Band 15 / 2016

Smart Grid Security Guidance – $(SG)^2$

Sicherheitsmaßnahmen für Stromnetzbetreiber in Österreich

Johannes Göllner, Lucie Langer und Matthias Tischlinger (Hrsg.)

Schriftenreihe der
Landesverteidigungsakademie

www.bundesheer.at

SCHUTZ UND HILFE

Schriftenreihe der
Landesverteidigungsakademie

Johannes Göllner, Lucie Langer, Matthias Tischlinger (Hrsg.)

Smart Grid
Security Guidance – $(SG)^2$

Sicherheitsmaßnahmen für Stromnetzbetreiber in Österreich

15/2016
Wien, Mai 2016

Impressum:

Medieninhaber, Herausgeber, Hersteller:
Republik Österreich / Bundesministerium für Landesverteidigung und Sport
Rossauer Lände 1
1090 Wien

Redaktion:
Landesverteidigungsakademie
Zentraldokumentation und Information
Stiftgasse 2a
1070 Wien

Schriftenreihe der Landesverteidigungsakademie

Copyright:
© Republik Österreich / Bundesministerium für Landesverteidigung und Sport
Alle Rechte vorbehalten

Mai 2016
ISBN 978-3-902944-xx-x

Druck:
HDruckZ-ASt Stift xxxx/16
Stiftgasse 2a
1070 Wien

Inhaltsverzeichnis

Vorwort 9
Abstract 15

Teil I: IKT-Architekturmodell 19
1. Zielsetzung und Vorgehensweise 19
2. IKT-Architekturmodell für Smart Grids in Österreich 22
2.1. Herleitung des Architekturmodells 22
2.2. Ergebnis 23
2.3. Beschreibung der einzelnen Architekturkomponenten 25
2.4. Bewertung der Ergebnisse 31

Teil II: Bedrohungs- und Risikoanalyse 33
1. Zielsetzung und Vorgehensweise 33
2. IKT-Bedrohungen im Smart Grid 34
2.1. Betrachtung von allgemeinen Bedrohungen im Smart-Grid-Kontext 34
2.2. Granularität und Konsolidierung von Bedrohungen 35
2.3. Bedrohungskatalog 36
2.4. Bedrohungsmatrix 38
2.5. Abstimmung mit Herstellern und Netzbetreibern in den Entwicklungsphasen 38
3. Risikomatrix 39
3.1. Bewertung 39
3.2. Visualisierung 41
3.3. Auswertung 42
4. Fazit 42

Teil III: Rechtliche und gesellschaftliche Aspekte 45
1. Einleitung 45
2. Strafrechtliche Untersuchung ausgewählter Bedrohungsszenarien im intelligenten Stromnetz 46
2.1. Vorab: Übereinkommen des Europarates über Computerkriminalität vom 23.11.2001 47
2.2. Vorab: Rahmenbeschluss 2005/222/JI des Rates über Angriffe auf Informationssysteme 47

2.3. Szenario 1: Stromdiebstahl 48
2.4. Szenario 2: Abrechnungsbetrug 51
2.5. Szenario 3: Pures Hacken eines fremden Smart Meters 85
2.6. Szenario 4: „Ausspähen" von Daten fremder Smart Meter bzw. des Konzentrators für kriminelle Zwecke 95
2.7. Szenario 5: Manipulation der Daten fremder Smart Meter / des Konzentrators für kriminelle Zwecke 111
2.8. Ausblick: Geplante Strafrechtsnovelle 117
3. Gesellschaftliche Aspekte 125
3.1. Privacy in der ökonomischen Literatur 125
3.2. Cybersecurity und Individuum 127
3.3. Cybersecurity durch das Individuum 129

