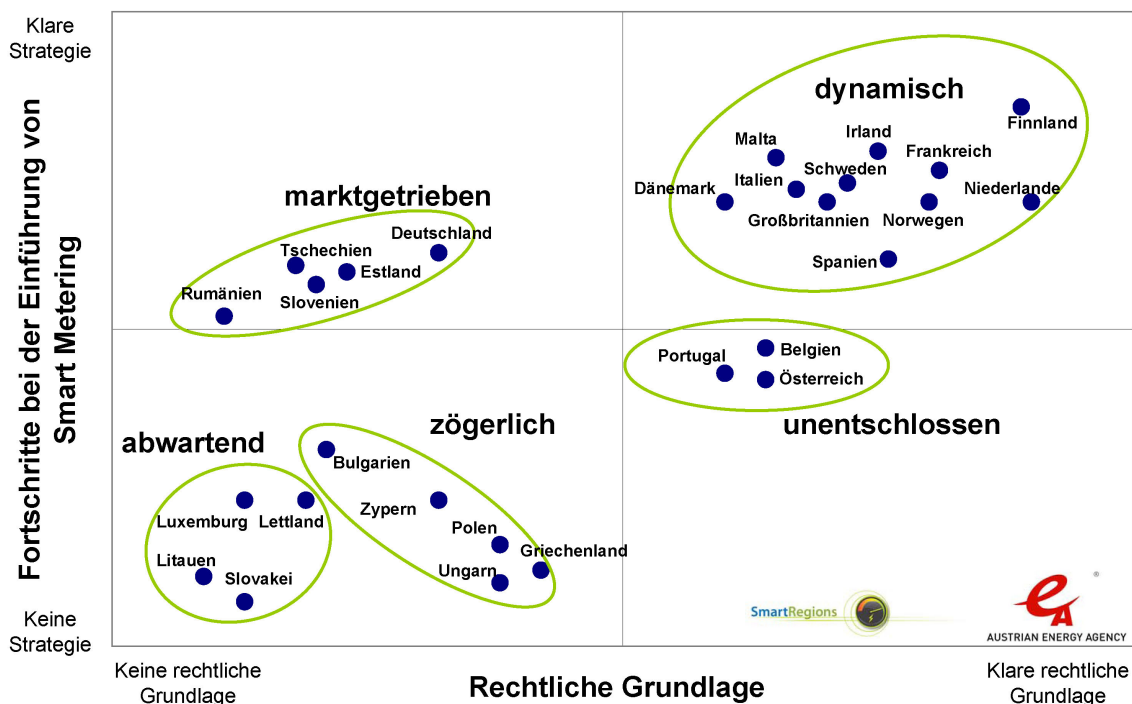
<sup>98</sup>Vgl. Tokio Electric Power Company: CSR at the TEPCO Group (2010), [\[88\]](#), S. 3.

<sup>99</sup>Vgl. Japan-U.S. Smart Grid Demonstration Project, [\[107\]](#).

<sup>100</sup>Vgl. Rogai: ENEL's Metering System and Telegestore Project (2006), [\[84\]](#).

<sup>101</sup>Vgl. Annual Report on the Progress in Smart Metering 2009 (2010), [\[44\]](#), S. 12.

<sup>102</sup>Quelle: Österreichische Energieagentur: Smart Metering Landscape Report, [\[133\]](#).

Abbildung 2.3: Smart Metering in der EU<sup>102</sup>

- marktgetrieben (market drivers): Die Gruppe der marktgetriebenen Länder umfasst jene, die bereits Projekte zur Einführung von Smart Metern gestartet haben, auch wenn die rechtlichen Rahmenbedingungen noch nicht abschließend geklärt sind.
- unentschlossen (ambiguous movers): Österreich, Belgien und Portugal weisen zwar Bestrebungen zum Aufbau in Form von Projekten einzelner Netzbetreiber auf, die rechtlichen Anforderungen sind allerdings noch nicht genau definiert.
- zögerlich (waverers) und abwartend (laggards): Zu den beiden Gruppen zählen Länder in denen Smart Metering bisher kaum ein Rolle spielt.<sup>103</sup>

Italien und Niederlande befinden sich in der Gruppe der „dynamischen“ Länder, da hier der Smart Meter Rollout bereits fast abgeschlossen ist und die rechtlichen Grundlagen vorliegen. Niederlande sind in der Matrix weiter rechts einsortiert als Italien, da Energiesparmaßnahmen in ihren rechtlichen Grundlagen stärker berücksichtigt werden.<sup>104</sup> Deutschland befindet sich dagegen in der Gruppe der marktgetriebenen Ländern. Seit Veröffentlichung der Studie haben sich die rechtlichen Grundlagen, vor allem durch umfangreiche Änderungen im EnWG (siehe Abschnitt 2.4.2), verändert. Aus diesem Grund wäre Deutschland bei aktueller Betrachtung wahrscheinlich eher im Bereich zwischen dynamisch und unentschlossen innerhalb der Matrix einsortiert worden.

<sup>103</sup> Anm.: Die im European Smart Metering Landscape Report verwendeten Bezeichnungen sind in Klammern dargestellt.

<sup>104</sup> Vgl. Renner u. a.: European Landscape Report (2011), [82], S. 1-7; Österreichische Energieagentur: Smart Metering Landscape Report, [133].

### 2.5.2 National

In Deutschland ist die Umsetzung eines Smart Grid bisher vor allem im Leuchtturmprojekt E-Energy erfolgt. Es wurde vom [Bundesministerium für Wirtschaft und Technologie \(BMWi\)](#) in Kooperation mit dem Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) in Form eines Forschungs- und Entwicklungs-Förderprogramm initiiert.<sup>105</sup> In den sechs Modellregionen Baden-Württemberg, Rhein-Neckar, Aachen, Rhein-Ruhr, Harz sowie Cuxhaven werden Beispiellösungen für Smart Grids entwickelt. Mehr als 5.000 Testteilnehmern erproben diese Beispiellösungen bis Ende 2012.<sup>106</sup> Neben dem Leuchtturmprojekt haben einige Elektrizitätsversorgungsunternehmen (EUV) in Rahmen von Pilotprojekten damit begonnen ihre Kunden mit intelligenten Messsystemen auszustatten. Zum Beispiel hat die Vattenfall AG in Berlin<sup>107</sup> und die E.ON Bayern AG<sup>108</sup> jeweils 10.000 Haushalte mit Smart Metern ausgestattet. In einem größeren Pilotprojekt der RWE AG erschloss man 100.000 Mühlheimer Haushalte.<sup>109</sup> Abgesehen von den meist regionalen Pilotprojekten werden Smart Meter auch bundesweit z. B. von der Yello Strom GmbH<sup>110</sup> oder von der Discovery GmbH<sup>111</sup>, die beide als Messstellenbetreiber auftreten, angeboten. Abbildung 2.4 zeigt eine Übersicht über abgeschlossene und laufende Smart Metering Projekte innerhalb Deutschlands.

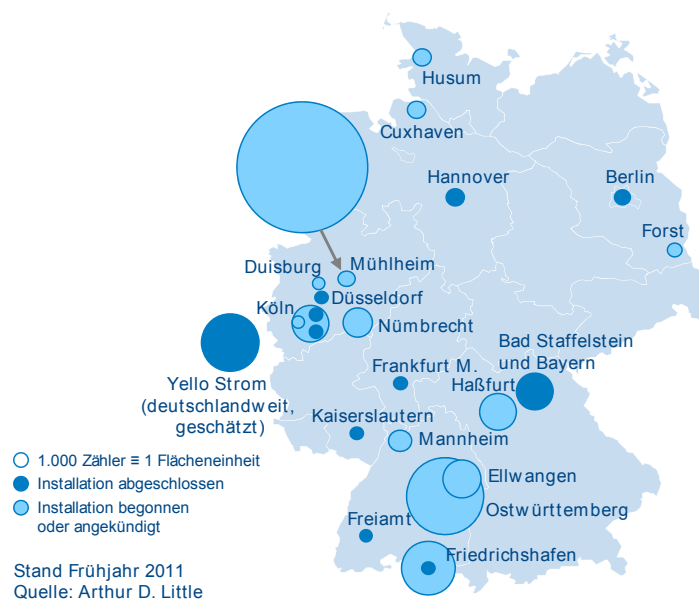


Abbildung 2.4: Übersicht Smart Metering Projekte in Deutschland<sup>112</sup>

<sup>105</sup>Vgl. Picot und Neumann: E-Energy (2009), [33], S. 2-9.

<sup>106</sup>Vgl. [BMWi](#), Referat Öffentlichkeitsarbeit: Brüderle eröffnet zweiten E-Energy Jahreskongress (2011), [98].

<sup>107</sup>Vgl. Märkisches Viertel - Vattenfall (2011), [113].

<sup>108</sup>Vgl. E.ON Energie - Der Stromzähler wird intelligent (2010), [105].

<sup>109</sup>Vgl. RWE - Mühlheim zählt, [115].

<sup>110</sup>Vgl. Heringhaus: Yello startet national den Wettbewerb bei intelligenten Stromzählern. (2008), [68].

<sup>111</sup>Vgl. Discovery GmbH: Energiekosten dauerhaft senken (2010), [58].

<sup>112</sup>Quelle: Arthur D. Little: Smart Metering vor dem Durchbruch (2011), [46], S. 2.



## 3 Sicherheit und Datenschutz

### 3.1 Sicherheitsarten

Unter dem Begriff „Sicherheit“ wird ein Zustand verstanden, der gefahrenfrei bzw. risikofrei ist.<sup>113</sup> Der Begriff ist im deutschen Sprachgebrauch etwas unklar definiert. In ihm werden die beiden englischen Begriffe „safety“ (dt. Funktionssicherheit) für den Schutz vor ungeplanten Ereignissen und „security“ (dt. Informationssicherheit) für den Schutz vor geplanten Angriffen zusammengefasst beschrieben.<sup>114</sup>

Die Funktionssicherheit, die auch als Betriebssicherheit bezeichnet wird, beschreibt die Eigenschaft eines Systems, die gegeben ist, wenn die Funktionsweise eines Systems der erwarteten bzw. festgelegten Funktionsweise entspricht. Ein funktionssicheres System befindet sich in einem Zustand in dem von ihm keine Gefahren für das System selbst oder dessen Umwelt ausgehen.<sup>115</sup>

Zunächst sollen in Abbildung 3.1 die Zusammenhänge der Begriffe dargestellt werden, bevor auf die Informationssicherheit im nächsten Abschnitt eingegangen wird.

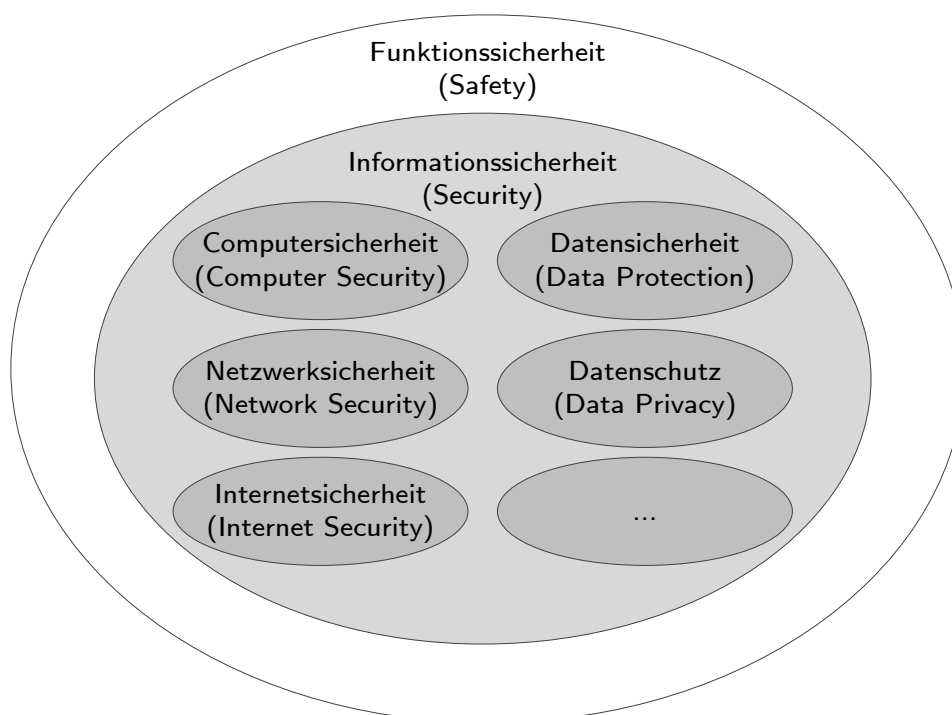


Abbildung 3.1: Aspekte der Sicherheit<sup>116</sup>

<sup>113</sup>Vgl. Schmidt: Der IT Security Manager (2006), [38], S. 14.

<sup>114</sup>Vgl. Beenken: Schutz sicherheitsrelevanter Informationen in verteilten Energieinformationssystemen (2010), [5], S. 7f; Schneider und Werner: Taschenbuch der Informatik (2007), [39], S. 488.

<sup>115</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 6; Pohl: Taxonomie und Modellbildung in der Informationssicherheit (2004), [34], S. 678f.

<sup>116</sup>Angelehnt an ebd., S. 679; Beenken: Schutz sicherheitsrelevanter Informationen in verteilten Energieinformationssystemen (2010), [5], S. 8; Anm.: ... = nicht dargestellte weitere Aspekte.



### 3.1.1 Informationssicherheit

„Die Informationssicherheit (engl. security) ist die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen.“<sup>117</sup>

Folgende weitere Begriffe lassen sich der Informationssicherheit unterordnen (siehe [Abb. 3.1](#)):

- Computersicherheit (engl. computer security): Sicherheit von Informationen auf Computersystemen.
- Netzwerksicherheit (engl. network security): Schutz von Informationen, die zwischen IT-Systemen über ein Netzwerk ausgetauscht werden; Schutz vor unautorisiertem Netzwerkzugang.
- Internetsicherheit (engl. internet security): Netzwerksicherheit bezogen auf das Internet; Schutz von Informationen, die zwischen IT-Systemen über das Internet ausgetauscht werden.<sup>118</sup>
- Datensicherheit (engl. data protection): Schutz vor nicht autorisiertem Zugriff auf Daten und Systemressourcen; Schutz von Daten gegen Beschädigung.<sup>119,120</sup>
- Datenschutz (engl. data privacy): Schutz von personenbezogener Daten vor Missbrauch.<sup>121</sup>

### 3.1.2 Datenschutz

Informationen, die sich auf natürliche Personen beziehen, sind personenbezogene Daten. Sie fallen unter einen besonderen Schutz. Der Datenschutz kümmert sich um den Schutz vor Missbrauch dieser personenbezogenen Daten.

Rechtliche Grundlage für den Datenschutz ist in Deutschland das [Bundesdatenschutzgesetz \(BDSG\)](#). Zusammen mit dem Recht auf informationelle Selbstbestimmung<sup>122</sup>, als Datenschutz-Grundrecht, erhält eine natürliche Person das Recht über die eigenen Daten selbst zu verfügen. Somit kann diese den Zugriff und die Weitergabe kontrollieren.<sup>123</sup> Auf europäischer Ebene ist der Datenschutz in Artikel 8 der [EU-Grundrechtecharta](#) geregelt.<sup>124</sup> In der [EU-Datenschutzrichtlinie](#)<sup>125</sup> und deren Erweiterung in Form der [EU-Datenschutzrichtlinie für](#)

<sup>117</sup>Eckert: IT-Sicherheit (2012), [12], S. 6.

<sup>118</sup>Vgl. Schmitz: Security in IT-Systemen: Grundlagen (2010), [86], S. 2.

<sup>119</sup>Vgl. Beenken: Schutz sicherheitsrelevanter Informationen in verteilten Energieinformationssystemen (2010), [5], S. 152.

<sup>120</sup>Anm.: Das [BSI](#) sieht Datensicherheit als Synonym für Informationssicherheit; Vgl. [BSI](#): IT-Grundschutz-Kataloge: 12. EL Stand 2011 (2011), [91], S. 41

<sup>121</sup>Vgl. Beenken: Schutz sicherheitsrelevanter Informationen in verteilten Energieinformationssystemen (2010), [5], S.7f.

<sup>122</sup>Vgl. Bundesverfassungsgericht: Volkszählungsurteil (1983), [174], Anm.: Das Recht auf informationelle Selbstbestimmung wird im Grundgesetz nicht explizit erwähnt. Es wurde vom Bundesverfassungsgericht im Rahmen des Volkszählungsurteils von 1983 als Grundrecht anerkannt.

<sup>123</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 6.

<sup>124</sup>Vgl. Charta der Grundrechte der Europäischen Union (2007/C 303/01) (2007), [175].

<sup>125</sup>Siehe [EU-Datenschutzrichtlinie 95/46/EG](#) (1996), [186].

elektronische Kommunikation werden darüber hinaus Datenschutzmindeststandards beschrieben.<sup>126</sup>

Unternehmen die Daten erheben, nutzen und speichern, müssen gemäß § 9 BDSG technische und organisatorische Maßnahmen treffen. Diese sollen gewährleisten, dass nur der berechtigte Personenkreis Zugriff auf die Daten erhält. In der Anlage zu § 9 werden dabei für die automatisierte Verarbeitung von personenbezogenen Daten folgende Maßnahmen genannt: Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle, Einsatz von Verschlüsselungsverfahren, die dem Stand der Technik entsprechen und die getrennte Verarbeitung von Daten, die zu unterschiedlichem Zweck erhoben wurden.<sup>127</sup>

Wesentliche Grundsätze des Datenschutzes, die auch im BDSG verankert sind, finden sich in folgenden Prinzipien wieder:

- Datenvermeidung bzw. Datensparsamkeit: Nach diesem Prinzip sollen möglichst wenig Daten erhoben, verarbeitet und genutzt werden.<sup>128</sup>
- Zweckbindung: Personenbezogene Daten sollen nur für die Zwecke verarbeitet werden, in deren Rahmen sie erhoben wurden.<sup>129</sup>
- Erforderlichkeit: Es dürfen nur Daten erhoben werden, wenn sie zur Erfüllung eines Zwecks erforderlich sind.<sup>130</sup>
- Transparenz: Die betroffene Person soll in Kenntnis darüber gesetzt werden, wenn Daten über sie erhoben werden.<sup>131</sup>

Als Maßnahmen zur Unterstützung des Datenschutzes gibt es die Anonymisierung und die Pseudonymisierung von Daten. Bei der Anonymisierung werden personenbezogenen Daten so verändert, dass diese nicht mehr bzw. nur mit großem Aufwand einer Person zugeordnet werden können. Dabei werden identifizierende Merkmale wie z. B. der Name, das Geburtsdatum oder die Adresse einer Person innerhalb der personenbezogenen Daten entfernt. Als abgeschwächte Form der Anonymisierung werden bei der Pseudonymisierung identifizierende Merkmale nicht entfernt, sondern an Hand einer Vorschrift ersetzt. Die personenbezogenen Daten werden z. B. durch eine Zahl ersetzt. Ohne Kenntnis dieser wird eine Zuordnung der Daten zu einer Person erschwert.<sup>132</sup>

Die Erfassung von Verbrauchsdaten in zeitlich kurzen Abständen mit Hilfe von Smart Metern und deren Auswertung im Vergleich zur bislang üblichen jährlichen Ablesung ermöglicht eine Profilbildung über das Verhalten, welche die Privatsphäre eines Menschen bedroht. So lassen sich detaillierte Rückschlüsse über Tagesabläufe und Gewohnheiten der Personen eines Haushalts ziehen. Es lässt sich z. B. feststellen, ob und zu welcher Uhrzeit sich eine Person zu Hause

---

<sup>126</sup>Vgl. EU-Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (2002), [184].

<sup>127</sup>Siehe BDSG (2009), [173], Anlage (zu § 9 Satz 1).

<sup>128</sup>Vgl. ebd., § 3a.

<sup>129</sup>Vgl. ebd., § 28, § 31.

<sup>130</sup>Vgl. ebd., § 28.

<sup>131</sup>Vgl. ebd., § 4.

<sup>132</sup>Vgl. ebd., § 3.

aufhält, wann die Personen eines Haushalts schlafen gehen oder auch der Zeitpunkt zu dem üblicherweise Essen im Haushalt zubereitet wird. Ebenso lassen sich einzelne Geräte feststellen. Mit Daten höherer Auflösung (z. B. eine Messung pro Sekunde) lassen sich noch genauere Aussagen treffen.<sup>133</sup> Laut den Ergebnissen von Forschern der Fachhochschule Münster lässt sich durch Auswertung des Lastprofils sogar feststellen, welcher Film bzw. welches Fernsehprogramm konsumiert wurde.<sup>134</sup> Hieraus ergeben sich Anforderungen an Datenschutz und Datensicherheit. Für eine umfassende datenschutzrechtliche Untersuchung von Smart Grids soll an dieser Stelle auf die Literatur verwiesen.<sup>135</sup>

## 3.2 Schutzziele

„Ein Schutzziel ist eine von einer allgemeinen Sicherheitsanforderung geforderte konkretisierte Sicherheitseigenschaft.“<sup>136</sup>

In der Literatur finden sich unterschiedliche Schutzziele. Zunächst werden hier folgende drei grundlegende Schutzziele unterschieden, die im Bezug auf das Smart Grid erläutert werden:

- **Vertraulichkeit** (engl. confidentiality): Der Schutz vor unberechtigter Einsicht von Informationen wird als Vertraulichkeit bezeichnet. Im Smart Grid sollten Lastprofile vor unberechtigter Kenntnisnahme geschützt werden. Denn Lastprofile, welche auf der Grundlage von kurzen Messintervallen erstellt werden, können detaillierte Rückschlüsse auf den Tagesablauf der Nutzer ermöglichen (siehe 3.1.2).
- **Integrität** (engl. integrity): Sie ermöglicht die Erkennung und Feststellung von unautorisierter, unbemerkter Veränderung von Informationen. Für den Energieversorger ist die Integrität insbesondere im Hinblick auf die gemessenen Verbrauchsdaten wichtig, da sie die Grundlage für die Rechnungsstellung bilden.
- **Verfügbarkeit** (engl. availability): Die Verfügbarkeit stellt sicher, dass Systemressourcen oder Dienste korrekt funktionieren und nutzbar sind. Sind die unterschiedlichen Komponenten des Smart Grid nicht verfügbar, hat dies verschiedene Auswirkungen. Bei Nicht-Verfügbarkeit der Stromversorgung können elektrische Geräte nicht mehr benutzt werden. Fallen die Kommunikationsverbindungen aus, ist die Steuerung der Komponenten nicht mehr möglich.

Sie werden oft als CIA bezeichnet, welches ein Akronym ist, das sich aus den Begriffen **confidentiality**, **integrity** und **availability** ableitet.

<sup>133</sup>Vgl. Quinn: Smart Metering and Privacy (2009), [80], S. 1-11; Müller: Gewinnung von Verhaltensprofilen am intelligenten Stromzähler (2010), [29]; Molina-Markham u. a.: Smart Metering and Privacy (2010), [78].

<sup>134</sup>Vgl. Greveler, Justus und Löhr: Multimedia Content Identification Through Smart Meter Power Usage Profiles (2012), [67]; Greveler, Justus und Löhr: Hintergrund und experimentelle Ergebnisse zum Thema „Smart Meter und Datenschutz“ (2011), [66].

<sup>135</sup>Siehe Raabe u. a.: Datenschutz in Smart Grids (2011), [35]; Karg: Datenschutzrechtliche Bewertung des Einsatzes von „intelligenten“ Messeinrichtungen für die Messung von gelieferter Energie (Smart Meter) (2009), [71].

<sup>136</sup>Beenen: Schutz sicherheitsrelevanter Informationen in verteilten Energieinformationssystemen (2010), [5], S. 11.

In der Literatur werden weitere Schutzziele und verwandte Begriffe, die im Zusammenhang mit diesen stehen genannt. Je nach Anwendungsgebiet können sie auch als Schutzziel aufgefasst werden. Beispielhaft werden hier folgende erwähnt:

- Verbindlichkeit bzw. Nichtabstreitbarkeit (engl. non-repudiation): Die Verbindlichkeit stellt sicher, dass die Durchführung getätigter Aktionen bewiesen und nicht nachträglich abgestritten werden kann.
- Authentizität (engl. authenticity): Sie garantiert die Echtheit von Informationen oder einer Identität.
- Authentifikation (engl. authentication): Sie sichert die Echtheit und Glaubwürdigkeit einer Nachricht oder die Identität von Personen durch Verifikation ab, sodass diese überprüfbar wird.
- Autorisierung (engl. authorization): Zuweisung und Vergabe von Rechten, nachdem die Authentifikation stattgefunden hat.
- Zugangskontrolle (engl. access control): Kontrolliert mit Hilfe eines Mechanismus den Zugang zu Ressourcen und ermöglicht deren Nutzung für autorisierte Nutzer.
- Zurechenbarkeit (engl. accountability): Ausgeführte Aktionen oder Informationen können dem Auslöser, also einer Person bzw. einem System zugerechnet werden.<sup>137</sup>

### 3.3 Schutzmaßnahmen

Eine Schutzmaßnahme ist eine Maßnahme, die zur Gewährleistung der Schutzziele beiträgt. Dabei kann es sich um organisatorische oder technische Maßnahmen handeln. Organisatorische Maßnahmen umfassen z. B. die Überprüfung von Zuständigkeiten und Berechtigungen oder die Durchführung von Audits.

Für verschiedene technische Maßnahmen wie beispielsweise die Verschlüsselung oder die elektronische Signatur wird auf Algorithmen aus dem Bereich der Kryptologie zurückgegriffen. Die eingesetzten Verschlüsselungsverfahren lassen sich in symmetrische und asymmetrische Verfahren unterscheiden. Die symmetrischen Verfahren setzen für Verschlüsselung und Entschlüsselung den selben Schlüssel ein, wohingegen die asymmetrischen Verfahren jeweils unterschiedliche Schlüssel einsetzen. Tabelle 3.1 gibt einen Überblick über einige ausgewählte, allgemeine technische Schutzmaßnahmen und die damit adressierten Schutzziele.<sup>138</sup>

---

<sup>137</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 5-13; Beenken: Schutz sicherheitsrelevanter Informationen in verteilten Energieinformationssystemen (2010), [5], S. 11f.

<sup>138</sup>Vgl. ebd., S. 12f; Anm.: Für detaillierte Beschreibungen zu den verschiedenen hier genannten Maßnahmen siehe Eckert: IT-Sicherheit (2012), [12].

<b>Schutzmaßnahme</b>	<b>Realisierung</b>	<b>Schutzziel</b>
Verschlüsselung	Transformiert eine Information mit Hilfe eines Verfahrens in eine nicht bzw. schwer interpretierbare Information.	Vertraulichkeit
Prüfwert	Digitaler Fingerabdruck eines Datenobjektes.	Integrität
Zertifikat	Digitale Bescheinigung; bescheinigt die Zuordnung eines öffentlichen Schlüssels (engl. public key) zu einer Person.	Authentizität
Elektronische Signatur	Digitale Unterschrift als Gegenstück zur handschriftlichen Unterschrift.	Authentizität, Verbindlichkeit
Redundanz	Vorhalten technischer Ressourcen in mehrfacher Ausführung.	Verfügbarkeit

Tabelle 3.1: Übersicht Schutzmaßnahmen<sup>139</sup>

### 3.4 Bewertungskriterien von Sicherheit

#### 3.4.1 Common Criteria

Die „Common Criteria for Information Technology Security Evaluation“<sup>140</sup> (dt. „Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“<sup>141</sup>) bzw. **Common Criteria (CC)** haben sich als internationaler Standard zur Bewertung der Sicherheit von Produkten bzw. Systemen der Informationstechnik herausgebildet. Sie wurden im Jahr 1999 als **ISO/IEC Standard 15408** anerkannt und zuletzt im Jahr 2009 aktualisiert. Für eine Zertifizierung nach **CC** stehen verschiedene Evaluierungsstufen (**EAL**, engl. Evaluation Assurance Level; **EAL 1** bis **EAL 7**) mit ansteigendem Umfang und ansteigender Prüftiefe bereit. Die Zertifizierung bezieht sich zunächst auf einen Evaluierungsgegenstand (**EVG**, engl. Target of Evaluation) der ggf. nur einen kleinen Teil eines gesamten Produktes ausmacht. Sie bescheinigt, dass der **EVG** der zertifizierten Sicherheitsspezifikation entspricht. Mit der Einschränkung auf den **EVG** können CC-Zertifikate somit sehr spezifisch sein.

#### 3.4.2 Schutzprofil

Aus diesem Grund wurde das Konzept der Schutzprofile (**PP**; engl. protection profile) in den **CC** verankert. **Schutzprofile** ermöglichen es unterschiedliche Produkte derselben Kategorie hinsichtlich ihrer Sicherheitseigenschaften miteinander zu vergleichen. Diese werden unabhängig von einer Implementierung festgelegt.<sup>142</sup>

<sup>139</sup>Angelehnt an: Beenken: Schutz sicherheitsrelevanter Informationen in verteilten Energieinformationssystemen (2010), [5], S. 12f.

<sup>140</sup>**Anm.:** Für weitere Informationen zu den Common Criteria siehe <http://www.commoncriteriaportal.org/>.

<sup>141</sup>**BSI:** BSI: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (2011), [126].

<sup>142</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 240-250; Fox: Schutzprofile - Protection Profiles (2011), [16].

Anfang 2011 wurde vom [BSI](#) in Zusammenarbeit mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ([BfDI](#)), der Physikalisch-Technischen Bundesanstalt ([PTB](#)) und der [BNetzA](#) ein Entwurf zum „[Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen](#)“ ([Gateway PP](#), engl. Protection Profile for the Gateway of a Smart Metering System) erarbeitet. Seit 26. August 2011 wird es evaluiert.<sup>143</sup> Das im [Gateway PP](#) behandelte [Smart Meter Gateway](#) empfängt, speichert die Messdaten und sendet sie aufbereitet an Marktteilnehmer. Gleichzeitig übernimmt es Filteraufgaben, ähnlich einer Firewall<sup>144</sup> und trennt die einzelnen angeschlossenen Netze [HAN](#), [LMN](#) und [WAN](#) (siehe Abschnitt [2.3.2](#)) voneinander. Neben der Übertragung von Messwerten werden auch Administrations- und Konfigurationsinformationen ausgetauscht. Zu diesen gehören z. B. Tarifinformationen, [SM-GW](#) Softwareupdates und Berechtigungsprofile, in denen hinterlegt ist, welche Aktionen durchgeführt werden dürfen. Zusätzlich bietet das [SM-GW](#) einen Wake-Up-Service über den mit Hilfe eines speziellen Datenpakets eine Verbindung nach außen zum Messstellenbetreiber angetriggert werden kann. Folgende weitere Funktionalitäten sollen vom [SM-GW](#) bereitgestellt werden:

- **Protokollierung:** Protokollierung von eichtechnisch relevanten Ereignissen (z. B. Fehler bei der Zeitsynchronisierung), wichtigen Events (z. B. Ausfall der WAN-Verbindung) oder Transaktionen (z. B. übertragene Informationen).
- **Nutzerverwaltung:** Verwaltung unterschiedlicher Anschlussnutzer, wenn ein [SM-GW](#) Messwerte von Smart Metern unterschiedlicher Anschlussnutzer, wie es in einem Mehrfamilienhaus der Fall ist, erfasst und speichert.
- **Pseudonymisierung** (siehe Abschnitt [3.1.2](#)): Die Zähleridentifikationsnummer in jedem Verbrauchsdatensatz wird vor Versendung durch ein Pseudonym ersetzt.
- **Zeitdienst:** Gültige und vertrauenswürdige Uhrzeit, die sich mit einer externen Zeitquelle synchronisiert.
- **kryptographische Funktionen:** Schlüsselerzeugung, Verschlüsselung bzw. Entschlüsselung von Daten sowie die Erzeugung und Prüfung von elektronischen Signaturen. Diese werden durch ein separates Sicherheitsmodul bereitgestellt (siehe weiter unten).<sup>145</sup>

Um die vom [Smart Meter Gateway](#) ausgehende Kommunikation hinsichtlich Authentizität, Integrität, und Vertraulichkeit (siehe Abschnitt [3.2](#)) abzusichern, wird ein Sicherheitsmodul eingesetzt. Dessen Anforderungen sind im „[Schutzprofil für das Sicherheitsmodul eines intelligenten Messsystems](#)“ ([Security Module PP](#), engl. Protection Profile for the Security Module of a Smart Metering System) festgelegt.

---

<sup>143</sup>Vgl. [BSI: BSI: Schutzprofil für Smart Meter](#) (2011), [\[127\]](#).

<sup>144</sup>**Anm.:** Kontrolliert und filtert Datenverkehr nach bestimmten Kriterien (Firewall-Regeln).

<sup>145</sup>Vgl. [BSI: BSI TR-03109](#) (2011), [\[164\]](#), S. 13-20.

Das Sicherheitsmodul übernimmt dabei folgende Aufgaben:

- Schlüsselgenerierung
- Schlüsselaushandlung
- Schlüsselspeicherung
- Signaturerstellung und Signaturprüfung
- Zufallzahlengenerierung<sup>146</sup>

Später sollen Schutzprofile für das Smart Meter und für ein dazugehöriges Sicherheitsmodul folgen.<sup>147</sup> Zusätzlich zu den Schutzprofilen erarbeitet das BSI die Technische Richtlinie „Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems“ (BSI TR-03109). In dieser werden die in den Schutzprofilen getroffenen Sicherheitsanforderungen weiter ausgestaltet. Darüber hinaus werden funktionale Vorgaben festgelegt, um Interoperabilität zwischen den unterschiedlichen Komponenten innerhalb eines Smart Metering Systems zu gewährleisten.<sup>148</sup>

### 3.5 Risiko

Der Risikobegriff kann je nach Anwendungsgebiet unterschiedlich aufgefasst werden.<sup>149</sup> In der vorliegenden Arbeit werden Risiken bezogen auf Bedrohungen (siehe 3.6.2) definiert. Das Risiko einer Bedrohung ist die Wahrscheinlichkeit bzw. die Häufigkeit mit der ein Schadensereignis eintritt, unter Berücksichtigung der Schadenshöhe bzw. des Schadensausmaßes.<sup>150</sup>

Das Risiko  $R$  lässt sich nach folgender Formel berechnen:

$$R = P_E * S_E \text{ bzw. } R = H_E * S_E \quad (3.1)$$

Dabei beschreibt  $P_E$  die Eintrittswahrscheinlichkeit,  $H_E$  die Eintrittshäufigkeit und  $S_E$  die Schadenshöhe. Der Wertebereich für  $P_E$  und  $H_E$  liegt dabei zwischen 0 und 1. Im Fall von  $S_E$  entspricht er dem finanziellen Schaden. Für diese Werte wird auf statistische Erfahrungswerte, wie sie Versicherungen über Schadensereignisse z. B. Naturkatastrophen führen, zurückgegriffen. Im Bereich der Informationstechnik bzw. für das Smart Grid gibt es solche Erfahrungswerte entweder nicht oder sie sind dem Autor dieser Arbeit nicht zugänglich. Aus diesem Grund erfolgt eine qualitative Abschätzung der Eintrittswahrscheinlichkeit in einzelne Klassen. Für die Abschätzung des Schadensausmaßes wird ebenso verfahren. Die Einstufung der Eintrittswahrscheinlichkeit erfolgt dabei in die Klassen niedrig, mittel, hoch und sehr hoch (siehe Tabelle 3.2). In die

<sup>146</sup>Vgl. BSI: BSI: Schutzprofil für das Sicherheitsmodul eines intelligenten Messsystems (2011), [128].

<sup>147</sup>Vgl. Müller: Verordnete Sicherheit - das Schutzprofil für das Smart Metering Gateway (2011), [30], S. 549.

<sup>148</sup>Vgl. Laupichler u. a.: Das BSI-Schutzprofil: Anforderungen an den Datenschutz und die Datensicherheit für Smart Metering Systeme (2011), [27], S. 545f; Anm.: Für weitere Informationen siehe BSI: BSI TR-03109 (2011), [129].

<sup>149</sup>Vgl. Königs: IT-Risiko-Management mit System (2009), [23], S. 9; Schmidt: Der IT Security Manager (2006), [38], S. 9-12.

<sup>150</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 18.

Eintrittswahrscheinlichkeit wird neben einer Abschätzung der Häufigkeit des Eintritts eines Ereignisses, auch der Nutzen des Angriffs und der vom Angreifer benötigte Aufwand für eine erfolgreiche Durchführung eines Angriffs mit einbezogen.<sup>151</sup> Denn ein Angriff, der mit geringerem Aufwand durchführbar ist und einen hohen Nutzen verspricht, ist verglichen mit einem aufwendigeren Angriff bei niedrigerem Nutzen, als wahrscheinlicher anzusehen.

Klasse	Beschreibung
niedrig	Es ist sehr unwahrscheinlich, dass das Ereignis eintritt. Der Aufwand für einen erfolgreichen Angriff ist höher als der Nutzen für den Angreifer.
mittel	Es ist unwahrscheinlich, dass das Ereignis eintritt. Der Aufwand für einen erfolgreichen Angriff und der Nutzen für den Angreifer weisen die selbe Größenordnung auf.
hoch	Es ist wahrscheinlich, dass das Ereignis eintritt. Der Aufwand für einen erfolgreichen Angriff ist geringer als der Nutzen für den Angreifer.
sehr hoch	Es ist sehr wahrscheinlich, dass das Ereignis eintritt. Für einen erfolgreichen Angriff ist ein niedriger Aufwand bei sehr hohem Nutzen erforderlich.

Tabelle 3.2: Übersicht Eintrittswahrscheinlichkeit<sup>152</sup>

Bei der Abschätzung des Schadensausmaßes werden die Auswirkungen eines Schadens berücksichtigt. Die Einstufung erfolgt dabei in die Klassen unwesentlich, geringfügig, kritisch und katastrophal (siehe Tabelle 3.3).

Klasse	Beschreibung
unwesentlich	Die Auswirkung des Schadens ist tragbar. Schäden dieser Kategorie haben keine oder nur geringe Auswirkungen.
geringfügig	Die Auswirkung des Schadens ist absehbar. Schäden dieser Kategorie haben überschaubare Auswirkungen.
kritisch	Die Auswirkung des Schadens ist enorm. Schäden dieser Kategorie haben erhebliche Konsequenzen in verschiedenen Bereichen.
katastrophal	Die Auswirkung des Schadens ist untragbar. Schäden dieser Kategorie haben starke Auswirkungen. Es können Menschenleben gefährdet werden.

Tabelle 3.3: Übersicht Schadensausmaß<sup>153</sup>

<sup>151</sup>Vgl. Charzinski: IT Sec 01 Intro (2011), [55], S. 20.

<sup>152</sup>Anm.: Eigene Einstufung der Klassen.

<sup>153</sup>Anm.: Kategorien nach DIN EN 60601-1-4 (2001), [138]



Im Rahmen einer Risikoanalyse werden Risiken identifiziert, analysiert und anschließend bewertet.<sup>154</sup> Als Hilfsmittel zur Einschätzung von Risiken wird dabei häufig eine zweidimensionale Risiko-Karte (engl. Risk-Map), auch Risikomatrix oder Risikograph genannt, eingesetzt. In ihr können mehrere Risiken übersichtlich dargestellt werden.<sup>155</sup>

Abbildung 3.2 zeigt eine solche Risiko-Karte, ohne eingetragene Bedrohungen, wie sie für die Risikoanalysen in den Abschnitten 4.2.3 und 4.3.2 verwendet werden.