Teil IV: Sicherheitsanalyse 135
1. Zielsetzung 135
2. Vorgehensweise 135
2.1 Analysearten 138
2.2. Einzelrisikobewertung 140
3. Analyse von Smart-Grid-Systemen 141
3.1. Übersicht der analysierten Komponenten 141
3.2. Topologie der Komponenten 142
4. Analyse von Smart-Metering-Systemen 144
4.1. Übersicht der analysierten Komponenten 144
4.2. Topologie der Komponenten 145
5. Analyse McAfee Application Control 146
5.1. Übersicht der analysierten Software 146
5.2. Durchgeführte Testklassen 147
6. Ergebnisse 150

Teil V: Maßnahmenkatalog und Tool-Implementierung 153
1. Zielsetzung und Vorgehensweise 153
2. Herleitung der Sicherheitsmaßnahmen 154
2.1. Definition generischer und spezifischer Maßnahmen 154
2.2. Einschränkung auf Bedrohungen mit hohem Risikopotential 156
2.3. Erweiterung auf übergeordnete Maßnahmen („Maßnahmen-Cluster") 156
2.4. Priorisierung der Maßnahmen-Cluster 159

2.5. Ideale Umsetzungsszenarien inkl. Definition der verantwortlichen Stakeholder 162
2.6. Konkrete Umsetzungsbeispiele 167
3. Fazit und Ausblick zum Maßnahmenkatalog 172
4. Tool-Implementierung des Maßnahmenkatalogs 173
4.1. Vorteile einer Tool-Implementierung 173
4.2. Auswahl des Tools 174
5. Vorgehensweise bei der Tool-Implementierung 175
5.1. Abbildung der Komponenten des IKT-Architekturmodells und des Maßnahmenkatalogs 176
5.2. Schutzbedarfsfeststellung der Assets 178
5.3. Abbildung des Maßnahmenkatalogs 180
6. Evaluierung der Tool-Implementierung 182
7. Ausblick zur Tool-Implementierung 186

Teil VI: Evaluierung der Sicherheitsmaßnahmen bei der Energie AG 187
1. Zielsetzung und Vorgehensweise 187
2. Teststellung bei der Energie AG 188
2.1. Beschreibung der Komponente zentraler Netzrechner 189
2.2. Beschreibung und Funktion der Komponentengruppe AMIS Metering 191
3. Festlegung der Anwendungsszenarien für die Evaluierung 192
3.1. Maßnahmen-Cluster 1: Authentizität und Integrität 192
3.2. Maßnahmen-Cluster 2: Sicherheitsevaluierung & Funktions-, Interoperabilitäts- und Penetrations-Tests 195
3.3. Maßnahmen-Cluster 3: Minimalprinzip 196
3.4. Maßnahmen-Cluster 4: Netzwerksegmentierung & Abschottung verschiedener (Sicherheits-) Bereiche 197
3.5. Maßnahmen-Cluster 5: Schutz von (Fern-) Wartungs-zugängen & verpflichtende Transparenz seitens der Hersteller 200
3.6. Maßnahmen-Cluster 6: Sicherheitsanforderungen für Hersteller 202
3.7. Maßnahmen-Cluster 7: Change Management, Patch Management, Configuration Management 203
3.8. Maßnahmen-Cluster 8: Physische Sicherheitsmaßnahmen 205
3.9. Maßnahmen-Cluster 9: Incident Management 207
3.10. Maßnahmen-Cluster 10: Mehrstufiges Sicherheitskonzept 209
4. Ergebnisse der Evaluierung des Zentralen Netzrechners 212

4.1. Maßnahmen-Cluster 1: Authentizität und Integrität 212
4.2. Maßnahmen-Cluster 3: Minimalprinzip für sicherheitskritische Schnittstellen 213
4.3. Maßnahmen-Cluster 4: Netzwerksegmentierung & Abschottung verschiedener (Sicherheits-) Bereiche 215
4.4. Maßnahmen-Cluster 5: Schutz von (Fern-) Wartungszugängen & verpflichtende Transparenz seitens der Hersteller 215
4.5. Maßnahmen-Cluster 8: Physische Sicherheitsmaßnahmen 217
4.6. Maßnahmen-Cluster 9: Incident Management 217
4.7. Maßnahmen-Cluster 10: Mehrstufiges Sicherheitskonzept 218
5. Ergebnisse der Evaluierung des zentralen Netzwerkes zwischen den Umspannwerken 219
5.1. Maßnahmen-Cluster 1: Authentizität und Integrität 219
5.2. Maßnahmen-Cluster 3: Minimalprinzip für sicherheitskritische Schnittstellen 221
5.3. Maßnahmen-Cluster 4: Netzwerksegmentierung & Abschottung verschiedener (Sicherheits-) Bereiche 222
5.4. Maßnahmen-Cluster 5: Schutz von (Fern-) Wartungszugängen & verpflichtende Transparenz seitens der Hersteller 223
5.5. Maßnahmen-Cluster 8: Physische Sicherheitsmaßnahmen 224
5.6. Maßnahmen-Cluster 9: Incident Management 225
5.7. Maßnahmen-Cluster 10: Mehrstufiges Sicherheitskonzept 226
6. Ergebnisse der Evaluierung der Metering-Umgebung 227
6.1. Maßnahmen-Cluster 1: Authentizität und Integrität 227
6.2. Maßnahmen-Cluster 3: Minimalprinzip für sicherheitskritische Schnittstellen 229
6.3. Maßnahmen-Cluster 4: Netzwerksegmentierung & Abschottung verschiedener (Sicherheits-) Bereiche 230
6.4. Maßnahmen-Cluster 5: Schutz von (Fern-) Wartungszugängen & verpflichtende Transparenz seitens der Hersteller 231
6.5. Maßnahmen-Cluster 8: Physische Sicherheitsmaßnahmen 232
6.6. Maßnahmen-Cluster 9: Incident Management 232
6.7. Maßnahmen-Cluster 10: Mehrstufiges Sicherheitskonzept 234
7. Anwendung des Maßnahmenkataloges 235
8. Evaluierung der Methodik 237

Abkürzungsverzeichnis 239
Literaturverzeichnis 241

Abbildungsverzeichnis 247
Tabellenverzeichnis 249
Herausgeber und Autoren 251

Vorwort

Bundesministerium für Inneres

Im Rahmen der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) und des Österreichischen Programms zum Schutz kritischer Infrastrukturen (APCIP) werden Unternehmen, die kritische Infrastrukturen betreiben, angehalten, eine umfassende Sicherheitsarchitektur zu implementieren. Betreiber sensibler Infrastruktur aus Sektoren wie Energieversorgung, Bankenwesen, Transport, Gesundheitswesen usw. tragen mit ihren Leistungen wesentlich zur Aufrechterhaltung der öffentlichen Sicherheit bei. Eine enge Kooperation zwischen diesen Anbietern und Regierungsbehörden ist daher unerlässlich, um für eine Stärkung der Widerstandskraft der jeweiligen Einrichtungen gegen Bedrohungen und für eine Erhöhung der Resilienz beizutragen.

Der Bereich der Energieversorgung erfüllt dabei für die österreichische Bevölkerung eine eminente gesellschaftliche Funktion, die rund um die Uhr in einer hochkomplexen Systemarchitektur durch ein Zusammenspiel automatisierter und manueller Regelungstechniken sowie intelligenter Messgeräte und ausfallssicherer Kommunikationswege gewährleistet werden muss. Vor diesem Hintergrund wurde dieses Projekt vom BM.I als Bedarfsträger in der Einreichung unterstützt und im gesamten Projektablauf gerne begleitet.