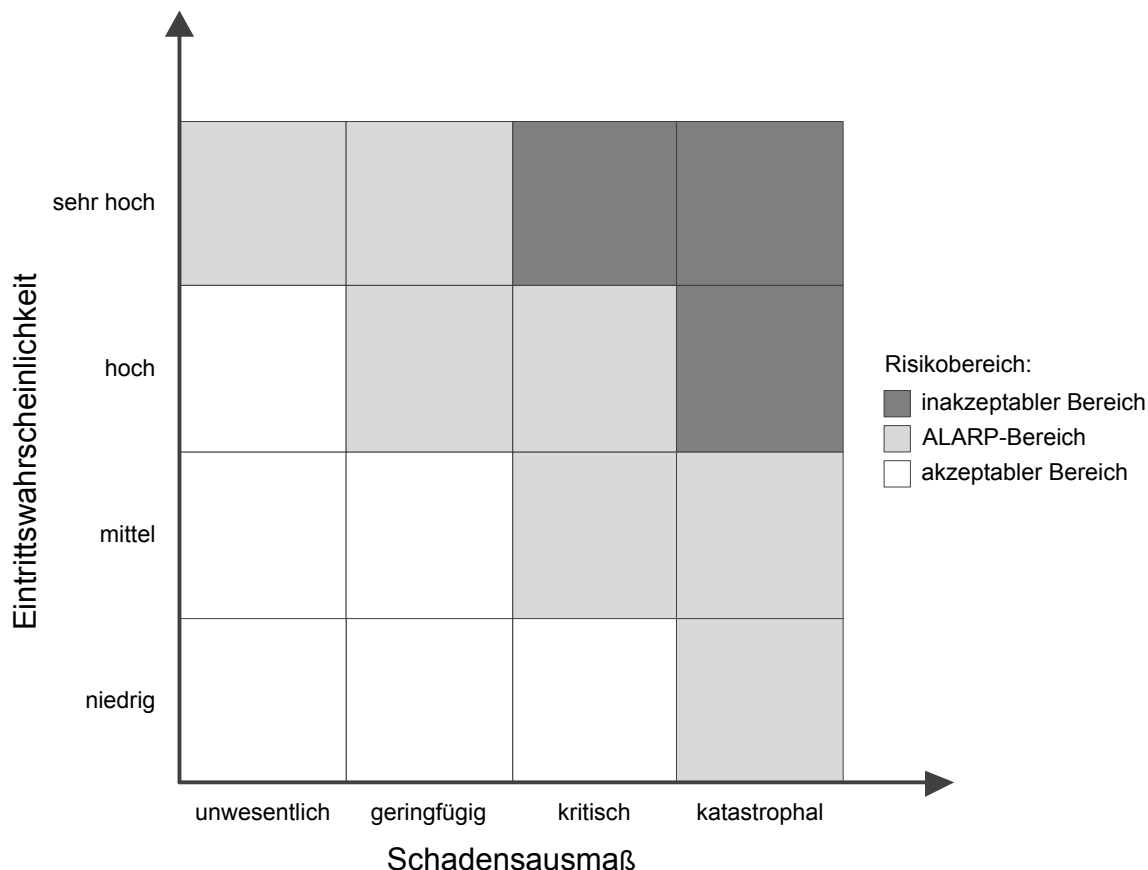


Abbildung 3.2: Risikokarte (Beschreibung der Achsen gemäß Tabelle 3.2 und 3.3)<sup>156</sup>

Die Risikobereiche sind farblich voneinander abgegrenzt. Dunkelgrau werden jene Risiken dargestellt, die in den inakzeptablen Bereich der Risiko-Karte fallen. Diese sind nicht vertretbar. Sie sollten durch Reduzierung des Schadensausmaßes bzw. der Eintrittswahrscheinlichkeit der Gefährdung mit Hilfe von Maßnahmen in die beiden anderen Bereiche übertragen werden. Der hellgrau dargestellte ALARP-Bereich (engl. **as low as reasonable practicable**, dt. so niedrig, wie vernünftigerweise praktikabel) liegt zwischen dem inakzeptablen und dem akzeptablen Bereich. Die Risiken, die sich in diesem Bereich befinden sind tolerierbar. Sie sollten allerdings näher untersucht werden.<sup>157</sup>

<sup>154</sup>Vgl. Königs: IT-Risiko-Management mit System (2009), [23], S. 34-37.

<sup>155</sup>Vgl. ebd., S. 20.

<sup>156</sup>Angelehnt an: Klipper: Information Security Risk Management (2011), [21], S. 151.

<sup>157</sup>Vgl. ebd., S. 150f.

Ziel einer Risikoanalyse und nachfolgender Schutzmaßnahmen sollte es sein, alle Risikofaktoren in den akzeptablen Risikobereich zu transferieren. Risiken, die im akzeptablen Bereich liegen sind vertretbar. Somit müssen keine Maßnahmen durchgeführt werden. (Bei Bedarf können diese trotzdem durchgeführt werden).

Die folgenden vier Risikobewältigungsstrategien werden dabei bei der Maßnahmengestaltung eingesetzt:

- Risikovermeidung: Verlagern des Risikos z. B. an einen Ort an dem das Risiko nicht auftritt.
- Risikoreduktion: Reduzieren der Wahrscheinlichkeit des Risikoeintritts oder begrenzen des Schadensausmaßes.
- Risikotransfer: Risiko an andere übertragen, wie z. B. an eine Versicherung, die das Risiko übernimmt.
- Risikoakzeptanz: Risiko bewusst annehmen. Das Restrisiko kann beispielsweise akzeptiert werden, wenn weitere Maßnahmen bereits ergriffen wurden.<sup>158</sup>

## 3.6 Risikoentstehungsfaktoren

### 3.6.1 Schwachstelle und Verwundbarkeit

Eine Schwachstelle (engl. weakness) bezeichnet den Ort an dem ein System für Störungen anfällig ist oder eine Eigenschaft dieses Systems, das zur Schwäche werden und so zu einem verwundbaren System führen kann. Die Verwundbarkeit (engl. vulnerability) bezeichnet eine Schwachstelle, die zur Umgehung, Täuschung oder der nicht autorisierten Modifikation der Sicherheitsdienste eines Systems verwendet werden kann. Schwachstellen treten in verschiedenen Bereichen auf. Dazu zählen beispielsweise Schwachstellen, welche auf Grund von Fehlverhalten entstehen, natürliche Schwachstellen oder technische Schwachstellen.<sup>159</sup> Sie werden innerhalb vorgefertigter Exploits, d.h. Techniken bzw. Programme, die diese Methoden einsetzen, dazu verwendet, um in ein System einzubrechen.<sup>160</sup>

### 3.6.2 Bedrohung

Eine Bedrohung (engl. threat) nutzt Schwachstellen bzw. Verwundbarkeiten aus und richtet sich gegen die Schutzziele eines Systems.<sup>161</sup> Dabei unterscheidet man zwischen potentiellen und akuten Bedrohungen. Potentielle Bedrohungen, sind jene die prinzipiell möglich sind. Eine solche denkbare Bedrohung muss allerdings nicht zu einer gefährlichen Situation führen.<sup>162</sup> Aus einer potentiellen Bedrohung wird eine akute Bedrohung, wenn ein System eine Schwachstelle aufweist, ein Angreifer diese kennt und einen Angriff auf das System plant. Bei einer akuten

<sup>158</sup>Vgl. Königs: IT-Risiko-Management mit System (2009), [23], S. 49f.

<sup>159</sup>Vgl. Schmidt: Der IT Security Manager (2006), [38], S. 21f; Eckert: IT-Sicherheit (2012), [12], S. 16.

<sup>160</sup>Vgl. Geschonneck: Computer-Forensik (2011), [17], S. 16.

<sup>161</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 16.

<sup>162</sup>Vgl. Schmidt: Der IT Security Manager (2006), [38], S. 23f.

Bedrohung besteht also das Risiko eines Angriffs, welcher noch nicht erfolgt ist. Nach Umsetzung des Angriffs entsteht aus einer akuten Bedrohung schließlich ein sicherheitsrelevantes Ereignis.<sup>163</sup> In den IT-Grundschutz-Katalogen<sup>164</sup> des BSI werden Bedrohungen, zusammengefasst mit Schwachstellen, als sogenannte Gefährdungen behandelt. Gefährdungen, die das BSI lokalisiert hat, sind in folgende sechs Gefährdungskataloge G0 bis G5 einsortiert:

- G0 Elementare Gefährdungen
- G1 Höhere Gewalt
- G2 Organisatorische Mängel
- G3 Menschliche Fehlhandlungen
- G4 Technisches Versagen
- G5 Vorsätzliche Handlungen

Die fünf Gefährdungskataloge G1 bis G5 umfassen dabei zusammen eine hohe Anzahl (über 500) an Einzelgefährdungen. Eine Risikoanalyse nach BSI-Standard 100-3 auf Basis dieser Gefährdungskataloge, bei Betrachtung und Bewertung sämtlicher Gefährdungen, wird durch diesen Sachverhalt erschwert. Aus diesem Grund wurde als Ergänzung der Gefährdungskatalog G0, der nunmehr aus 46 Gefährdungen besteht, entwickelt. Damit soll die Durchführung von Risikoanalysen nach BSI-Standard 100-3 erleichtert werden.<sup>165,166</sup>

#### 3.6.3 Angriff

Angriffe (engl. attack) stellen nicht autorisierte Zugriffe bzw. nicht autorisierte Zugriffsversuche dar. Sie bedrohen die Schutzziele (siehe Abschnitt 3.2) und lassen sich in passive und aktive Angriffe unterscheiden. Passive Angriffe beabsichtigen den Verlust der Vertraulichkeit und zeichnen sich dadurch aus, dass hier keine Daten verändert werden, sondern unautorisiert Informationen gewonnen werden. Bei aktiven Angriffen werden dagegen nicht autorisierte Manipulationen an Informationen oder Systemen vorgenommen. Sie bedrohen somit die Integrität und Verfügbarkeit eines IT-Systems.<sup>167</sup>

Abhören (engl. eavesdropping) einer Datenkommunikation zwischen Systemen innerhalb eines Netzwerks oder unautorisiertes Auslesen von Daten sind Beispiele für passive Angriffe. Werden Daten während der Übertragung manipuliert, Nachrichten wieder eingespielt (Replay-Attacke) oder erfolgt ein Dateizugriff unautorisiert handelt es sich um aktive Angriffe. Andere Angriffe dieser Angriffsform richten sich gegen die Verfügbarkeit (**Denial-of-Service (DoS)**) oder die Authentizität (Maskierungsangriff). Bei einem **DoS**-Angriff wird das Ziel mit Hilfe vieler

<sup>163</sup>Vgl. Schmidt: Der IT Security Manager (2006), [38], S. 23f.

<sup>164</sup>Anm.: Für weitere Informationen zum IT-Grundschutz siehe <https://www.bsi.de/gshb>.

<sup>165</sup>Vgl. BSI: IT-Grundschutz-Kataloge: 12. EL Stand 2011 (2011), [91], S. 9.

<sup>166</sup>Anm.: In Abschnitt 4.2.2 ist eine Bedrohungsanalyse für ein Beispielszenario (siehe Abschnitt 4.2.1) zu finden. Diese und die darauf aufbauende Risikoanalyse (siehe Abschnitte 4.2.3 und 4.3.2) wurde allerdings nicht auf Basis des BSI Standards 100-3 erstellt.

<sup>167</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 19.

Anfragen überflutet, sodass es schlecht oder gar nicht mehr erreichbar ist. Maskierungsangriffe bzw. Spoofing-Attacken dienen dem Vortäuschen einer anderen Identität. Bekannte Spoofing-Attacken sind beispielsweise [Domain Name System \(DNS\)](#)<sup>168</sup>-Spoofing (Fälschung der Zuordnung zwischen IP-Adresse und DNS-Name), IP-Spoofing (Fälschung der IP-Adresse) und E-Mail-Spoofing (Fälschung der Absenderadresse innerhalb einer E-Mail).

Zuletzt gibt es neben den vorher genannten Angriffsformen mit dem Social Engineering eine weitere, nicht technische Angriffsform. Personen werden dabei durch zwischenmenschliche Beeinflussung vom Angreifer dazu gebracht unberechtigt Informationen herauszugeben oder Zugang zu technischen Infrastrukturen zu ermöglichen.<sup>169</sup>

#### 3.6.4 Angreifer

Die im vorherigen Abschnitt erläuterten Angriffe werden von verschiedenen Angreifern durchgeführt. Diese Angreifer lassen sich in verschiedene Angreifer-Typen einteilen. Sie unterscheiden sich dabei in den zur Verfügung stehenden Ressourcen (z. B. Geld, Zeit, Wissen) und ihrer Motivation (sozial, technisch, politisch, finanziell). Beispielhaft werden hier folgende aufgeführt:

- Hacker (Cracker, Skriptkiddie)
- Organisiertes Verbrechen/Kriminalität
- Terrorist
- Staatliche Einrichtung (Polizei, Nachrichtendienst/Geheimdienst, Militär)
- Industriespion (Konkurrenten, Wettbewerber)
- Presse
- Betreiber, Dienstleister, Hersteller
- Insider (Mitarbeiter, Entwickler, Wartungstechniker, Berater, Vertragspartner)
- Bürger als Angreifer (Endkunden, Nachbarn)

Hacker werden als technisch gebildete Angreifer gesehen. Sie zielen darauf ab, mit Systemen zu experimentieren ohne sie zu beschädigen, um dabei Schwachstellen zu finden. Die gewonnenen Informationen verwenden sie, um mögliche Angriffsmöglichkeiten aufzuzeigen und sie in Form von Exploits (siehe Abschnitt 3.6.1) zu veröffentlichen. Cracker ähneln den Hackern, ihre Beweggründe sind aber meist unterschiedlich. Sie beschädigen z. B. Zielsysteme oder stehlen Daten. Skriptkiddies unterscheiden sich von den beiden erstgenannten, dadurch dass sie selbst meist nicht über tiefes technisches Wissen verfügen, sondern vorgefertigte Exploits einsetzen und ausnutzen. Als Gemeinsamkeit haben alle drei meist viel Zeit gepaart mit einem geringen Budget, außer sie Arbeiten im Auftrag eines anderen Angreifer-Typs wie z. B. dem Organisierten

---

<sup>168</sup>Siehe Mockapetris: [RFC 1034](#) (1987), [152]; Mockapetris: [RFC 1035](#) (1987), [153].

<sup>169</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 26.

Verbrechen. Dieses hat neben seinen klassischen Kerngeschäften wie Betrug und Drogenhandel die digitale Welt erreicht und ist z. B. im Bereich des Identitätsdiebstahls oder der Erpressung als Angreifer aktiv. Terroristen arbeiten zur Finanzierung auch mit Methoden des organisierten Verbrechens. Sie sind allerdings meist religiös, ethisch oder politisch motiviert. Staatliche Einrichtungen stehen im Gegensatz zu den vorher genannten Angreifer-Typen. Zum Angreifer werden sie um Informationen zu sammeln, die verborgen bleiben sollen oder wenn andere Staaten angegriffen werden sollen. Teilweise sollen Nachrichtendienste auch Industriespionage betreiben um Wirtschaftsgeheimnisse über Wettbewerber zu erhalten. Als besondere Form von Industriespionage kann die Presse betrachtet werden, die zum Angreifer wird wenn Informationen gesammelt und veröffentlicht werden, um die eigene Auflage zu stärken oder einer Person zu Schaden.<sup>170</sup> So wurde z. B. der Stromverbrauch des Friedensnobelpreisträgers Al Gore in der Presse veröffentlicht.<sup>171</sup> Betreiber und Hersteller eines Systems, aber auch Dienstleister können zum Angreifer werden, wenn sie Industriespionage betreiben oder eigene Kunden angreifen, indem von ihnen Daten gesammelt werden, obwohl ihnen die Berechtigung dafür fehlt. Insider und Bürger können z. B. auf Grund von Rache zum Angreifer werden, da ihnen gekündigt wurde oder um einen Nachbar zu ärgern. Ein weiteres Motiv für einen Bürger kann es sein Geld sparen zu wollen.<sup>172</sup>

Die hier besprochenen personellen Angreifer-Typen nutzen im Rahmen eines Angriffs auch Schadsoftware (engl. Malware). Dies umfasst Computerviren, Computerwürmer, Trojanische Pferde, Bot-Netze sowie weitere Formen.<sup>173</sup>

---

<sup>170</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 21-26, 179; Eckert: Sicherheit im Smart Grid (2011), [62], S. 21-26; Schneier: Secrets & lies (2001), [41], S. 39-54.

<sup>171</sup>Vgl. The Beacon Center of Tennessee: Editor: Al Gores Personal Energy Use Is His Own Inconvenient Truth, [121].

<sup>172</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 21-26, 179; Eckert: Sicherheit im Smart Grid (2011), [62], S. 21-26; Schneier: Secrets & lies (2001), [41], S. 39-54.

<sup>173</sup>Anm.: Da eine detaillierte Beschreibung der verschiedenen Arten von Schadsoftware an dieser Stelle zu weit führt, soll auf folgende Literatur verwiesen werden: Eckert: IT-Sicherheit (2012), [12], S. 55-64; Schneier: Secrets & lies (2001), [41], S. 144-151.

### 4 Angriffe und Bedrohungsszenarien

#### 4.1 Mögliche Angreifer

Im vorherigem Kapitel wurden generische Angreifer-Typen unterschieden. Für diese Arbeit soll zwischen diesen generischen Angreifer-Typen nicht weiter unterschieden werden. Stattdessen werden folgende drei Angreifer unterschieden:

- Nutzer: Der Nutzer ist der Kunde eines Netzbetreibers/Messstellenbetreibers. Beim Nutzer wird nicht davon ausgegangen, dass er terroristische Angriffe durchführt.
- Nachbar: Nachbar des Nutzers, der mit ihm im selben Mehrfamilienhaus wohnt. Beim Nachbar wird ebenso wie beim Nutzer nicht davon ausgegangen, dass er terroristische Angriffe durchführt. Er verfolgt hauptsächlich das Ziel dem Nutzer zu schaden. Er ist Kunde bei einem anderen Messstellenbetreiber.
- Externer Angreifer: Ein Angreifer, der von extern über das Internet Angriffe durchführt. Diesem Angreifer werden auch terroristische Angriffe zugetraut. Der Angreifer weiß zudem kriminelle Energie auf.

#### 4.2 Mögliche Angriffsziele und Bedrohungen

Die Bedrohungsanalyse in diesem Abschnitt erfolgt in Anlehnung an bewährte Methoden des Security Engineerings, welches sich mit der Konstruktion sicherer Systeme befasst.<sup>174</sup> Im Rahmen dieser Arbeit soll kein System konstruiert werden, sondern die Sicherheit einer bestehenden Smart Grid Implementierung evaluiert werden. Da in beiden Fällen Bedrohungen und deren Konsequenzen analysiert werden, sind die Methodiken des Security Engineerings für das Vorgehen der Arbeit dennoch sinnvoll und anwendbar. In einer Bedrohungsanalyse sollen systematisch die Ursachen für potentielle Bedrohungen, technischer, organisatorischer und benutzerbedingter Natur untersucht werden. Bedrohungen, die auf Grund natürlicher Auslöser infolge höherer Gewalt entstehen wie z. B. Erdbeben, Wetter, Feuer oder Störungen im Magnetfeld der Erde, sollen hier nicht betrachtet werden.

Alle unterschiedlichen Ausprägungen eines Smart Grid in einer Bedrohungsanalyse abzudecken würde allerdings den Rahmen dieser Arbeit sprengen. Deshalb wird diese (siehe Abschnitt 4.2.2) an Hand eines zum heutigen Stand (Jahr 2012) typischen Szenarios (siehe Abschnitt 4.2.1) durchgeführt. Um abgesehen vom Szenario auch andere Bedrohungen heutiger und zukünftiger Smart Grids anzusprechen, sollen zunächst einige Angriffe aufgezeigt werden, welche keine Relevanz für das Szenario haben:

- Hohe Strompreise bei Nutzung, abgeleitet vom individuellen Lastprofil: Das Energieversorgungsunternehmen wertet das Lastprofil eines Kunden aus. Nach Auswertung ergeben sich für den Kunden hohe Preise bzw. Preissprünge immer dann wenn er üblicherweise den Strom nutzt. Dies erfordert allerdings dynamische Tarife (siehe Abschnitt 2.3.2)

---

<sup>174</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 187.

- Manipulation des Strompreises durch verändern der Uhrzeit im **SM-GW**: Dies hat nur Auswirkungen bei zeitvariablen Tarifen, wenn im **SM-GW** die Zuordnung von Zeit und Tarif erfolgt und die Messdaten in größerem zeitlichem Abstand (z. B. einmal täglich) versendet werden.
- Manipulation von Preisinformationen: Bei Tarifen, bei denen Preisinformationen ausgewertet werden, hat dies Auswirkungen. Preise können dabei an verschiedenen Stellen manipuliert werden z. B. im **SM-GW** während der Übertragung über Datennetze oder durch Manipulation des Energie-Börsenpreises.
- Zugriff auf detailliertere Messdaten, d. h. mit einer höheren Auflösung (ein Messwert pro Sekunde anstatt alle 15 Minuten), als vertraglich vereinbart.
- Zusammenlegung von Lastprofilen mit Internetverkehrsdaten: Dadurch wird eine noch genauere Profilbildung ermöglicht. Dies könnte z. B. möglich werden, wenn der genutzte Internetprovider und Messstellenbetreiber identisch ist.
- Erstellung von Bewegungsprofilen bei Nutzung von Elektromobilen: Es werden also nicht nur die Lastprofile des Verbrauchers ausgewertet, sondern auch die Orte an denen das Elektrofahrzeug mit Strom geladen wird.
- Missbrauch der Smart Meter Fernabschaltfunktion: Es könnten nicht nur einzelne Smart Meter vom Netz getrennt, sondern auch mehrere gleichzeitig, wenn die Fernabschaltfunktion von zentraler Stelle aus aktiviert werden kann und ein Angreifer Zugriff auf diese erhält.<sup>175</sup> Für den Fall, dass die Fernabschaltfunktion durch eine Schadsoftware (z. B. Wurm) aktiviert werden kann, könnte dies zu einer weitflächigen Abschaltung führen.<sup>176</sup>
- Entziehung elektrischer Energie<sup>177</sup> bei Prepaid Smart Metern mit lokalem Guthaben-Abrechnungssystem: Ein Betrug ist beispielsweise möglich durch Manipulation des Guthabens auf dem Guthabentoken (z. B. Keycard), durch das Fälschen des Tokens<sup>178</sup> oder einer Manipulation der Funktionsweise des Tokenreaders (egal welches Token eingelegt wird - auch ohne Guthaben - wird erkannt als ein Token mit vollem Guthaben).<sup>179</sup>
- Entziehung elektrischer Energie beim Einsatz von Prepaid Smart Metern mit zentralisiertem Abrechnungssystem: Neben der Manipulation des Guthabens im Guthabenverwaltungssystem (ein Zugriff auf dieses ist hierfür notwendig) können z. B. gefälschte

<sup>175</sup>Vgl. Anderson und Fuloria: Who controls the off switch? (2010), [43].

<sup>176</sup>Anm.: Für eine Simulation der Ausbreitung eines Wurmangriffs im Smart Grid siehe „Worm Attack Simulation video #1 bis #3“ auf [http://www.ioactive.com/services\\_grid\\_research.html](http://www.ioactive.com/services_grid_research.html).

<sup>177</sup>Anm.: Unter Entziehung elektrischer Energie (ugs. Stromklau) wird in dieser Arbeit neben dem Tatbestand aus StGB (2012), [189], § 248c, auch die missbräuchliche, unentgeltliche Nutzung von elektrischer Energie Verstanden (in Anlehnung an ebd., § 263a Computerbetrug und ebd., § 265a Erschleichung von Leistungen).

<sup>178</sup>Anm.: Laut Hamill: Prepaid Electricity Meter Fraud (2010), [109] bzw. Schneier: Prepaid Electricity Meter Fraud (2010), [119] wurden Token bereits gefälscht und zum Betrug von Kunden genutzt.

<sup>179</sup>Anm.: Für weitere Angriffe auf Prepaid Smart Meter siehe Anderson und Bezuidenhout: On the Reliability of Electronic Payment Systems (1996), [3] bzw. Anderson und Bezuidenhout: Cryptographic credit control in pre-payment metering systems (1995), [2]

VoucherCodes genutzt werden (Erstellung gefälschter VoucherCodes mittels Key-Generator, Funktionsweise des dabei verwendeten Algorithmus muss dafür bekannt sein)

- Betrug bei der Einspeisung von elektrischer Energie: Dies kann etwa durch Manipulation der gemessenen Einspeisedaten (z. B. Manipulation der Smart Meter Kalibrierungsfunktion), durch Manipulation der Einspeisedaten während der Übertragung (z. B. Abhören der Datenkommunikation und einspielen von veränderten Einspeisedaten) oder durch Manipulation der gespeicherten Daten (z. B. Manipulation der gespeicherten Einspeisedaten im Abrechnungssystem) erfolgen.
- Übernahme der Steuerung intelligenter Haushaltsgeräte, die mit dem **SM-GW** verbunden sind: Damit wäre eine unerwünschte Aktivierung/Deaktivierung von Geräten wie beispielsweise der Klimaanlage oder der Waschmaschine bis hin zu einer Änderung der Gerätekonfiguration möglich.<sup>180</sup>

### 4.2.1 Szenario

Die Discovery GmbH ist ein unabhängiger Energieberater für Haushaltskunden und Kleinbetriebe. Das Unternehmen wurde Anfang 2009 gegründet und tritt als Messstellenbetreiber bzw. Messstellendienstleister deutschlandweit auf. Neben der Messung des Stromverbrauchs mittels Smart Meter führt die Discovery GmbH eine Analyse des Verbrauchsprofils durch, um den Kunden hinsichtlich eines passenden Anbieters und Tarifs zu beraten.<sup>181</sup>

Als Smart Meter wird ein elektronischer 3-Phasen Drehstromzähler mit Rücklaufperre und verschweißtem Zählergehäuse eingesetzt. Dieses basiert auf dem Modell Q3D-A1004<sup>182</sup> der EasyMeter GmbH. Alle 2 Sekunden werden Messwerte aufgezeichnet<sup>183</sup> und unidirektional über eine optische D0-Schnittstelle<sup>184</sup> an das **SM-GW** (Discovery Meteroit<sup>185</sup>) gesendet. Das **SM-GW** ist per Fernwartung updatebar. Es ist physikalisch über dem Smart Meter angebracht und mit diesem über zwei Schrauben verbunden, wobei eine der beiden Schrauben mit einer Plombe versehen ist.<sup>186</sup> Es speichert die Messdaten in einem Zwischenspeicher ab und leitet die Daten anschließend per Ethernet oder Wireless M-Bus an einen Kundenrouter (DSL-Router) weiter von dem es per DHCP<sup>187</sup> seine IP-Adresse bezieht.<sup>188</sup> Vom Kundenrouter

---

<sup>180</sup> **Anm.:** Bei diesem Angriff handelt es sich um einen Angriff der sich im Grenzbereich zwischen Smart Grid und Smart Home befindet. Zusätzlich ist für einen solchen Angriff ein zukünftiges Smart Home erforderlich. Der Autor sieht diese Funktion eher im Bereich des Smart Homes. Dieser Grenzfall bedarf einer genaueren Untersuchung, die nicht im Rahmen dieser Arbeit durchgeführt wird.

<sup>181</sup> Vgl. Discovery : FAQ, [103];

<sup>182</sup> Siehe Abb. B.7 und Abb. B.8; EasyMeter GmbH: EasyMeter Betriebsanleitung (2011), [61].

<sup>183</sup> Vgl. Greveler, Justus und Löhr: Multimedia Content Identification Through Smart Meter Power Usage Profiles (2012), [67].

<sup>184</sup> Siehe DIN EN 62056-21 (2003), [143]; EasyMeter GmbH: D0 Schnittstelle (2009), [60].

<sup>185</sup> Siehe GmbH: Discovery Produktflyer Meteroit (2010), [65], das **SM-GW** entspricht bisher nicht den Vorgaben des BSI Schutzprofils Gateway PP (siehe Abschnitt 3.4.2; siehe Abb. B.7 und Abb. B.8).

<sup>186</sup> Vgl. Bachfeld, Carluccio und Wegener: Wer hat an der Uhr gedreht? (2011), [4].

<sup>187</sup> Siehe Droms: RFC 2131 (1997), [145].

<sup>188</sup> **Anm.:** Im Fall einer Übertragung per Wireless M-Bus wird ein zusätzlicher Adapter vor den Router zwischengeschaltet, der eine Umwandlung nach Ethernet vornimmt.



gelangen die Messdaten per DSL über das Internet schließlich zu den Discovery Servern.<sup>189</sup> Alternativ unterstützt das SM-GW auch die Übertragung per GPRS als Reservesystem.<sup>190</sup> Die Messdaten werden vom SM-GW mit Hilfe von HTTP-POST-Requests<sup>191</sup> an den Discovery Server (feste IP-Adresse 85.214.93.99) gesendet. Dort sind die Verbrauchsdaten (nur die letzten 3 Monate sind sichtbar) im Discovery Online Kundenportal mittels Webbrowser zugänglich.<sup>192</sup> Als Kunde soll ein Paar<sup>193</sup>, das innerhalb eines Mehrfamilienhauses mit vier Parteien im ersten Obergeschoss wohnt und ihren Strom von einem kleinen Stadtwerk bezieht, dienen. Als Stromtarif wird ein Eintarif (Kosten sind zu jeder Uhrzeit gleich) mit monatlich genauer Abrechnung eingesetzt. Hierzu wird der Zählerstand von Discovery am Ende jeden Monats an das Stadtwerk übermittelt. Das Smart Meter befindet sich im Kellerbereich des Hauses in einem nicht abgeschlossenen Zählerschrank, der für alle Parteien zugänglich ist. Das Paar verfügt nicht über eine dezentrale Stromerzeugungsanlage und speist somit auch keinen Strom ins Netz ein. Für dieses Szenario wird weiter angenommen, dass am Ethernet Anschluss des SM-GW ein PLC-Adapter angeschlossen ist, da eine direkte Verbindung vom Keller bis zum 1. OG nicht vorhanden ist und auch nicht verlegt werden kann. Der PLC-Adapter im Keller überträgt die Daten transparent verschlüsselt (Advanced Encryption Standard (AES) 128 Bit<sup>194</sup>) und signiert zu dem PLC-Adapter in der Wohnung. Von dort gelangen die Daten unverschlüsselt per Ethernet bis zum DSL-Router des Kunden. Nicht genutzte Schnittstellen (z. B. Wireless M-Bus) sind deaktiviert.

### 4.2.2 Bedrohungsanalyse

Bei der Bedrohungsanalyse in diesem Abschnitt werden die nach Meinung des Autors wichtigsten Ursachen für Bedrohungen aus unterschiedlichen Bereichen aufgestellt. Zusätzlich erfolgt eine Abschätzung des für den Angreifer zu erbringenden Aufwands für eine erfolgreiche Durchführung eines Angriffs sowie der Nutzen eines Angriffs für den Angreifer. Bei der Abschätzung wurde generell davon ausgegangen, dass Angriffe die viele Personen betreffen, einen größeren Nutzen für den externen Angreifer aufweisen als Angriffe die einzelne Personen betreffen. Diese Abschätzung erfolgt nach bestem Wissen und wird gestützt durch Erfahrungen des Autors. Personen mit einem anderen Einblick in das Thema können zu anderen Bedrohungen und zu einer anderen Abschätzung des Aufwands oder des Nutzens für den Angreifer kommen. In den Tabellen 4.1 bis 4.8 werden die einzelnen Bedrohungen nacheinander für die verschiedenen Angreifer (Nutzer, Nachbar und externer Angreifer, siehe Abschnitt 4.1) beschrieben.<sup>195</sup> Dabei ist für jede Bedrohung eine Nummer, gefolgt von einer Beschreibung sowie der geschätzte Aufwand und der geschätzte Nutzen für den Angreifer aufgeführt. Der Aufwand bzw. der Nutzen für den

---

<sup>189</sup>Anm.: Laut Discovery : FAQ, [103] wird ein DSL Vertrag benötigt.

<sup>190</sup>Vgl. GmbH: Discovery Produktflyer Meteorit (2010), [65].

<sup>191</sup>Siehe Fielding u. a.: RFC 2616 (1999), [146].

<sup>192</sup>Vgl. Brinkhaus u. a.: Vortrag: Smart Hacking for Smart Privacy (2011), [52], 23ff; Bachfeld, Carluccio und Wegener: Wer hat an der Uhr gedreht? (2011), [4].

<sup>193</sup>Anm.: Entspricht repräsentativem Durchschnittshaushalt; vgl. Bundesamt: Statistisches Jahrbuch 2011 (2011), [54], S. 63.

<sup>194</sup>Siehe NIST: FIPS PUB 180-2 (2002), [171].

<sup>195</sup>Anm.: Für detailliertere Aufschlüsselungen einzelner Bedrohungen siehe Anhang B.2.

Angreifer wird den Werten niedrig, mittel, hoch oder sehr hoch zugeordnet.

Die Tabellen 4.1 und 4.2 zeigen Angriffe des Angriffstyps Abhören<sup>196</sup>, durch welche das Schutzziel der Vertraulichkeit bedroht wird. Die Manipulation von Messdaten, in Tabelle 4.3 und 4.4 dargestellt, führt zu einer Bedrohung der Integrität. Durch die beschriebenen Angriffe werden zusätzlich die Schutzziele der Verbindlichkeit und der Authentizität bedroht. In den darauf folgenden Tabellen werden Angriffe beschrieben, die zu einer Einschränkung der Verfügbarkeit der Abrechnung (siehe Tabelle 4.5 und 4.6) und der Stromversorgung (siehe Tabelle 4.7 und 4.8) führen können. Für den externen Angreifer wird bei allen Hauptschutzzielverletzungen der Nutzen als größer angesehen, wenn statt eines einzelnen Nutzers, viele Nutzer betroffen sind. Vor allem bei der Hauptbedrohung Einschränkung der Verfügbarkeit der Abrechnung unterscheidet sich der Nutzen für den Angreifer durch die Anzahl der Nutzer. Der Angreifer kann durch den Angriff die Verfügbarkeit des Abrechnungssystems, mit der Motivation den Messstellenbetreiber/Netzbetreiber zu erpressen, einschränken. Im Folgenden sollen Begriffe, die im Rahmen der Angriffsbeschreibung verwendet werden, kurz erläutert werden:

- Phishing: Mit Hilfe gefälschter E-Mails und Webseiten soll der Nutzer dazu gebracht werden, persönliche Daten wie beispielsweise Passwörter an den Angreifer preiszugeben.<sup>197</sup>
- Pharming: Wird der Nutzer beim Phishing mit Hilfe manipulierter DNS-Anfragen (z. B. durch DNS-Spoofing; siehe 3.6.3) auf gefälschte Webseiten weitergeleitet, spricht man von Pharming.<sup>198</sup>
- Man-in-the-middle-Angriff: Angriffsform bei der sich ein Angreifer in die Kommunikation zwischen zwei Kommunikationspartnern einschleust und somit die ausgetauschten Informationen einsehen oder manipulieren kann.<sup>199</sup>
- DNS-Cache Poisoning: DNS-Server speichern Abfrageergebnisse in Zwischenspeichern (Caches). Beim DNS-Cache Poisoning verändert der Angreifer diesen Zwischenspeicher so, dass bei erneuter DNS-Anfrage die vom Angreifer gefälschten Daten ausgegeben werden.<sup>200</sup>
- Zero-Day-Exploit: In einem Zero-Day-Exploit werden Schwachstellen an dem Tag, an dem sie allgemein bzw. für die Entwickler einer Software bekannt werden (Zero-Day) oder noch davor, bereits in einem Exploit (siehe 3.6.1) ausgenutzt.<sup>201</sup>
- SQL-Injection: Bei SQL-Injection wird die mangelhafte bzw. fehlende Eingabepfung in Benutzereingabefeldern (z. B. Passwort Login-Maske) ausgenutzt, um Datenbankabfragen in eine SQL-Datenbank einzuschleusen. Dies kann z. B. genutzt werden um Passwörter von Benutzerkonten zu ändern.<sup>202</sup>

---

<sup>196</sup> **Anm.:** In dieser Arbeit wird unter Abhören, das Abhören an sich, als auch die unautorisierte Einsicht von Informationen verstanden.

<sup>197</sup> Vgl. Geschonneck: Computer-Forensik (2011), [17], S. 14.

<sup>198</sup> Vgl. Schneier: Schneier on Security (2008), [40], S. 211.

<sup>199</sup> Vgl. Eckert: IT-Sicherheit (2012), [12], S. 446f.

<sup>200</sup> Vgl. Eschweiler und Psille: Security@Work (2006), [14], S. 75.

<sup>201</sup> Vgl. Schönbohm: Deutschlands Sicherheit (2011), [42], S. 57.

<sup>202</sup> Vgl. Eckert: IT-Sicherheit (2012), [12], S. 177.

- Brute-Force-Angriff: Bei einem Brute-Force-Angriff werden alle möglichen Kombinationsmöglichkeiten durchprobiert, um beispielsweise an ein Passwort zu gelangen.<sup>203</sup>
- Wörterbuchangriff: Beim einem Wörterbuchangriff werden Passwortmöglichkeiten aus einem Wörterbuch ausgelesen. Dies gelingt häufig, da Benutzer oft Passwörter benutzen die sich in Wörterbüchern wiederfinden lassen.<sup>204</sup>
- ARP-Spoofing: Das Address Resolution Protocol<sup>205</sup> wird in Ethernet Netzwerken mit Internet Protocol Version 4 (IPv4)<sup>206</sup>-Adressierung dazu genutzt die MAC-Adresse (Hardware-Adresse) zu einer gegebenen IP-Adresse zu ermitteln. Beim ARP-Spoofing werden vom Angreifer manipulierte ARP-Nachrichten verschickt, sodass anschließend der Datenverkehr an den Computer des Angreifers übermittelt wird.<sup>207</sup>
- TCP-SYN-flood-Angriff: Beim Aufbau einer Transmission Control Protocol (TCP)<sup>208</sup>-Verbindung wird ein sogenannter 3-Wege-Handshake durchgeführt. Dabei wird ein SYN-Paket (Paket mit Flag SYN gesetzt) versendet, dass vom Empfänger (Paket mit Flag SYN, ACK gesetzt) und anschließend vom Sender bestätigt wird (Paket mit Flag ACK gesetzt). Beim TCP-SYN-flood-Angriff verschickt der Angreifer sehr viele SYN-Pakete an sein Opfer in denen die Absenderadresse gefälscht wurde. Das Opfer bestätigt die Verbindungsanfrage und wartet danach vergeblich auf eine Bestätigung des Senders. Diese offenen Verbindungen werden in einem Zwischenspeicher vorgehalten. Verschickt der Angreifer nun sehr viele SYN-Pakete füllt sich der Zwischenspeicher bis er vollständig gefüllt ist. Danach können keine weiteren Verbindungen aufgebaut werden.<sup>209</sup>
- Portscan: Darunter versteht man eine mit einem Portscanner durchgeführte Untersuchung. Ein Portscanner ist eine Software die erkennt welche Dienste in einem laufenden System über das Internetprotokoll angeboten werden.<sup>210</sup> Siehe [Abb. B.12](#) für einen beispielhaft durchgeführten Portscan mit dem Programm Nmap<sup>211</sup>.
- CVE: Common Vulnerabilities and Exposures (CVE) ist ein Standard zur einheitlichen Benennung von Schwachstellen bzw. Verwundbarkeiten. Die Verwundbarkeiten erhalten dabei eine einheitliche Nummer (CVE-Nummer).<sup>212</sup>
- SM-GW-ID: Discovery verwendet die MAC-Adresse des SM-GW zur Identifizierung von welchem Smart Meter die Messdaten stammen.<sup>213</sup> Der von Discovery reservierte

<sup>203</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 363f.

<sup>204</sup>Vgl. Hunt: A brief Sony password analysis (2011), [112]; Oberheide: Brief analysis of the Gawker password dump (2010), [116].

<sup>205</sup>Siehe Plummer: RFC 826 (1987), [154].

<sup>206</sup>Siehe University of Southern California: RFC 791 (1981), [159].

<sup>207</sup>Vgl. Lockhart: Netzwerksicherheit Hacks (2007), [28], S. 204.

<sup>208</sup>Siehe University of Southern California: RFC 793 (1981), [160].

<sup>209</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 121.

<sup>210</sup>Vgl. ebd., S. 184.

<sup>211</sup>Siehe <http://nmap.org/>.

<sup>212</sup>Vgl. The MITRE Corporation: CVE - About CVE (2012), [123].

<sup>213</sup>Vgl. Bachfeld, Carluccio und Wegener: Wer hat an der Uhr gedreht? (2011), [4].

#### 4 Angriffe und Bedrohungsszenarien

MAC-Adressbereich ist bekannt und lautet: 2C:DD:0C:00:00:00 - 2C:DD:0C:FF:FF:FF.<sup>214</sup>

Bedrohung Nr.	Beschreibung	Aufwand für Angreifer	Nutzen für Angreifer
B1.1	Abhören der Messdaten (Zählerstände) eines Nutzers über einen längeren Zeitraum durch den Nutzer selbst: Eine leicht durchführbare Variante des Angriffs besteht darin, die Datenkommunikation bei der Übertragung zwischen dem PLC-Adapter in der Wohnung und dem DSL-Router mit Hilfe eines zwischengeschalteten Hub bzw. Switch mit eingerichtetem Mirror-Port (ohne zusätzliche Hardware mit einem am DSL-Router eingerichteter Mirror-Port, unterstützt allerdings nicht jeder DSL-Router), welcher mit einem PC verbunden wird abzuhören. Falls der DSL-Router die Funktion unterstützt einen Mitschnitt der Datenübertragung zu erstellen (z.B. Router mit OpenWrt Betriebssystem und dem Programm tcpdump, oder AVM FRITZ!Box) kann der Angriff alternativ mit Hilfe dieser Variante erfolgen. Mit diesem Angriff könnte z. B. der Nutzer das Verhalten seines Partners ausspionieren. Der Angreifer könnte den Angriff auch durchführen, damit er die Messdaten direkt in hoher Auflösung (ein Messwert alle 2 Sekunden) verfügbar hat und so nicht auf das Discovery Online Portal angewiesen ist. Denn im Discovery Online Portal (Webschnittstelle) sind die Daten zunächst nur in aggregierter Form verfügbar. Über angepasste HTTP-GET-Requests (Siehe Fielding u.a.: RFC 2616 (HTTP 1.1) (1999)) ist auch ein Zugriff auf Messwerte in hoher Auflösung möglich. (Vgl. Brinkhaus u.a.: Vortrag: Smart Hacking for Smart Privacy (2011), S. 9)	niedrig	mittel
B1.2	Abhören der Messdaten (Zählerstände) eines Nutzers über einen längeren Zeitraum durch seinen Nachbarn: Eine leicht durchführbare Variante des Angriffs besteht darin, die Datenkommunikation bei der Übertragung zwischen SM-GW und PLC-Adapter mit Hilfe eines zwischengeschalteten Hub bzw. Switch mit eingerichtetem Mirror-Port, welcher mit einem PC verbunden wird, abzuhören. Das Abhören der Messdaten ist auch bei der Übertragung zwischen Smart Meter und SM-GW (verplombtes Gehäuse, D0-Schnittstelle) und bei der Übertragung zwischen den PLC-Adaptoren (verschlüsselte und signierte Übertragung) möglich, allerdings sind diese Angriffe dann mit einem höheren Aufwand verbunden. Für diese drei Angriffsvarianten ist allerdings ein Zugang zum Zählerschrank im Keller des Hauses erforderlich. Darüber hinaus ist auch eine unautorisierte Einsicht auf gespeicherte Messdaten im Discovery Online Portal möglich. Hierzu benötigt der Angreifer die Zugangsdaten des Nutzers. An diese kann er z.B. mit Hilfe von Social Engineering gelangen. Da sich der Benutzername laut Brinkhaus und Carluccio vom Vorname des Nutzers ableitet und das Passwort leicht erratbar sein soll, kann der Nachbar mit relativ wenig Aufwand auf die Zugangsdaten schließen. (Vgl. Brinkhaus u.a.: Vortrag: Smart Hacking for Smart Privacy (2011), S. 24) Eine weitere Möglichkeit wäre das Abhören einer Übertragung, während der Nutzer auf die Zählerstände im Online Portal zugreift. (Falls der Nutzer z.B. mit einem Notebook per WLAN auf das Online Portal zugreift, kann der Angreifer durch Zugriff auf das WLAN den Datenverkehr abhören). <i>Anmerkung: Das einmalige Ablesen eines Zählerstandes direkt am Smart Meter Display wird hier vernachlässigt, da es sich nicht von der heutigen Möglichkeit des Ablesens eines Stromzählers unterscheidet.</i>	mittel	mittel
B1.3	Abhören der Messdaten (Zählerstände) eines Nutzers über einen längeren Zeitraum durch einen externen Angreifer: Eine unautorisierte Einsicht auf gespeicherte Messdaten kann über den Zugriff auf das Discovery Online Portal erfolgen. Hierfür werden die Zugangsdaten des Nutzers benötigt. Der Angreifer kann dabei über unterschiedliche Methoden wie beispielsweise Phishing (Social-Engineering), Pharming, Übermittlung einer Schadsoftware (Trojaner) auf dem Computer des Nutzers und abgreifen der Daten während des Einloggenvorgangs des Benutzers auf dem Discovery Server oder durch einen Man-in-the-middle-Angriff mit Hilfe von DNS-Spoofing (z. B. DNS-Cache Poisoning) an die Zugangsdaten gelangen. Eine weitere Möglichkeit besteht darin, in den Server des Online-Portals durch Ausnutzen von Fehlern in nicht aktualisierter Serversoftware z.B. mit Hilfe von Zero-Day-Exploits (Vgl. Armstrong: Analysis of Sony PSN Hack (2011)) einzudringen. Eventuell ist die Login Maske des Online Portals auch anfällig für SQL-Injection, sodass der Angreifer darüber Zugriff erhalten kann. Auch der Zugang über ein Administratorkonto des Servers erscheint denkbar. An die Zugangsdaten des Administrators kann der Angreifer z.B. per Phishing gelangen. Ist ihm der Benutzername eines Administrators bekannt, kann auch versucht werden an das Passwort mit Hilfe eines Brute-Force-Angriffs oder eines Wörterbuchangriffs zu gelangen. Anstatt auf die gespeicherten Messdaten zuzugreifen kann der Angreifer die Messdaten während der Übertragung zwischen DSL-Router des Kunden und dem Discovery Server abhören. Der Datenverkehr kann hierfür an einem Router des Internetproviders (Zugriff auf den Router erforderlich) abgehört werden. Allerdings ist dieser Angriff mit einem höheren Aufwand verbunden.	hoch	mittel

Tabelle 4.1: Bedrohungsanalyse-Abhören einzelner Nutzer<sup>215</sup>

<sup>214</sup>IEEE: Search Results: IEEE Standards OUI Public Database (2012), [131]; Hardware Address (MAC Address) Lookup :: Search by hardware address, [110].

<sup>215</sup>Vgl. Brinkhaus u. a.: Vortrag: Smart Hacking for Smart Privacy (2011), [52]; Armstrong: Analysis of Sony PSN Hack (2011), [45]

Bedrohung Nr.	Beschreibung	Aufwand für Angreifer	Nutzen für Angreifer
B1.4	<p>Abhören der Messdaten (Zählerstände) vieler Nutzer über einen längeren Zeitraum durch einen Nutzer: Eine unautorisierte Einsicht auf gespeicherte Messdaten kann über den Zugriff auf das Discovery Online Portal erfolgen. Hierfür werden die Zugangsdaten der Nutzer benötigt. An diese kann der Angreifer z.B. mit Hilfe von Phishing (Social-Engineering) gelangen. Eine weitere Möglichkeit auf die Messdaten vieler Nutzer zuzugreifen besteht darin, in den Server des Online-Portals durch ausnutzen von Fehlern in nicht aktualisierter Serversoftware z.B. mit Hilfe von Zero-Day-Exploits (Vgl. Armstrong: Analysis of Sony PSN Hack (2011)) einzudringen. Eventuell ist die Login Maske des Online Portals auch anfällig für SQL-Injection, sodass der Angreifer darüber Zugriff erhalten kann. Auch der Zugang über ein Administratorkonto des Servers erscheint denkbar. An die Zugangsdaten des Administrators kann der Angreifer z.B. per Phishing gelangen. Ist ihm der Benutzername eines Administrators bekannt, kann auch versucht werden an das Passwort mit Hilfe eines Brute-Force-Angriffs oder eines Wörterbuchangriffs zu gelangen.</p>	hoch	mittel
B1.5	<p>Abhören der Messdaten (Zählerstände) vieler Nutzer über einen längeren Zeitraum durch den Nachbar: Eine unautorisierte Einsicht auf gespeicherte Messdaten kann über den Zugriff auf das Discovery Online Portal erfolgen. Hierfür werden die Zugangsdaten der Nutzer benötigt. Für eine Beschreibung der möglichen Angriffe siehe B1.4.</p>	hoch	mittel
B1.6	<p>Abhören der Messdaten (Zählerstände) vieler Nutzer über einen längeren Zeitraum durch einen externen Angreifer: Eine unautorisierte Einsicht auf gespeicherte Messdaten kann über den Zugriff auf das Discovery Online Portal erfolgen. Hierfür werden die Zugangsdaten der Nutzer benötigt. Für eine Beschreibung der möglichen Angriffe siehe B1.4. Anstatt auf die gespeicherten Messdaten zuzugreifen, kann der Angreifer die Messdaten während der Übertragung von den Nutzern an die Discovery Server abhören. Der Datenverkehr kann hierfür an einem Router des Internetproviders (Zugriff auf den Router erforderlich) abgehört werden, allerdings ist dieser Angriff mit einem höheren Aufwand verbunden.</p>	hoch	hoch

Tabelle 4.2: Bedrohungsanalyse-Abhören vieler Nutzer

#### 4 Angriffe und Bedrohungsszenarien

Bedrohung Nr.	Beschreibung	Aufwand für Angreifer	Nutzen für Angreifer
B1.7	Manipulation der Messdaten (Zählerstände) eines Nutzers durch den Nutzer selbst: Eine leicht durchführbare Variante des Angriffs besteht darin über einen Man-in-the-middle-Angriff (ARP-Spoofing) die Datenkommunikation bei der Übertragung zwischen dem PLC-Adapter in der Wohnung und dem DSL-Router mit Hilfe eines zwischengeschalteten Hub bzw. Switch mit eingerichtetem Mirror-Port (ohne zusätzliche Hardware mit einem am DSL-Router eingerichteter Mirror-Port, unterstützt allerdings nicht jeder DSL-Router), welcher mit einem PC verbunden wird, abzufangen und anschließend einspielen von mit Hilfe eines Programms veränderter, generierter oder bereits abgehörter Messdaten (Replay-Angriff). Eine Manipulation kann auch bedeuten, dass nur die SM-GW ID (Mac-Adresse) in den Messdaten verändert wird und damit die Verbrauchswerte einem anderen Nutzer zugewiesen werden.	mittel	sehr hoch
B1.8	Manipulation der Messdaten (Zählerstände) eines Nutzers durch seinen Nachbarn: Eine leicht durchführbare Variante des Angriffs besteht darin über einen Man-in-the-middle-Angriff (ARP-Spoofing) die Datenkommunikation bei der Übertragung zwischen dem SM-GW und PLC-Adapter mit Hilfe eines zwischengeschalteten Hub bzw. Switch mit eingerichtetem Mirror-Port, welcher mit einem PC verbunden wird, abzufangen und anschließend einspielen von mit Hilfe eines Programms veränderter, generierter oder bereits abgehörter Messdaten (Replay-Angriff). Eine Manipulation kann auch bedeuten, dass nur die SM-GW ID (Mac-Adresse) in den Messdaten verändert wird. Die Manipulation der Messdaten ist auch bei der Übertragung zwischen Smart Meter und SM-GW (verplombtes Gehäuse, D0-Schnittstelle) und bei der Übertragung zwischen den PLC-Adaptoren (verschlüsselte und signierte Übertragung) möglich, allerdings sind diese Angriffe dann mit einem höheren Aufwand verbunden. Für alle drei Angriffsvarianten ist ein Zugang zum Zählerschrank im Keller des Hauses erforderlich. Ein weiterer Angriff der nur funktioniert, wenn der Nachbar auch Kunde bei Discovery ist, besteht darin die SM-GWs auszutauschen, d.h. der Nachbar montiert sein SM-GW auf, das des Nutzers und umgekehrt. Allerdings müssen dafür die beiden verplombten Gehäuse geöffnet werden. Zusätzlich ist auch die Manipulation der gespeicherten Messdaten (Discovery Online Portal) möglich (siehe B1.9)	mittel	hoch
B1.9	Manipulation der Messdaten (Zählerstände) eines Nutzers über durch einen externen Angreifer: Eine Möglichkeit auf die Messdaten vieler Nutzer zuzugreifen um sie zu manipulieren besteht darin, in den Server des Online-Portals durch Ausnutzen von Fehlern in nicht aktualisierter Serversoftware z.B. mit Hilfe von Zero-Day-Exploits (Vgl. mit Sony PSN Hack) einzudringen. Eventuell ist die Login Maske des Online Portals auch anfällig für SQL-Injection, sodass der Angreifer darüber Zugriff erhalten kann. Auch der Zugang über ein Administratorkonto des Servers erscheint denkbar. An die Zugangsdaten des Administrators kann der Angreifer z.B. per Phishing gelangen. Ist ihm der Benutzername eines Administrators bekannt kann auch versucht werden an das Passwort mit Hilfe eines Brute-Force-Angriff oder eines Wörterbuchangriffs zu gelangen. Der Angreifer kann die Messdaten vieler Nutzer während der Übertragung zwischen DSL-Router der Kunden und dem Discovery Server manipulieren. Hierfür werden die Messdaten an einem Router des Internetproviders abgefangen (Zugriff auf den Router erforderlich) und anschließend veränderte, generierte oder bereits abgehörter Messdaten (Replay-Angriff) eingespielt.	hoch	

Tabelle 4.3: Bedrohungsanalyse-Manipulation von Messdaten einzelner Nutzer

Bedrohung Nr.	Beschreibung	Aufwand für Angreifer	Nutzen für Angreifer
B1.10	Manipulation der Messdaten (Zählerstände) vieler Nutzer durch einen Nutzer: Für eine Beschreibung der möglichen Angriffe siehe B1.9.	hoch	hoch
B1.11	Manipulation der Messdaten (Zählerstände) vieler Nutzer durch den Nachbar: Für eine Beschreibung der möglichen Angriffe siehe B1.9.	hoch	hoch
B1.12	Manipulation der Messdaten (Zählerstände) vieler Nutzer durch einen externen Angreifer: Für eine Beschreibung der möglichen Angriffe siehe B1.9.	hoch	hoch
B1.13	Ein anderer Angriff, der vom Nutzer, Nachbar oder externen Angreifer ausgeführt werden könnte, besteht darin gleichzeitig sehr viele gefälschte Messdaten an den Discovery Server zu übermitteln. Hierfür müssten Messdaten, die unterschiedliche SM-GW IDs (MAC-Adresse, Adressbereich 2C:DD:0C:00:00:00 – 2C:DD:0C:FF:FF:FF) enthalten, generiert werden. Das Ziel des Angriffs ist dabei, dass bei allen Kunden von Discovery fehlerhafte Abrechnungen erstellt werden. (Der Nutzer (als Angreifer) kann mit dem Angriff z. B. das Ziel verfolgen auf die Zahlung seiner Rechnung, mit der Begründung die Messungen seien fehlerhaft, verzichteten zu können, sobald die fehlerhaften Abrechnungen öffentlich werden (Presse)).	mittel	hoch

Tabelle 4.4: Bedrohungsanalyse-Manipulation von Messdaten vieler Nutzer

## 4 Angriffe und Bedrohungsszenarien

Bedrohung Nr.	Beschreibung	Aufwand für Angreifer	Nutzen für Angreifer
B1.14	Übertragung der Messdaten (für Abrechnung relevant) bei einem einzelnen Benutzer verhindern durch den Nutzer selbst: Der Angreifer könnte hierzu die PLC-Adapter aus der Steckdose entfernen oder die Ethernet Verbindung zwischen PLC-Adapter und Router bzw. zwischen SM-GW und PLC-Adapter trennen. Alternativ könnte die Übertragung der Messdaten auch durch entsprechende Einträge in der Firewall des Routers (Weiterleitung von Daten an die IP-Adresse 85.214.93.99) oder durch Anpassung des DHCP-Servers im Router (SM-GW bekommt keine IP-Adresse zugewiesen) unterbunden werden. Eine Störung bei der Übertragung ist auch an der D0-Schnittstelle zwischen Smart Meter und SM-GW möglich, allerdings muss dafür das verplombte Gehäuse geöffnet werden. Die Zerstörung des Smart Meters oder SM-GWs sind zwar auch möglich, die anderen Angriffe sind aber leichter durchführbar.	niedrig	sehr hoch
B1.15	Übertragung der Messdaten (für Abrechnung relevant) bei einem einzelnen Benutzer verhindern durch den Nachbar: Für den Angriff ist ein Zugang zum Zählerschrank im Keller des Hauses erforderlich. Der Angreifer könnte hierzu den PLC-Adapter im Keller aus der Steckdose entfernen oder die Ethernet Verbindung zwischen SM-GW und PLC-Adapter trennen. Eine Störung bei der Übertragung ist auch an der D0-Schnittstelle zwischen Smart Meter und SM-GW möglich, allerdings muss dafür das verplombte Gehäuse geöffnet werden. Die Zerstörung des Smart Meters oder SM-GWs sind zwar auch möglich, die anderen Angriffe sind aber leichter durchführbar.	niedrig	mittel
B1.16	Übertragung der Messdaten (für Abrechnung relevant) bei einem einzelnen Benutzer verhindern durch externen Angreifer: Der Angreifer könnte, falls er Zugriff auf den Router des Nutzers per Fernverwaltung erhält (z.B. Standardpasswort und Benutzername des Routers wurden nicht verändert und sind für alle Router eines bestimmten Modells identisch), die Übertragung der Messdaten durch entsprechende Einträge in der Firewall des Routers (Weiterleitung von Daten an die IP-Adresse 85.214.93.99) oder durch Anpassung des DHCP-Servers im Router (SM-GW bekommt keine IP-Adresse zugewiesen) unterbinden. Eine andere Möglichkeit besteht darin die Messdaten während der Übertragung zwischen DSL-Router des Kunden und dem Discovery Server an einem Router des Internetproviders (Zugriff auf den Router erforderlich) abgefangen.	hoch	niedrig

Tabelle 4.5: Bedrohungsanalyse-Einschränkung der Verfügbarkeit der Abrechnung für einzelne Nutzer

Bedrohung Nr.	Beschreibung	Aufwand für Angreifer	Nutzen für Angreifer
B1.17	Übertragung der Messdaten (für Abrechnung relevant) vieler Nutzer verhindern, durch einzelnen Nutzer mit Hilfe eines Denial-of-Service Angriffs auf den Discovery Server: Verschiedene Arten von DoS-Angriffen sind vorstellbar. Der Nutzer kann wiederholt seine Messdaten in sehr kurzen Abständen an die Discovery Server senden oder eine TCP-SYN-Flood-Attacke durchführen. Eventuell reicht es auch aus Messdaten in bestimmter Weise zu manipulieren (z.B. negativer Zeitstempel), sodass ein Softwarefehler die Serversoftware zum Absturz bringt. Eine andere Variante, welche vorstellbar ist, besteht darin gleichzeitig sehr viele gefälschte Messdaten an den Discovery Server zu übermitteln, um diesen zu überlasten. Hierfür müssten Messdaten die unterschiedliche SM-GW IDs (MAC-Adresse, Adressbereich 2C:DD:0C:00:00:00 – 2C:DD:0C:FF:FF:FF) enthalten generiert werden. Laut Portscan (Abbildung B.7) setzt Discovery einen Apache HTTP Server in Version 2.2.8 unter Linux (Ubuntu) ein. Falls für die Apache Version nicht die neusten Updates installiert sind, besteht die Möglichkeit die unter CVE-2011-3192 verzeichnete Sicherheitslücke für einen DoS-Angriff auszunutzen. Zusätzlich ist der Apache HTTP Server in Version 2.X, falls keine Vorkehrungen getroffen wurden (z. B. Einsatz des Apache Moduls „mod_noloris.c“) eventuell anfällig für einen DoS-Angriff, der mit dem Programm slowloris.pl durchgeführt wird.	hoch	hoch
B1.18	Übertragung der Messdaten (für Abrechnung relevant) vieler Nutzer verhindern durch den Nachbar mit Hilfe eines Denial-of-Service Angriffs auf den Discovery Server. Für eine Beschreibung der möglichen Angriffe siehe B1.17.	hoch	mittel
B1.19	Übertragung der Messdaten (für Abrechnung relevant) vieler Nutzers verhindern durch externen Angreifer, mit Hilfe eines Denial-of-Service Angriffs auf den Discovery Server. Für eine Beschreibung der möglichen Angriffe siehe B1.17.	hoch	hoch

Tabelle 4.6: Bedrohungsanalyse-Einschränkung der Verfügbarkeit der Abrechnung für viele Nutzer<sup>216</sup>

<sup>216</sup> Anm.: Für einen Screenshot des Portscan siehe Abb. B.12, für weitere Informationen zu CVE-2011-3192 siehe <http://www.cvedetails.com/cve/CVE-2011-3192/>; für weitere Informationen zu mod\_noloris.c siehe [http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/experimental/mod\\_noloris.c](http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/experimental/mod_noloris.c); für weitere Informationen und eine Beschreibung der Funktionsweise des Programms slowloris.pl siehe <http://hackers.org/slowloris/>.



#### 4 Angriffe und Bedrohungsszenarien

Bedrohung Nr.	Beschreibung	Aufwand für Angreifer	Nutzen für Angreifer
B1.20	Ausfall oder Störung der Stromversorgung bei einzelnen Nutzern durch den Nutzer: In erster Linie sind hier physikalische Angriffe möglich wie z. B. trennen der Hauptleitung des Nutzers oder auslösen eines Kurzschlusses. Solch ein Angriff unterscheidet sich damit nicht von den Angriffen die auch im heutigen Stromnetz möglich sind. Der Nutzer wird diesen Angriff kaum selbst bei sich durchführen. Ein weitere Angriffsmöglichkeit würde die Fernabschaltfunktion des Smart Meters bieten. Einem Angreifer dem es gelingt diese unautorisiert zu aktivieren, könnte damit eine Trennung der Stromversorgung aus der Ferne durchführen. Das Smart Meter im ausgewählten Szenario unterstützt die Fernabschaltfunktion allerdings nicht.	mittel	niedrig
B1.21	Ausfall oder Störung der Stromversorgung einzelne Nutzer durch den Nachbar: In erster Linie sind hier physikalische Angriffe möglich wie z. B. trennen der Hauptleitung des Nutzers oder auslösen eines Kurzschlusses. Solch ein Angriff unterscheidet sich damit nicht von den Angriffen die auch im heutigen Stromnetz möglich sind. Ein weitere Angriffsmöglichkeit würde die Fernabschaltfunktion des Smart Meters bieten. Einem Angreifer dem es gelingt diese unautorisiert zu aktivieren, könnte damit eine Trennung der Stromversorgung aus der Ferne durchführen. Das Smart Meter im ausgewählten Szenario unterstützt die Fernabschaltfunktion allerdings nicht.	mittel	niedrig
B1.22	Ausfall oder Störung der Stromversorgung bei einzelnen Nutzern durch einen externen Angreifer: In erster Linie sind hier physikalische Angriffe möglich. Der Angreifer benötigt allerdings auch Zugang zum Gebäude in dem der Nutzer wohnt. Dies geschieht z. B. durch unbefugtes Eindringen in Räumlichkeiten. Für eine Beschreibung der möglichen Angriffe siehe B1.21.	hoch	mittel

Tabelle 4.7: Bedrohungsanalyse-Einschränkung der Verfügbarkeit der Stromversorgung für einzelne Nutzer

Bedrohung Nr.	Beschreibung	Aufwand für Angreifer	Nutzen für Angreifer
B1.23	Ausfall oder Störung der Stromversorgung bei vielen Nutzern durch einen Nutzer als Angreifer: Eine Möglichkeit besteht beispielsweise darin eine Übertragungsleitung zu zerstören oder in ein Kraftwerk einzudringen und es abzuschalten. Allerdings ist der erforderliche Aufwand für solche Angriffe als hoch anzusehen. Eine andere Möglichkeit, die auch ohne Smart Grid durchführbar ist, besteht darin in industrielle Steuerungsanlagen einzudringen und mit Hilfe der Steuerung z.B. Umspannwerke zu deaktivieren. Diese Angriffe unterscheiden sich allerdings nicht von den Angriffen die auch auf heutige Stromnetze möglich sind. Ein weitere Angriffsmöglichkeit würde die Fernabschaltfunktion der Smart Meter bieten. Einem Angreifer dem es gelingt diese für mehrere Nutzer unautorisiert zu aktivieren könnte, damit eine Trennung der Stromversorgung aus der Ferne durchführen. Das Smart Meter im ausgewählten Szenario unterstützt die Fernabschaltfunktion allerdings nicht. Bei zukünftigen Smart Grids sollte dieser Angriff allerdings beachtet werden.	sehr hoch	niedrig
B1.24	Ausfall oder Störung der Stromversorgung bei vielen Nutzern durch den Nachbar als Angreifer: Für eine Beschreibung der möglichen Angriffe siehe B1.23.	sehr hoch	niedrig
B1.25	Ausfall oder Störung der Stromversorgung bei vielen Nutzern durch einen externen Angreifer: Für eine Beschreibung der möglichen Angriffe siehe B1.23.	sehr hoch	hoch

Tabelle 4.8: Bedrohungsanalyse-Einschränkung der Verfügbarkeit der Stromversorgung für viele Nutzer<sup>217</sup>

<sup>217</sup> Anm.: Das Ausnutzen der Fernabschaltfunktion wird z. B. im Paper Anderson und Fuloria: Who controls the off switch? (2010), [43] thematisiert; Auf Industrielle Steuerungsanlagen kann eventuell über das Internet zugegriffen werden. Zumindest wird das Webinterface einiger industrieller Steuerungssysteme über Suchmaschinen gefunden (siehe z. B. <http://www.shodanhq.com/search?q=scada>, <http://www.shodanhq.com/search?q=plc> oder <http://www.google.de/search?q=m1e+webserver>). Auch sind Angriffe auf industrielle Steuerungssysteme durch Schadsoftware möglich, wie im Jahr 2010 Stuxnet gezeigt hat (Vgl. Brunner u. a.: Infiltrating critical infrastructures with next-generation attacks (2010), [53]). Einige Wissenschaftler konnte zudem laut CNN einen Generator mit Hilfe einer Cyber-Attacke zerstören (Vgl. Meserve: Sources: Staged cyber attack reveals vulnerability in power grid (2007), [114].)



### 4.2.3 Risikoanalyse

Im Folgenden werden die einzelnen Risiken bestimmt, indem die Eintrittswahrscheinlichkeiten, abgeleitet vom geschätzten Aufwand und Nutzen für den Angreifer, und das Schadensausmaß für die im vorherigem Abschnitt aufgeführten Bedrohungen abgeschätzt werden. Diese Abschätzung erfolgt wie bereits die Bedrohungsanalyse nach bestem Wissen und wird gestützt durch Erfahrungen des Autors aus der Vergangenheit. Zusätzlich fließt eine Prognose für zukünftige Ereignisse mit in die Abschätzung ein. Eine Person mit anderem Vorwissen z. B. ein Entwickler des Smart Meter bzw. SM-GW oder ein Mitarbeiter des Netzbetreibers würde die Risiken eventuell anders einschätzen. Die Einschätzung der Risiken ist zusätzlich auch von der Risikobereitschaft einer Person abhängig. Es zu beachten, dass es sowohl Personen mit höherer Risikobereitschaft, als auch Personen mit niedrigerer Risikobereitschaft (risikoscheue Personen) gibt. Dem Autor ist durchaus die Subjektivität der Risiko-Einschätzung bewusst.<sup>218</sup>

Tabelle 4.9 zeigt die Abschätzung für das Schadensausmaß der Hauptbedrohungen, jeweils aus Sicht des Netzbetreibers bzw. Messstellenbetreibers sowie aus der Sicht des Nutzers bzw. Verbrauchers.

<b>Hauptbedrohung / Hauptschutzzielverletzung</b>	<b>Erwartetes Schadensausmaß</b>	
	<b>Sicht Netzbetreiber/ Messstellenbetreiber</b>	<b>Sicht Nutzer/ Verbraucher</b>
Abhören einzelner Nutzer	unwesentlich	geringfügig
Abhören vieler Nutzer	geringfügig	geringfügig
Entdeckbare Manipulation von Messdaten einzelner/vieler Nutzer	unwesentlich	-
Nicht entdeckbare Manipulation von Messdaten einzelner/vieler Nutzer	kritisch	kritisch
Einschränkung der Verfügbarkeit der Abrechnung für einzelne Nutzer	geringfügig	unwesentlich
Einschränkung der Verfügbarkeit der Abrechnung für viele Nutzer	kritisch	unwesentlich
Einschränkung der Verfügbarkeit der Stromversorgung für einzelne Nutzer	kritisch	kritisch
Einschränkung der Verfügbarkeit der Stromversorgung für viele Nutzer	katastrophal	kritisch

Tabelle 4.9: Normierung des Schadensausmaßes der Hauptbedrohungen / Hauptschutzzielverletzungen<sup>219</sup>

Bei der Normierung des Schadensausmaßes wurden zunächst die Hauptbedrohungen einander gegenübergestellt. Danach wurde gegeneinander abgewogen wie hoch die erwarteten finanziellen Auswirkungen bzw. die Einschränkungen, welche im Schadensfall entstehen, sind. Vor allem bei der Einschränkung der Verfügbarkeit der Stromversorgung wurde berücksichtigt, dass im

<sup>218</sup>Vgl. Königs: IT-Risiko-Management mit System (2009), [23], S. 14f.

<sup>219</sup>Anm.: Einsortierung und Festlegung der Hauptbedrohungen/Hauptschutzzielverletzungen ist in Zusammenarbeit mit Prof. Dr. Joachim Charzinski während einer Besprechung am 16.02.2012 entstanden.

Fälle langandauernder Stromausfälle auch viele anderen Infrastrukturen betroffen wären.<sup>220</sup> Die Unterscheidung von Manipulationen in entdeckbare und nicht entdeckbare Manipulation geht davon aus, dass eine Manipulation an Messdaten stattfinden kann welche nicht entdeckbar ist. Solch eine Manipulation ist als kritisch anzusehen im Vergleich zu einer Manipulation, welche leicht erkannt wird.

In den Tabellen 4.10 bis 4.23 sind die identifizierten Risiken nacheinander aufgeführt. Dabei ist für jedes Risiko eine Nummer, die Bedrohung aus der Bedrohungsanalyse, die Eintrittswahrscheinlichkeit, das erwartete Schadensausmaß und eine kurze Erläuterung aufgetragen.

Als Besonderheit resultiert aus den Bedrohungen B1.7 (Manipulation der Messdaten bei einzelner Nutzer durch den Nutzer als Angreifer) und B1.14 (Einschränkung der Verfügbarkeit der Abrechnung für einzelnen Nutzer durch den Nutzer als Angreifer) kein Risiko für den Nutzer bzw. Verbraucher. Denn eine Manipulation der Messwerte würde ein Nutzer bei sich selbst Nutzen, um die Verbrauchswerte zu verringern und eine Unterbrechung der Übertragung wäre auch zu Gunsten des Nutzers, da ihm die Kosten nicht in Rechnung gestellt werden können.

Im Anschluss der Tabellen folgt eine übersichtliche Darstellung der Risiken in Form von Risikokarten aus Sicht des Netzbetreibers bzw. Messstellenbetreibers (siehe Abb. 4.1) und aus Sicht des Nutzers/Verbrauchers (siehe Abb. 4.2).

---

<sup>220</sup>Vgl. Petermann u. a.: Was bei einem Blackout geschieht (2011), [32].

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R1.1	B1.1	hoch	unwesentlich	Der Angriff wird lokal oder durch Zugriff auf das Discovery Online Portal durchgeführt. Es ist eine hohe Eintrittswahrscheinlichkeit anzunehmen, da der Nutzer mit niedrigem Aufwand bei mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören eines einzelnen Nutzers, ein unwesentlicher Schaden für den Netzbetreiber/Messstellenbetreiber verursacht wird, solange er nicht für einen zusätzlichen Beitrag im Monat die Daten in höherer Auflösung anbietet (Erschleichung von Diensten).
R1.2	B1.1	hoch	geringfügig	Der Angriff wird lokal oder durch Zugriff auf das Discovery Online Portal durchgeführt. Es ist eine hohe Eintrittswahrscheinlichkeit anzunehmen, da der Nutzer mit niedrigem Aufwand bei mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören eines einzelnen Nutzers (z. B. Familienmitglied), nur ein geringfügiger Schaden für den Nutzer zu erwarten ist.
R1.3	B1.2	mittel	unwesentlich	Der Angriff wird lokal ausgeführt, außer der Angreifer greift auf die Daten im Discovery Portal mit Hilfe der Zugangsdaten des Nutzers zu. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit mittlerem Aufwand und zugleich mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören eines einzelnen Nutzers, ein unwesentlicher Schaden (Imageschaden, eventuell Verlust eines Kunden) für den Netzbetreiber/ Messstellenbetreiber verursacht wird.
R1.4	B1.2	mittel	geringfügig	Der Angriff wird lokal ausgeführt, außer der Angreifer greift auf die Daten im Discovery Portal mit Hilfe der Zugangsdaten des Nutzers zu. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit mittlerem Aufwand und zugleich mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören des Nutzers durch seinen Nachbar ein geringfügiger Schaden für den Nutzer zu erwarten ist (Der Nachbar erhält Einblick in die Privatsphäre des Nutzers).

Tabelle 4.10: Risikoanalyse 1, Teil 1

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R1.5	B1.3	niedrig	unwesentlich	Der Angriff wird durch Zugriff auf das Discovery Online Portal durchgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer mit hohem Aufwand bei mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören eines einzelnen Nutzers, ein unwesentlicher Schaden (Imageschaden, eventuell Verlust eines Kunden) für den Netzbetreiber/ Messstellenbetreiber zu erwarten ist.
R1.6	B1.3	niedrig	geringfügig	Der Angriff wird durch Zugriff auf das Discovery Online Portal durchgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer mit hohem Aufwand bei mittlerem Nutzen Zugriff erhält. (Informationen werden genutzt um einen Einbruch beim Nutzer durchzuführen). Es ist davon auszugehen, dass durch das Abhören eines einzelnen Nutzers (Einblick in die Privatsphäre) ein geringfügiger Schaden für den Nutzer zu erwarten ist.
R1.7	B1.4	niedrig	geringfügig	Der Angriff wird durch Zugriff auf das Discovery Online Portal durchgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer mit hohem Aufwand bei mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören vieler Nutzer, ein geringfügiger Schaden (Imageschaden, eventuell Verlust von einigen Kunden) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.8	B1.4	niedrig	geringfügig	Der Angriff wird durch Zugriff auf das Discovery Online Portal durchgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer mit hohem Aufwand bei mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören vieler Nutzer, ein geringfügiger Schaden für den Nutzer zu erwarten ist. Es wird weiter angenommen, dass es für einen Nutzer/Verbraucher als weniger schwerwiegend empfunden wird, wenn viele Nutzer betroffen sind, als wenn er der einzige betroffene ist.

Tabelle 4.11: Risikoanalyse 1, Teil 2

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R1.9	B1.5	niedrig	geringfügig	Der Angriff wird durch Zugriff auf das Discovery Online Portal durchgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer mit hohem Aufwand bei mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören vieler Nutzer, ein geringfügiger Schaden (Imageschaden, eventuell Verlust von einigen Kunden) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.10	B1.5	niedrig	geringfügig	Der Angriff wird durch Zugriff auf das Discovery Online Portal durchgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer mit hohem Aufwand bei mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören vieler Nutzer, ein geringfügiger Schaden für den Nutzer entsteht. Es wird weiter angenommen, dass es für einen Nutzer/Verbraucher als weniger schwerwiegend empfunden wird, wenn viele Nutzer betroffen sind als wenn er der einzige betroffene ist.
R1.11	B1.6	mittel	geringfügig	Der Angriff wird durch Zugriff auf das Discovery Online Portal durchgeführt. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer mit hohem Aufwand bei hohem Nutzen Zugriff erhält. Der Angreifer kann die Informationen nutzen, um Einbrüche durchzuführen, wenn sich keine Person vor Ort (Wohnung/Haus) befindet. Es ist davon auszugehen, dass durch das Abhören vieler Nutzer, ein geringfügiger Schaden (Imageschaden, eventuell Verlust von einigen Kunden) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.12	B1.6	mittel	geringfügig	Der Angriff wird durch Zugriff auf das Discovery Online Portal durchgeführt. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer mit hohem Aufwand bei hohem Nutzen Zugriff erhält. Der Angreifer kann die Informationen nutzen um Einbrüche durchzuführen wenn sich keine Person vor Ort (Wohnung/Haus) befindet. Es ist davon auszugehen, dass durch das Abhören vieler Nutzer, ein geringfügiger Schaden für den Nutzer/Verbraucher zu erwarten ist.

Tabelle 4.12: Risikoanalyse 1, Teil 3

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R1.13	B1.7	sehr hoch	unwesentlich	Der Angriff wird lokal durchgeführt. Es ist eine sehr hohe Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit mittlerem Aufwand, bei zu gleich sehr hohem Nutzen (Abrechnungsbetrug wird ermöglicht), durchführen kann. Ist die Manipulation der Messdaten durch den Nutzer vom Netzbetreiber/Messstellenbetreiber entdeckbar, wird davon ausgegangen, dass ein unwesentlicher Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.14	B1.7	sehr hoch	kritisch	Der Angriff wird lokal durchgeführt. Es ist eine sehr hohe Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit mittlerem Aufwand, bei zu gleich sehr hohem Nutzen (Abrechnungsbetrug wird ermöglicht), durchführen kann. Ist die Manipulation der Messdaten durch den Nutzer vom Netzbetreiber/ Messstellenbetreiber nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.15	B1.8	hoch	unwesentlich	Der Angriff wird lokal durchgeführt. Es ist eine hohe Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit mittlerem Aufwand, bei zu gleich hohem Nutzen durchführen kann. Ist die Manipulation der Messdaten durch den Nachbar vom Netzbetreiber/Messstellenbetreiber entdeckbar, wird davon ausgegangen, dass ein unwesentlicher Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.16	B1.8	hoch	kritisch	Der Angriff wird lokal durchgeführt. Es ist eine hohe Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit mittlerem Aufwand, bei zu gleich hohem Nutzen durchführen kann. Ist die Manipulation der Messdaten durch den Nachbar vom Netzbetreiber/Messstellenbetreiber nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.

Tabelle 4.13: Risikoanalyse 1, Teil 4

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R1.17	B1.8	hoch	kritisch	Der Angriff wird lokal durchgeführt. Es ist eine hohe Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit mittlerem Aufwand, bei zu gleich hohem Nutzen durchführen kann. Ist die Manipulation der Messdaten durch den Nachbar vom Nutzer/Verbraucher nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.
R1.18	B1.9	niedrig	unwesentlich	Der Angriff wird durch Zugriff auf den Discovery Server durchgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit hohem Aufwand, bei zu gleich mittlerem Nutzen durchführen kann. Ist die Manipulation der Messdaten durch einen externen Angreifer vom Netzbetreiber/Messstellenbetreiber entdeckbar, wird davon ausgegangen, dass ein unwesentlicher Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.19	B1.9	niedrig	kritisch	Der Angriff wird durch Zugriff auf den Discovery Server durchgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit hohem Aufwand, bei zu gleich mittlerem Nutzen durchführen kann. Ist die Manipulation der Messdaten durch einen externen Angreifer vom Netzbetreiber/Messstellenbetreiber nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.20	B1.9	niedrig	kritisch	Der Angriff wird durch Zugriff auf den Discovery Server durchgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit hohem Aufwand, bei zu gleich mittlerem Nutzen durchführen kann. Ist die Manipulation der Messdaten durch einen externen Angreifer vom Nutzer/Verbraucher nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.

Tabelle 4.14: Risikoanalyse 1, Teil 5

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R1.21	B1.10	mittel	unwesentlich	Der Angriff wird durch Zugriff auf den Discovery Server durchgeführt. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten → keine Zahlung). Ist die Manipulation der Messdaten durch einen Nutzer vom Netzbetreiber/Messstellenbetreiber entdeckbar, wird davon ausgegangen, dass ein unwesentlicher Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.22	B1.10	mittel	kritisch	Der Angriff wird durch Zugriff auf den Discovery Server durchgeführt. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten → keine Zahlung). Ist die Manipulation der Messdaten durch einen Nutzer vom Netzbetreiber/Messstellenbetreiber nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.23	B1.10	mittel	kritisch	Der Angriff wird durch Zugriff auf den Discovery Server durchgeführt. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten → keine Zahlung). Ist die Manipulation der Messdaten durch einen Nutzer vom Nutzer/Verbraucher nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.
R1.24	B1.11	mittel	unwesentlich	Der Angriff wird durch Zugriff auf den Discovery Server durchgeführt. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzer). Ist die Manipulation der Messdaten durch den Nachbar vom Netzbetreiber/Messstellenbetreiber entdeckbar, wird davon ausgegangen, dass ein unwesentlicher Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.

Tabelle 4.15: Risikoanalyse 1, Teil 6



Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R1.25	B1.11	mittel	kritisch	Der Angriff wird durch Zugriff auf den Discovery Server durchgeführt. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzer). Ist die Manipulation der Messdaten durch den Nachbar vom Netzbetreiber/Messstellenbetreiber nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.26	B1.11	mittel	kritisch	Der Angriff wird durch Zugriff auf den Discovery Server durchgeführt. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzer). Ist die Manipulation der Messdaten durch den Nachbar vom Nutzer/Verbraucher nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.
R1.27	B1.12	mittel	unwesentlich	Der Angriff wird durch Zugriff auf den Discovery Server durchgeführt. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzer → Erpressung). Ist die Manipulation der Messdaten durch einen externen Angreifer vom Netzbetreiber /Messstellenbetreiber entdeckbar, wird davon ausgegangen, dass ein unwesentlicher Schaden für den Netzbetreiber /Messstellenbetreiber zu erwarten ist.
R1.28	B1.12	mittel	kritisch	Der Angriff wird durch Zugriff auf den Discovery Server durchgeführt. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzern → Erpressung). Ist die Manipulation der Messdaten durch einen externen Angreifer vom Netzbetreiber /Messstellenbetreiber nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Netzbetreiber /Messstellenbetreiber zu erwarten ist.

Tabelle 4.16: Risikoanalyse 1, Teil 7

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R1.29	B1.12	mittel	kritisch	Der Angriff wird durch Zugriff auf den Discovery Server durchgeführt. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzern → Erpressung). Ist die Manipulation der Messdaten durch einen externen Angreifer vom Nutzer /Verbraucher nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Nutzer/ Verbraucher zu erwarten ist.
R1.30	B1.13	hoch	unwesentlich	Der Angriff wird durch Zugriff auf den Discovery Server durchgeführt. Für diesen Angriff ist eine hohe Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer gefälschte Messdaten mit mittlerem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzern → Erpressung). Ist die Manipulation der Messdaten vom Netzbetreiber /Messstellenbetreiber entdeckbar, wird davon ausgegangen, dass ein unwesentlicher Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.31	B1.13	hoch	kritisch	Bei diesem Angriff werden generierte Messdaten an den Discovery Server übermittelt. Für diesen Angriff ist eine hohe Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer gefälschte Messdaten mit mittlerem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzern → Erpressung). Ist die Manipulation der Messdaten vom Netzbetreiber/Messstellenbetreiber nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.

Tabelle 4.17: Risikoanalyse 1, Teil 8

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R1.32	B1.13	hoch	kritisch	Bei diesem Angriff werden generierte Messdaten an den Discovery Server übermittelt. Für diesen Angriff ist eine hohe Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer gefälschte Messdaten mit mittlerem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzern → Erpressung). Ist die Manipulation der Messdaten nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Nutzer/ Verbraucher zu erwarten ist.
R1.33	B1.14	sehr hoch	geringfügig	Der Angriff wird lokal durchgeführt. Es ist eine sehr hohe Eintrittswahrscheinlichkeit anzunehmen, da der Nutzer mit niedrigem Aufwand bei sehr hohem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten eines einzelnen Nutzers, ein geringfügiger Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.34	B1.15	hoch	geringfügig	Der Angriff wird lokal durchgeführt. Es ist eine hohe Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit niedrigem Aufwand bei mittlerem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten eines einzelnen Nutzers, ein geringfügiger Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.35	B1.15	hoch	unwesentlich	Der Angriff wird lokal durchgeführt. Es ist eine hohe Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit niedrigem Aufwand bei mittlerem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten, ein unwesentlicher Schaden für den Nutzer/Verbraucher zu erwarten ist.