Im Rahmen der Vernetzung des vom BM.I eingebrachten Expertenwissens, hier vor allem aus den Bereichen Netzwerktechnik und Informationssicherheit, mit dem Know-How der beteiligten Stromversorger sowie der wissenschaftlichen Begleitung konnte eine umfassende Risikobewertung der für die Versorgungssicherheit systemrelevanten IKT-Systeme durchgeführt werden. Hervorzuheben ist an dieser Stelle der durch die Beteiligung an Forschungsprojekten erzielbare Mehrwert, der sich nicht nur in mess- oder überprüfbaren Ergebnissen zeigt, sondern speziell im durch gegenseitigen Austausch erreichten Erkenntnisgewinn und gegenseitigen Verständnis der spezifischen Herausforderungen der involvierten Partner besteht.

Für die Erstellung des Maßnahmenkataloges zur Absicherung einer wie in der Energiewirtschaft bestehenden komplexen IKT-Infrastruktur, mit ihren großen Angriffsflächen und multiplen Angriffsvektoren, wurde in diesem Projekt eine eigene Methodik für die Herangehensweise entwickelt. Die begleitend eingesetzten Softwarewerkzeuge auf open-source Basis stehen nach Projektende auch anderen interessierten Energieversorgen zur Verfügung und tragen so zu einer weiteren Erhöhung der Sensibilisierung in der Branche bei.

Gefährdungspotentiale der Sicherheit von Smart Metern bzw. deren modular aufgebauten Einzelkomponenten wurden als Bestandteil der Studie an von der Industrie zur Verfügung gestellten Geräten konkretisiert und von einem Projektpartner aus dem Bereich Sicherheitstechnik geprüft und bewertet. So kann der Fokus der öffentlichen Wahrnehmung um die Sicherheit von Smart Metern von einer emotionalen zu einer faktenbasierenden Diskussion gelenkt werden.

Das Interesse aus dem Umfeld der Energieversorger nach Projektende bzw. auch die zweimalige Auszeichnung dieses Projekts durch den BMVIT Smart Grids Award zeigt, dass alle Partner in jeder Studienphase ausgezeichnete Arbeit geleistet haben. Diese Würdigung ist einmal mehr Bestätigung des im Rahmen des Sicherheitsforschungsprogramm KIRAS erreichbaren Qualitätsniveaus, der ich mich durch den Ausdruck meiner Wertschätzung für die beteiligten Projekt- und Kooperationspartner nur anschließen kann.

Mag. Markus Popolari
Leiter der Abteilung IKT-Sicherheit und E-Government
Bundesministerium für Inneres

Bundesministerium für Landesverteidigung und Sport

Technologien der Zukunft werden sich immer mehr auf Informations- und Kommunikationstechnologien abstützen. Insbesondere die Stromversorgung sieht sich als kritische Infrastruktur daher vermehrt mit neuen Ereignissen, Gefahren, Bedrohungen, Risiken und Herausforderungen in Sicherheitsfragen konfrontiert. Für das Österreichische Bundesheer (ÖBH) liegt es im fundamentalen Interesse, diese Entwicklungen früh zu verfolgen, an neuartigen Sicherheitsmechanismen und Prozessen mitzuarbeiten und entsprechende Ableitungen zu treffen. Auf der Basis der permanenten Suche nach geeigneten und wirksamen Verfahren und Maßnahmen kann in Zukunft auf Cyberattacken auf Stromnetzwerke bzw. Smart Grids richtig und effizient reagiert werden, um die Stromversorgung Österreichs und auch die Elektrizitätsversorgung von BMLVS-Objekten und Liegenschaften aufrechtzuerhalten.

Der vorliegende Band liefert für den interessierten Leser einen ausgezeichneten Über- und Einblick in die vorgestellten Projektergebnisse des KIRAS-Forschungsprojektes „Smart Grid Security Guidance – $(SG)^2$“, in dem die Mitarbeiter des Hauptreferats Wissensmanagement, Abteilung Zentraldokumentation und Information der Landesverteidigungsakademie maßgeblich ihre Kompetenzen, ihr Wissen und ihre langjährigen Erfahrungen, besonders im Bereich Wissens- und Risikomanagement aus verschiedenen Forschungsprojekten einbringen konnten. Dieser Leistung und dem Stellenwert des Projektes innerhalb der Forschungslandschaft wurde zweimal mit der Verleihung des Smart Grids Awards des BMVIT Rechnung getragen.