Tabelle 4.18: Risikoanalyse 1, Teil 9

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R1.36	B1.16	niedrig	geringfügig	Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein externer Angreifer mit hohem Aufwand (Zugriff auf den DSL-Router von Nutzer oder Router im Internet) bei niedrigem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten eines einzelnen Nutzers ein geringfügiger Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.37	B1.16	niedrig	unwesentlich	Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein externer Angreifer mit hohem Aufwand (Zugriff auf den DSL-Router von Nutzer oder Router im Internet) bei niedrigem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten eines einzelnen Nutzers ein unwesentlicher Schaden für den Nutzer/Verbraucher zu erwarten ist.
R1.38	B1.17	mittel	kritisch	Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Nutzer mit hohem Aufwand bei hohem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten vieler Nutzer ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.39	B1.17	mittel	unwesentlich	Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Nutzer mit hohem Aufwand bei hohem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten vieler Nutzer ein unwesentlicher Schaden für den Nutzer/Verbraucher zu erwarten ist.

Tabelle 4.19: Risikoanalyse 1, Teil 10

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R1.40	B1.18	niedrig	kritisch	Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit hohem Aufwand bei mittlerem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten vieler Nutzer ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.41	B1.18	niedrig	unwesentlich	Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit hohem Aufwand bei mittlerem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten vieler Nutzer ein unwesentlicher Schaden für den Nutzer/Verbraucher zu erwarten ist.
R1.42	B1.19	mittel	kritisch	Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da der externe Angreifer mit hohem Aufwand bei mittlerem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten vieler Nutzer ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.43	B1.19	mittel	unwesentlich	Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da der externe Angreifer mit hohem Aufwand bei mittlerem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten vieler Nutzer ein unwesentlicher Schaden für den Nutzer/Verbraucher zu erwarten ist.

Tabelle 4.20: Risikoanalyse 1, Teil 11

<b>Risiko Nr.</b>	<b>Bedrohung</b>	<b>Eintrittswahrscheinlichkeit</b>	<b>Schadensausmaß</b>	<b>Bemerkung</b>
R1.44	B1.20	niedrig	kritisch	Der Angriff wird lokal ausgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Nutzer mit mittlerem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem einzelnen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung ein kritischer Schaden (Imageschaden, Verlust von Kunden) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.45	B1.20	niedrig	kritisch	Der Angriff wird lokal ausgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Nutzer mit mittlerem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem einzelnen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung, ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.
R1.46	B1.21	niedrig	kritisch	Der Angriff wird lokal ausgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit mittlerem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem einzelnen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung ein kritischer Schaden (Imageschaden, Verlust von Kunden) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.47	B1.21	niedrig	kritisch	Der Angriff wird lokal ausgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit mittlerem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem einzelnen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.

Tabelle 4.21: Risikoanalyse 1, Teil 12

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R1.48	B1.22	niedrig	kritisch	Der Angriff wird lokal ausgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein externer Angreifer mit hohem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem einzelnen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung ein kritischer Schaden (Imageschaden, Verlust von Kunden) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.49	B1.22	niedrig	kritisch	Der Angriff wird lokal ausgeführt. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein externer Angreifer mit hohem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem einzelnen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.
R1.50	B1.23	niedrig	katastrophal	Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Nutzer mit sehr hohem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem vielen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung vieler Nutzer ein katastrophaler Schaden (Image-schaden, Verlust von Kunden, Regressansprüche) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.51	B1.23	niedrig	kritisch	Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Nutzer mit sehr hohem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem vielen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung vieler Nutzer ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.

Tabelle 4.22: Risikoanalyse 1, Teil 13

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R1.52	B1.24	niedrig	katastrophal	Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit sehr hohem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem vielen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung vieler Nutzer ein katastrophaler Schaden (Image-schaden, Verlust von Kunden, Regressansprüche) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.53	B1.24	niedrig	kritisch	Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit sehr hohem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem vielen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung vieler Nutzer ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.
R1.54	B1.25	niedrig	katastrophal	Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein externer Angreifer mit sehr hohem Aufwand bei hohem Nutzen den Ausfall oder Störung der Stromversorgung bei einem vielen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung vieler Nutzer ein katastrophaler Schaden (Imageschaden, Verlust von Kunden, Regressansprüche) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R1.55	B1.25	niedrig	kritisch	Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein externer Angreifer mit sehr hohem Aufwand bei hohem Nutzen den Ausfall oder Störung der Stromversorgung bei einem vielen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung vieler Nutzer ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.

Tabelle 4.23: Risikoanalyse 1, Teil 14



Abbildung 4.1 zeigt eine übersichtliche Darstellung der identifizierten Risiken aus Sicht des Netzbetreibers bzw. Messstellenbetreibers.<sup>221</sup> Im inakzeptablen Bereich und im ALARP-Bereich befinden sich Risiken bei denen es um die Manipulation von Messdaten (R1.13/B1.7, R1.14/B1.7\*, R1.16/B1.8\*, R1.22/B1.10\*, R1.25/B1.11\*, R1.28/B1.12\*, R1.31/B1.13\*), die Verfügbarkeit von Abrechnungsdaten (R1.33/B1.14, R1.34/B1.15, R1.38/B1.17, R1.42/B1.19) und die Verfügbarkeit der Stromversorgung (R1.50/B1.23, R1.52/B1.24, R1.54/B1.25) geht. Alle weiteren Risiken liegen im akzeptablen Bereich.

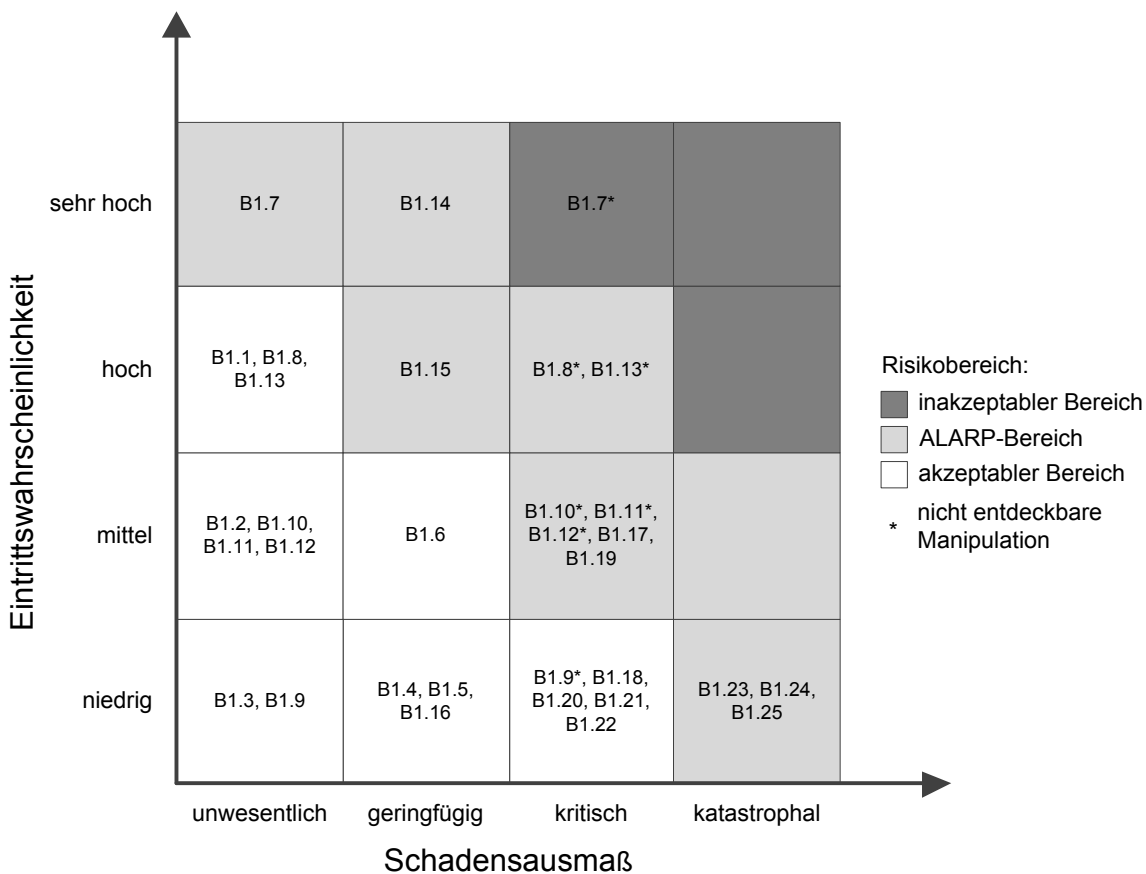


Abbildung 4.1: Risikokarte aus Sicht des Netzbetreibers/Messstellenbetreibers

<sup>221</sup>Für eine Erklärung des Aufbaus der Risikokarte siehe Abschnitt 3.5.

Die Risikokarte in [Abbildung 4.2](#) zeigt die identifizierten Risiken aus Sicht des Nutzers bzw. Verbrauchers. Im ALARP-Bereich befinden sich Risiken bei denen es um das Abhören der Messdaten (R1.2/B1.1) sowie um die Manipulation von Messdaten (R1.17/B1.8\*, R1.23/B1.10\*, R1.26/B1.11\*, R1.29/B1.12\*, R1.32/B1.13\*) geht.

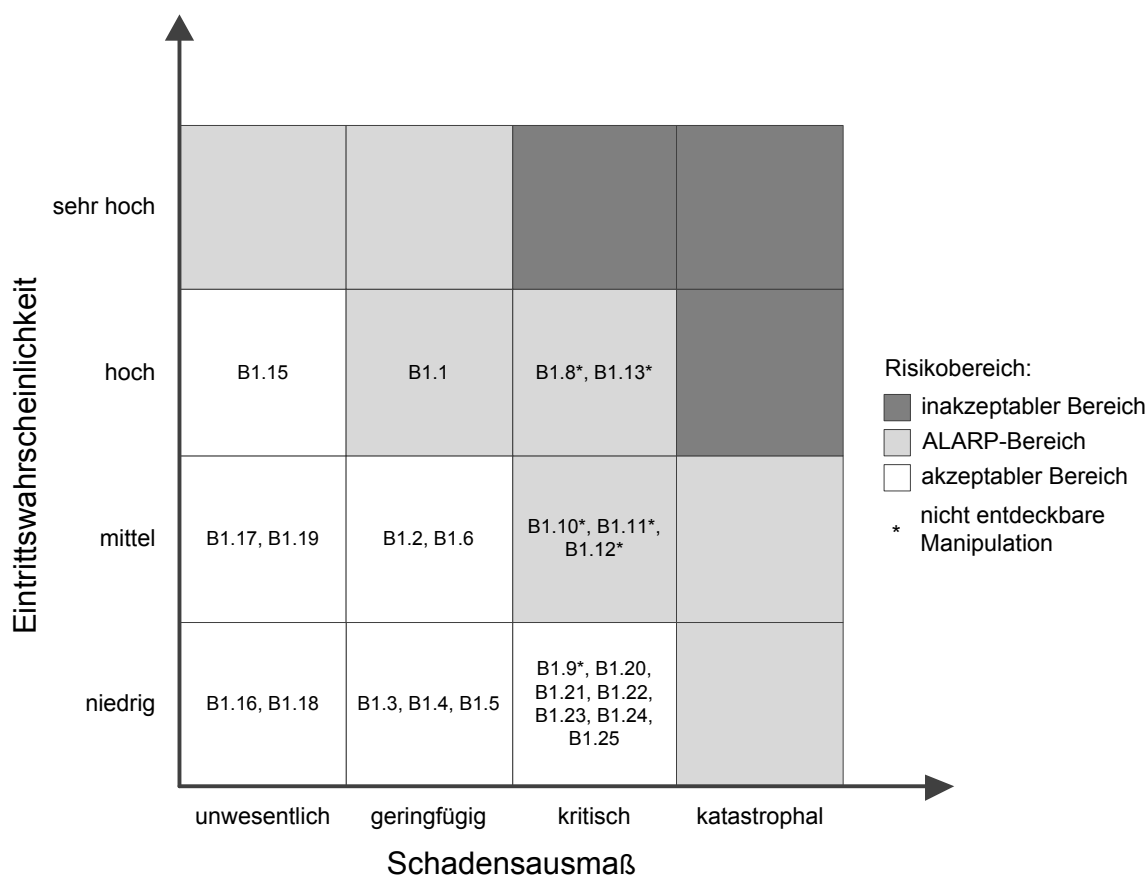


Abbildung 4.2: Risikokarte aus Sicht des Nutzers/Verbrauchers

#### 4.2.4 Maßnahmen

Die festgestellten Risiken für das Szenario können mit unterschiedlichen Maßnahmen behandelt werden, sodass die Schutzziele erreicht werden. Die Maßnahmen sollen dabei die Eintrittswahrscheinlichkeit, das Schadensausmaß oder beide Kriterien reduzieren. In den Tabellen [4.3](#) und [4.4](#) werden Maßnahmen aufgezeigt, welche sich aus der Bedrohungs- und Risikoanalyse ableiten. Maßnahmen, die auf Seite des Netzbetreibers bzw. Messstellenbetreibers durchgeführt werden, haben Auswirkungen auf die Risiken aus Sicht des Verbrauchers und umgekehrt. Tabelle [4.3](#) zeigt die vom Netzbetreiber bzw. Messstellenbetreiber zu treffenden Maßnahmen, wohingegen in Tabelle [4.4](#) die vom Verbraucher bzw. Nutzer durchzuführenden Maßnahmen aufgezeigt werden. Im Anschluss an die Tabellen erfolgt jeweils eine Beschreibung der einzelnen Maßnahmen.

Maßnahmen Nr.	Maßnahme
M1.1	Integritätsschutz der Messdaten
M1.2	Übertragung der Abrechnungsdaten per GPRS
M1.3	Integration der PLC Funktionalität in das SM-GW
M1.4	Einsatz einer Firewall
M1.5	Einsatz mehrerer Server zur Serverlastverteilung
M1.6	Vorhalten von Reservekraftwerken
M1.7	Industrielle Steuerungssysteme vom Internet trennen
M1.8	Verschlüsselung und Authentifizierung der Kommunikation zwischen Online Portal und Browser
M1.9	Verschlüsselung der Messdaten
M1.10	Zugang nach mehrmaliger Falscheingabe des Passworts für bestimmte Zeit sperren
M1.11	Sensibilisierung der Mitarbeiter/Kunden
M1.12	Passwortrichtlinie für Benutzer und Administratoren festlegen
M1.13	Zwei-Faktor-Authentifizierung für Administratorzugänge
M1.14	Webserver sicher konfigurieren
M1.15	Regelmäßige Aktualisierung der eingesetzten Server Software
M1.16	Schutz gegen SQL-Injection

Abbildung 4.3: Übersicht Maßnahmen Netzbetreibers/Messstellenbetreiber

### M1.1 Integritätsschutz der Messdaten

In der Risikoanalyse wurde festgestellt, dass viele der Risiken mit der Manipulation von Messdaten zusammenhängen. Um eine Manipulation als solche zu erkennen und damit eine Sicherstellung der Integrität zu erzielen werden Message Authentication Codes (MAC)<sup>222</sup> verwendet. Als Maßnahme sollte der Netzbetreiber einen solchen Integritätsschutz bei der Datenübertragung verwenden. Der Integritätsschutz sollte durchgehend vom Smart Meter über das **SM-GW** bis zum Discovery Server gewährleistet sein. Discovery verwendet bisher das unverschlüsselte HTTP-Protokoll. Stattdessen soll das Hypertext Transfer Protocol Secure (HTTPS)<sup>223</sup> in Verbindung mit dem Transportprotokoll Transport Layer Security (TLS)<sup>224</sup>, das kryptographische Mechanismen zur Gewährleistung von Integrität, aber auch zur Gewährleistung von Vertraulichkeit und Authentizität übertragener Daten nutzt, eingesetzt werden. Innerhalb von TLS sollte als Integritätsschutz der Secure Hash Algorithm (SHA)<sup>225</sup> mit mindestens 256 Bit langem Hashwert zum Einsatz kommen.

### M1.2 Übertragung der Abrechnungsdaten per GPRS

Falls die Messdaten, welche für die Abrechnung benötigt werden, über einen längere Zeitraum (einen Monat) nicht übertragen werden können, sollten das Reservesystem des **SM-GW** genutzt und die abrechnungsrelevanten Daten per GPRS übermittelt werden.

<sup>222</sup>Anm.: Eine Hashfunktion, die bei der Berechnung der Prüfsumme einen geheimen Schlüssel mit einbezieht. Für eine weitere Erklärung siehe Eckert: IT-Sicherheit (2012), [12], S. 387.

<sup>223</sup>Siehe Rescorla: RFC 2818 (2000), [156].

<sup>224</sup>Siehe Dierks und Allen: RFC 2246 (1999), [144].

<sup>225</sup>Siehe NIST: FIPS PUB 180-2 (2002), [171]; Eckert: IT-Sicherheit (2012), [12], S. 382ff.

### **M1.3 Integration der PLC Funktionalität in das SM-GW**

Eine Maßnahme, um die Übertragung der Abrechnungsdaten durch ein einfaches ausstecken des PLC-Adapters im Zählerschrank zu verhindern, besteht darin, die PLC Funktionalität in das SM-GW zu integrieren.

### **M1.4 Einsatz einer Firewall**

Um DoS-Angriffe auf den Webserver mittels TCP-SYN-Flooding und damit die Speicherung der für die Abrechnung relevanten Messdaten zu verhindern, soll eine Firewall eingesetzt und so konfiguriert werden, dass SYN-Flooding vereitelt wird.

### **M1.5 Einsatz mehrerer Server zur Serverlastverteilung**

Als weitere Maßnahme gegen DoS Angriffe sollen mehrere Server eingesetzt werden und die Serverlast auf diese per Serverlastverteilung aufgeteilt werden.

### **M1.6 Vorhalten von Reservekraftwerken**

Um das Risiko zu minimieren, dass es zu einem Stromausfall kommt, auf Grund des Ausfalls eines einzelnen Kraftwerks (ungewollt oder von einem Angreifer abgeschaltet), sollen Reservekraftwerke vorgehalten werden.

### **M1.7 Industrielle Steuerungssysteme vom Internet trennen**

Industrielle Steuerungssysteme sollen nicht über das öffentliche Internet erreichbar sein.

### **M1.8 Verschlüsselung und Authentifizierung der Kommunikation zwischen Online Portal und Browser**

Beim Zugriff auf das Discovery Online Portal sollen die Daten abhörsicher übertragen werden. Hierfür soll HTTPS in Verbindung mit TLS eingesetzt werden. TLS verwendet sogenannte Cipher Suites, in denen kryptografische Algorithmen, die zusammen verwendet werden, definiert sind. Die Server sind so zu konfigurieren, dass nur Cipher Suites die starke kryptografische Verfahren einsetzen (z. B. TLS\_RSA<sup>226</sup>\_WITH\_AES\_128\_CBC<sup>227</sup>\_SHA256)<sup>228</sup> unterstützt werden. Serverseitig ist ein Digitales Zertifikat für die URL <https://www.discovery.com> auszustellen.<sup>229</sup>

### **M1.9 Verschlüsselung der Messdaten**

Aus der Risikoanalyse geht hervor, dass das Abhören von Messdaten nicht mit einem hohen Risiko einhergeht. Allerdings hat dies auch mit der Normierung des Schadensmaßes bei der

<sup>226</sup>Siehe RSA Laboratories: PKCS #1 v2.1: RSA Cryptography Standard (2002), [155].

<sup>227</sup>Anm.: Cipher Block Chaining Mode (CBC), siehe Eckert: IT-Sicherheit (2012), [12], S. 329f.

<sup>228</sup>Anm.: Cipher Suite, welche RSA für den Schlüsselaustausch, AES mit 128 Bit Schlüsseln im CBC-Modus für die Verschlüsselung und SHA 256 Bit langem Hashwert für den Integritätsschutz verwendet.

<sup>229</sup>Anm.: Das bisher von Discovery verwendete Zertifikat wurde für [\\*.discovery.com](https://www.discovery.com) ausgestellt; vgl. Brinkhaus u. a.: Vortrag: Smart Hacking for Smart Privacy (2011), [52], S. 23; Abb. B.9; Abb. B.10; Abb. B.11.

Gegenüberstellung zu tun. Laut Einschätzung des Autors sollte in Hinblick auf den Personenbezug der Messdaten und den Einblick den diese in die Privatsphäre erlauben, Maßnahmen gegen das Abhören umgesetzt werden. Durch Verschlüsselung der Messdaten kann die Vertraulichkeit der Messdaten gewährleistet und das Abhören verhindert werden. In der Maßnahme M1.1 wurde TLS als Protokoll angesprochen, dieses soll auch für die Verschlüsselung verwendet werden. Als Verschlüsselungsverfahren für übertragene Messdaten sollte das symmetrische Verschlüsselungsverfahren AES mit mindestens 128-Bit langen Schlüsseln im CBC-Modus eingesetzt werden. Zur gegenseitigen Authentifizierung sollen Smart Meter, **SM-GW** und der Discovery Server jeweils Zertifikate einsetzen. Für den Schlüsselaustausch wird der geheime symmetrische Schlüssel mit Hilfe eines öffentlichen RSA-Schlüssels des Discovery Servers verschlüsselt. Zu diesem Zweck ist der RSA-Schlüssel über ein digitales Zertifikat<sup>230</sup> zur Verfügung zu stellen. Die beim RSA-Verfahren verwendeten Schlüssel sollen mindestens 2.048 Bit lang sein. Innerhalb der zuvor genannten kryptographischen Verfahren werden z. B. zur Erzeugung von Schlüsseln Zufallszahlen benötigt. Diese werden mit Hilfe von Zufallszahlengeneratoren erzeugt. Je nach Implementierung können diese unterschiedlich zufällige Zahlen generieren, wodurch die Sicherheit der Verschlüsselung eingeschränkt sein kann. Deshalb soll ein sicherer Zufallszahlengenerator (z. B. K4-Generator<sup>231</sup>) eingesetzt werden.<sup>232</sup> Außerdem ist zu beachten, dass eine sichere Implementierung von TLS verwendet wird.<sup>233,234</sup>

### **M1.10 Zugang nach mehrmaliger Falscheingabe des Passworts für bestimmte Zeitsperren**

Um Brute-Force-Angriffe oder Wörterbuchangriffe zu erschweren, sollte der Zugang zum Online Portal nach mehrmaliger Falscheingabe z. B. fünf mal hintereinander für eine bestimmte Zeit gesperrt werden.

### **M1.11 Sensibilisierung der Mitarbeiter/Kunden**

Social Engineering Angriffe können durch eine Sensibilisierung erschwert werden. Hierzu müssen die Mitarbeiter geschult und die Kunden darauf hingewiesen werden, dass Sie in E-Mails niemals zur Passworteingabe aufgefordert werden.

---

<sup>230</sup> **Anm.:** Das Zertifikat enthält den öffentlichen Schlüssel des Servers; benötigt eine Public-Key-Infrastruktur, siehe Eckert: IT-Sicherheit (2012), [12], S. 409-422.

<sup>231</sup> Vgl. BSI: AIS20, Version 1 (1999), [162].

<sup>232</sup> Vgl. BNetzA: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) (2011), [90]; BSI: BSI TR-02102 (2008), [163].

<sup>233</sup> **Anm.:** Vor allem bei Verwendung eines Debian basierten Linux Servers ist zu prüfen, dass nicht eine Version 0.9.8c-1 bis 0.9.8g-9 von OpenSSL zum Einsatz kommt, bei der durch einen Fehler im Zufallszahlengenerator vorhersagbare Schlüssel erstellt wurden. Siehe <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0166> für weitere Informationen.

<sup>234</sup> **Anm.:** Eine genaue Erklärung der hier angesprochenen Verfahren würde den Rahmen dieser Arbeit sprengen in Eckert: IT-Sicherheit (2012), [12], werden die Begriffe genauer erläutert.

### **M1.12 Passwortrichtlinie für Benutzer und Administratoren festlegen**

Eine sichere Passwortrichtlinie ist zu konfigurieren. Diese soll eine minimale Kennwortlänge von acht Zeichen aufweisen. Als zusätzliche Komplexitätsvoraussetzung soll das Passwort aus alphanumerischen Zeichen mit Groß- und Kleinschreibung bestehen.

### **M1.13 Zwei-Faktor-Authentifizierung für Administratorzugänge**

Als Schutz des Discovery Server Administratorzugangs soll eine zusätzliche Authentifizierungsmethode neben dem Passwort (z.B. Smart Card oder TAN-Generator) verwendet werden.

### **M1.14 Webserver sicher konfigurieren**

Der eingesetzte Webserver ist sicher zu konfigurieren. Zusätzlich sollen Module eingesetzt werden, die Attacken wie Slowloris verhindern können (z.B. mod\_noloris).

### **M1.15 Regelmäßige Aktualisierung der eingesetzten Server Software**

Angreifer können Schwachstellen in Software-Produkten ausnutzen, um in Systeme einzudringen. Die Softwarehersteller veröffentlichen regelmäßig Patches oder Updates, die solche Schwachstellen beheben. Als Maßnahme dagegen, dass Schwachstellen in Software dazu genutzt werden in Systeme einzudringen, sollten veröffentlichte Aktualisierungen möglichst zeitnah eingespielt werden.

### **M1.16 Schutz gegen SQL-Injection**

Als Schutz gegen SQL-Injection ist eine Trennung des SQL-Interpreter und der Benutzereingabe vorzunehmen. Hierfür kann auf die Verwendung von Prepared Statements, bei denen die Benutzereingaben an vorgefertigte Anweisungen übergeben werden, zurückgegriffen werden.

Maßnahmen Nr.	Maßnahme
M1.17	Verschluss des Zählerschranks
M1.18	Lokale Ersatzstromversorgung
M1.19	Wechsel des Netzbetreiber/Messstellenbetreiber zu einem Anbieter, der einen Integritätsschutz der Messdaten vorsieht
M1.20	Wahl „sicherer“ Passwörter
M1.21	Sicherer Umgang mit E-Mails
M1.22	Einsatz von Schadsoftware-Schutzprogrammen
M1.23	Zeitnahe Aktualisierung der eingesetzten Software
M1.24	Arbeiten mit eingeschränkten Rechten
M1.25	Absicherung des WLAN

Abbildung 4.4: Übersicht Maßnahmen Nutzer/Verbraucher

### **M1.17 Verschluss des Zählerschranks**

Eine für den Verbraucher einfach umsetzbare Maßnahme, stellt die Ausstattung des Zählerschranks mit einem Türschloss dar. Der Zählerschrank wird abgeschlossen und der Schlüssel bei einer vertrauenswürdigen Person z. B. beim Hausverwalter deponiert. Alternativ besteht die Möglichkeit pro Wohnpartei einen separaten und abschließbaren Zählerschrank zu installieren. Allerdings ist dies mit höheren Kosten verbunden als ein Zählerschrank für das gesamte Mehrfamilienhaus. Das Risiko, dass Messdaten manipuliert (R1.17) bzw. abgehört werden (R1.4) oder die Übertragung der Abrechnungsdaten verhindert wird (R1.35) reduziert sich, da sich der Aufwand für den Nachbar als Angreifer erhöht sobald er keinen Zugriff auf das Smart Meter und das **SM-GW** im Zählerschrank hat.<sup>235</sup>

### **M1.18 Lokale Ersatzstromversorgung**

Das Risiko eines Ausfalls oder Störung der Stromversorgung (R1.44-R1.55) kann eventuell durch eine lokale Ersatzstromversorgung minimiert werden. Hierfür kann eine dezentrale Energieerzeugungsanlage, z. B. Miniblockheizkraftwerk oder eine Photovoltaikanlage, in Kombination mit einem Energiespeicher dienen.

### **M1.19 Wechsel des Netzbetreiber/Messstellenbetreiber zu einem Anbieter, der einen Integritätsschutz der Messdaten vorsieht**

Für den Verbraucher besteht das Risiko, dass die an Discovery übermittelten Messdaten von einem Angreifer manipuliert werden. Der Verbraucher kann als einfache Maßnahme zu einem anderen Netzbetreiber/Messstellenbetreiber wechseln, der einen Integritätsschutz für die Messdaten vorsieht. Allerdings beträgt die Mindestvertragslaufzeit zwei Jahre<sup>236</sup>, sodass erst mit Ablauf der Frist ein Wechsel zu einem anderen Messstellenbetreiber möglich ist.

<sup>235</sup>Vgl. BSI: IT-Grundschutz-Kataloge: 12. EL Stand 2011 (2011), [91], S. 1331.

<sup>236</sup>Vgl. Discovery : FAQ, [103].

Weitere Maßnahmen, die der Verbraucher umsetzen kann, erschweren oder verhindern, dass ein Angreifer an seine Zugangsdaten gelangt, um damit die Messdaten abzuhören oder gar zu manipulieren. Durch eine Umsetzung der Maßnahmen erhöht sich der Aufwand für einen Angreifer und somit kann dies eine Verringerung der Eintrittswahrscheinlichkeit der daraus resultierenden Risiken bewirken.

### **M1.20 Wahl „sicherer“ Passwörter**

An verschiedenen Stellen wie beispielsweise dem Online Portal oder zum Zugriff auf den DSL-Router werden Passwörter zur Zugangskontrolle eingesetzt. Die verwendeten voreingestellten Passwörter können dabei leicht zu erraten sein<sup>237</sup> oder wurden vom Benutzer nicht verändert und entsprechen somit den Standardpasswörtern<sup>238</sup>. Eine Maßnahme, die der Nutzer durchführen kann, ist eine Änderung des voreingestellten Passworts. Nach Möglichkeit sollte sich das verwendete Passwort mindestens aus acht alphanumerischen Zeichen zusammensetzen und nicht in Wörterbüchern vorkommen. Zusätzlich sollte es regelmäßig geändert werden. Eine Wiederverwendung des Passwortes für andere Dienste sollte auch nicht vorgenommen werden.

### **M1.21 Sicherer Umgang mit E-Mails**

Um Phishing oder die Ausführung von Schadsoftware durch den Benutzer zu erschweren sollten E-Mails wachsam durchgelesen werden. Der Verzicht auf die HTML-E-Mailansicht und damit die Verwendung der Textansicht sowie der bedachte Umgang mit E-Mailanhängen, welche nicht ohne weiteres geöffnet werden, können zum Schutz vor Phishing und der Ausführung von Schadsoftware beitragen. Eine Phishing E-Mail von einer echten zu unterscheiden gestaltet sich nicht immer als leichte Aufgabe<sup>239</sup>, allerdings können E-Mail-Programme wie beispielsweise Mozilla Thunderbird<sup>240</sup>, den Benutzer mit Hilfe von Warnungen bei der Erkennung von Phishing E-Mails unterstützen. Auf der Internetseite der „Arbeitsgruppe Identitätsschutz im Internet“, können Nutzer Phishing-Mails zusätzlich melden und nachlesen, welche schon bekannt sind.<sup>241</sup>

### **M1.22 Einsatz von Schadsoftware-Schutzprogrammen**

Der Einsatz von Schadsoftware-Schutzprogrammen kann zusätzlich die Infektion der Computer des Nutzers mit Schadsoftware (z. B. Trojaner) verhindern bzw. erschweren. Dabei ist auf eine regelmäßige Aktualisierung des Schutzprogramms inklusive seiner Signaturen zu achten, um neu aufgetretene Schadprogramme erkennen zu können.<sup>242</sup>

---

<sup>237</sup>Vgl. Brinkhaus u. a.: Vortrag: Smart Hacking for Smart Privacy (2011), [52], S. 24.

<sup>238</sup>Siehe z. B. [http://router-faq.de/index.php?id=router\\_ip\\_pw](http://router-faq.de/index.php?id=router_ip_pw) für eine Auflistung von in Routern verwendeter Zugangsdaten.

<sup>239</sup>Siehe z. B. [http://german.mailfrontier.com/survey/phishing\\_de.jsp](http://german.mailfrontier.com/survey/phishing_de.jsp) für einen „Phishing-IQ-Test“.

<sup>240</sup>Anm.: Für eine Beschreibung siehe [http://www.thunderbird-mail.de/wiki/Datenschutz\\_in\\_Thunderbird#Beitragsversuche\\_\\_28Phishing.29](http://www.thunderbird-mail.de/wiki/Datenschutz_in_Thunderbird#Beitragsversuche__28Phishing.29).

<sup>241</sup>Vgl. Arbeitsgruppe Identitätsschutz im Internet: A-I3.org - Phishing (2012), [95].

<sup>242</sup>Vgl. BSI: IT-Grundschutz-Kataloge: 12. EL Stand 2011 (2011), [91], S. 1617.



### M1.23 Zeitnahe Aktualisierung der eingesetzten Software

Angreifer können Schwachstellen in Software-Produkten ausnutzen, um in Systeme einzudringen. Die Softwarehersteller veröffentlichen regelmäßig Patches oder Updates, die solche Schwachstellen beheben. Als Maßnahme dagegen, dass Schwachstellen in Software dazu genutzt werden in Systeme einzudringen, sollten Benutzer darauf achten, dass veröffentlichte Aktualisierungen möglichst zeitnah eingespielt werden. Teilweise kann die Software auch so konfiguriert werden, dass automatisch Software Updates installiert werden.<sup>243,244</sup>

### M1.24 Arbeiten mit eingeschränkten Rechten

Das Arbeiten mit eingeschränkten Rechten bzw. mit einer Einschränkung der Benutzerrechte, auf die für einen Vorgang benötigten Funktionen,<sup>245</sup> kann die Auswirkungen von Schadsoftware minimieren.

### M1.25 Absicherung des WLAN/Verzicht auf WLAN

Setzt der Nutzer WLAN ein, sollte die Übertragung verschlüsselt (im Wi-Fi Protected Access 2 (WPA2)-Verfahren)<sup>246</sup> erfolgen. Der Benutzer sollte dabei möglichst die maximal verfügbare Schlüssellänge (z. B. 63 Zeichen) ausnutzen. Als Alternative könnte der Nutzer auch auf die „drahtlose“ WLAN-Übertragung verzichten und auf kabelgebundene Technologien wie Ethernet zurückgreifen.

## 4.3 Überprüfung der Angriffsziele und Bedrohungen

Nach Umsetzung der Maßnahmen<sup>247</sup> ist eine erneute Prüfung der Bedrohungslage erforderlich um festzustellen, ob die Maßnahmen zum gewünschten Ergebnis geführt haben. Außerdem können nach Umsetzung der Maßnahmen neue Angriffe möglich werden. Aus diesem Grund wird im Folgenden erneut eine Bedrohungs- sowie eine Risikoanalyse durchgeführt. Am Ende des Abschnitts folgt eine Auflistung von Maßnahmen.

### 4.3.1 Bedrohungsanalyse

Im Rahmen der Bedrohungsanalyse werden in diesem Teil Angriffsschritte, die sich stark verändert haben bzw. die durch Umsetzung der Maßnahmen möglich werden, aufgeführt. Bedrohungen aus dem vorherigen Abschnitt, bei denen einzelne Angriffsschritte nicht mehr möglich sind und damit ein Angriff mit höherem Aufwand durchgeführt werden muss, werden im Rahmen der Risikoanalyse angesprochen, an dieser Stelle aber nicht nochmal ausführlich aufgeführt. Dabei wird auf die entsprechende Bedrohung aus der ersten durchgeführten Bedrohungsanalyse verwiesen (z. B. siehe B1.1). Allen Bedrohungen aus der Bedrohungsanalyse im letzten Abschnitt

<sup>243</sup>Siehe z. B. <http://windows.microsoft.com/de-DE/windows7/Understanding-Windows-automatic-updating>

<sup>244</sup>Vgl. BSI: IT-Grundschutz-Kataloge: 12. EL Stand 2011 (2011), [91], S. 1744.

<sup>245</sup>Vgl. Saltzer: Protection and the control of information sharing in multics (1974), [36].

<sup>246</sup>Siehe IEEE 802.11-2007 (2007), [168].

<sup>247</sup>Anm.: Maßnahme M1.19 wird nicht umgesetzt.

wird in diesem Abschnitt die Zahl 2 vorangestellt (aus B1.1 wird B2.1). Der jeweils abgeschätzte Nutzen für den Angreifer bei den einzelnen Bedrohungen, ändert sich im Vergleich zu den Werten in der 1. Bedrohungsanalyse nicht.

### **B2.3 Abhören der Messdaten (Zählerstände) eines Nutzers über einen längeren Zeitraum durch einen externen Angreifer**

Eine unautorisierte Einsicht auf gespeicherte Messdaten kann über den Zugriff auf das Discovery Online Portal erfolgen. Hierfür sind die Zugangsdaten erforderlich. Es wird angenommen, dass die in B1.3 (siehe Tabelle 4.1) beschriebenen Angriffe, um an die Zugangsdaten zu gelangen, weiterhin möglich sind, allerdings durch die umgesetzten Maßnahmen dies für den Angreifer mit einem höheren Aufwand verbunden ist. Der Autor geht davon aus, dass die im Folgenden genannten Angriffe mit einem höheren Aufwand für den Angreifer verbunden sind. Der Datenverkehr kann während der Übertragung zwischen DSL-Router des Kunden und dem Discovery Server an einem Router des Internetproviders (Zugriff auf den Router erforderlich) abgehört werden. Auf Grund der verschlüsselten Übertragung der Messdaten hat der Angreifer allerdings keinen direkten Zugriff. Als Ausweg besteht die Möglichkeit eines Man-in-the-middle Angriffs auf die TLS geschützte Übertragung.<sup>248</sup> Zusätzlich sind Angriffe auf verwendete Verschlüsselungsmethoden<sup>249</sup> oder deren Implementierung<sup>250</sup> denkbar. Auch kann es sein, dass der erzeugte RSA-Schlüssel nicht so zufällig ist wie es erwartet wird.<sup>251</sup>

**Aufwand:** sehr hoch, **Nutzen:** mittel

### **B2.7 Manipulation der Messdaten (Zählerstände) eines Nutzers durch einen einzelnen Nutzer**

Die grundsätzlichen Angriffsmöglichkeiten entsprechen den unter B1.7 (siehe Tabelle 4.3) beschriebenen. Durch die integritätsgeschützte Übertragung mit einem MAC kann eine Manipulation festgestellt werden. Zusätzlich werden die Messdaten verschlüsselt vom Smart Meter übertragen. Der Angreifer müsste sich z. B. mit Hilfe eines Man-in-the-middle in die Kommunikation einbringen, um die Messdaten manipulieren zu können. Replay-Angriffe werden durch die in TLS verwendete Nonce erschwert.<sup>252</sup> Aus diesem Grund wird der für den Angreifer benötigte Aufwand für einen Angriff mit sehr hoch eingeschätzt im Vergleich zum mittleren Aufwand bei B1.7.

**Aufwand:** sehr hoch; **Nutzen:** sehr hoch

---

<sup>248</sup>Vgl. Oppliger, Hauser und Basin: SSL/TLS Session-Aware User Authentication: A Lightweight Alternative to Client-Side Certificates (2008), [31]; Oppliger, Hauser und Basin: SSL/TLS Session-Aware User Authentication - Or how to effectively thwart the man-in-the-middle (2006), [79]; Soghoian und Stamm: Certified lies: Detecting and defeating government interception attacks against SSL (2010), [87].

<sup>249</sup>Siehe Biryukov und Khovratovich: Related-Key Cryptanalysis of the Full AES-192 and AES-256 (2009), [6]; Bernstein: Cache-timing attacks on AES (2005), [49].

<sup>250</sup>Vgl. Kocher: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems (1996), [24]; Duong und Rizzo: Here Come The Ninjas (2011), [59].

<sup>251</sup>Vgl. Lenstra u. a.: Ron was wrong, Whit is right (2012), [75].

<sup>252</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 733f.

### **B2.9 Manipulation der Messdaten (Zählerstände) eines Nutzers durch einen externen Angreifer**

Die grundsätzlichen Angriffsmöglichkeiten entsprechen den unter B1.9 (siehe Tabelle 4.3) beschriebenen. Eine Angriffsmöglichkeit besteht darin, die gespeicherten Messdaten im Discovery Online Portal zu verändern. Hierfür ist allerdings der Zugriff auf den Server notwendig. Durch die Umsetzung der Maßnahmen wird angenommen, dass der Administrator vorsichtiger umgeht und der Zugang zum Server nicht mehr so leicht möglich ist. Aus diesem Grund wird ein noch höherer Aufwand für den Angreifer angenommen. Auch die alternative Angriffsmöglichkeit einer Manipulation, während der Übertragung zwischen DSL-Router und den Discovery Servern, wird durch den Einsatz des Integritätsschutz erschwert (siehe B2.7).

**Aufwand:** sehr hoch; **Nutzen:** mittel

### **B2.13 Übermittlung manipulierter Messdaten (Zählerstände) durch den Nutzer, Nachbar oder einen externen Angreifer**

Ein anderer Angriff, der vom Nutzer, Nachbar oder externen Angreifer ausgeführt werden könnte, besteht darin gleichzeitig sehr viele gefälschte Messdaten an den Discovery Server zu übermitteln. Hierfür müssten Messdaten die unterschiedliche SM-GW IDs (MAC-Adresse, Adressbereich 2C:DD:0C:00:00:00 - 2C:DD:0C:FF:FF:FF) enthalten generiert werden. Da sich SM-GW und Discovery Server mit Hilfe von Zertifikaten gegenseitig authentisieren, müsste der Angreifer an die Zertifikate gelangen, um manipulierte Messdaten zu erstellen. Darüber könnten dann TLS-Verbindungen zum Server aufgebaut und manipulierte Messdaten eingespielt werden.

**Aufwand:** sehr hoch; **Nutzen:** hoch

### **B2.14 Übertragung der Messdaten (für Abrechnung relevant) bei individuellem Nutzer verhindern durch den Nutzer**

Die grundsätzlichen Angriffsmöglichkeiten entsprechen den unter B1.14 (siehe Tabelle 4.5) beschriebenen. Durch Umsetzung der Maßnahme M1.2 (siehe 4.2.4) werden die Abrechnungsdaten per GPRS übermittelt. Um auch die Übertragung per GPRS zu stören, müsste der Angreifer entweder das SM-GW abschirmen oder einen GSM Störsender (Jammer) einsetzen. Der Angreifer kann diesen entweder selbst herstellen<sup>253</sup> oder aus dem Ausland importierten<sup>254</sup>. Der Einsatz ist in Deutschland allerdings verboten.<sup>255</sup> Der Aufwand für den Angreifer wird aus diesen Gründen als sehr hoch eingeschätzt.

**Aufwand:** sehr hoch; **Nutzen:** sehr hoch

---

<sup>253</sup>Vgl. Fried: Social Defense Mechanisms (2005), [64]; Green Bay Professional Packet Radio: GBPPR Cellular Phone Jammers, [108].

<sup>254</sup>Siehe z. B. <http://www.jammer-store.com/> oder <http://www.globalgadgetuk.com/rx10.html>

<sup>255</sup>Vgl. StGB (2012), [189], § 317.

### **B2.15 Übertragung der Messdaten (für Abrechnung relevant) bei individuellem Nutzer verhindern durch einen Nachbar**

Die grundsätzlichen Angriffsmöglichkeiten entsprechen den unter B1.15 (siehe Tabelle 4.5) beschriebenen. Zusätzlich muss der Angreifer die Übertragung per GPRS stören (siehe B2.14).

**Aufwand:** sehr hoch; **Nutzen:** mittel

### **B2.16 Übertragung der Messdaten (für Abrechnung relevant) bei individuellem Nutzer verhindern durch einen externen Angreifer**

Die grundsätzlichen Angriffsmöglichkeiten entsprechen den unter B1.16 (siehe Tabelle 4.5) beschriebenen. Zusätzlich muss der Angreifer die Übertragung per GPRS stören (siehe B2.14). Die Motivation hinter einem solchen Angriff kann sein, dass dem Messstellenbetreiber bewusst Schaden zugeführt werden soll, da diesem durch die Übertragung per GPRS zusätzliche Kosten entstehen.

**Aufwand:** sehr hoch; **Nutzen:** niedrig

### **B2.17 Übertragung der Messdaten (für Abrechnung relevant) bei vielen Nutzern verhindern durch einzelnen Nutzer**

Die grundsätzlichen Angriffsmöglichkeiten entsprechen den unter B1.17 (siehe Tabelle 4.6) beschriebenen. Die Übertragung der Messdaten kann durch eine Überlastung des Abrechnungssystems (Discovery Server) erreicht werden. Hierfür kann der Nutzer DoS-Angriffe auf den Discovery Server durchführen. Die Messdaten werden verschlüsselt per TLS an die Discovery Server übertragen (siehe Maßnahme M1.9). Beim TLS-Verbindungsaufbau wird für die Aushandlung des Sitzungsschlüssels, ein einmalig benutzbarer symmetrischer Schlüssel, das RSA Verfahren eingesetzt. Das Verfahren sorgt dabei auf Seite des Servers für mehr Last, da dieser die bei RSA Verfahren aufwendige Entschlüsselung<sup>256</sup>vornimmt, als auf Seite des Clients. Dies kann für einen TLS Renegotiation DoS-Angriff ausgenutzt werden. Der Angreifer fordert dabei nach dem Verbindungsaufbau die Neuaushandlung des Schlüssels immer wieder an. Wird dies mit mehreren Verbindungen gleichzeitig gemacht, kann dies zu einer Überlastung des Servers und damit zu einem Denial-of-Service des Servers führen. Der Angriff kann z.B. mit Hilfe des Programms „THC-SSL-DOS“ durchgeführt werden.<sup>257</sup>

**Aufwand:** hoch; **Nutzen:** hoch

---

<sup>256</sup>Vgl. Bicakci, Crispo und Tanenbaum: Reverse SSL (2006), [50]; Challa und Pradhan: Performance Analysis of Public key Cryptographic Systems RSA and NTRU (2007), [10], bei 512 Bit-2048 Bit.

<sup>257</sup>Vgl. THC-SSL-DOS (2011), [122]; Bernat: SSL computational DoS mitigation (2011), [101]; EKR: SSL/TLS and Computational DoS (2011), [104].

### 4.3.2 Risikoanalyse

In den Tabellen 4.24 bis 4.37 sind die identifizierten Risiken nacheinander aufgeführt. Der Aufbau entspricht den Tabellen in Abschnitt 4.2.3. Im Anschluss der Tabellen folgt erneut eine übersichtliche Darstellung der Risiken in Form von Risikokarten aus Sicht Netzbetreibers bzw. Messstellenbetreibers (siehe Abb. 4.5) und aus Sicht des Nutzers/Verbrauchers (siehe Abb. 4.6)

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R2.1	B2.1	mittel	unwesentlich	Der Angriff wird durch Zugriff auf das Discovery Online Portal und angepassten HTTP-GET-Requests (siehe B1.1) durchgeführt, da dieser Angriff mit mittlerem Aufwand, bei zugleich mittlerem Nutzen durchführbar ist. Durch die verschlüsselte Übertragung (M1.9) sind die anderen in B1.1 beschriebenen Angriffe mit einem höheren Aufwand für den Angreifer durchführbar. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da der Nutzer mit mittlerem Aufwand bei mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören eines einzelnen Nutzers ein unwesentlicher Schaden für den Netzbetreiber/Messstellenbetreiber verursacht wird, solange er nicht für einen zusätzlichen Beitrag im Monat die Daten in höherer Auflösung anbietet (Erschleichung von Diensten).
R2.2	B2.1	mittel	geringfügig	Für die Angriffsbeschreibung siehe R2.1. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da der Nutzer mit mittlerem Aufwand bei mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören eines einzelnen Nutzers (z. B. Familienmitglied) nur ein geringfügiger Schaden für den Nutzer zu erwarten ist.

Tabelle 4.24: Risikoanalyse 2, Teil 1

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R2.3	B2.2	niedrig	unwesentlich	Der Angreifer greift auf die Daten im Discovery Online Portal mit Hilfe der Zugangsdaten des Nutzers zu, an die er z. B. per Social Engineering (siehe B1.2) gelangt. Der Aufwand für den Nachbar als Angreifer wird nach Umsetzung der Maßnahmen als hoch angesehen und liegt damit höher als in B1.2. Auch die in B1.2 beschriebenen lokal durchgeführten Angriffe sind möglich. Durch Umsetzung der Maßnahmen (M1.9, M1.17) ist die Durchführung allerdings mit einem sehr hohen Aufwand für den Angreifer verbunden. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit hohem Aufwand und zugleich mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören eines einzelnen Nutzers, ein unwesentlicher Schaden (Imageschaden, eventuell Verlust eines Kunden) für den Netzbetreiber/ Messstellenbetreiber verursacht wird.
R2.4	B2.2	niedrig	geringfügig	Für die Angriffsbeschreibung siehe R2.3. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit hohem Aufwand und zugleich mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören des Nutzers durch seinen Nachbar ein geringfügiger Schaden für den Nutzer zu erwarten ist (Der Nachbar erhält Einblick in die Privatsphäre des Nutzers).
R2.5	B2.3	niedrig	unwesentlich	Für die Beschreibung der Bedrohung inklusive Angriffsbeschreibungen siehe Abschnitt 4.3.1, B2.3. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein externer Angreifer mit sehr hohem Aufwand bei mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören eines einzelnen Nutzers, ein unwesentlicher Schaden (Imageschaden, eventuell Verlust eines Kunden) für den Netzbetreiber/ Messstellenbetreiber zu erwarten ist.

Tabelle 4.25: Risikoanalyse 2, Teil 2

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R2.6	B2.3	niedrig	geringfügig	Für die Angriffsbeschreibung siehe R2.5. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein externer Angreifer mit sehr hohem Aufwand bei mittlerem Nutzen Zugriff erhält. (Informationen werden genutzt um z. B. einen Einbruch beim Nutzer durchzuführen). Es ist davon auszugehen, dass durch das Abhören eines einzelnen Nutzers (Einblick in die Privatsphäre) ein geringfügiger Schaden für den Nutzer zu erwarten ist.
R2.7	B2.4	niedrig	geringfügig	Für die Angriffsbeschreibung siehe B1.4. Der Aufwand für den Nutzer wird nach Umsetzung der Maßnahmen als sehr hoch angesehen und liegt damit höher als in B1.4. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer mit sehr hohem Aufwand bei mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören vieler Nutzer ein geringfügiger Schaden (Imageschaden, eventuell Verlust von einigen Kunden) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.8	B2.4	niedrig	geringfügig	Für die Angriffsbeschreibung siehe R2.7. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer mit sehr hohem Aufwand bei mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören vieler Nutzer, ein geringfügiger Schaden für den Nutzer zu erwarten ist. Es wird weiter angenommen, dass es für einen Nutzer/Verbraucher als weniger schwerwiegend empfunden wird, wenn viele Nutzer betroffen sind als wenn er der einzige Betroffene ist.
R2.9	B2.5	niedrig	geringfügig	Für die Angriffsbeschreibung siehe B1.5. Der Aufwand für den Nutzer wird nach Umsetzung der Maßnahmen als sehr hoch angesehen und liegt damit höher als in B1.5. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer mit sehr hohem Aufwand bei mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören vieler Nutzer ein geringfügiger Schaden (Imageschaden, eventuell Verlust von einigen Kunden) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.

Tabelle 4.26: Risikoanalyse 2, Teil 3

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R2.10	B2.5	niedrig	geringfügig	Für die Angriffsbeschreibung siehe R2.9. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer mit sehr hohem Aufwand bei mittlerem Nutzen Zugriff erhält. Es ist davon auszugehen, dass durch das Abhören vieler Nutzer, ein geringfügiger Schaden für den Nutzer entsteht. Es wird weiter angenommen, dass es für einen Nutzer/Verbraucher als weniger schwerwiegend empfunden wird, wenn viele Nutzer betroffen sind als wenn er der einzige Betroffene ist.
R2.11	B2.6	niedrig	geringfügig	Für die Angriffsbeschreibung siehe B1.6. Der Aufwand für den Nutzer wird nach Umsetzung der Maßnahmen als sehr hoch angesehen und liegt damit höher als in B1.6. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer mit sehr hohem Aufwand bei hohem Nutzen Zugriff erhält. Der Angreifer kann die Informationen nutzen, um Einbrüche durchzuführen, wenn sich keine Person vor Ort (Wohnung/Haus) befindet. Es ist davon auszugehen, dass durch das Abhören vieler Nutzer ein geringfügiger Schaden (Imageschaden, eventuell Verlust von einigen Kunden) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.12	B2.6	niedrig	geringfügig	Für die Angriffsbeschreibung siehe R2.11. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer mit sehr hohem Aufwand bei hohem Nutzen Zugriff erhält. Der Angreifer kann die Informationen nutzen, um Einbrüche durchzuführen, wenn sich keine Person vor Ort (Wohnung/Haus) befindet. Es ist davon auszugehen, dass durch das Abhören vieler Nutzer ein geringfügiger Schaden für den Nutzer/Verbraucher zu erwarten ist.

Tabelle 4.27: Risikoanalyse 2, Teil 4



<b>Risiko Nr.</b>	<b>Bedrohung</b>	<b>Eintrittswahrscheinlichkeit</b>	<b>Schadensausmaß</b>	<b>Bemerkung</b>
R2.13	B2.7	mittel	unwesentlich	Für die Beschreibung der Bedrohung inklusive Angriffsbeschreibungen siehe 4.3.1, B2.7. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich sehr hohem Nutzen (Abrechnungsbetrug wird ermöglicht), durchführen kann. Ist die Manipulation der Messdaten durch den Nutzer vom Netzbetreiber/Messstellenbetreiber entdeckbar, wird davon ausgegangen, dass ein unwesentlicher Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.14	B2.7	mittel	kritisch	Für die Angriffsbeschreibung siehe R2.13. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich sehr hohem Nutzen (Abrechnungsbetrug wird ermöglicht), durchführen kann. Ist die Manipulation der Messdaten durch den Nutzer vom Netzbetreiber/ Messstellenbetreiber nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.

Tabelle 4.28: Risikoanalyse 2, Teil 5

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R2.15	B2.8	niedrig	unwesentlich	Der Angriff wird lokal oder während der Übertragung durchgeführt. Für die Angriffsbeschreibung eines lokal durchgeführten Angriffs siehe Abschnitt 4.3.1, B2.7. Für die Angriffsbeschreibung eines während der Übertragung zwischen DSL-Router und den Discovery Servern durchgeführten Angriffs siehe Abschnitt 4.3.1, B2.9. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann. Ist die Manipulation der Messdaten durch den Nachbar vom Netzbetreiber/Messstellenbetreiber entdeckbar, wird davon ausgegangen, dass ein unwesentlicher Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.16	B2.8	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.15. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann. Ist die Manipulation der Messdaten durch den Nachbar vom Netzbetreiber/Messstellenbetreiber nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.17	B2.8	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.15. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann. Ist die Manipulation der Messdaten durch den Nachbar vom Nutzer/Verbraucher nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.

Tabelle 4.29: Risikoanalyse 2, Teil 6

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensmaß	Bemerkung
R2.18	B2.9	niedrig	unwesentlich	Für die Beschreibung der Bedrohung inklusive Angriffsbeschreibungen siehe 4.3.1, B2.9. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich mittlerem Nutzen durchführen kann. Ist die Manipulation der Messdaten durch einen externen Angreifer vom Netzbetreiber/Messstellenbetreiber entdeckbar, wird davon ausgegangen, dass ein unwesentlicher Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.19	B2.9	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.18. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich mittlerem Nutzen durchführen kann. Ist die Manipulation der Messdaten durch einen externen Angreifer vom Netzbetreiber/Messstellenbetreiber nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.20	B2.9	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.18. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich mittlerem Nutzen durchführen kann. Ist die Manipulation der Messdaten durch einen externen Angreifer vom Nutzer/Verbraucher nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.
R2.21	B2.10	niedrig	unwesentlich	Für die Beschreibung der Bedrohung inklusive Angriffsbeschreibungen siehe Abschnitt 4.3.1, B2.10. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten → keine Zahlung). Ist die Manipulation der Messdaten durch einen Nutzer vom Netzbetreiber/Messstellenbetreiber entdeckbar, wird davon ausgegangen, dass ein unwesentlicher Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.

Tabelle 4.30: Risikoanalyse 2, Teil 7

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R2.22	B2.10	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.21. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten → keine Zahlung). Ist die Manipulation der Messdaten durch einen Nutzer vom Netzbetreiber/Messstellenbetreiber nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.23	B2.10	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.21. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten → keine Zahlung). Ist die Manipulation der Messdaten durch einen Nutzer vom Nutzer/Verbraucher nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.
R2.24	B2.11	niedrig	unwesentlich	Für die Angriffsbeschreibung siehe R2.21. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzer). Ist die Manipulation der Messdaten durch den Nachbar vom Netzbetreiber/Messstellenbetreiber entdeckbar, wird davon ausgegangen, dass ein unwesentlicher Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.25	B2.11	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.21. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzer). Ist die Manipulation der Messdaten durch den Nachbar vom Netzbetreiber/Messstellenbetreiber nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.

Tabelle 4.31: Risikoanalyse 2, Teil 8

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R2.26	B2.11	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.21. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzer). Ist die Manipulation der Messdaten durch den Nachbar vom Nutzer/Verbraucher nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.
R2.27	B2.12	niedrig	unwesentlich	Für die Angriffsbeschreibung siehe R2.18. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzer→Erpressung). Ist die Manipulation der Messdaten durch einen externen Angreifer vom Netzbetreiber /Messstellenbetreiber entdeckbar, wird davon ausgegangen, dass ein unwesentlicher Schaden für den Netzbetreiber /Messstellenbetreiber zu erwarten ist.
R2.28	B2.12	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.18. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzern → Erpressung). Ist die Manipulation der Messdaten durch einen externen Angreifer vom Netzbetreiber /Messstellenbetreiber nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Netzbetreiber /Messstellenbetreiber zu erwarten ist.
R2.29	B2.12	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.18. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer die Manipulation mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzern → Erpressung). Ist die Manipulation der Messdaten durch einen externen Angreifer vom Nutzer/Verbraucher nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Nutzer/ Verbraucher zu erwarten ist.

Tabelle 4.32: Risikoanalyse 2, Teil 9

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R2.30	B2.13	niedrig	unwesentlich	Für die Beschreibung der Bedrohung inklusive Angriffsbeschreibungen siehe Abschnitt 4.3.1, B2.13. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer gefälschte Messdaten mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzern → Erpressung). Ist die Manipulation der Messdaten vom Netzbetreiber/Messstellenbetreiber entdeckbar, wird davon ausgegangen, dass ein unwesentlicher Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.31	B2.13	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.30. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer gefälschte Messdaten mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzern → Erpressung). Ist die Manipulation der Messdaten vom Netzbetreiber/Messstellenbetreiber nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.32	B2.13	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.30. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Angreifer gefälschte Messdaten mit sehr hohem Aufwand, bei zu gleich hohem Nutzen durchführen kann (fehlerhafte Daten bei Nutzern → Erpressung). Ist die Manipulation der Messdaten nicht entdeckbar, wird davon ausgegangen, dass ein kritischer Schaden für den Nutzer/ Verbraucher zu erwarten ist.
R2.33	B2.14	mittel	geringfügig	Für die Beschreibung der Bedrohung inklusive Angriffsbeschreibungen siehe Abschnitt 4.3.1, B2.14. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da der Nutzer mit sehr hohem Aufwand bei sehr hohem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten eines einzelnen Nutzers, ein geringfügiger Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.

Tabelle 4.33: Risikoanalyse 2, Teil 10

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R2.34	B2.15	niedrig	geringfügig	Für die Beschreibung der Bedrohung inklusive Angriffsbeschreibungen siehe Abschnitt 4.3.1, B2.15. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit sehr hohem Aufwand bei mittlerem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten eines einzelnen Nutzers, ein geringfügiger Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.35	B1.15	niedrig	unwesentlich	Für die Angriffsbeschreibung siehe R2.34. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit sehr hohem Aufwand bei mittlerem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten, ein unwesentlicher Schaden für den Nutzer/Verbraucher zu erwarten ist.
R2.36	B2.16	niedrig	geringfügig	Für die Beschreibung der Bedrohung inklusive Angriffsbeschreibungen siehe Abschnitt 4.3.1, B2.16. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein externer Angreifer mit sehr hohem Aufwand (Zugriff auf den DSL-Router des Nutzers oder Router im Internet) bei niedrigem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten eines einzelnen Nutzers, ein geringfügiger Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.37	B2.16	niedrig	unwesentlich	Für die Angriffsbeschreibung siehe R2.36. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein externer Angreifer mit sehr hohem Aufwand (Zugriff auf den DSL-Router des Nutzers oder Router im Internet) bei niedrigem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten eines einzelnen Nutzers, ein unwesentlicher Schaden für den Nutzer/Verbraucher zu erwarten ist.

Tabelle 4.34: Risikoanalyse 2, Teil 11

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R2.38	B2.17	mittel	kritisch	Für die Beschreibung der Bedrohung inklusive Angriffsbeschreibungen siehe Abschnitt 4.3.1, B2.17. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Nutzer mit hohem Aufwand bei hohem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten vieler Nutzer, ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.39	B2.17	mittel	unwesentlich	Für die Angriffsbeschreibung siehe R2.38. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da ein Nutzer mit hohem Aufwand bei hohem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten vieler Nutzer, ein unwesentlicher Schaden für den Nutzer/Verbraucher zu erwarten ist.
R2.40	B2.18	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.38. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit hohem Aufwand bei mittlerem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten vieler Nutzer, ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.41	B2.18	niedrig	unwesentlich	Für die Angriffsbeschreibung siehe R2.38. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit hohem Aufwand bei mittlerem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten vieler Nutzer, ein unwesentlicher Schaden für den Nutzer/Verbraucher zu erwarten ist.

Tabelle 4.35: Risikoanalyse 2, Teil 12



Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R2.42	B2.19	mittel	kritisch	Für die Angriffsbeschreibung siehe R2.38. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da der externe Angreifer mit hohem Aufwand bei hohem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten vieler Nutzer ein kritischer Schaden für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.43	B2.19	mittel	unwesentlich	Für die Angriffsbeschreibung siehe R2.38. Es ist eine mittlere Eintrittswahrscheinlichkeit anzunehmen, da der externe Angreifer mit hohem Aufwand bei hohem Nutzen die Übertragung der Abrechnungsdaten verhindern kann. Es ist davon auszugehen, dass durch die Unterbrechung der Übertragung der Abrechnungsdaten vieler Nutzer ein unwesentlicher Schaden für den Nutzer/Verbraucher zu erwarten ist.
R2.44	B2.20	niedrig	kritisch	Der Angriff wird lokal ausgeführt. Für die Angriffsbeschreibung siehe B1.20. Der Aufwand für den Nutzer wird nach Umsetzung der Maßnahmen als hoch angesehen und liegt damit höher als in B1.20, da zusätzlich die lokale Ersatzstromversorgung deaktiviert werden muss. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Nutzer mit hohem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem einzelnen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung ein kritischer Schaden (Imageschaden, Verlust von Kunden) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.

Tabelle 4.36: Risikoanalyse 2, Teil 13

<b>Risiko Nr.</b>	<b>Bedrohung</b>	<b>Eintrittswahrscheinlichkeit</b>	<b>Schadensausmaß</b>	<b>Bemerkung</b>
R2.45	B2.20	niedrig	kritisch	Der Angriff wird lokal ausgeführt. Für die Angriffsbeschreibung siehe R2.44. Der Aufwand für den Nutzer wird nach Umsetzung der Maßnahmen als hoch angesehen und liegt damit höher als in B1.20, da zusätzlich die lokale Ersatzstromversorgung deaktiviert werden muss. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Nutzer mit hohem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem einzelnen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung, ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.
R2.46	B2.21	niedrig	kritisch	Der Angriff wird lokal ausgeführt. Für die Angriffsbeschreibung siehe B1.21. Der Aufwand für den Nachbar wird nach Umsetzung der Maßnahmen als hoch angesehen und liegt damit höher als in B1.21, da zusätzlich die lokale Ersatzstromversorgung deaktiviert werden muss. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit hohem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem einzelnen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung ein kritischer Schaden (Imageschaden, Verlust von Kunden) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.

Tabelle 4.37: Risikoanalyse 2, Teil 14

<b>Risiko Nr.</b>	<b>Bedrohung</b>	<b>Eintrittswahrscheinlichkeit</b>	<b>Schadensausmaß</b>	<b>Bemerkung</b>
R2.47	B2.21	niedrig	kritisch	Der Angriff wird lokal ausgeführt. Für die Angriffsbeschreibung siehe R2.6. Der Aufwand für den Nachbar wird nach Umsetzung der Maßnahmen als hoch angesehen und liegt damit höher als in B1.21, da zusätzlich die lokale Ersatzstromversorgung deaktiviert werden muss. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit hohem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem einzelnen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.
R2.48	B2.22	niedrig	kritisch	Der Angriff wird lokal ausgeführt. Für die Angriffsbeschreibung siehe B1.22. Der Aufwand für den Nutzer wird nach Umsetzung der Maßnahmen als sehr hoch angesehen und liegt damit höher als in B1.22, da zusätzlich die lokale Ersatzstromversorgung deaktiviert werden muss. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein externer Angreifer mit sehr hohem Aufwand bei mittlerem Nutzen den Ausfall oder Störung der Stromversorgung bei einem einzelnen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung ein kritischer Schaden (Imageschaden, Verlust von Kunden) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.

Tabelle 4.38: Risikoanalyse 2, Teil 15

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R2.49	B2.22	niedrig	kritisch	Der Angriff wird lokal ausgeführt. Für die Angriffsbeschreibung siehe R2.48. Der Aufwand für den Nutzer wird nach Umsetzung der Maßnahmen als sehr hoch angesehen und liegt damit höher als in B1.22, da zusätzlich die lokale Ersatzstromversorgung deaktiviert werden muss. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein externer Angreifer mit sehr hohem Aufwand bei mittlerem Nutzen den Ausfall oder Störung der Stromversorgung bei einem einzelnen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.
R2.50	B2.23	niedrig	katastrophal	Für die Angriffsbeschreibung siehe B1.23. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Nutzer mit sehr hohem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem vielen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung vieler Nutzer ein katastrophaler Schaden (Image-schaden, Verlust von Kunden, Regressansprüche) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.51	B2.23	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.50. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein Nutzer mit sehr hohem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem vielen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung vieler Nutzer ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.

Tabelle 4.39: Risikoanalyse 2, Teil 16

Risiko Nr.	Bedrohung	Eintrittswahrscheinlichkeit	Schadensausmaß	Bemerkung
R2.52	B2.24	niedrig	katastrophal	Für die Angriffsbeschreibung siehe B1.24. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit sehr hohem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem vielen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung vieler Nutzer ein katastrophaler Schaden (Image-schaden, Verlust von Kunden, Regressansprüche) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.53	B2.24	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.52. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da der Nachbar mit sehr hohem Aufwand bei niedrigem Nutzen den Ausfall oder Störung der Stromversorgung bei einem vielen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung vieler Nutzer ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.
R2.54	B2.25	niedrig	katastrophal	Für die Angriffsbeschreibung siehe B1.25. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein externer Angreifer mit sehr hohem Aufwand bei hohem Nutzen den Ausfall oder Störung der Stromversorgung bei einem vielen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung vieler Nutzer ein katastrophaler Schaden (Imageschaden, Verlust von Kunden, Regressansprüche) für den Netzbetreiber/Messstellenbetreiber zu erwarten ist.
R2.55	B2.25	niedrig	kritisch	Für die Angriffsbeschreibung siehe R2.54. Es ist eine niedrige Eintrittswahrscheinlichkeit anzunehmen, da ein externer Angreifer mit sehr hohem Aufwand bei hohem Nutzen den Ausfall oder Störung der Stromversorgung bei einem vielen Nutzer bewirken kann. Es ist davon auszugehen, dass durch die Unterbrechung der Stromversorgung vieler Nutzer ein kritischer Schaden für den Nutzer/Verbraucher zu erwarten ist.

Tabelle 4.40: Risikoanalyse 2, Teil 17

Die Risikokarte in [Abbildung 4.5](#) zeigt die Risiken aus Sicht des Netzbetreibers bzw. Messstellenbetreibers. Im Vergleich zur Risikokarte aus der ersten Risikoanalyse (siehe [Abb. 4.1](#)) sind keine Risiken mehr vorhanden, die mit hoher oder sehr hoher Eintrittswahrscheinlichkeit auftreten. Insbesondere das Risiko R1.14/B1.7\* aus [Abb. 4.1](#) befindet sich nun nicht mehr im inakzeptablen Bereich, sondern als R2.14/B2.7\* im ALARP-Bereich. Die beiden Risiken R1./B1.17 und R1./B1.19 befinden sich in Form von R2.38/B2.17 und R2.38/B2.17 weiter im ALARP-Bereich, da durch Umsetzung der Maßnahmen M1.8 und M1.9 (siehe Abschnitt [4.2.4](#)) die Möglichkeit von DoS-Angriffen bestehen bleibt. Durch die Umsetzung der Maßnahmen ändert sich nichts an der Einstufung des Risikos eines Ausfalls oder der Störung der Stromversorgung von der viele Menschen betroffen sind (R2.50/B2.23, R2.52/B2.24, R2.54/B2.25). Diese bleiben weiter im ALARP-Bereich, da ein Risikoeintritt starke Auswirkungen für den Netzbetreiber/Messstellenbetreiber haben kann.

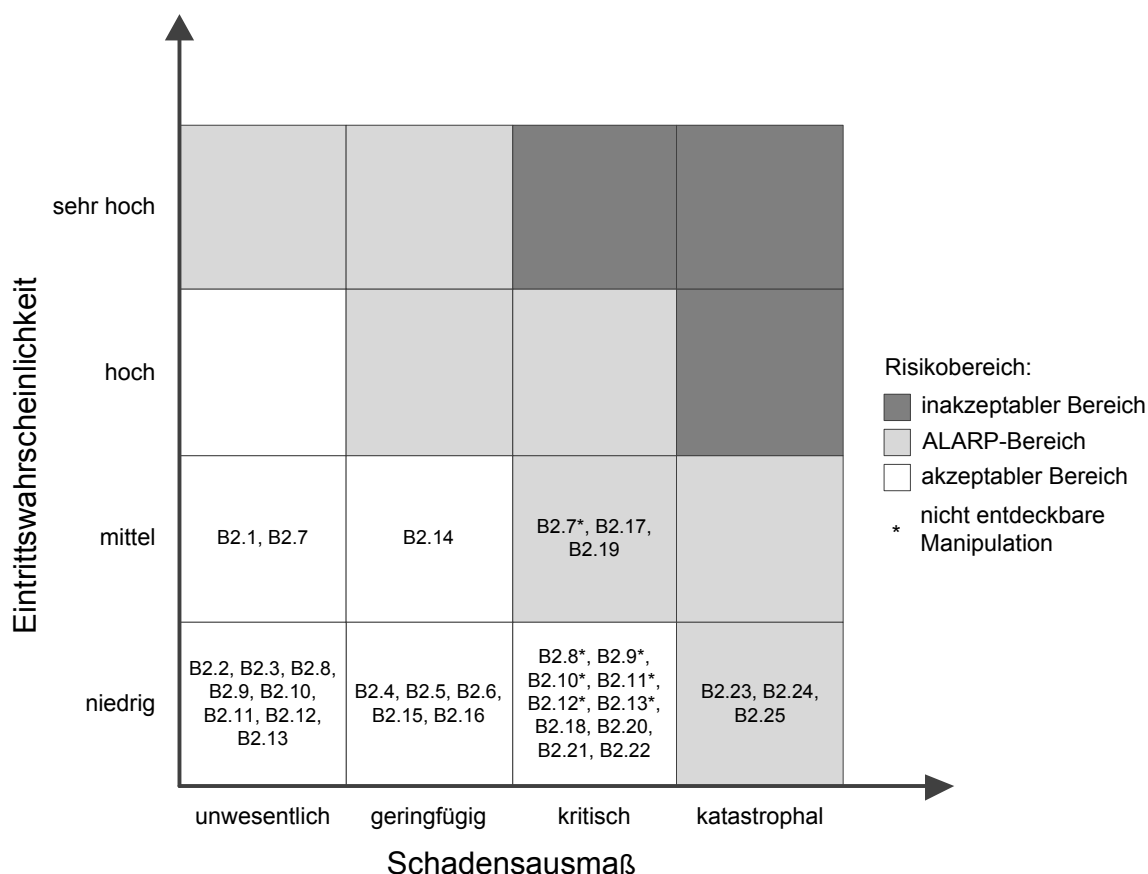


Abbildung 4.5: Risikokarte aus Sicht des Netzbetreibers/Messstellenbetreibers

Abbildung 4.6 zeigt die Risikokarte aus Sicht des Nutzers bzw. Verbrauchers. Alle Risiken, die sich in der ersten Risikoanalyse (siehe Abb. 4.2) noch im ALARP-Bereich befunden haben, konnten durch Umsetzung der Maßnahmen in den akzeptablen Bereich transferiert werden.

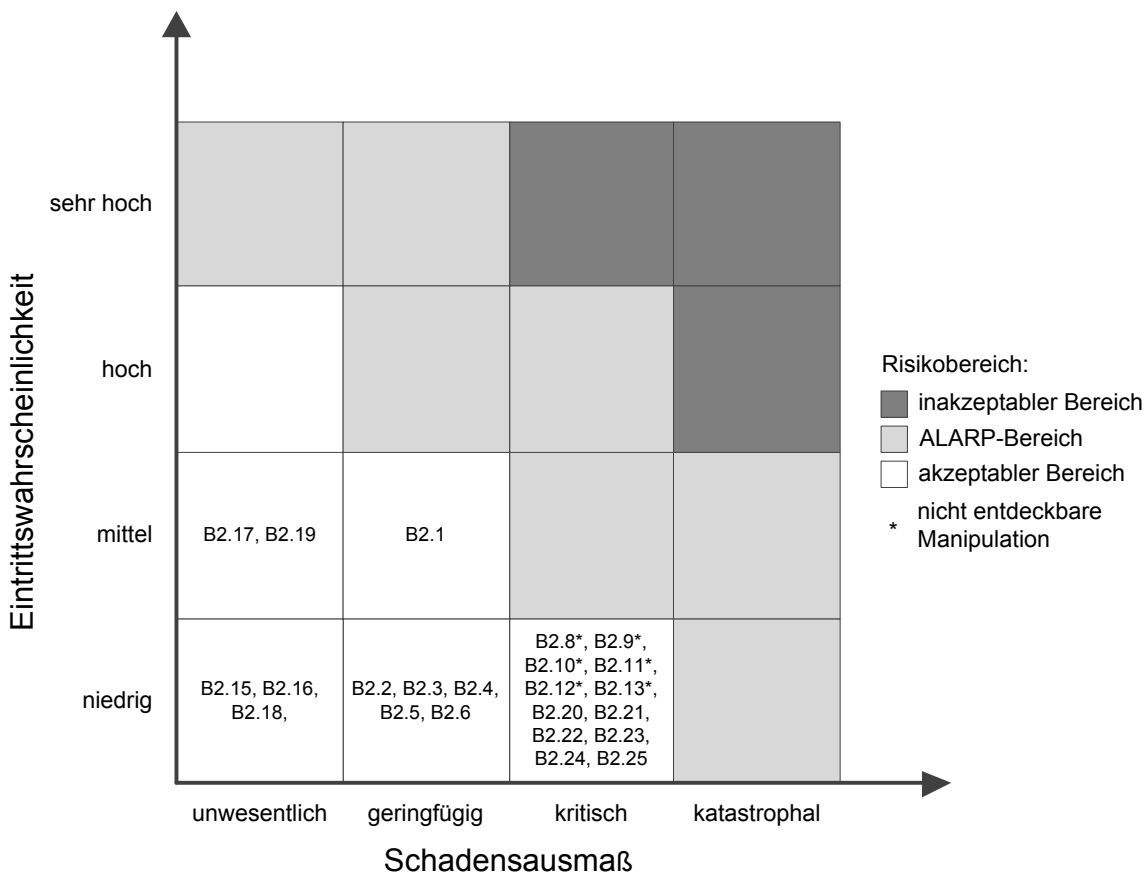


Abbildung 4.6: Risikokarte aus Sicht des Nutzers/Verbrauchers

### 4.3.3 Maßnahmen

Abschließend werden in Tabelle 4.7 Maßnahmen aufgeführt, welche vom Netzbetreiber bzw. Messstellenbetreiber durchzuführen sind. Für den Verbraucher bzw. Nutzer werden keine weiteren Maßnahmen aufgeführt, da dies nach Auswertung der Risikoanalyse 2 (siehe Abb. 4.6) nicht notwendig ist. Im Anschluss der Tabelle erfolgt wie bereits in Abschnitt 4.2.4 eine Beschreibung der einzelnen Maßnahmen.

Maßnahmen Nr.	Maßnahme
M2.1	Übertragung der Messdaten per PLC
M2.2	TLS-Renegotiation deaktivieren
M2.3	Serverkapazität für TLS Schlüsselerzeugung erhöhen
M2.4	Einsatz von Elliptischer-Kurven-Kryptographie für Schlüsselaustausch und Authentifizierung bei der Verschlüsselung
M2.5	Zugriff auf detaillierte Verbrauchsdaten verhindern

Abbildung 4.7: Übersicht Maßnahmen Netzbetreibers/Messstellenbetreiber

### M2.1 Übertragung der Messdaten per PLC

Die Übertragung von Messdaten per DSL und per GPRS kann durch einen Angreifer verhindert werden. Zusätzlich entstehen dem Messstellenbetreiber/Netzbetreiber weitere Kosten, wenn die Übertragung per GPRS stattfindet. Einen Ausweg stellt die Übertragung der Messdaten per PLC bis zum Messstellenbetreiber/Netzbetreiber dar. Hierfür kann Breitband PLC (BPL)<sup>258</sup> eingesetzt werden.

### M2.2 TLS-Renegotiation deaktivieren

Beim TLS-DoS-Angriff fordert der Angreifer nach dem Verbindungsaufbau die Neuaushandlungen der Schlüssel an. Durch Abschalten der TLS-Renegotiation Funktion wird der Angriff erschwert.

### M2.3 Serverkapazität für TLS Schlüsselerzeugung erhöhen

Als Maßnahme gegen TLS-DoS-Angriff können Hardware-TLS-Beschleuniger (Hardware accelerator) oder zusätzliche Serverkapazität mit Hilfe weiterer Prozessoren bzw. Prozessorkernen verwendet werden.<sup>259,260</sup>

### M2.4 Einsatz von Elliptischer-Kurven-Kryptographie für Schlüsselaustausch und Authentifizierung bei der Verschlüsselung

Das ressourcenintensive und asymmetrische kryptographische Verfahren RSA soll durch Verfahren ersetzt werden, die Elliptische-Kurven-Kryptographie einsetzen. Der Vorteil von Verfahren die elliptische Kurven<sup>261</sup> einsetzen ist, dass es im Vergleich zu anderen Verfahren wie z. B. im Fall von RSA bei vergleichbarer Sicherheit mit kürzeren Schlüssellängen auskommt<sup>262</sup> und somit eine geringere Last auf dem Server erzeugen. Ein Angreifer der einen TLS-DoS-Angriff durchführt erzeugt somit eine geringere Last auf dem Server und der Angreifer muss mehr TLS-Verbindungen öffnen, um den Server damit zu belasten. Für den Schlüsselaustausch soll das Diffie-Hellman Verfahren<sup>263</sup> in der Variante Elliptic Curve Diffie-Hellman (ECDH) und zur gegenseitigen Authentifizierung sollen Digitale Signaturen, die mit dem Elliptic Curve Digital Signature Algorithmus (ECDSA) erstellt wurden, verwendet werden.

Eine vom BSI empfohlene elliptische Kurve<sup>264</sup> wie z. B. „brainpoolP256t1“<sup>265</sup> soll verwendet werden.<sup>266</sup>

---

<sup>258</sup>Siehe Hrasnica, Haidine und Lehnert: Broadband Powerline Communications (2005), [18], S. 19.

<sup>259</sup>Vgl. THC-SSL-DOS (2011), [122]; Bernat: SSL computational DoS mitigation (2011), [101].

<sup>260</sup>Siehe Coarfa, Druschel und Wallach: Performance analysis of TLS Web servers (2006), [11].

<sup>261</sup>Siehe Standards for Efficient Cryptography (SEC) (2000), [157].

<sup>262</sup>Vgl. Eckert: IT-Sicherheit (2012), [12], S. 362f.

<sup>263</sup>Siehe *ebd.*, S. 441-447.

<sup>264</sup>Vgl. BSI: BSI TR-02102 (2008), [163], S. 36f.

<sup>265</sup>Siehe Lochter: ECC Brainpool Standard Curves and Curve Generation (2005), [151].

<sup>266</sup>**Anm.:** Die Maßnahme soll die generelle Last des Servers verringern. Neben der Serverlast verringert sich auch die Last auf Clientseite, wodurch ein Angreifer mit mehr Verbindungen und Neuaushandlungen reagieren kann.



### **M2.5 Zugriff auf detaillierte Verbrauchsdaten verhindern**

Im Discovery Online Portal sind die Verbrauchsdaten in detaillierter Form mit Hilfe eigener HTTP-GET Requests abrufbar. Der Zugriff sollte verhindert werden, indem die Webschnittstelle des Online Portals verändert wird.<sup>267</sup>

---

<sup>267</sup>Vgl. Brinkhaus u. a.: Vortrag: Smart Hacking for Smart Privacy (2011), [\[52\]](#), S. 9.

### 5 Zusammenfassung und Ausblick

Die zukünftigen Elektrizitätsversorgungssysteme verwenden Informations- und Telekommunikationssysteme zur Steuerung und Verwaltung. Erste Schritte für den Aufbau von Smart Grids, sind bereits in Form einer Umrüstung von immer mehr Haushalten auf Smart Meter umgesetzt. Diese Arbeit beschäftigte sich mit Sicherheit und Datenschutz in Smart Grids. Anhand eines Szenarios wurde gezeigt, dass eine derzeit für Verbraucher in Deutschland verfügbare Smart Grid Umsetzung, Risiken aus Sicht des Messstellenbetreibers in Form der Discovergy GmbH und aus Sicht des Verbrauchers aufweist. Aus der Bedrohungs- und der Risikoanalyse ist erkennbar, dass Messstellenbetreiber und Verbraucher gegenwärtig mit Problemen wie Manipulation, Spionage oder einer Einschränkung der Verfügbarkeit von Systemen konfrontiert werden können. Dies veranschaulicht die Bedeutung der Umsetzung von Schutzmaßnahmen, durch die das Risiko für beide Seiten minimiert werden kann.

Bei anderen Netzbetreibern oder Messstellenbetreibern kann sich die Situation unterschiedlich darstellen. Die vom [BSI](#) entwickelten Schutzprofile und Technischen Richtlinien für Intelligente Messsysteme werden in dieser Hinsicht für technische Sicherheits-Mindeststandards sorgen. Nach den bisher veröffentlichten Entwürfen ist zu erwarten, dass die im Szenario festgestellten Probleme bei Einhaltung der Schutzprofile und der Technischen Richtlinie in dieser Form nicht mehr ohne weiteres auftreten. Messsysteme, die den Anforderungen nicht genügen, dürfen allerdings noch bis spätestens zum Jahr 2020 verbaut sein.<sup>268</sup> Dies erscheint aus ökonomischer Sicht nachvollziehbar, aus Sicherheitssicht ist die Situation allerdings bedenklich.

Ebenso bedenklich ist für den Autor dieser Arbeit die weitreichende Sammlung von Verbrauchsdaten. In anderen Lebensbereichen wie z. B. bei der Nutzung von Mobiltelefonen werden zwar ebenfalls Daten erhoben, die sogar eine Erstellung von Bewegungsprofilen ermöglichen,<sup>269</sup> allerdings bleibt die Nutzung von Mobiltelefonen jedem selbst überlassen und im Bedarfsfall kann dieses abgeschaltet werden. Im Smart Grid kann solch eine Entscheidung nicht getroffen werden, da bei der Nutzung jeglicher elektrischer Systeme Verbrauchsdaten in hoher Auflösung erhoben werden, um daraus Lastprognosen zu erstellen und die Vision des Smart Grid zu verwirklichen. Leider ermöglicht dies einen Einblick in die Privatsphäre und ist somit aus datenschutzrechtlicher Sicht problematisch. Hervorzuheben ist, dass die Entwicklung von Smart Grids noch nicht abgeschlossen ist. So ergeben sich Chancen für den Einsatz von Verfahren bei denen beide Seiten in Einklang gebracht werden.<sup>270</sup> Außerdem ist die Steuerung von einzelnen Verbrauchern und Erzeugern durch Energieversorgungsunternehmen bis auf einzelne Pilotprojekte noch nicht realisiert. Dies beinhaltet auch die Steuerung von Haushaltsgeräten, wodurch sich Nahtstellen zum Smart Home ergeben, die weiter untersucht werden sollten. In vielen weiteren Bereichen besteht Forschungsbedarf. Dieser umfasst z. B. sichere Hardware für Smart Meter bzw. [SM-GW](#) oder sichere Kommunikationsnetze. Die geplante Integration der Elektromobilität bietet zusätzliche Untersuchungsmöglichkeiten.

---

<sup>268</sup>Siehe Abschnitt [2.4.2](#)

<sup>269</sup>Vgl. ZEIT ONLINE: Verräterisches Handy (2011), [\[125\]](#).

<sup>270</sup>Vgl. Molina-Markham u. a.: Smart Metering and Privacy (2010), [\[78\]](#); Jeske: Datenschutzfreundliches Smart Metering (2011), [\[19\]](#).

## Anhang

### A Smart Grid Referenzarchitektur

#### A.1 Entities & Networks

Domain	Entity / Network	Beschreibung
Generation	Generation Network	Netzwerk das innerhalb eines Kraftwerks benutzt wird
	Plant Control	Kraftwerkssteuerung; steuert die Energieumwandlung; fährt Kraftwerke je nach Bedarf hoch und runter
Transmission	Substation Networks	Umspannnetzwerke verbinden Geräte innerhalb von Umspannwerken
	ICS/ Field Devices	Industrielle Steuerungssysteme (ICS) dienen der Regelung und Steuerung; als Übertragungsprotokolle werden z.B. Modbus oder DNP3 eingesetzt; Feldgeräte sammeln Statusinformationen und unterstützen die Überwachung und Steuerung durch die Leittechnik
Distribution	FAN	Field Area Network (FAN); Feldgerätenetzwerk; verbindet mehrere Feldgeräte bzw. industrielle Steuerungssysteme (ICS)
	ICS/ Field Devices	Industrielle Steuerungssysteme (ICS) dienen der Regelung und Steuerung; als Übertragungsprotokolle werden z.B. Modbus oder DNP3 eingesetzt; Feldgeräte sammeln Statusinformationen und unterstützen die Überwachung und Steuerung durch die Leittechnik
Customer	CLS	Controllable Local Systems (CLS); dezentral steuerbare Verbraucher- oder Erzeugersysteme wie z.B. Photovoltaikanlagen oder Elektrofahrzeuge
	Display	Anzeigeeinheit; dient der Anzeige von im SM-GW gespeicherten Informationen
	Smart Meter	Elektronische Messeinrichtung; Messung der Verbrauchswerte
	SM-GW	Smart Meter Gateway (SM-GW); zentrale Kommunikationseinheit in der Verbrauchswerte gesammelt werden; Trennung der am SM-GW angeschlossenen Netze
	HAN	Home Area Network (HAN); lokales Heimnetzwerk an dem CLS und Display angeschlossen sind; Verwendete Übertragungsstandards z.B. Fast-Ethernet (IEEE 802.3 Clause 25), Gigabit-Ethernet (IEEE 802.3 Clause 40), WLAN (IEEE 802.11 g/n), PLC
	LMN	Local Metrological Network (LMN), lokales Messeinrichtungsnetz an dem ein oder mehrere Smart Meter angeschlossen sind; Verwendete Übertragungsstandards: z.B. M-Bus (EN 13757-2, EN 13757-3 ), Wireless M-Bus (EN 13757-4), ZigBee/IEEE 802.2.15.4, WLAN (IEEE 802.11), PLC (ITU-T G.9955/9956 oder proprietäre Standards), seriell

Tabelle A.1: Referenzarchitektur - Entities & Networks Teil 1

Domain	Entity / Network	Beschreibung
Markets	Energy Market	Handel mit Energie an Energiebörsen z.B. European Energy Exchange (EEX) in Leipzig; die Energiemärkte stellen Informationen über Energiepreise zur Verfügung
Services	Services	Messdienstleistung; Abrechnung; Kundenportal, Fremdhersteller-Dienste stellen dem Verbraucher verschiedene Zusatzdienste wie z.B. Energieberatung oder Steuerung von Verbrauchern zur Verfügung
Control & Operations	Control- / Operations Center	Leittechnik; Steuerung und Überwachung der Erzeugung, Übertragung und Verteilung von Energie
-	MAN	Metropolitan Area Network (MAN); Verbindung mehrerer Kraftwerknetzwerke über eigene Netze der Netzbetreiber oder über Backbonenetze von Telekommunikationsnetzbetreibern, zur Übertragung werden dabei z.B. Glasfasernetze mit SDH-Übertragung eingesetzt
-	WAN/Backhaul	Wide Area Network (WAN), Weitverkehrsnetz das zur Anbindung der MAN dient; Backhaul verbindet die Leittechnik mit den Umspannnetzwerken, den Feldgeräten und den industriellen Steuerungssystemen. Das Backhaul Netz gehört entweder dem Netzbetreiber oder es wird auf das Netz eines öffentlichen Telekommunikationsnetzbetreibers zurückgegriffen. Dabei werden kabelgebundene (z.B. Glasfaser) oder kabellose (z.B. Richtfunk) Kommunikationstechnologien eingesetzt
-	AMI/NAN	AMI (Advanced Metering Infrastructure) bzw. Neighborhood Area Network (NAN); Netzwerkstruktur zur Zählerfernauslesung, verbindet die Leittechnik mit Feldgerätenetzwerken, Smart Meter Gateway oder dezentrale Energieerzeuger beim Verbraucher; Dabei werden kabelgebundene (z.B. Glasfaser) oder kabellose (z.B. WLAN, GPRS, UMTS) Kommunikationstechnologien bzw. Standards eingesetzt
-	Internet	Das öffentliche Internet dient zur Übertragung von Informationen; Verbraucher greifen darüber z.B. auf Fremdhersteller-Dienste oder auf das Kundenportal ihres Netzbetreibers zu

Tabelle A.2: Referenzarchitektur - Entities & Networks Teil 2

## A.2 Reference Points

Reference Point	Entity 1 / Network 1	Entity 1 / Network 2	Beschreibung
R1	CLS	HAN	Verbindet das SM-GW über das Home Area Network mit steuerbaren Verbrauchern (z.B. Kühlschrank, Elektrofahrzeug) bzw. Erzeugern (z.B. Photovoltaik-Anlagen)
R2	Display	HAN	Verbindet Anzeigeeinheiten mit dem SM-GW über das Home Area Network
R3	HAN	SM-GW	Verbindung des Heimgerätenetzwerk an das SM-GW per Ethernet (802.3 Clause 25/40) oder W-LAN (IEEE 802.11 g/n)
R4	LMN	SM-GW	Anbindung von Smart Metern an das Smart Meter Gateway, verwendete Standards z.B. M-Bus (EN 13757-2, EN 13757-3 ), Wireless M-Bus (EN 13757-4), ZigBee/IEEE 802.2.15.4, WLAN (IEEE 802.11 g/n), PLC (ITU-T G.hn & G.hnem oder proprietäre Standards); Smart Meter setzen z.B. auch auf optische (Infrarot) Datenschnittstelle D0 nach DIN EN 62056-21
R5	SM-GW	AMI/NAN	Verbindet das SM-GW mit der Netzwerkstruktur zur Zählerfernauslesung, Anbindung per PLC (BPL), W-LAN (IEEE 802.11 g/n), ZigBee/IEEE 802.2.15.4
R6	AMI/NAN	FAN	Verbindet das NAN an das Feldgerätenetzwerk
R7	FAN	ICS/Field Devices	Verbindung von Feldgerätenetzwerken mit Feldgeräten bzw. Industriellen Steuerungssystemen; als Protokolle werden z.B. DNP3, IEC 61850 oder Modbus eingesetzt
R8	AMI/NAN	WAN/Backhaul	Verbindung von AMI/NANA mit dem Weitverkehrsnetz bzw. Backhaul
R9	WAN/Backhaul	Substation Networks	Verbindung der Umspannnetzwerke an das Backhaul Netz bzw. an ein öffentliches Weitverkehrsnetz
R10	Substation Networks	ICS/Field Devices	Verbindung von Umspannnetzwerken mit Feldgeräten bzw. Industriellen Steuerungssystemen, Als Protokolle werden z.B. DNP3, Modbus oder IEC 61850 eingesetzt
R11	WAN/Backhaul	MAN	Verbindung des Weitverkehrsnetz mit regionalen Netzen
R12	MAN	Generation Network	Verbindung der lokalen Kraftwerksnetze an regionale Netze

Tabelle A.3: Referenzarchitektur - Reference Points, Teil 1

Reference Point	Entity 1 / Network 1	Entity 1 / Network 2	Beschreibung
R13	Generation Network	Plant Control	Verbindung der Kraftwerkssteuerung an das lokale Kraftwerksnetz
R14	MAN	Control-/ Operations Center	Verbindung der Leittechnik mit regionalen Netzen
R15	WAN/ Backhaul	Control-/ Operations Center	Verbindung der Leittechnik mit dem Weitverkehrsnetz bzw. Backhaul
R16	AMI/NAN	Control-/ Operations Center	Verbindung der Leittechnik mit dem Zählerfernauslesungsnetz. Ermöglicht Zugriff auf die Feldgerätenetzwerke und die dort angeschlossenen Feldgeräte
R17	Control-/ Operations Center	Internet	Verbindung der Leittechnik an das Internet
R18	Control-/ Operations Center	Services	Verbindet Leittechnik mit Dienstleistern um Informationen (z.B. aktuelle Verbrauchsinformationen oder um Laststeuerung zu ermöglichen)
R19	Internet	Services	Verbindung zwischen Dienstleistern und dem Internet
R20	Internet	SM-GW	Verbindet das SM-GW mit dem Internet; Anbindung z. B. per DSL, Kabel, Satellit, GSM, UMTS, ISDN, PLC (BPL)
R21	Services	Energy Market	Verbindet Energiemärkte und Dienstleister, Austausch von Energiepreisinformationen
R22	Internet	Energy Market	Verbindet Energiemärkte mit dem Internet
R23	Energy Market	WAN/ Backhaul	Verbindet Energiemärkte mit dem Weitverkehrsnetz; Informationen der Energiemärkte gelangen darüber Zwischenschritte weiter bis zur Kraftwerkssteuerung

Tabelle A.4: Referenzarchitektur - Reference Points, Teil 2

## B Angriffe und Bedrohungsszenarien

### B.1 Bedrohungsbäume

Als ein mögliches Hilfsmittel zur Erfassung von Bedrohungen können Bedrohungs- bzw. Angriffs-bäume (engl. attack tree) dienen wie sie in diesem Abschnitt gezeigt werden. In der Wurzel des Baumes wird dabei ein mögliches Hauptangriffsziel bzw. eine mögliche Bedrohung eingetragen. Die inneren Knoten bzw. Ebenen darunter beschreiben jeweils verschiedene Kombinationen von Bedingungen, als Zwischenziele, die erfüllt werden müssen damit das Hauptangriffsziel eintritt. Mit UND- bzw. ODER-Verbindungen sind die Zwischenziele miteinander verknüpft. Diese beschreiben, ob die Zwischenziele gemeinsam erfüllt sein müssen oder es ausreicht das mindestens eines erfüllt wird. Bedrohungen, die alternativ zum Eintreten übergeordneter Zwischenziele bzw. des Hauptziels beitragen, werden ODER-verknüpft, wohingegen Bedrohungen, die gemeinsam eintreten müssen, damit ein übergeordnetes Zwischenziel bzw. das Hauptziel eintritt, UND-verknüpft werden. Einzelne Angriffsschritte werden durch die Blätter des Baumes beschrieben. Die möglichen Pfade innerhalb des Baumes von den einzelnen Blättern bis zur Wurzel beschreiben unterschiedliche Angriffswege.<sup>271</sup> Die in [Abb. B.1](#) bis [B.6](#) dargestellten Bedrohungsbäume sind allgemein gehalten. Einzelne Blätter sind nicht unbedingt vollständig oder sie sind zusammengefasst und können noch weiter unterteilt werden. Sie sollen Einblick in Bedrohungen geben, welche nicht im Rahmen der Bedrohungsanalyse behandelt wurden.

---

<sup>271</sup>Vgl. Eckert: IT-Sicherheit (2012), [\[12\]](#), S. 200-208.

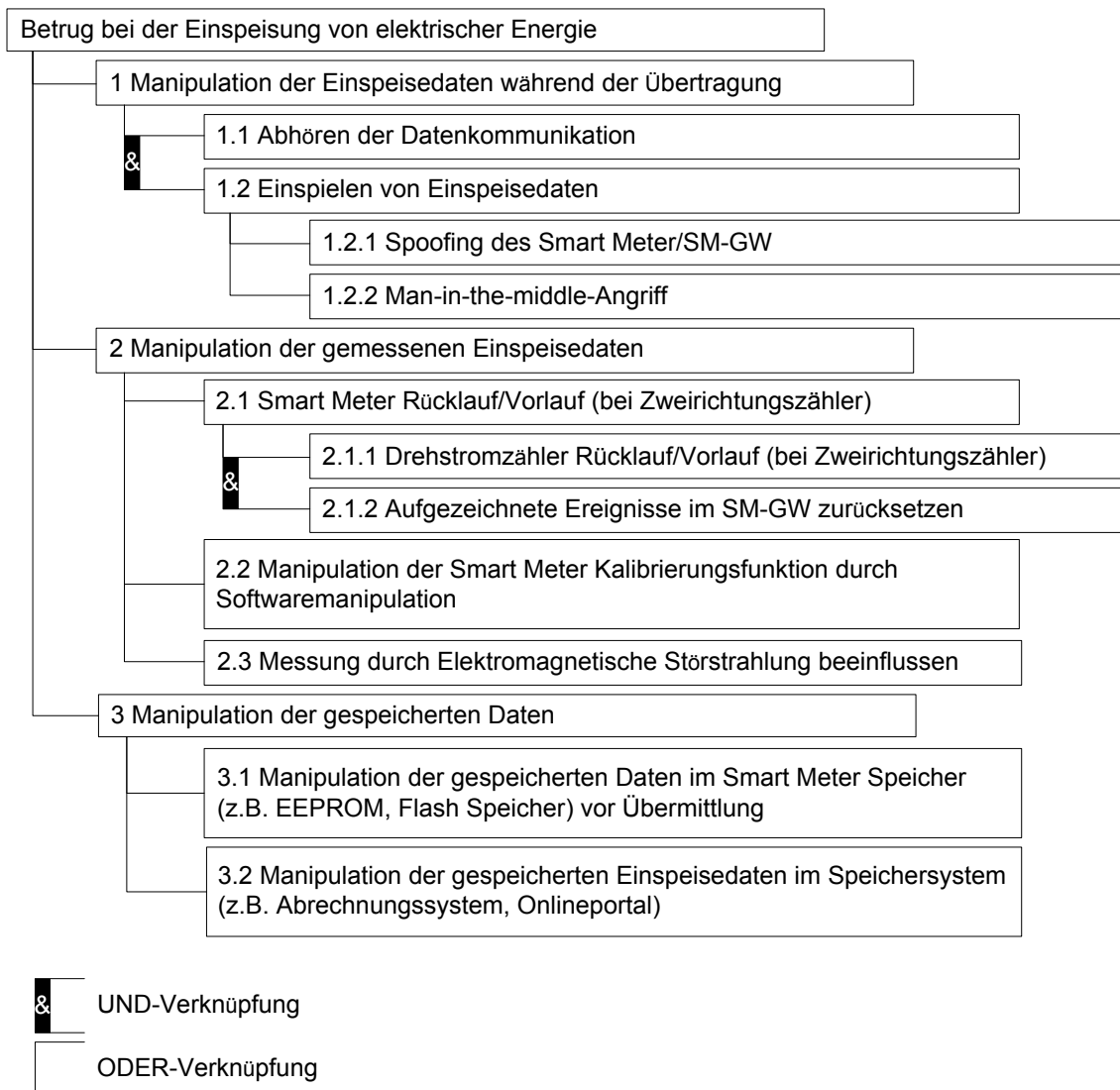


Abbildung B.1: Allgemeiner Bedrohungsbaum-Betrug bei der Einspeisung von elektrischer Energie



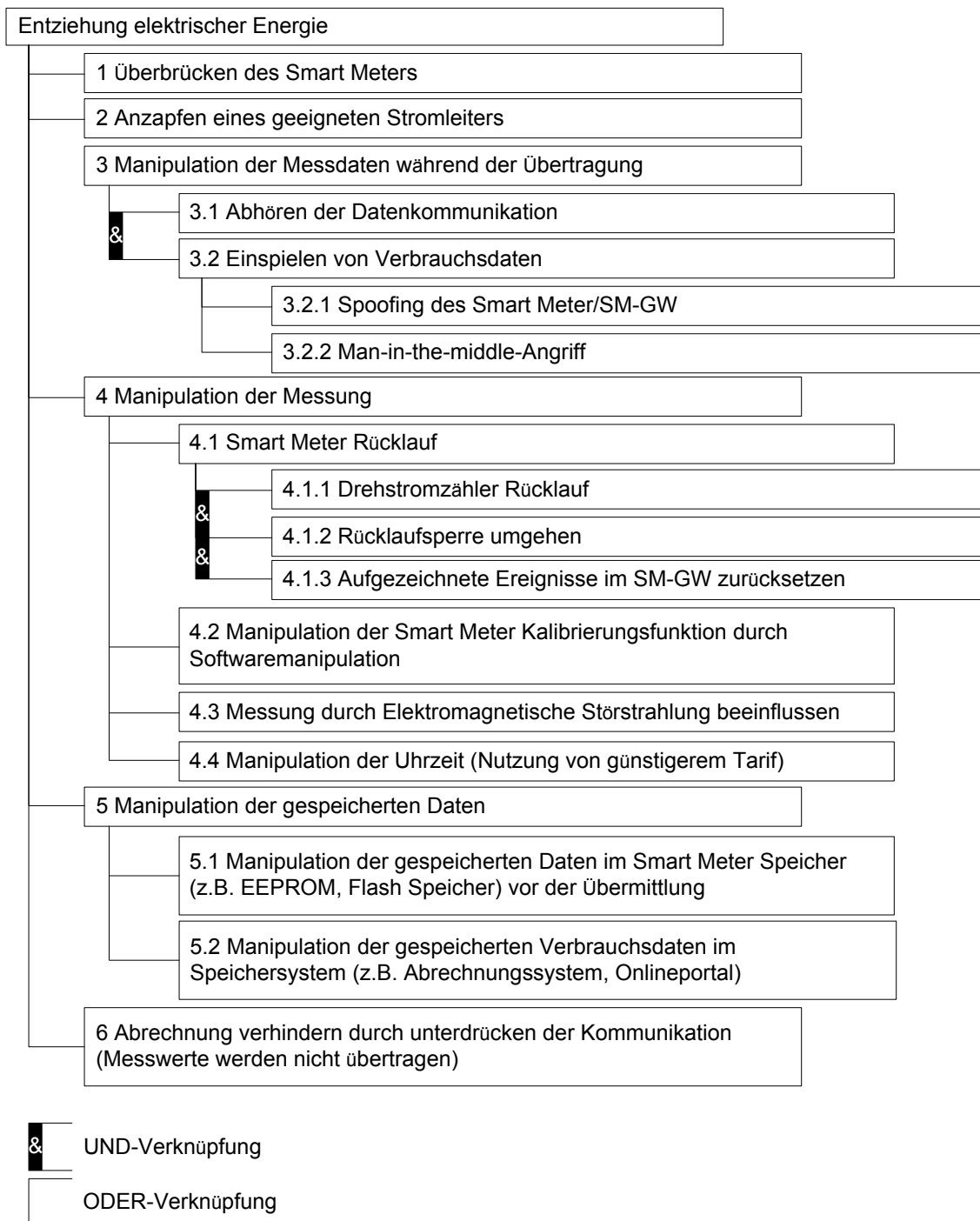


Abbildung B.2: Allgemeiner Bedrohungsbaum-Entziehung elektrischer Energie

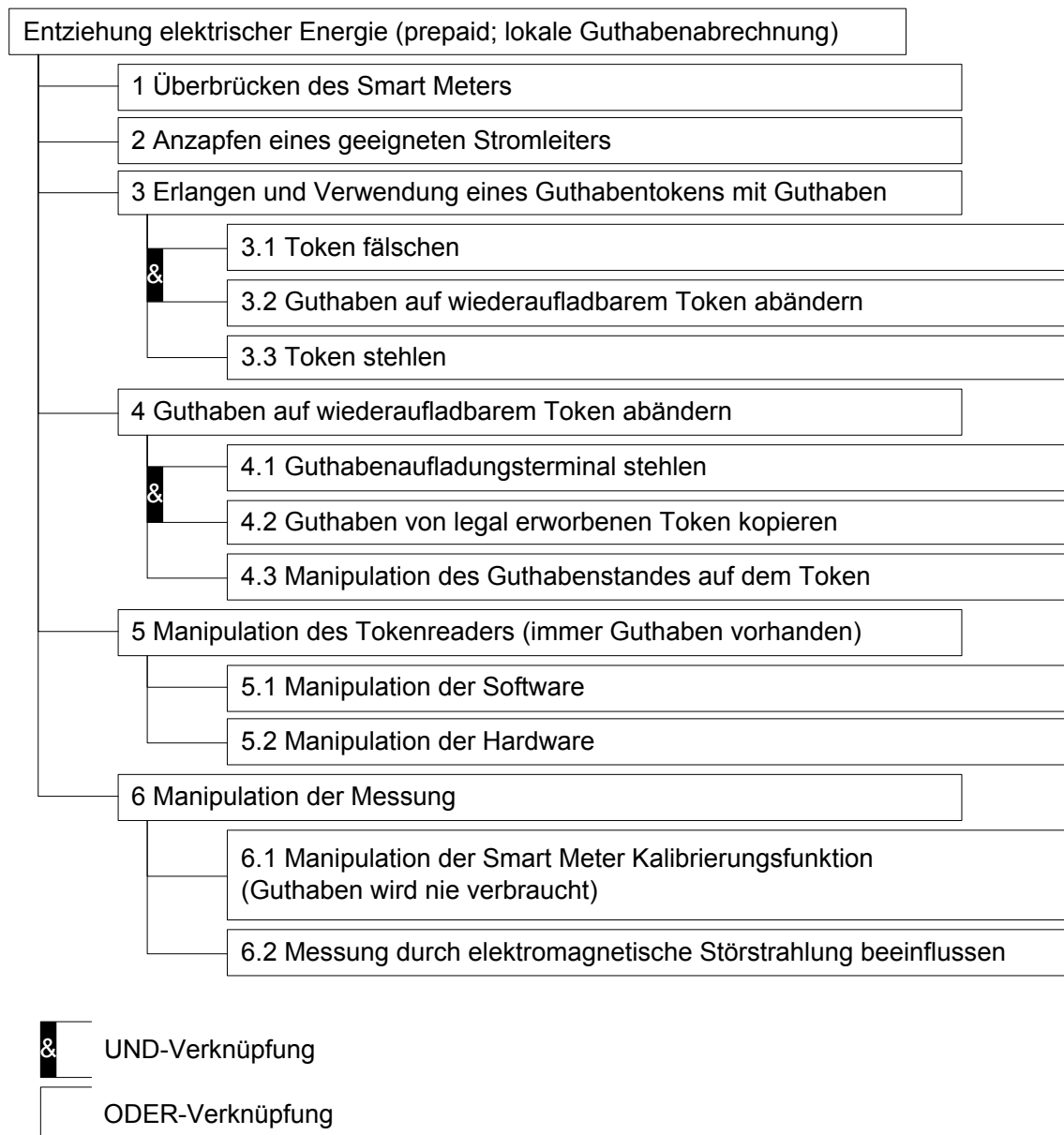


Abbildung B.3: Allgemeiner Bedrohungsbaum-Entziehung elektrischer Energie beim Einsatz von Prepaid Smart Metern mit lokalem Guthaben Abrechnungssystem

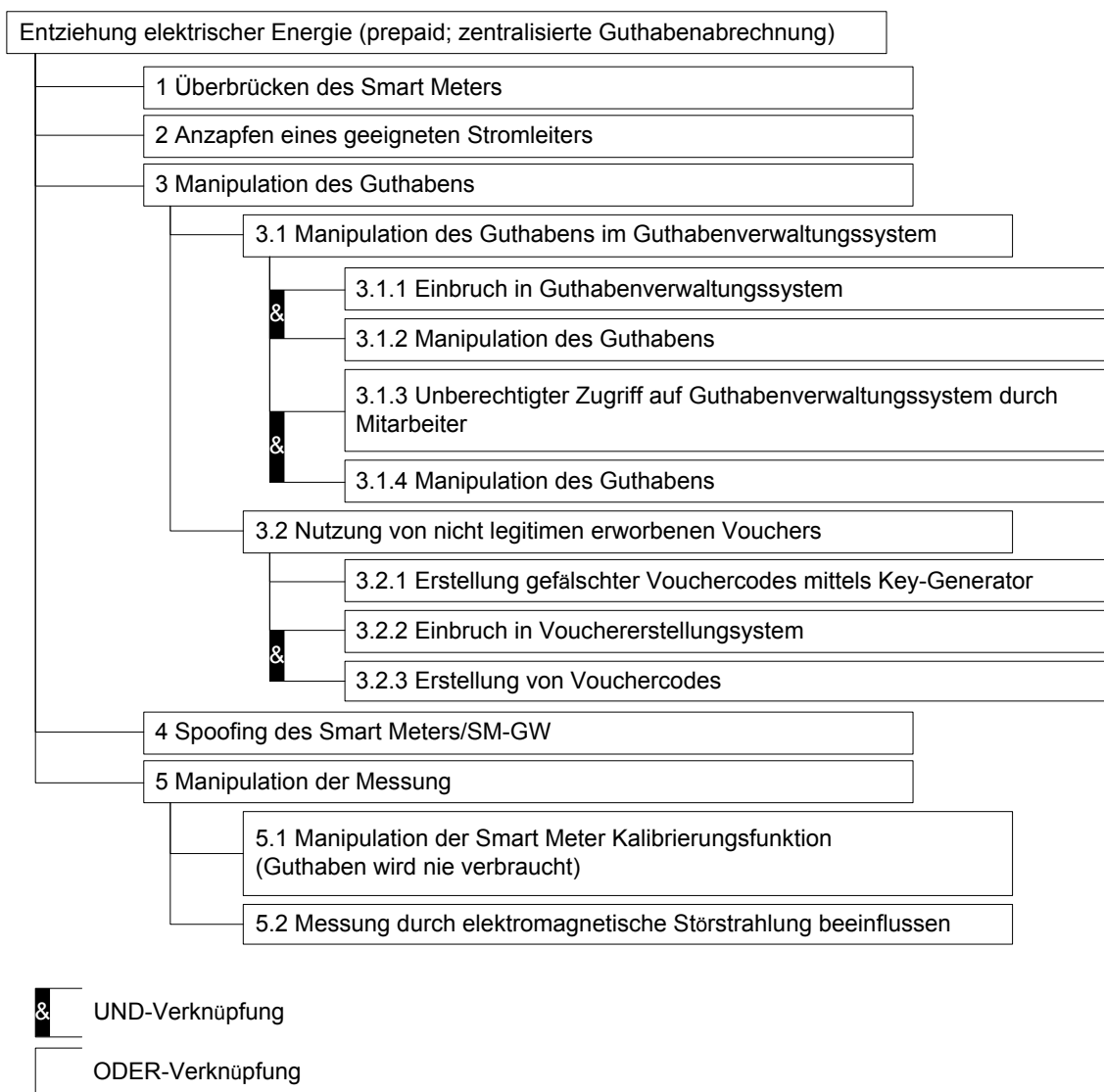
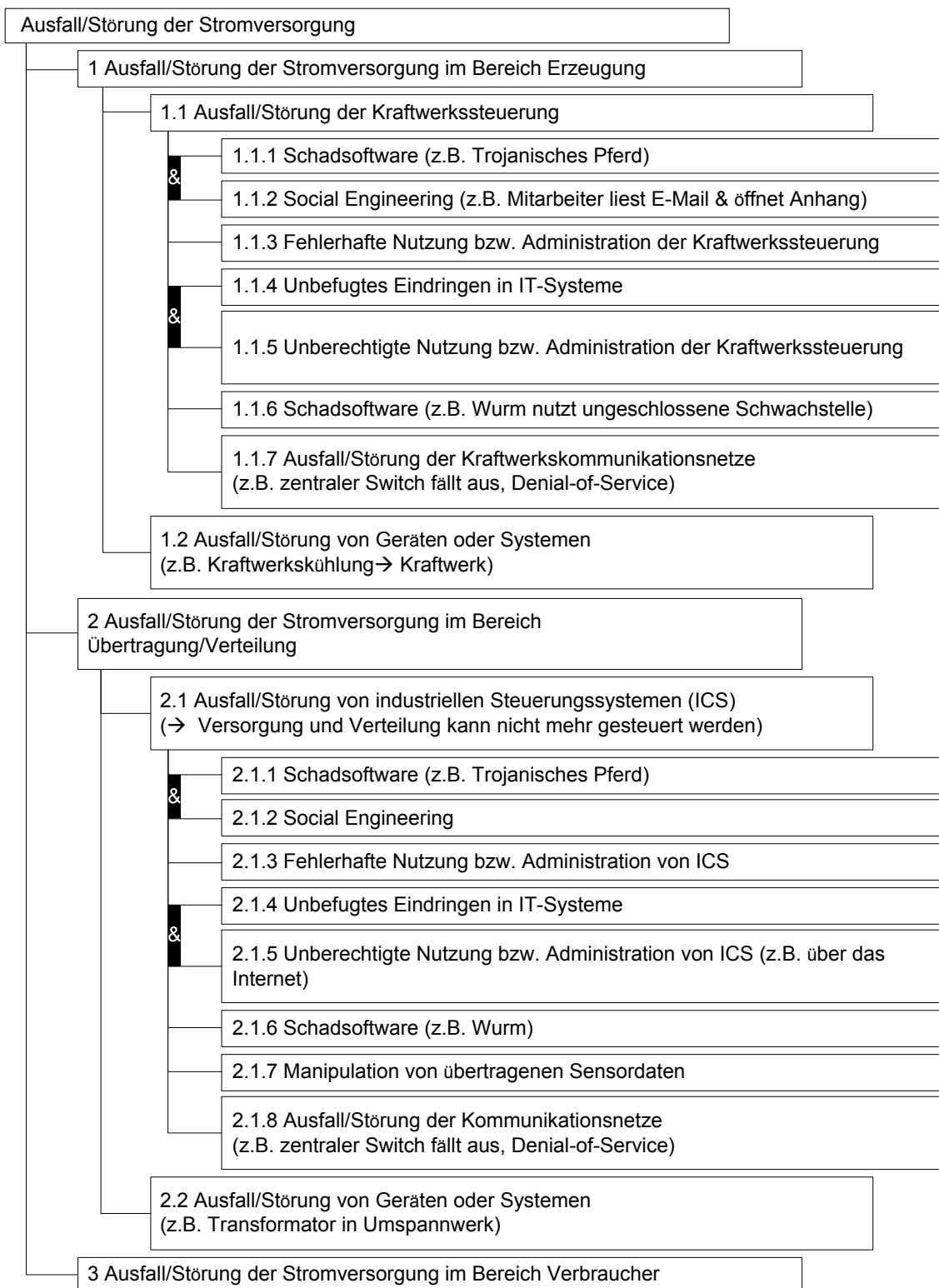


Abbildung B.4: Allgemeiner Bedrohungsbaum-Entziehung elektrischer Energie beim Einsatz von Prepaid Smart Metern mit zentralisiertem Abrechnungssystem





-  UND-Verknüpfung
-  ODER-Verknüpfung

Abbildung B.5: Allgemeiner Bedrohungsbaum-Ausfall/Störung der Stromversorgung in den Bereichen Erzeugung, Übertragung, Verteilung und Verbraucher, Teil 1

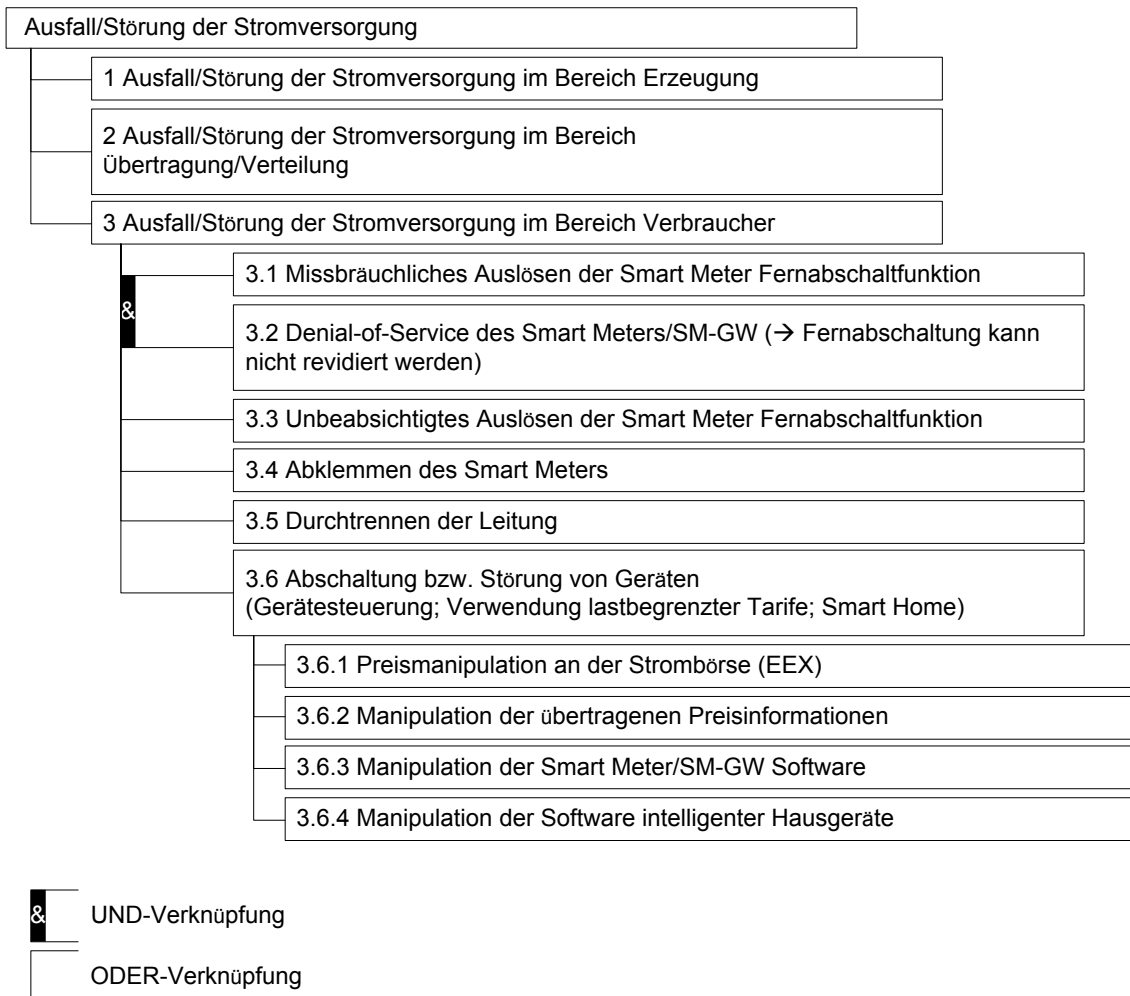


Abbildung B.6: Allgemeiner Bedrohungsbaum-Ausfall/Störung der Stromversorgung in den Bereichen Erzeugung, Übertragung, Verteilung und Verbraucher, Teil 2

## B.2 Bedrohungsanalyse




Abbildung B.7: Discovery Smart Meter/SM-GW mit geöffnetem SM-GW Gehäuse<sup>272</sup>



Abbildung B.8: Discovery Smart Meter/SM-GW mit geschlossenem SM-GW Gehäuse<sup>273</sup>

<sup>272</sup>Quelle: Hornung: Das Vierte Quartal: Aussicht auf Erfolg (2012), [111].

<sup>273</sup>Quelle: Bachfeld, Carluccio und Wegener: Wer hat an der Uhr gedreht? (2011), [4]; Anm.: Die Plombe ist gut zu erkennen



### Dieser Verbindung wird nicht vertraut

Sie haben Firefox angewiesen, eine gesicherte Verbindung zu **discovery.com** aufzubauen, es kann aber nicht überprüft werden, ob die Verbindung sicher ist.

Wenn Sie normalerweise eine gesicherte Verbindung aufbauen, weist sich die Website mit einer vertrauenswürdigen Identifikation aus, um zu garantieren, dass Sie die richtige Website besuchen. Die Identifikation dieser Website dagegen kann nicht bestätigt werden.

#### Was sollte ich tun?

Falls Sie für gewöhnlich keine Probleme mit dieser Website haben, könnte dieser Fehler bedeuten, dass jemand die Website fälscht. Sie sollten in dem Fall nicht fortfahren.

#### ▼ Technische Details

discovery.com verwendet ein ungültiges Sicherheitszertifikat.

Das Zertifikat gilt nur für [\\*.discovery.com](https://*.discovery.com).  
Das Zertifikat ist am 29.01.2012 00:59 abgelaufen. Die aktuelle Zeit ist 30.01.2012 13:43.

(Fehlercode: ssl\_error\_bad\_cert\_domain)

#### ▼ Ich kenne das Risiko

Wenn Sie wissen, warum dieses Problem auftritt, können Sie Firefox anweisen, der Identifikation dieser Website zu vertrauen. **Selbst wenn Sie der Website vertrauen, kann dieser Fehler bedeuten, dass jemand ihre Verbindung manipuliert.**

Fügen Sie keine Ausnahme hinzu, außer Sie wissen, dass es einen guten Grund dafür gibt, warum diese Website keine vertrauenswürdige Identifikation verwendet.

Abbildung B.9: Zertifikatsfehler beim Aufruf von <https://discovery.com><sup>274</sup>

---

<sup>274</sup>Screenshot des Programms Firefox vom 30.01.2012.

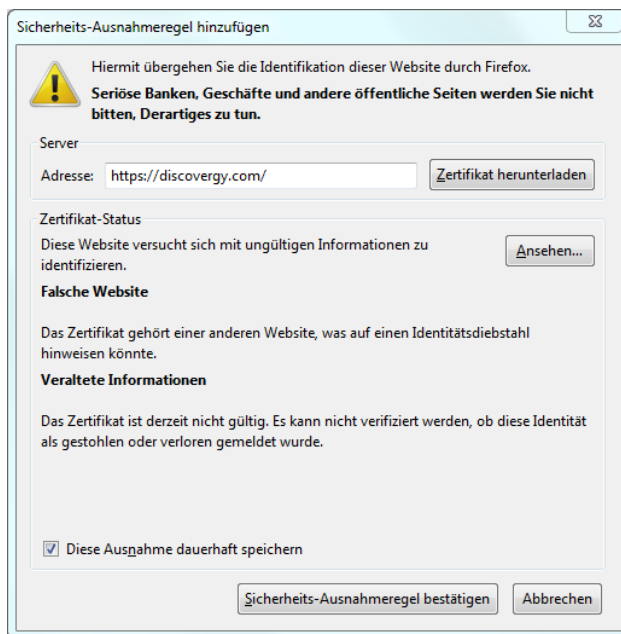


Abbildung B.10: Zertifikat-Status der Adresse <https://discovery.com><sup>275</sup>

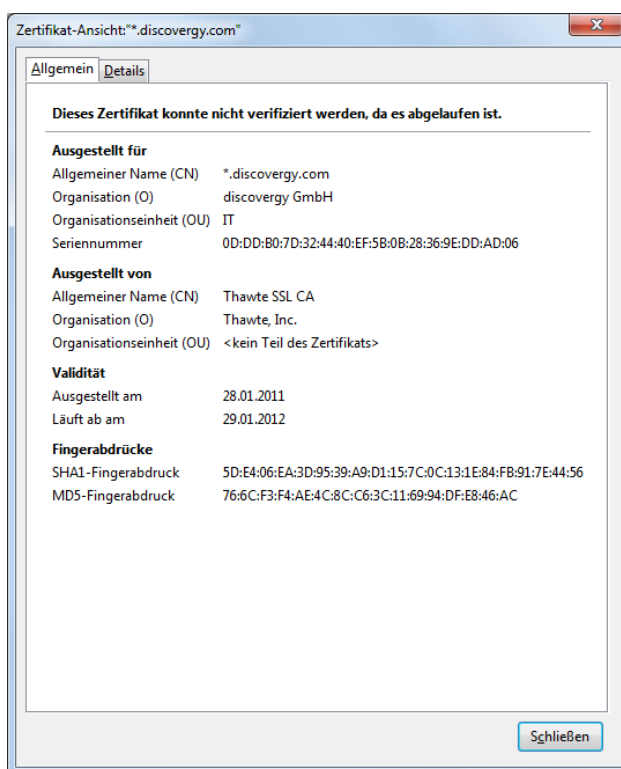


Abbildung B.11: Informationen zum Zertifikat der Adresse <https://discovery.com><sup>276</sup>

<sup>275</sup>Screenshot des Programms Firefox vom 30.01.2012.

<sup>276</sup>Screenshot des Programms Firefox vom 30.01.2012.



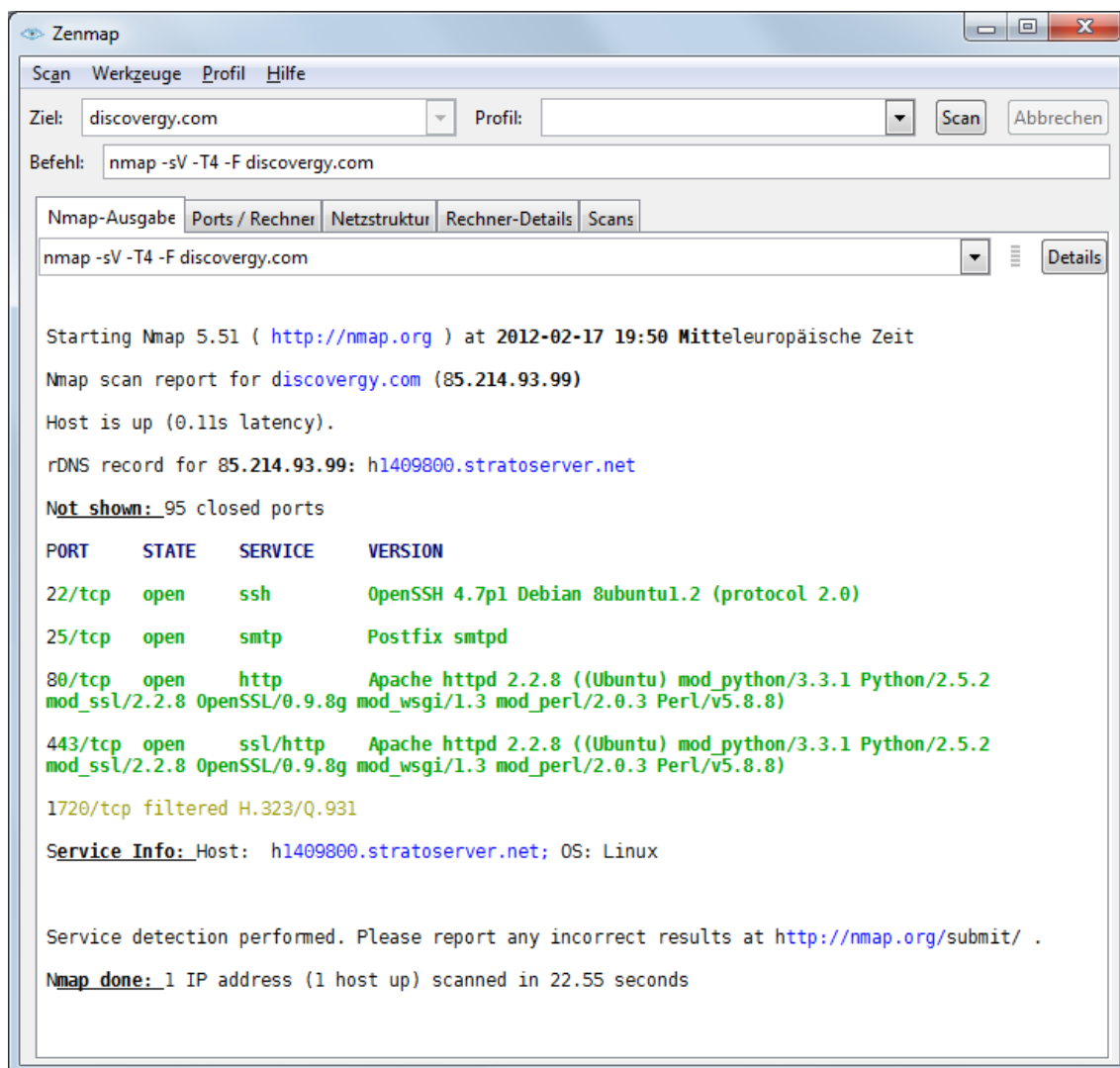


Abbildung B.12: Diensterkennung mit dem Portscanner Nmap für das Ziel discoverygy.com<sup>277</sup>

Die Ursachen für Bedrohungen werden in der Bedrohungsanalyse in den Tabellen B.1 bis B.9 in der Spalte „Bedrohung Nr.“ mit B für Bedrohung gekennzeichnet. Bei Bedrohungen, die mit „AB“ gekennzeichnet sind, handelt es sich um abstrakte Bedrohungen. Diese Bedrohungen können noch weiter in detailliertere Bedrohungen aufgeteilt werden.

<sup>277</sup>Screenshot des Programms Zenmap vom 17.02.2012.

<b>Bedrohung Nr.</b>	<b>Beschreibung</b>
AB1	Unautorisierter Einsicht von Informationen
AB1.1	Unautorisierte Einsicht auf Messdaten
AB1.1.1	Unautorisierte Einsicht auf Messdaten (Zählerstand, Summe der momentanen Leistung der Phasen) am Smart Meter/SM-GW : Für einen Angriff ist der Zugang zum Zählerschrank im Keller des Hauses erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in die Räumlichkeiten.
B1	am Smart Meter durch öffnen des Zählerschranks und ablesen der Messwerte auf dem Smart Meter Display (LCD).
B2	am SM-GW durch öffnen des Zählerschranks und auslesen an der USB-Schnittstelle.
B3	Unautorisierte Einsicht auf Leistungswerte am Smart Meter durch öffnen des Zählerschranks und auslesen am Impulsausgang (LED) mit Hilfe eines Impulslesers und einem PC.
AB1.1.2	Unautorisierte Einsicht auf Messdaten (Zählerstandes, Summe der momentanen Leistung der Phasen, momentane Einzelleistung der Phasen sowie Statusinformationen) bei der Übertragung...
B4	zwischen Smart Meter und SM-GW durch Abhören der Datenkommunikation an der D0-Schnittstelle. Das verplombte Gehäuse des SM-GW muss hierfür geöffnet werden und an die optische D0-Schnittstelle muss außerdem ein optischer Auslesekopf angeschlossen werden, der mit einem PC verbunden wird. Für den Angriff ist ein Zugang zum Zählerschrank im Keller des Hauses erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
B5	zwischen SM-GW und PLC-Adapter mit Hilfe eines zwischengeschalteten Hub oder Switch (mit eingerichteten Mirror-Port). Für den Angriff ist ein Zugang zum Zählerschrank im Keller des Hauses erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
B6	zwischen dem PLC-Adapter im Keller und PLC-Adapter in der Wohnung durch Abhören des Datenverkehrs (Stromleitung = Shared Medium vgl. mit Ethernet Hub) mit Hilfe eines PLC-Adapters der am selben Stromkreis angeschlossen wird. Da die Daten transparent mit AES 128 Bit verschlüsselt übertragen werden müssen die mitgehörten Daten vor der Einsicht entschlüsselt werden. Für den Angriff ist ein Zugang zum Haus erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
B7	zwischen dem PLC-Adapter im Keller und PLC-Adapter in der Wohnung durch Abhören des Datenverkehrs (Stromleitung = Shared Medium vgl. mit Ethernet Hub) mit einem PLC-Adapter der am selben Stromkreis angeschlossen wird und anschließender Verkehrsanalyse. Für den Angriff ist ein Zugang zum Haus erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.

Tabelle B.1: Detaillierte Bedrohungsanalyse, Teil 1

<b>Bedrohung Nr.</b>	<b>Beschreibung</b>
AB1.1.2	Unautorisierte Einsicht auf Messdaten (Zählerstand, Summe der momentanen Leistung der Phasen, momentane Einzelleistung der Phasen sowie Statusinformationen) bei der Übertragung...
B8	zwischen dem PLC-Adapter in der Wohnung und DSL-Router durch Abhören der Datenkommunikation mit Hilfe eines an einen zwischengeschalteten Hub oder Switch (mit eingerichteten Mirror-Port) angeschlossenen PC. Für den Angriff ist ein Zugang zur Wohnung des DSL-Anschlussnehmers erforderlich. Falls dieser dort nicht wohnt, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
B9	zwischen dem PLC-Adapter in der Wohnung und DSL-Router durch Abhören des Datenverkehrs am Switch des DSL-Routers mit Hilfe eines man-in-the-middle-Angriff mittels ARP-Spoofing. Für den Angriff ist ein Zugang zur Wohnung des DSL-Anschlussnehmers erforderlich. Falls dieser dort nicht wohnt, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
B10	zwischen PLC-Adapter und DSL-Router durch Abhören des Datenverkehrs mit Hilfe des DSL-Routers (z.B. Router mit OpenWrt und tcpdump, oder AVM FRITZ!Box). Der Angreifer muss hierzu die Kontrolle über den DSL-Router haben. Bei einem entfernten Angreifer ist dies z. B. über einen Fernwartungszugang möglich.
B11	zwischen DSL-Router und Discovery Server durch Abhören des Datenverkehrs an einem Router des Internetproviders (Zugriff auf den Router erforderlich)
AB1.1.3	Unautorisierte Einsicht auf gespeicherte Messdaten
AB1.1.3.1	Unautorisierte Einsicht der gespeicherten Verbrauchsdaten/des Lastprofils im Speichersystem Discovery Onlineportal
B12	durch einloggen mit gestohlenen Zugangsdaten
B13	durch einloggen mit Zugangsdaten (erlangen der Zugangsdaten durch durch Bedrohung des Benutzers)
B14	durch einloggen mit Zugangsdaten (erlangen der Zugangsdaten durch Erpressung)
B15	durch einloggen mit Hilfe abgehörter Zugangsdaten (Abhören des Datenverkehrs zum Einlogzeitpunkt, mittels eines auf dem Computer gespeicherten Trojaners)
B16	durch einloggen mit Hilfe abgehörter Zugangsdaten (Abhören des Datenverkehrs zum Einlogzeitpunkt, Abhören des Datenverkehrs an einem Router des Internetproviders (Zugriff auf den Router erforderlich))
B17	durch einloggen mit Hilfe abgehörter Zugangsdaten (Man-in-the-middle Angriff mit Hilfe von DNS Cache Poisoning des DNS-Servers->Umleitung des Datenverkehrs)
B18	durch einloggen mit Hilfe abgehörter Zugangsdaten (DNS-Einträge des DSL-Routers werden z.B. durch den Trojaner DNS-Changer modifiziert An einem Zwischengeschaltetem System (man-in-the-middle) können die Daten abgehört werden.)

Tabelle B.2: Detaillierte Bedrohungsanalyse, Teil 2

<b>Bedrohung Nr.</b>	<b>Beschreibung</b>
AB1.1.3.1	Unautorisierte Einsicht der gespeicherten Verbrauchsdaten/des Lastprofils im Speichersystem Discovery Onlineportal
B19	durch einloggen mit Zugangsdaten (erlangen der Zugangsdaten durch Social Engineering mit Hilfe einer Phishing E-Mail, sodass der Benutzer seine Zugangsdaten z.B. auf einer vorgefertigten Webseite eingibt)
B20	durch einloggen mit Zugangsdaten (das Passwort des Benutzers wird per Brute-Force ermittelt)
B21	durch einloggen mit Zugangsdaten (das Passwort des Benutzers wird per Wörterbuchangriff ermittelt)
B22	Mittels SQL-Injection in der Login-Maske gelangt der Angreifer an die Informationen
B23	Ausnutzen einer Fehlkonfigurationen, Zugangsdaten des Administrator Accounts entsprechen Default Einstellung (z.B user: admin, passwort: admin)
B24	durch Missbrauch von Berechtigungen. Insider mit Zugang zum Speichersystem und Berechtigung zum Zugriff auf die Daten
B25	durch unbeabsichtigte Veröffentlichung. (Fehlerhafte Nutzung bzw. Administration des Online Portals)
AB1.1.3.2	Unautorisierte Einsicht der gespeicherten Verbrauchsdaten/des Lastprofils im Speichersystem der Stadtwerke
B25	Unautorisierte Einsicht der Zählerstände im Speichersystem (Abrechnungssystem der Stadtwerke, nur im LAN der Stadtwerke abrufbar) durch Missbrauch von Berechtigungen. Insider mit Zugang zum Speichersystem und Berechtigung zum Zugriff auf die Daten
B26	Unautorisierte Einsicht der Zählerstände im Speichersystem (Abrechnungssystem der Stadtwerke, nur im LAN der Stadtwerke abrufbar) durch Schadsoftware im Stadtwerke LAN, welche die Daten an einen Angreifer weiterleitet
AB1.2	Unautorisierte Einsicht auf Konfigurationsdaten
B28	Unautorisierte Einsicht der SM-GW Konfiguration durch öffnen des Zählerschranks und auslesen an der USB-Schnittstelle. Für den Angriff ist ein Zugang zum Zählerschrank im Keller des Hauses erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
AB1.3	Unautorisierte Einsicht auf Kundendaten
B29	Unautorisierte Einsicht der Kundendaten von Discovery (Excel Tabellen)
AB1.4	Unautorisierte Einsicht auf Daten von Industriellen Steuerungssystemen (Bereich Übertragung, Verteilung, Kraftwerkssteuerung)
AB1.4.1	Unautorisierte Einsicht auf Daten von Industriellen Steuerungssystemen (z.B. Statusmeldungen vom Anlagenzustand, Fehler) und Zugriff über das Internet
B30	durch einloggen mit Zugangsdaten (Nutzung festkodierter Nutzernamen- und Passwortkombination)
B31	durch einloggen mit Zugangsdaten (Passwort wird per Brute-Force ermittelt)
B32	durch einloggen mit Zugangsdaten (erlangen der Zugangsdaten durch Social Engineering mit Hilfe einer Phishing E-Mail, sodass der Benutzer seine Zugangsdaten z.B. auf einer vorgefertigten Webseite eingibt)
B33	Mittels SQL-Injection in der Login-Maske erlangt der Angreifer Zugriff
B34	durch Missbrauch von Berechtigungen. Insider mit Zugang zum Industriellen Steuerungssystem und Berechtigung zum Zugriff auf die Daten

Tabelle B.3: Detaillierte Bedrohungsanalyse, Teil 3<sup>278</sup>

<sup>278</sup>Anm.:Zu B29 vgl. Hornung: Das Vierte Quartal: Aussicht auf Erfolg (2012), [111].

<b>Bedrohung Nr.</b>	<b>Beschreibung</b>
AB1.4	Unautorisierte Einsicht auf Daten von Industriellen Steuerungssystemen (Bereich Übertragung, Verteilung, Kraftwerkssteuerung)
AB1.4.2	Unautorisierte Einsicht auf Daten von Industriellen Steuerungssystemen (z.B. Statusmeldungen vom Anlagenzustand, Fehler) und Zugriff über das Internet
AB1.4.2.1	bei der Übertragung im Kraftwerksnetzwerk.
AB1.4.2.2	bei der Übertragung im MAN
AB1.4.2.3	bei der Übertragung im WAN/Backhaul
AB1.4.2.4	bei der Übertragung im FAN
AB1.4.2.5	bei der Übertragung in Umspannnetzwerken
AB2	Manipulation von oder Diebstahl von Informationen
AB2.1	Manipulation der Messdaten
AB2.1.1	Manipulation bei der Messung (Für einen Angriff ist der Zugang zum Zähler-schrank im Keller des Hauses erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.)
B35	Manipulation der Messung in dem die Rücklaufsperrung (durch Manipulation der Hardware) umgangen und anschließend ein Smart Meter Rücklauf durchgeführt wird.
B36	Manipulation der Smart Meter Kalibrierungsfunktion durch Manipulation der Smart Meter Software
B37	Manipulation der Smart Meter Kalibrierungseinstellung durch Manipulation der Smart Meter Konfiguration
B38	Manipulation der Messung indem das Smart Meter über elektromagnetische Störstrahlung beeinflusst wird
AB2.1.2	Manipulation der Messdaten während der Übertragung
AB2.1.2.1	Manipulation der Messdaten bei der Übertragung zwischen Smart Meter und SM-GW durch Abhören der Datenkommunikation an der D0-Schnittstelle des Smart Meter und anschließendes Einspielen von
B39	veränderten Messdaten an der D0-Schnittstelle des SM-GW. Das verplombte Gehäuse des SM-GW muss geöffnet werden und an die optische D0-Schnittstelle des Smart Meters muss außerdem ein optischer Auslesekopf angeschlossen werden, der mit einem PC verbunden wird. Die Messdaten werden mit Hilfe eines Programms verändert und anschließend vom PC mittels einer Schaltung (z. B. Infrarot-Seriell Adapter), welche an das SM-GW angeschlossen ist, weitergeben. Für den Angriff ist ein Zugang zum Zählerschrank im Keller des Hauses erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
B40	generierten Messdaten an der D0-Schnittstelle des SM-GW. Das verplombte Gehäuse des SM-GW muss geöffnet werden und an die optische D0 Schnittstelle des Smart Meters muss außerdem ein optischer Auslesekopf gemäß angeschlossen werden der mit einem PC verbunden wird. Die am PC mit Hilfe eines Programms generierten Messdaten werden mittels einer Schaltung (z. B. Infrarot-Seriell Adapter), welche an das SM-GW angeschlossen ist, weitergeben. Für den Angriff ist ein Zugang zum Zählerschrank im Keller des Hauses erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.

Tabelle B.4: Detaillierte Bedrohungsanalyse, Teil 4

Bedrohung Nr.	Beschreibung
AB2.1.2.1	Manipulation der Messdaten bei der Übertragung zwischen Smart Meter und SM-GW durch Abhören der Datenkommunikation an der D0-Schnittstelle des Smart Meter und anschließendes Einspielen von
B41	bereits abgehörten Messdaten an der D0 Schnittstelle des SM-GW. Das verplombte Gehäuse des SM-GW muss geöffnet werden und an die optische D0-Schnittstelle muss außerdem ein optischer Auslesekopf angeschlossen werden der mit einem PC verbunden wird. Bereits abgehörte Messdaten (Replay-Angriff) werden vom PC mittels einer Schaltung (z. B. Infrarot-Seriell Adapter), welche an das SM-GW angeschlossen ist, weitergeben. Für den Angriff ist ein Zugang zum Zählerschrank im Keller des Hauses erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
AB2.1.2.2	Manipulation der Messdaten bei der Übertragung zwischen SM-GW und PLC-Adapter durch Abhören der Datenkommunikation mit Hilfe eines zwischengeschalteten Hub oder Switch (mit eingerichtetem Mirror-Port) und anschließendem einspielen von
B41	mit Hilfe eines Programms veränderter Messdaten. Für den Angriff ist ein Zugang zum Zählerschrank im Keller des Hauses erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
B42	mit Hilfe eines Programms generierten Messdaten. Für den Angriff ist ein Zugang zum Zählerschrank im Keller des Hauses erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
B43	bereits abgehörten Messdaten (Replay-Angriff). Für den Angriff ist ein Zugang zum Zählerschrank im Keller des Hauses erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
AB2.1.2.3	Manipulation der Messdaten bei der Übertragung zwischen PLC-Adapter im Keller und PLC-Adapter in der Wohnung durch Abhören des Datenverkehrs (Stromleitung = Shared Medium vgl. mit Ethernet Hub) mit Hilfe eines PLC-Adapters, welcher am selben Stromkreis angeschlossen wird, einem man-in-the-middle-Angriff (ARP-Spoofing), anschließendes Einspielen von
B44	am PC mit einem Programm veränderter Messdaten und weiterleiten per PLC. Da die Messdaten transparent mit AES 128 Bit verschlüsselt übertragen werden, müssen sie vor der Manipulation entschlüsselt, angepasst, erneut verschlüsselt und signiert werden. Für den Angriff ist ein Zugang zum Haus erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
B45	am PC mit einem Programm generierten Messdaten per PLC. Da die Messdaten transparent mit AES 128 Bit verschlüsselt übertragen werden, müssen die mit einem Programm generieren Messdaten auch verschlüsselt und signiert werden. Für den Angriff ist ein Zugang zum Haus erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
B46	bereits abgehörten Messdaten (Replay-Angriff; die abgehörten Messdaten können auch verschlüsselt sein). Für den Angriff ist ein Zugang zum Haus erforderlich. Falls der Angreifer nicht ein Bewohner des Hauses ist, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.

Tabelle B.5: Detaillierte Bedrohungsanalyse, Teil 5

<b>Bedrohung Nr.</b>	<b>Beschreibung</b>
AB2.1.2.3	Manipulation der Messdaten bei der Übertragung zwischen PLC-Adapter im Keller und PLC-Adapter in der Wohnung durch Abhören des Datenverkehrs (Stromleitung = Shared Medium vgl. mit Ethernet Hub) mit Hilfe eines PLC-Adapters, welcher am selben Stromkreis angeschlossen wird, einem man-in-the-middle-Angriff (ARP-Spoofing), anschließendes Einspielen von
B47	Veränderung der SM-GW ID (Mac-Adresse->MAC-Spoofing) in den Messdaten und weiterleiten per Ethernet. Für den Angriff ist ein Zugang zur Wohnung des DSL-Anschlussnehmers erforderlich. Falls dieser dort nicht wohnt, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
AB2.1.2.4	Manipulation der Messdaten bei der Übertragung zwischen PLC-Adapter und DSL-Router durch Abhören des Datenverkehrs am Switch des DSL-Routers mit Hilfe eines man-in-the-middle-Angriff mittels ARP-Spoofing,
B48	anschließendes Einspielen von am PC mit einem Programm veränderter Messdaten und weiterleiten per Ethernet. Für den Angriff ist ein Zugang zur Wohnung des DSL-Anschlussnehmers erforderlich. Falls dieser dort nicht wohnt, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
B49	anschließendes Einspielen von am PC mit einem Programm generierten Messdaten und weiterleiten per Ethernet. Für den Angriff ist ein Zugang zur Wohnung des DSL-Anschlussnehmers erforderlich. Falls dieser dort nicht wohnt, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
B50	anschließendes Einspielen von bereits aufgezeichneten Messdaten (Replay-Angriff) und weiterleiten per Ethernet. Für den Angriff ist ein Zugang zur Wohnung des DSL-Anschlussnehmers erforderlich. Falls dieser dort nicht wohnt, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
B51	anschließende Veränderung der SM-GW ID (Mac-Adresse->Mac-Spoofing) in den Messdaten und weiterleiten per Ethernet. Für den Angriff ist ein Zugang zur Wohnung des DSL-Anschlussnehmers erforderlich. Falls dieser dort nicht wohnt, geschieht dies durch unbefugtes Eindringen in Räumlichkeiten.
AB2.1.2.5	Manipulation der Messdaten bei der Übertragung zwischen DSL-Router und Discovery Server durch Abhören des Datenverkehrs an einem Router des Internetproviders,
B53	anschließendes Einspielen von am PC, mit einem Programm veränderter Messdaten an diesem Router und weiterleiten an die Discovery Server.
B54	anschließendes Einspielen von am PC, mit einem Programm generierter Messdaten und weiterleiten an die Discovery Server.
B55	anschließendes Einspielen von bereits aufgezeichneten Messdaten (Replay-Angriff) und weiterleiten an die Discovery Server.
B56	Änderung der SM-GW ID (Mac-Adresse->MAC-Spoofing) und weiterleiten an die Discovery Server.
B57	Manipulation der Messdaten bei der Übertragung zwischen Discovery Server und DSL-Router durch Abhören des Datenverkehrs an einem Router des Internetproviders, anschließendes Einspielen von veränderten Messdaten und weiterleiten an den Benutzer. → Benutzer sieht gefälschte Daten

Tabelle B.6: Detaillierte Bedrohungsanalyse, Teil 6

<b>Bedrohung Nr.</b>	<b>Beschreibung</b>
AB2.1.3	Manipulation von gespeicherten Messdaten
AB2.1.3.1	Manipulation der gespeicherten Daten im Smart Meter
B58	Manipulation der gespeicherten Daten im Smart Meter Speicher (z.B. EEPROM, Flash Speicher) durch öffnen des Zählergehäuses und nutzen einer nicht dokumentierten Serviceschnittstelle/Debugschnittstelle (JTAG). Über diese kann der Speicher Inhalt verändert werden
B59	Manipulation der gespeicherten Daten im Smart Meter Speicher (z.B. EEPROM, Flash Speicher) mit Hilfe von elektromagnetischer Störstrahlung
B60	Manipulation der gespeicherten Daten im Smart Meter Speicher (z.B. EEPROM, Flash Speicher) mit Hilfe einer Schadsoftware
AB2.1.3.2	Manipulation der gespeicherten Daten im SM-GW
B61	Manipulation der gespeicherten Daten im SM-GW Speicher (z.B. EEPROM, Flash Speicher) durch öffnen des verplombten Gehäuses und nutzen einer nicht dokumentierten Serviceschnittstelle. Über diese kann der Speicher Inhalt direkt angesprochen und verändert werden
B62	Manipulation der gespeicherten Daten im SM-GW Speicher (z.B. EEPROM, Flash Speicher) durch Manipulation der Software
AB2.1.3.3	Manipulation der gespeicherten Daten im Speichersystem (Discovery Online-portal)
AB2.1.3.4	Manipulation der gespeicherten Daten im Speichersystem (Abrechnungssystem der Stadtwerke, nur im LAN der Stadtwerke abrufbar) durch Schadsoftware im Stadtwerke LAN, welche die Daten an einen Angreifer weiterleitet
AB2.1.3.5	Manipulation von gespeicherten Messdaten von industriellen Steuerungssystemen (z.B. Statusmeldungen vom Anlagenzustand, Fehler) bei der Übertragung
AB2.1.3.5.1	bei der Übertragung im Kraftwerksnetzwerk
AB2.1.3.5.2	bei der Übertragung im MAN
AB2.1.3.5.3	bei der Übertragung im WAN/Backhaul
AB2.1.3.5.4	bei der Übertragung im FAN
AB2.1.3.5.5	bei der Übertragung in Umspannnetzwerken
AB2.2	Manipulation von Software
AB2.2.1	Manipulation der Software des Smart Meters
B63	Manipulation der Software des Smart Meters durch öffnen des verschweißten Zählergehäuses und Nutzung einer nicht dokumentierten Serviceschnittstelle/Debugschnittstelle (JTAG) zum einspielen einer manipulierten Software/Softwareupdate

Tabelle B.7: Detaillierte Bedrohungsanalyse, Teil 7



<b>Bedrohung Nr.</b>	<b>Beschreibung</b>
AB2.2.2	Manipulation der Software des SM-GW
B64	Manipulation der Software des Smart Meters durch öffnen des verschweißten Zählergehäuses und Nutzung einer nicht dokumentierten Serviceschnittstelle/Debuggschnittstelle (JTAG) zum einspielen einer manipulierten Software/Softwareupdate
B65	durch öffnen des verplombten Zählergehäuses und Nutzung einer nicht dokumentierten Serviceschnittstelle/Debuggschnittstelle (JTAG) zum einspielen einer manipulierten Software/Softwareupdate
B66	durch einspielen eines manipulierten Softwareupdates über den Fernwartungszugang des SM-GW
B67	durch Schadsoftware
AB2.2.3	Manipulation der Software von Industriellen Steuerungssystemen durch Zugriff über das Internet, Zugriff und einspielen der manipulierten Software.
B68	Mittels SQL Injection in der Login-Maske erlangt der Angreifer Zugriff
B69	Insider mit Zugang zum Industriellen Steuerungssystem und Berechtigung zum Zugriff spielt manipulierte Software ein
AB2.3	Manipulation von Hardware
AB2.3.1	Manipulation der Hardware des Smart Meters
AB2.3.2	Manipulation der Hardware des SM-GWs
AB2.3.3	Manipulation der Hardware von Industriellen Steuerungssystemen im Bereich der Verteilung
AB2.3.4	Manipulation der Hardware von Industriellen Steuerungssystemen im Bereich der Übertragung
AB2.1.3.3	Manipulation der Hardware der Kraftwerkssteuerung im Bereich der Erzeugung
AB2.4	Manipulation der Konfiguration
AB2.4.1	Manipulation der Konfiguration von Industriellen Steuerungssystemen im Bereich der Verteilung
AB2.4.2	Manipulation der Konfiguration von Industriellen Steuerungssystemen im Bereich der Übertragung
AB2.4.3	Manipulation der Konfiguration der Kraftwerkssteuerung im Bereich der Erzeugung
AB2.4.4	Manipulation der Konfiguration des Smart Meters
AB2.4.5	Manipulation der Konfiguration des Smart Meter Gateways
AB3	Einschränkung der Verfügbarkeit
AB3.1	Einschränkung der Verfügbarkeit Abrechnung
AB3.1.1	durch unterdrücken der Kommunikation (Messwerte werden nicht übertragen)
B70	Abrechnung verhindern durch unterdrücken der Kommunikation zwischen Smart Meter und Smart Meter Gateway (optische Übertragung an der D0 Schnittstelle durch einbringen eines Fremdkörpers verhindern)
B71	Abrechnung verhindern durch unterdrücken der Kommunikation zwischen Smart Meter Gateway und PLC-Adapter
B72	Abrechnung verhindern durch unterdrücken der Kommunikation zwischen PLC-Adapter und Router (Kabelverbindung trennen)
B73	Abrechnung verhindern durch unterdrücken der Kommunikation zwischen Router und Discovery Server (Router Firewall Discovery Weiterleitung sperren)

Tabelle B.8: Detaillierte Bedrohungsanalyse, Teil 8

<b>Bedrohung Nr.</b>	<b>Beschreibung</b>
AB3.1	Einschränkung der Verfügbarkeit der Abrechnung
AB3.1.2	durch Denial-of-Service
AB3.1.2.1	DoS des SM-GW
B74	Mehrfach Messdaten an das SM-GW übertragen, so dass es überlastet
AB3.1.2.2	DoS des Discovery Servers
B75	Mehrfach Messdaten an die Discovery Server senden
AB3.2	Einschränkung der Verfügbarkeit der Stromversorgung
B76	Durchtrennen der Hauptleitung
B77	Zugriff Kraftwerkssteuerung und Zerstörung eines Generators
B78	Zugriff industrielle Steuerungssysteme im Bereich Übertragung, Verteilung
B79	Aktivieren der Fernabschaltfunktion des Smart-Meters (unterstützt Smart Meter im Szenario nicht)
AB4	Unautorisierte Nutzung von Systemen
AB4.1	Zugriff auf das Discovery Online Portal
AB4.2	Zugriff auf industrielle Steuerungssysteme
AB4.3	Zugriff Kraftwerkssteuerung
AB5	Missbrauch personenbezogener Daten
AB5.1	Missbräuchliche Nutzung von Lastprofilen
B80	Auswertung der Lastprofile um festzustellen wie viele Personen sich in einem Haushalt befinden
B81	Weiterverkauf der Daten (z.B. für Marketingzwecke)
B82	Hohe Strompreise abgeleitet vom individuellen Lastprofil (Preissprünge immer dann wenn üblicherweise Strom (laut Lastprofil) genutzt wird; bei Real Time Pricing/dynamisch)
B83	Nutzung der Daten zur Feststellung was die Person macht (spielt, arbeitet, Privacy Problem)
B84	Verbrauchsinformationen abgreifen, beobachten und dazu nutzen, zu wissen, dass sich niemand im Haus befindet und dann einbrechen
AB5.1.1	Auswertung der Lastprofile für strafrechtliche Verfolgung
B85	Nutzung der Daten zur Feststellung des Anbaus von z.B. illegalen Betäubungsmitteln
B86	Nutzung der Daten zur Feststellung der Nutzung urheberrechtlich geschützter Medien

Tabelle B.9: Detaillierte Bedrohungsanalyse, Teil 9

## **C Ausdruck von Quellen**

Auf der beiliegenden CD befinden sich im Ordner „Quellen“ komplette Screenshots der Internetquellen sowie einige elektronische Quellen im Portable Document Format. Diese liegen der ausgedruckten Fassung nicht bei.

## Quellenverzeichnis

### Literaturquellen

- [1] Hans-Josef Allelein u. a.: Energietechnik. Systeme zur Energieumwandlung. Kompaktwissen für Studium und Beruf. Hrsg. von Richard Zahoransky. 5., überarb. u. erw. Aufl. Wiesbaden, Vieweg+Teubner Verl. (2010).
- [2] R. J. Anderson und S. J. Bezuidenhout: Cryptographic credit control in pre-payment metering systems. In: Proceedings of the 1995 IEEE Symposium on Security and Privacy, May 8-10, 1995, Oakland, California, Washington, IEEE Computer Society Press (1995).
- [3] Ross Anderson und S. Johann Bezuidenhout: On the Reliability of Electronic Payment Systems. In: IEEE Transactions on Software Engineering 22.5, S. 294–301. Piscataway, IEEE Press (1996).
- [4] Daniel Bachfeld, Dario Carluccio und Christoph Wegener: Wer hat an der Uhr gedreht? Sicherheit bei intelligenten Stromzählern. In: C't : Magazin für Computer-Technik 2011, Heft 23, S. 88–90. Hannover, Heise Zeitschriften Verl. (2011).
- [5] Petra Beenken: Schutz sicherheitsrelevanter Informationen in verteilten Energieinformationssystemen. Diss. Edewecht, OIWR, Oldenburger Verl. für Wirtschaft, Informatik und Recht (2010).
- [6] Alex Biryukov und Dmitry Khovratovich: Related-Key Cryptanalysis of the Full AES-192 and AES-256. In: Advances in Cryptology - ASIACRYPT 2009: 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009, Proceedings, S. 1–18. Berlin, Springer Verl. (2009).
- [7] Andreas Bluschke, Michael Matthews und Anatol Badach: XDSL-Fibel. Offenbach, VDE-Verl. (2001).
- [8] Xavier Carcelle: Power Line Communications in Practice. Boston, Artech House Inc (2009).
- [9] Andres Carvallo und John Cooper: The Advanced Smart Grid. Hrsg. von Edge Power Driving Sustainability. Boston, Artech House Inc (2011).
- [10] Narasimham Challa und Jayaram Pradhan: Performance Analysis of Public key Cryptographic Systems RSA and NTRU. In: IJCSNS International Journal of Computer Science and Network Security Vol. 7, Nr. 8, S. 87–96. Seoul, IJCSNS (2007).
- [11] Cristian Coarfa, Peter Druschel und Dan S. Wallach: Performance analysis of TLS Web servers. In: ACM Trans. Comput. Syst. 24, 1, S. 39–69. New York, ACM (2006).
- [12] Claudia Eckert: IT-Sicherheit. Konzepte - Verfahren - Protokolle. 7., überarb. und erw. Aufl. München, Oldenbourg Verl. (2012).
- [13] Claudia Eckert und Christoph Krauß: Sicherheit im Smart Grid. In: Datenschutz und Datensicherheit - DuD Vol. 35, Nr. 8, S. 535–541. Wiesbaden, Vieweg+Teubner Verl. (2011).

- [14] Jörg Eschweiler und Daniel E. Atencio Psille: Security@Work. Berlin, Springer-Verl. (2006).
- [15] Tony Flick und Justin Morehouse: Securing the smart grid. Next Generation Power Grid Security. Amsterdam, Syngress (2011).
- [16] Dirk Fox: Schutzprofile - Protection Profiles. In: Datenschutz und Datensicherheit - DuD Vol. 35, Nr. 8, S. 570. Wiesbaden, Vieweg+Teubner Verl. (2011).
- [17] Alexander Geschonneck: Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. 5., aktualisierte und erw. Aufl. Heidelberg, dpunkt-Verl. (2011).
- [18] Halid Hrasnica, Abdelfatteh Haidine und Ralf Lehnert: Broadband Powerline Communications. Network Design. Chichester, John Wiley & Sons (2005).
- [19] Tobias Jeske: Datenschutzfreundliches Smart Metering. In: Datenschutz und Datensicherheit - DuD Vol. 35, Nr. 8, S. 530–534. Wiesbaden, Vieweg+Teubner Verl. (2011).
- [20] Christiana Köhler-Schute, Hrsg.: Smart Metering. Technologische, wirtschaftliche und juristische Aspekte des Smart Metering. Berlin, KS-Energy-Verl. (2009).
- [21] Sebastian Klipper: Information Security Risk Management. Risikomanagement mit ISO/IEC 27001, 27005 und 31010. Wiesbaden, Vieweg+Teubner Verl. (2011).
- [22] Eric D. Knapp: Industrial Network Security. Securing Critical Infrastructure Networks for Smart Grid, Scada, and Other Industrial Control Systems. Amsterdam, Syngress (2011).
- [23] Hans-Peter Königs: IT-Risiko-Management mit System. Von den Grundlagen bis zur Realisierung - Ein praxisorientierter Leitfadens. 3., überarbeitete und erweiterte Auflage. Wiesbaden, Vieweg+Teubner Verl. (2009).
- [24] Paul C. Kocher: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology. CRYPTO '96, S. 104–113. Berlin, Springer-Verl. (1996).
- [25] Thomas Kästner und Andreas Kießling: Energie in 60 Minuten. Ein Reiseführer durch die Stromwirtschaft. 1. Aufl. Wiesbaden, VS Verl. für Sozialwissenschaften (2009).
- [26] Mark E. Laubach, David J. Farber und Stephen D. Dukes: Delivering Internet Connections over Cable. Breaking the Access Barrier. Chichester, John Wiley & Sons (2001).
- [27] Dennis Laupichler u. a.: Das BSI-Schutzprofil: Anforderungen an den Datenschutz und die Datensicherheit für Smart Metering Systeme. In: Datenschutz und Datensicherheit - DuD Vol. 35, Nr. 8, S. 542–546. Wiesbaden, Vieweg+Teubner Verl. (2011).
- [28] Andrew Lockhart: Netzwerksicherheit Hacks. 125 Insider-Tricks & Tools. Dt. Übers. der 1. Aufl. von Andreas Bildstein. Aktualisierung der 2. Aufl. Kathrin Lichtenberg. 2. Aufl. Köln, O'Reilly Verl. (2007).
- [29] Klaus Müller: Gewinnung von Verhaltensprofilen am intelligenten Stromzähler. In: Datenschutz und Datensicherheit - DuD Vol. 34, Nr. 6, S. 359–364. Wiesbaden, Vieweg+Teubner Verl. (2010).

- [30] Klaus Müller: Verordnete Sicherheit - das Schutzprofil für das Smart Metering Gateway. In: Datenschutz und Datensicherheit - DuD Vol. 35, Nr. 8, S. 547–551. Wiesbaden, Vieweg+Teubner Verl. (2011).
- [31] Rolf Oppliger, Ralf Hauser und David Basin: SSL/TLS Session-Aware User Authentication: A Lightweight Alternative to Client-Side Certificates. In: IEEE Computer 41.3, S. 59–65. (2008).
- [32] Thomas Petermann u. a.: Was bei einem Blackout geschieht. Folgen eines langandauernden und großflächigen Stromausfalls. Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag, Bd. 33. Berlin, edition sigma (2011).
- [33] Arnold Picot und Karl-Heinz Neumann, Hrsg.: E-Energy. Wandel und Chance durch das Internet der Energie. Berlin, Springer-Verl. (2009).
- [34] Hartmut Pohl: Taxonomie und Modellbildung in der Informationssicherheit. In: Datenschutz und Datensicherheit - DuD Vol. 28, Nr. 11, S. 678–685. Wiesbaden, Vieweg+Teubner Verl. (2004).
- [35] Oliver Raabe u. a., Hrsg.: Datenschutz in Smart Grids. Anmerkungen und Anregungen. Berlin, Liber (2011).
- [36] Jerome H. Saltzer: Protection and the control of information sharing in multics. In: Commun. ACM 17, 7, S. 388–402. New York, ACM (1974).
- [37] Martin Sauter: Grundkurs Mobile Kommunikationssysteme. UMTS, HSDPA und LTE, GSM, GPRS und Wireless LAN. 4., überarb. und erw. Aufl. 2011. Wiesbaden, Vieweg+Teubner Verl. (2011).
- [38] Klaus Schmidt: Der IT Security Manager. München, Carl Hanser Verl. (2006).
- [39] Uwe Schneider und Dieter Werner, Hrsg.: Taschenbuch der Informatik. Mit 317 Bildern und 108 Tabellen. 6., neu bearb. Aufl. Leipzig und München, Fachbuchverl. Leipzig im Carl Hanser Verl. (2007).
- [40] Bruce Schneier: Schneier on Security. Indianapolis, Wiley Publishing (2008).
- [41] Bruce Schneier: Secrets & Lies. IT-Sicherheit in einer vernetzten Welt / Bruce Schneier. Übers. aus dem Amerikan. von Angelika Shafir. Heidelberg und Weinheim, dpunkt-Verl. und Wiley-VCH Verl. (2001).
- [42] Arne Schönbohm: Deutschlands Sicherheit. Cybercrime und Cyberwar. Münster, Verl.-Haus Monsenstein und Vannerdat (2011).

## Elektronische Dokumente

- [43] Ross Anderson und Shailendra Fuloria: Who controls the off switch? (2010). Abrufbar unter: <https://www.cl.cam.ac.uk/~rja14/Papers/meters-offswitch.pdf>.
- [44] Annual Report on the Progress in Smart Metering 2009. (2010). Abrufbar unter: [http://www.esma-home.eu/UserFiles/file/ESMA\\_WP5D18\\_Annual\\_Progress\\_Report\\_2009%281%29.pdf](http://www.esma-home.eu/UserFiles/file/ESMA_WP5D18_Annual_Progress_Report_2009%281%29.pdf).
- [45] Steve Armstrong: Analysis of Sony PSN Hack @31-Apr-11. (2011). Abrufbar unter: [http://www.logicallysecure.com/index.php/download\\_file/32/146/](http://www.logicallysecure.com/index.php/download_file/32/146/).
- [46] Arthur D. Little: Smart Metering vor dem Durchbruch. (2011). Abrufbar unter: [http://www.arthurdlittle.com/uploads/tx\\_extthoughtleadership/ADL\\_Energy\\_Uilities\\_Smart\\_Metering.pdf](http://www.arthurdlittle.com/uploads/tx_extthoughtleadership/ADL_Energy_Uilities_Smart_Metering.pdf).
- [47] Silvia Barnert u. a.: Der Brockhaus - Computer und Informationstechnologie: Standard. Hrsg. von Bibliographisches Institut & F. A. Brockhaus AG. (2005). Auf der beiliegenden CD finden Sie im Ordner Quellen einen Auszug.
- [48] Jörg Benze, Christian Hübner und Andreas Kießling: Das intelligente Energiesystem als zukünftige Basis für ein nachhaltiges Energiemanagement. (2011). Abrufbar unter: <http://www.user.tu-berlin.de/komm/CD/paper/060621.pdf>.
- [49] Daniel J. Bernstein: Cache-timing attacks on AES. (2005). Abrufbar unter: <http://cr.yp.to/antiforgery/cachetiming-20050414.pdf>.
- [50] Kemal Bicakci, Bruno Crispo und Andrew S. Tanenbaum: Reverse SSL: Improved Server Performance and DoS Resistance for SSL Handshakes. (2006). Abrufbar unter: <http://eprint.iacr.org/2006/212.pdf>.
- [51] Gunter Bolch und Ulrich Zahner: Vorlesungsunterlagen - Prozessautomatisierung - WS 2004/05 - Kapitel 1: Was heißt Prozessautomatisierung? (2004). Abrufbar unter: [http://www4.informatik.uni-erlangen.de/Lehre/WS04/V\\_PA/Skript/stp1-pa-ws04-kapitel1.pdf](http://www4.informatik.uni-erlangen.de/Lehre/WS04/V_PA/Skript/stp1-pa-ws04-kapitel1.pdf).
- [52] Stephan Brinkhaus u. a.: Smart Hacking for Smart Privacy (Vortrag vom 30.12.2011). (2011). Für das Abstract des Vortrags siehe [http://events.ccc.de/congress/2011/Fahrplan/attachments/1968\\_28c3-abstract-smart\\_hacking\\_for\\_privacy.pdf](http://events.ccc.de/congress/2011/Fahrplan/attachments/1968_28c3-abstract-smart_hacking_for_privacy.pdf) ; für eine Aufzeichnung des Vortrags siehe [https://www.youtube.com/watch?feature=player\\_embedded&v=xOArwu3lziQ](https://www.youtube.com/watch?feature=player_embedded&v=xOArwu3lziQ). Auf der beiliegenden CD finden Sie die Vortragsfolien als PDF im Ordner Quellen.
- [53] Martin Brunner u. a.: Infiltrating critical infrastructures with next-generation attacks: W32.Stuxnet as a showcase threat. Fraunhofer SIT, Darmstadt. (2010). Abrufbar unter: [http://www.aisec.fraunhofer.de/content/dam/aisec/en/pdf/studien/studie\\_stuxnet.pdf](http://www.aisec.fraunhofer.de/content/dam/aisec/en/pdf/studien/studie_stuxnet.pdf).

- [54] Statistisches Bundesamt: Statistisches Jahrbuch 2011: Für die Bundesrepublik Deutschland mit »Internationalen Übersichten«. (2011). Abrufbar unter: <http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/SharedContent/Oeffentlich/B3/Publikation/Jahrbuch/StatistischesJahrbuch,property=file.pdf>.
- [55] Joachim Charzinski: Vorlesungsfolien: Security in IT Systems Chapter - 01: Introduction. (2011).
- [56] Cisco Systems: Cisco Grid Blocks Reference Model. (2011). Abrufbar unter: [https://www.cisco.com/web/strategy/docs/energy/gridblocks\\_ref\\_model.pdf](https://www.cisco.com/web/strategy/docs/energy/gridblocks_ref_model.pdf).
- [57] Michael Coyne u. a.: Systems Architecture for Smart Grids. Case Study and proposed reference model. (2010). Abrufbar unter: [http://www.aesieap0910.org/upload/File/PDF/4-Technical%20Sessions/TS46/TS4603/TS4603\\_PPT.pdf](http://www.aesieap0910.org/upload/File/PDF/4-Technical%20Sessions/TS46/TS4603/TS4603_PPT.pdf).
- [58] Discovery GmbH: Energiekosten dauerhaft senken - ab sofort für alle deutschen Verbraucher durch unabhängige Energiesparberatung mit intelligenten Stromzählern. (2010). Abrufbar unter: [http://discovery.com/site\\_media/press/discovery\\_press\\_20101005.pdf](http://discovery.com/site_media/press/discovery_press_20101005.pdf).
- [59] Thai Duong und Juliano Rizzo: Here Come The Ninjas. (2011). Abrufbar unter: [https://www.infoworld.com/sites/infoworld.com/files/pdf/BEAST\\_Duong\\_Rizzo.pdf](https://www.infoworld.com/sites/infoworld.com/files/pdf/BEAST_Duong_Rizzo.pdf).
- [60] EasyMeter GmbH: D0 Schnittstelle. Q3Dx\_D0 Spezifikation\_v11. (2009). Abrufbar unter: [http://www.mikrocontroller.net/attachment/89888/Q3Dx\\_D0\\_Spezifikation\\_v11.pdf](http://www.mikrocontroller.net/attachment/89888/Q3Dx_D0_Spezifikation_v11.pdf).
- [61] EasyMeter GmbH: EasyMeter Betriebsanleitung. Elektronischer 3-Phasen 4-Leiter Zähler Q3D. (2011). Abrufbar unter: [http://www.easymeter.de/downloads/q3d\\_betriebsanleitung\\_rev06\\_dina5.pdf](http://www.easymeter.de/downloads/q3d_betriebsanleitung_rev06_dina5.pdf).
- [62] Claudia Eckert: Sicherheit im Smart Grid. Eckpunkte für ein Energieinformationsnetz. (2011). Abrufbar unter: [http://www.stiftungaktuell.de/files/sr90\\_sicherheit\\_im\\_energieinformationsnetz\\_gesamt\\_1.pdf](http://www.stiftungaktuell.de/files/sr90_sicherheit_im_energieinformationsnetz_gesamt_1.pdf).
- [63] Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids. (2011). Abrufbar unter: <ftp://ftp.cencenelec.eu/CENELEC/Smartgrid/SmartGridFinalReport.pdf>.
- [64] Limor Fried: Social Defense Mechanisms. Tools for Reclaiming our Personal Space. (2005). Abrufbar unter: [http://servv89pn0aj.sn.sourcedns.com/~gbpprogr/mil/celljam/ladyada\\_thesis.pdf](http://servv89pn0aj.sn.sourcedns.com/~gbpprogr/mil/celljam/ladyada_thesis.pdf).
- [65] Discovery GmbH: Discovery Produktflyer Meteroit. (2010). Abrufbar unter: [http://discovery.com/site\\_media/downloads/Discovery\\_Produktflyer\\_Meteroit.pdf](http://discovery.com/site_media/downloads/Discovery_Produktflyer_Meteroit.pdf).
- [66] Ulrich Greveler, Benjamin Justus und Dennis Löhr: Hintergrund und experimentelle Ergebnisse zum Thema „Smart Meter und Datenschutz“. (2011). Abrufbar unter: [http://www.its.fh-muenster.de/greveler/pubs/smartmeter\\_sep11\\_v06.pdf](http://www.its.fh-muenster.de/greveler/pubs/smartmeter_sep11_v06.pdf).



- [67] Ulrich Greveler, Benjamin Justus und Dennis Löhr: Multimedia Content Identification Through Smart Meter Power Usage Profiles. (2012). Abrufbar unter: [https://epic.org/privacy/smartgrid/smart\\_meter.pdf](https://epic.org/privacy/smartgrid/smart_meter.pdf).
- [68] Eva Heringhaus: Pressemitteilung. Yello startet national den Wettbewerb bei intelligenten Stromzählern. (2008). Abrufbar unter: [http://www2.yellostrom.de/presse/download/index.html?tname=PM\\_Sparzaehler\\_021208.pdf](http://www2.yellostrom.de/presse/download/index.html?tname=PM_Sparzaehler_021208.pdf).
- [69] Renate Höfer-Zygan, Erik Oswald und Mike Heidrich: Smart Grid Communications 2020. Fokus Deutschland. (2011). Bieziehbar unter: <http://www.esk.fraunhofer.de/de/publikationen/studien/SmartGrid2020.html>.
- [70] IEC Smart Grid Standardization Roadmap. (2010). Abrufbar unter: [http://www.iec.ch/smartgrid/downloads/sg3\\_roadmap.pdf](http://www.iec.ch/smartgrid/downloads/sg3_roadmap.pdf).
- [71] Moritz Karg: Datenschutzrechtliche Bewertung des Einsatzes von „intelligenten“ Messeinrichtungen für die Messung von gelieferter Energie (Smart Meter). (2009). Abrufbar unter: <https://www.datenschutzzentrum.de/smartmeter/20090925-smartmeter.pdf>.
- [72] Gerhard Knies, Uwe Möller und Michael Straub, Hrsg.: Clean Power from Deserts. The DESERTEC Concept for Energy, Water and Climate Security. (2007). Abrufbar unter: [http://www.desertec.org/fileadmin/downloads/DESERTEC-WhiteBook\\_en\\_small.pdf](http://www.desertec.org/fileadmin/downloads/DESERTEC-WhiteBook_en_small.pdf).
- [73] Pekka Koponen u. a.: Definition von Smart Metering, Anwendungen und Identifikation der Vorteile. Hrsg. von Pekka Koponen. (2008). Abrufbar unter: [http://www.esma-home.eu/UserFiles/file/downloads/Final\\_reports/D3%20Summary\\_de.pdf](http://www.esma-home.eu/UserFiles/file/downloads/Final_reports/D3%20Summary_de.pdf).
- [74] Lastenheft Multi Utility Communication (MUC); Version 1.01 (Arbeitsfassung). (2011). Abrufbar unter: [http://www.vde.com/de/fnn/arbeitsgebiete/messwesen/documents/fnn\\_lh-muc\\_1-01\\_2011-07-04.pdf](http://www.vde.com/de/fnn/arbeitsgebiete/messwesen/documents/fnn_lh-muc_1-01_2011-07-04.pdf).
- [75] Arjen K. Lenstra u. a.: Ron was wrong, Whit is right. (2012). Abrufbar unter: <http://eprint.iacr.org/2012/064.pdf>.
- [76] Jerry Li: From Strong to Smart: the Chinese Smart Grid and its relation with the Globe. (2009). Abrufbar unter: <http://www.aepfm.org/ufiles/pdf/Smart%20Grid%20-%20AEPN%20Sept.pdf>.
- [77] Microsoft: Smart Energy Reference Architecture. (2009). Abrufbar unter: <http://download.microsoft.com/download/0/c/2/0c2f64b1-241d-4433-9665-5f802e7510d6/microsoft%20smart%20energy%20reference%20architecture.pdf>.
- [78] Andres Molina-Markham u. a.: Private Memoirs of a Smart Meter. (2010). Abrufbar unter: <http://www.cs.umass.edu/~kevinfu/papers/molina-markham-buildsys10.pdf>.
- [79] Rolf Oppliger, Ralf Hauser und David Basin: SSL/TLS Session-Aware User Authentication - Or how to effectively thwart the man-in-the-middle. In: Computer Communications 29.12, Abrufbar unter: <http://www.inf.ethz.ch/personal/basin/pubs/mitm-cc.pdf>, S. 2238–2246. (2006).

- [80] Elias Leake Quinn: Smart Metering and Privacy: Existing Law and Competing Policies. A Report for the Colorado Public Utilities Commission. (2009). Abrufbar unter: [http://www.dora.state.co.us/puc%20/DocketsDecisions/DocketFilings/09I-593EG/09I-593EG\\_Spring2009Report-SmartGridPrivacy.pdf](http://www.dora.state.co.us/puc%20/DocketsDecisions/DocketFilings/09I-593EG/09I-593EG_Spring2009Report-SmartGridPrivacy.pdf).
- [81] Detlef Rehn: Viel Bewegung bei neuen Stromnetzen in Japan. (2011). Abrufbar unter: <http://www.gtai.de/GTAI/Navigation/DE/Trade/maerkte,did=262810.html?view=renderPdf>.
- [82] Stephan Renner u. a.: European Landscape Report. (2011). Abrufbar unter: <http://www.smartregions.net/GetItem.asp?item=digistorefile;253415;1522&params=open;gallery>.
- [83] Wolf-Fritz Riekert: Eine Dokumentvorlage für Diplomarbeiten und andere wissenschaftliche Arbeiten. (2002). Abrufbar unter: <http://v.hdm-stuttgart.de/~riekert/theses/thesis-arial11.doc>.
- [84] Sergio Rogai: ENEL's Metering System and Telegestore Project. (2006). Abrufbar unter: <http://www.narucmeetings.org/Presentations/ENEL.pdf>.
- [85] SCE-Cisco-IBM SGRA Team: Smart Grid Reference Architecture Volume 1. Using Information and Communication Services to Support a Smarter Grid. (2011). Abrufbar unter: <http://www.pointview.com/data/files/1/636/2181.pdf>.
- [86] Roland Schmitz: Vorlesungsfolien: Security in IT-Systemen SS 2010: Kapitel 1: Grundlagen. (2010). Als HdM Dozent/Student nach Anmeldung abrufbar unter: [https://www.mi.hdm-stuttgart.de/Downloads/Vorlesungsskripte/skripte/BACHELOR\\_Medieninformatik/Security\\_IT\\_Systeme/SS10/Kap1\\_Grundlagen.pdf](https://www.mi.hdm-stuttgart.de/Downloads/Vorlesungsskripte/skripte/BACHELOR_Medieninformatik/Security_IT_Systeme/SS10/Kap1_Grundlagen.pdf).
- [87] Christopher Soghoian und Sid Stamm: Certified lies: Detecting and defeating government interception attacks against SSL. (2010). Abrufbar unter: <http://files.cloudprivacy.net/ssl-mitm.pdf>.
- [88] Tokio Electric Power Company: Corporate Social Responsibility (CSR) at the TEPCO Group. Annual Report 2010. (2010). Abrufbar unter: <http://www.tepco.co.jp/en/corpinfo/ir/tool/annual/pdf/2010/ar201013-e.pdf>.
- [89] Mathias Uslar u. a.: Untersuchung des Normungsfeldes zum BMWi-Förderschwerpunkt „e-Energy - IKT-basiertes Energiesystem der Zukunft“. Studie für das Bundesministerium für Wirtschaft und Technologie (BMWi). (2009). Abrufbar unter: [http://www.e-energy.de/documents/2009-02-23\\_Untersuchung\\_des\\_Normungs-\\_und\\_Standardisierungsumfeldes\\_E-Energy.pdf](http://www.e-energy.de/documents/2009-02-23_Untersuchung_des_Normungs-_und_Standardisierungsumfeldes_E-Energy.pdf).
- [90] BNetzA: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen). (2011). Abrufbar unter: [http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2011\\_2\\_AlgoKatpdf.pdf;jsessionid=8CA37D4B7D6ED276D0D6A3C0AC587F4B?\\_\\_blob=publicationFile](http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2011_2_AlgoKatpdf.pdf;jsessionid=8CA37D4B7D6ED276D0D6A3C0AC587F4B?__blob=publicationFile).

- [91] **BSI**: IT-Grundschutz-Kataloge 12. Ergänzungslieferung. (2011). Abrufbar unter: <https://gsb.download.bva.bund.de/BSI/ITGSK12EL/IT-Grundschutz-Kataloge-12-EL.pdf>.
- [92] **NIST**: **NIST**: Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. **NIST** Special Publication 1108. (2010). Abrufbar unter: [http://www.nist.gov/public\\_affairs/releases/upload/smartgrid\\_interoperability\\_final.pdf](http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf).
- [93] **VDE**, Hrsg.: Die deutsche Normungsroadmap E-Energy / Smart Grid. (2010). Abrufbar unter: [http://www.e-energy.de/documents/DKE\\_Roadmap\\_Smart\\_Grid\\_230410\\_Deutsch.pdf](http://www.e-energy.de/documents/DKE_Roadmap_Smart_Grid_230410_Deutsch.pdf).

## Internetquellen

- [94] Announcement of master plans for the Demonstration of Next-Generation Energy and Social Systems / METI Ministry of Economy, Trade and Industry. (2010). [http://www.meti.go.jp/english/press/data/20100811\\_01.html](http://www.meti.go.jp/english/press/data/20100811_01.html). Abgerufen am 07.03.2012.
- [95] Arbeitsgruppe Identitätsschutz im Internet: A-I3.org - Phishing. (2012). <https://www.a-i3.org/content/category/5/36/216/>. Abgerufen am 07.03.2012.
- [96] Austin Energy Smart Grid Program. <http://www.austinenergy.com/aboutus/companyprofile/smartGrid/index.htm>. Abgerufen am 07.03.2012.
- [97] BMWi, Referat Öffentlichkeitsarbeit: BMWi - Elektromobilität. <http://www.bmwi.de/BMWi/Navigation/Wirtschaft/Industrie/elektromobilitaet.html>. Abgerufen am 07.03.2012.
- [98] BMWi, Referat Öffentlichkeitsarbeit: BMWi - Pressemitteilungen-11.1.2011 Brüderle eröffnet zweiten E-Energy Jahreskongress. (2011). <http://www.bmwi.de/BMWi/Navigation/Presse/pressemitteilungen,did=376170.html>. Abgerufen am 07.03.2012.
- [99] BMWi, Referat Öffentlichkeitsarbeit: BMWi - Stromnetze: Intelligente Netze und intelligente Zähler - Smart Grids/Smart Meter. (2011). <http://www.bmwi.de/BMWi/Navigation/Energie/stromnetze,did=354346.html>. Abgerufen am 07.03.2012.
- [100] BMWi, Referat Öffentlichkeitsarbeit: BMWi - Stromnetze. (2011). <http://www.bmwi.de/BMWi/Navigation/Energie/stromnetze,did=292512.html>. Abgerufen am 07.03.2012.
- [101] Vincent Bernat: SSL computational DoS mitigation. (2011). <http://vincent.bernat.im/en/blog/2011-ssl-dos-mitigation.html>. Abgerufen am 07.03.2012.
- [102] Catherine Cuellar: Press Release-Oncor Installs Two Millionth Advanced Meter. (2011). <http://www.oncor.com/news/newsrel/detail.aspx?prid=1310>. Abgerufen am 07.03.2012.
- [103] Discovergy : FAQ. <http://discovergy.com/pages/faq/>. Abgerufen am 07.03.2012.
- [104] EKR: SSL/TLS and Computational DoS. (2011). [http://www.educatedguesswork.org/2011/10/ssltls\\_and\\_computational\\_dos.html](http://www.educatedguesswork.org/2011/10/ssltls_and_computational_dos.html). Abgerufen am 07.03.2012.
- [105] E.ON Energie - Smart Meter, Stromzähler digital, Stromzähler Verbrauch, Stromzähler intelligent, Stromzähler Messung. (2010). [http://www.eon-energie.com/pages/eea\\_de/Innovation/Innovation/Perspektive\\_Kunde/Smart\\_Meter/index.htm](http://www.eon-energie.com/pages/eea_de/Innovation/Innovation/Perspektive_Kunde/Smart_Meter/index.htm). Abgerufen am 07.03.2012.
- [106] Fraunhofer-Gesellschaft: Überblick | mySmartGrid. <https://www.mysmartgrid.de/>. Abgerufen am 07.03.2012.

- [107] Governor Abercrombie Signs Memorandum Of Understanding For Japan-U.S. Smart Grid Demonstration Project - Office of the Governor. <http://hawaii.gov/gov/newsroom/press-releases/governor-abcrombie-signs-memorandum-of-understanding-for-japan-u.s.-smart-grid-demonstration-project>. Abgerufen am 07.03.2012.
- [108] Green Bay Professional Packet Radio: GBPPR Cellular Phone Jammers. <http://projects2.gbppr.org/mil/celljam/index.html>. Abgerufen am 07.03.2012.
- [109] Jasper Hamill: Thousands in city conned by cheaper energy scam. (2010). <http://www.eveningtimes.co.uk/news/editor-s-picks/thousands-in-city-conned-by-cheaper-energy-scam-1.1053149>. Abgerufen am 07.03.2012.
- [110] Hardware Address (MAC Address) Lookup :: Search by hardware address. <http://hwaddress.com/?q=discovergy>. Abgerufen am 07.03.2012.
- [111] Claus Hornung: Das Vierte Quartal: Aussicht auf Erfolg. (2012). <https://www.ftd.de/karriere-management/gruendung/:das-vierte-quartal-aussicht-auf-erfolg/60150217.html?mode=print>. Abgerufen am 07.03.2012.
- [112] Troy Hunt: A brief Sony password analysis. (2011). <http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html>. Abgerufen am 07.03.2012.
- [113] Märkisches Viertel - Vattenfall. (2011). <http://www.vattenfall.de/de/maerkisches-viertel.htm>. Abgerufen am 07.03.2012.
- [114] Jeanne Meserve: Sources: Staged cyber attack reveals vulnerability in power grid. (2007). <http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html#cnnSTCText>. Abgerufen am 07.03.2012.
- [115] Mülheim zählt. <http://www.rwe.com/web/cms/de/368410/muelheim-zaehlt/>. Abgerufen am 13.12.2011. Hinweis: Die Quelle hat sich in seit diesem Zeitpunkt verändert.
- [116] Jon Oberheide: Brief analysis of the Gawker password dump. (2010). - <http://blog.duosecurity.com/2010/12/brief-analysis-of-the-gawker-password-dump/>. Abgerufen am 07.03.2012.
- [117] Pacific Gas and Electric Company - SmartMeter Installation Progress. <http://www.pge.com/myhome/customerservice/smartmeter/deployment/index.shtml>. Abgerufen am 07.03.2012.
- [118] Verena Renneberg: Deutscher Bundestag: Bundestag beschließt Atomausstieg und Energiewende. [http://www.bundestag.de/dokumente/textarchiv/2011/34938007\\_kw26\\_de\\_energiewende/index.html](http://www.bundestag.de/dokumente/textarchiv/2011/34938007_kw26_de_energiewende/index.html). Abgerufen am 07.03.2012.
- [119] Bruce Schneier: Schneier on Security: Prepaid Electricity Meter Fraud. (2010). [https://www.schneier.com/blog/archives/2010/09/new\\_prepaid\\_ele.html](https://www.schneier.com/blog/archives/2010/09/new_prepaid_ele.html). Abgerufen am 07.03.2012.
- [120] Becca Talbot: Prepayment meters. <http://www.energychoices.co.uk/energy/prepayment-meters.html>. Abgerufen am 07.03.2012.

- [121] The Beacon Center of Tennessee: Editor: Al Gores Personal Energy Use Is His Own Inconvenient Truth. <http://www.beacontn.org/2007/02/al-gore%E2%80%99s-personal-energy-use-is-his-own-%E2%80%9Cinconvenient-truth/>. Abgerufen am 07.03.2012.
- [122] The Hackers Choice - THC-SSL-DOS. (2011). <http://www.thc.org/thc-ssl-dos/>. Abgerufen am 07.03.2012.
- [123] The MITRE Corporation: CVE - About CVE. (2012). <http://cve.mitre.org/about/>. Abgerufen am 07.03.2012.
- [124] Unterschied Normen und Standards - IHK Würzburg-Schweinfurt. (2011). <http://www.wuerzburg.ihk.de/innovation-umwelt/innovation-technologie/normen-und-standardisierung/unterschied-normen-und-standards.html>. Abgerufen am 07.03.2012.
- [125] ZEIT ONLINE: Verräterisches Handy. (2011). <http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten>. Abgerufen am 07.03.2012.
- [126] BSI: BSI: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik. (2011). <https://www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifierungnachCCundITSEC/ITSicherheitskriterien/CommonCriteria/cc.html>. Abgerufen am 07.03.2012.
- [127] BSI: BSI: Schutzprofil für Smart Meter. (2011). [https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil\\_Gateway/schutzprofil\\_smart\\_meter\\_gateway\\_node.html](https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html). Abgerufen am 07.03.2012.
- [128] BSI: BSI: Schutzprofil für das Sicherheitsmodul eines intelligenten Messsystems. (2011). [https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil\\_Security/security\\_module\\_node.html](https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Security/security_module_node.html). Abgerufen am 07.03.2012.
- [129] BSI: BSI TR-03109 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems für Stoff und Energiemengen. (2011). [https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR\\_node.html](https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html). Abgerufen am 07.03.2012.
- [130] IEEE: China - IEEE Smart Grid. <http://smartgrid.ieee.org/resources/public-policy/china>. Abgerufen am 07.03.2012.
- [131] IEEE: Search Results: IEEE Standards OUI Public Database. (2012). <http://standards.ieee.org/cgi-bin/ouisearch?discovergy>. Abgerufen am 07.03.2012.
- [132] IEEE: United States - IEEE Smart Grid. <http://smartgrid.ieee.org/resources/public-policy/united-states>. Abgerufen am 07.03.2012.
- [133] Österreichische Energieagentur: Smart Metering Landscape Report - Österreichische Energieagentur. <http://www.energyagency.at/energiewirtschaft/aktuelle-projekte/smart-regions/smart-metering-landscape-report.html>. Abgerufen am 07.03.2012.

## Standards, Normen, Technische Richtlinien und Schutzprofile

- [134] DIN EN 13757-2. Kommunikationssysteme für Zähler und deren Fernablesung - Teil 2: Physical und Link Layer; Englische Fassung EN 13757-2:2004. (2005).
- [135] DIN EN 13757-3. Kommunikationssysteme für Zähler und deren Fernablesung - Teil 3: Spezieller Application Layer; Englische Fassung EN 13757-3:2004. (2005).
- [136] DIN EN 13757-4. Kommunikationssysteme für Zähler und deren Fernablesung - Teil 4: Zählerauslesung über Funk (Fernablesung von Zählern im SRD-Band von 868 MHz bis 870 MHz); Deutsche Fassung EN 13757-4:2005. (2005).
- [137] DIN EN 50438; VDE 0435-901:2008-08:2008-08. Anforderungen für den Anschluss von Klein-Generatoren an das öffentliche Niederspannungsnetz; Deutsche Fassung EN 50438:2007. (2008).
- [138] DIN EN 60601-1-4. Medizinische elektrische Geräte - Teil 1-4: Allgemeine Festlegungen für die Sicherheit; Ergänzungsnorm: Programmierbare elektrische medizinische Systeme (IEC 60601-1-4:1996 + A1:1999); Deutsche Fassung EN 60601-1-4:1996 + A1:1999. (2001).
- [139] DIN EN 61508. Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme. (2011).
- [140] DIN EN 61850. Kommunikationsnetze und -systeme in Stationen. (2002).
- [141] DIN EN 61968. Integration von Anwendungen in Anlagen der Elektrizitätsversorgung - Systemschnittstellen für Netzführung. (2002).
- [142] DIN EN 61970. Schnittstelle der Anwendungsprotokolle von Energieverwaltungssystemen (EMS-API). (2006).
- [143] DIN EN 62056-21:2003-01. Messung der elektrischen Energie - Zählerstandsübertragung, Tarif- und Laststeuerung - Teil 21: Datenübertragung für festen und mobilen Anschluss (IEC 62056-21:2002); Deutsche Fassung EN 62056-21:2002, Text in Englisch. (2003).
- [144] T. Dierks und C. Allen: The TLS Protocol Version 1.0. RFC 2246. (1999). Abrufbar unter: <https://www.ietf.org/rfc/rfc2246.txt>.
- [145] R. Droms: Dynamic Host Configuration Protocol. RFC 2131. (1997). Abrufbar unter: <https://www.ietf.org/rfc/rfc2131.txt>.
- [146] Roy Fielding u. a.: Hypertext Transfer Protocol – HTTP/1.1. RFC 2616. (1999). Abrufbar unter: <https://www.ietf.org/rfc/rfc2616.txt>.
- [147] ISO/IEC 15408. Information technology - Security techniques - Evaluation criteria for IT security. (2009).
- [148] ISO/IEC 62351. Power systems management and associated information exchange - Data and communications security. (2007).
- [149] ISO/IEC TR 62357. Power system control and associated communications - Reference architecture for object models, services and protocols. (2003).

- [150] Helge Kreuzmann u. a.: BSI-CC-PP-0073. Protection Profile for the Gateway of a Smart Metering System (Gateway PP), Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, Version 01.01.01 (final draft). Hrsg. von BSI. (2011). Abrufbar unter: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?\\_\\_blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile).
- [151] Manfred Lochter, Hrsg.: ECC Brainpool Standard Curves and Curve Generation. (2005). Abrufbar unter: <http://www.ecc-brainpool.org/download/Domain-parameters.pdf>.
- [152] P. Mockapetris: Domain names - concepts and facilities. RFC 1034. (1987). Abrufbar unter: <https://www.ietf.org/rfc/rfc1034.txt>.
- [153] P. Mockapetris: Domain names - implementation and specification. RFC 1035. (1987). Abrufbar unter: <https://www.ietf.org/rfc/rfc1035.txt>.
- [154] David Plummer: An Ethernet Address Resolution Protocol. RFC 826. (1987). Abrufbar unter: <https://www.ietf.org/rfc/rfc826.txt>.
- [155] RSA Laboratories: PKCS #1 v2.1: RSA Cryptography Standard. (2002). Abrufbar unter: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf>.
- [156] E. Rescorla: HTTP Over TLS. RFC 2818. (2000). Abrufbar unter: <https://www.ietf.org/rfc/rfc2818.txt>.
- [157] Standards for Efficient Cryptography (SEC). Elliptic Curve Cryptography, Version 1.0. (2000). Abrufbar unter: [www.secg.org/download/aid-385/sec1\\_final.pdf](http://www.secg.org/download/aid-385/sec1_final.pdf).
- [158] Keith Stouffer, Joe Falco und Karen Scarfone: NIST Special Publication 800-82 - Guide to Industrial Control Systems (ICS) Security. Abrufbar unter: <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>. (2011).
- [159] University of Southern California: Internet Protocol. RFC 791. (1981). Abrufbar unter: <https://www.ietf.org/rfc/rfc791.txt>.
- [160] University of Southern California: Transmission Control Protocol. RFC 793. (1981). Abrufbar unter: <https://www.ietf.org/rfc/rfc793.txt>.
- [161] ZigBee Standards Organization: ZigBee-2007 specification. ZigBee Document 053474r17. (2008).
- [162] BSI: Application Notes and Interpretation of the Scheme (AIS). AIS 20, Version 1. (1999). Abrufbar unter: [https://www.bsi.bund.de/cae/servlet/contentblob/478152/publicationFile/30552/ais20e\\_pdf.pdf](https://www.bsi.bund.de/cae/servlet/contentblob/478152/publicationFile/30552/ais20e_pdf.pdf).
- [163] BSI: Technische Richtlinie BSI TR-02102. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. (2008). Abrufbar unter: [https://www.bsi.bund.de/cae/servlet/contentblob/477256/publicationFile/30629/BSI-TR-02102\\_V1\\_0\\_pdf.pdf](https://www.bsi.bund.de/cae/servlet/contentblob/477256/publicationFile/30629/BSI-TR-02102_V1_0_pdf.pdf).



- [164] **BSI**: Technische Richtlinie **BSI** TR-03109. Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, Version 0.20. (2011). Abrufbar unter: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR03109.pdf?\\_\\_blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR03109.pdf?__blob=publicationFile).
- [165] **BSI**: **BSI**-Standard 100-3. Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.5. (2008). Abrufbar unter: [https://www.bsi.bund.de/cae/servlet/contentblob/471454/publicationFile/30747/standard\\_1003.pdf](https://www.bsi.bund.de/cae/servlet/contentblob/471454/publicationFile/30747/standard_1003.pdf).
- [166] **IEEE** 1547-2003. **IEEE** Standard for Interconnecting Distributed Resources with Electric Power Systems. (2003). **IEEE** 1547-2003.
- [167] **IEEE** 2030-2011. **IEEE** Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads. (2011). **IEEE** 2030-2011.
- [168] **IEEE** 802.11-2007. **IEEE** Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. (2007).
- [169] **IEEE** 802.15.4-2006. **IEEE** Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). (2006).
- [170] **NIST**: NISTIR 7628. Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements. Abrufbar unter: [http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628\\_vol1.pdf](http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf). (2010).
- [171] **NIST**: Secure Hash Signature Standard (SHS) (FIPS PUB 180-2). Abrufbar unter: <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf>. (2002).

## Gesetze, Verordnungen und Richtlinien

- [172] American Recovery and Reinvestment Act of 2009. Public Law 111-5-FEB. 17, 2009. Abrufbar unter: <http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf>. (2009).
- [173] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist. (2009). In einer nicht amtlichen Fassung als vollständiger Gesetzestext abrufbar unter: [http://www.gesetze-im-internet.de/bundesrecht/bdsg\\_1990/gesamt.pdf](http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf).
- [174] Bundesverfassungsgericht: Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83. Volkszählungsurteil. (1983). Abrufbar unter: [https://cdn.zensus2011.de/live/fileadmin/material/pdf/gesetze/volkszaehlunsurteil\\_1983.pdf](https://cdn.zensus2011.de/live/fileadmin/material/pdf/gesetze/volkszaehlunsurteil_1983.pdf).
- [175] Charta der Grundrechte der Europäischen Union (2007/C 303/01). Abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:DE:PDF>. (2007).
- [176] Eichordnung vom 12. August 1988 (BGBl. I S. 1657), die zuletzt durch Artikel 1 der Verordnung vom 6. Juni 2011 (BGBl. I S. 1035) geändert worden ist. In einer nicht amtlichen Fassung abrufbar unter: [http://www.gesetze-im-internet.de/bundesrecht/eo\\_1988/gesamt.pdf](http://www.gesetze-im-internet.de/bundesrecht/eo_1988/gesamt.pdf).
- [177] Energy Independence and Security Act of 2007. Public Law 110-140-JAN. 12, 2007 - 110th Congress (2007 - 2008) H.R.6. Abrufbar unter: [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110\\_cong\\_bills&docid=f:h6enr.txt.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6enr.txt.pdf). (2007).
- [178] Energy Policy Act of 2005. Public Law 109-58-AUG. 08, 2005 - 109th Congress H.R.6. Abrufbar unter: [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109\\_cong\\_bills&docid=f:h6enr.txt.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h6enr.txt.pdf). (2005).
- [179] Gesetz über das Meß- und Eichwesen (Eichgesetz) in der Fassung der Bekanntmachung vom 23. März 1992 (BGBl. I S. 711), das zuletzt durch Artikel 1 des Gesetzes vom 7. März 2011 (BGBl. I S. 338 - Nr. 9) geändert worden ist. (2011). In einer nicht amtlichen Fassung als vollständiger Gesetzestext abrufbar unter: <http://www.gesetze-im-internet.de/bundesrecht/eichg/gesamt.pdf>.
- [180] Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG) vom 7. Juli 2005 (BGBl. I S. 1970, 3621) das zuletzt durch Artikel 1 des Gesetzes vom 29. August 2008 (BGBl. I S. 1790 - Nr. 40) geändert worden ist. (2008).
- [181] Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG) vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 22 des Gesetzes vom 24. November 2011 (BGBl. I S. 2302 - Nr. 60) geändert worden ist. (2011). In einer nicht amtlichen Fassung als vollständiger Gesetzestext abrufbar unter: [http://www.gesetze-im-internet.de/bundesrecht/enwg\\_2005/gesamt.pdf](http://www.gesetze-im-internet.de/bundesrecht/enwg_2005/gesamt.pdf).

- [182] Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG) vom 7. Juli 2005 (BGBl. I S. 1970, 3621). (2005).
- [183] Gesetz für den Vorrang Erneuerbarer Energien (Erneuerbare-Energien-Gesetz - EEG) vom 25. Oktober 2008 (BGBl. I S. 2074), das zuletzt durch Artikel 1 des Gesetzes vom 28. Juli 2011 (BGBl. I S. 1634) geändert worden ist. (2011). In einer nicht amtlichen Fassung als vollständiger Gesetzestext abrufbar unter: [http://www.gesetze-im-internet.de/bundesrecht/eeg\\_2009/gesamt.pdf](http://www.gesetze-im-internet.de/bundesrecht/eeg_2009/gesamt.pdf).
- [184] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation). Abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:DE:PDF>. (2002).
- [185] Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG. Abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0055:0093:DE:PDF>. (2009).
- [186] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:DE:PDF>. (1996).
- [187] Richtlinie 96/92/EG des Europäischen Parlaments und des Rates vom 19. Dezember 1996 betreffend gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt. Abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1997:027:0020:0029:DE:PDF>. (1996).
- [188] Richtlinie 98/30/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 betreffend gemeinsame Vorschriften für den Erdgasbinnenmarkt. Abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:204:0001:0012:DE:PDF>. (1998).
- [189] Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das durch Artikel 5 Absatz 3 des Gesetzes vom 24. Februar 2012 (BGBl. I S. 212) geändert worden ist. (2012). In einer nicht amtlichen Fassung als vollständiger Gesetzestext abrufbar unter: <http://www.gesetze-im-internet.de/bundesrecht/stgb/gesamt.pdf>.
- [190] Verordnung über Rahmenbedingungen für den Messstellenbetrieb und die Messung im Bereich der leitungsgebundenen Elektrizitäts- und Gasversorgung (Messzugangsverordnung - MessZV) vom 17. Oktober 2008 (BGBl. I S. 2006), die durch Artikel 2 der Verordnung vom 3. September 2010 (BGBl. I S. 1261) geändert worden ist. (2010). In einer nicht amtlichen Fassung als vollständiger Gesetzestext abrufbar unter: <http://www.gesetze-im-internet.de/bundesrecht/messzv/gesamt.pdf>.

- [191] Verordnung über den Zugang zu Elektrizitätsversorgungsnetzen (Stromnetzzugangsverordnung - StromNZV) vom 25. Juli 2005 (BGBl. I S. 2243), die zuletzt durch Artikel 10 des Gesetzes vom 28. Juli 2011 (BGBl. I S. 1634) geändert worden ist. (2011). In einer nicht amtlichen Fassung als vollständiger Gesetzestext abrufbar unter: <http://www.gesetze-im-internet.de/bundesrecht/stromnzv/gesamt.pdf>.
- [192] FERC: Smart Grid Policy; Final Rule. Abrufbar unter: <http://edocket.access.gpo.gov/2009/pdf/E9-17624.pdf>. (2009).

## **Danksagungen**

Hiermit möchte ich mich bei allen bedanken, die mich im Rahmen der Bachelor-Thesis und während meines Studiums unterstützt haben.

Für die intensive Betreuung, die hilfreichen Diskussionen und die konstruktiven Anregungen möchte ich mich bei meinen Betreuern Prof. Dr. Joachim Charzinski und Dipl.-Ing. Christoph Lindenmüller bedanken.

Besonders bedanken möchte ich mich bei meiner Schwester Daniela und meiner Freundin Olivia für die seelische und moralische Unterstützung sowie für das Korrekturlesen.

Mein Dank geht an meine beide Kommilitonen Petar Cvitkovic und Mahmoud Al-Asadi, die mich während meines Studiums unterstützt haben.

Nicht zuletzt möchte ich mich bei meinen Eltern dafür bedanken, dass sie mir dieses Studium ermöglicht haben.