Die Zusammenarbeit der Angehörigen des ÖBH mit den Forschern und Wissenschaftlern in ganz Österreich zählt zu den erklärten Zielen des Österreichischen Bundesheeres. Mit der konkreten Kooperation im Rahmen des gegenständlichen Sicherheitsforschungsprojektes „Smart Grid Security Guidance“ wurde der Beweis für erfolgreiche Kooperationen erbracht. Dies war auch deswegen möglich, weil durch die Kollegen des Hauptreferats Wissensmanagement der Landesverteidigungsakademie eine konsequente aktive Forschungstätigkeit erbracht wird und dies in Zukunft hoffentlich auch so bleiben wird.

Die Suche nach Lösungsansätzen und konkreten, nachvollziehbaren Lösungen sind nicht nur für das ÖBH, sondern für das gesamte Gemeinwohl von entscheidender Bedeutung. Forschung und technische Entwicklung leisten hierbei einen unverzichtbaren Beitrag. Mit dem österreichischen Sicherheitsforschungsprogramm KIRAS wird zur Sicherheit der Bürger und des Staates ein essentieller Beitrag geleistet. Das ÖBH ist sehr gerne Teil der an KIRAS beteiligten Organisationen und der zahlreichen Forschungspartner.

Für die Forschung an der Landesverteidigungsakademie wird in Zukunft neben der forschungsgeleiteten Lehre die aktive Beteiligung an der nationalen und europäischen Verteidigungsforschung in den Vordergrund rücken. Für diese Form der Wettbewerbsforschung braucht es hohe Fachkompetenz und ebenso leistungsfähige Partner. Die Teilnahme an KIRAS-Projekten ist eine ausgezeichnete Basis für eine erfolgreiche Teilnahme und eine sichere Zukunft.

Abschließend darf ich allen Kooperations- und Forschungspartnern des KIRAS-Projekts „$(SG)^2$ – Smart Grid Security Guidance“ Anerkennung und Wertschätzung für das Ergebnis des Projektes entgegenbringen und den werten Lesern eine spannende Lektüre wünschen.

Bgdr. Mag. Klemens Hofmeister
Leiter der Abteilung Wissenschaft, Forschung und Entwicklung
Bundesministerium für Landesverteidigung und Sport

Projektpartner (SG)^2 (in alphabetischer Reihenfolge)

AIT Austrian Institute for Technology GmbH
    Digital Safety & Security Department (Koordinator)
    Energy Department
Bundesministerium für Inneres
Bundesministerium für Landesverteidigung und Sport
Energie AG Oberösterreich Data GmbH
Energieinstitut an der Johannes Kepler Universität Linz
Innsbrucker Kommunalbetriebe AG
LINZ STROM GmbH
SEC Consult Unternehmensberatung GmbH
Siemens AG – Corporate Technology Österreich
Technische Universität Wien
    Automation Systems Group
    Institut für Computertechnik

Danksagung an Fördergeber

Das Projekt Smart Grid Security Guidance (SG)^2 wurde im Österreichischen Sicherheitsforschungs-Förderprogramm KIRAS vom Bundesministerium für Verkehr, Innovation und Technologie (BMVIT) gefördert.

Abstract

Die Stromversorgung der Zukunft wird weit mehr auf Informations- und Kommunikationstechnologien (IKT) setzen als bisher. Damit werden Cybersecurity-Risiken auch zu einer Gefahr für die Energieversorgung. Viele Sicherheitsfragen in diesen zukünftigen Netzen sind noch ungeklärt, denn die speziellen Umgebungen erfordern neuartige Sicherheitsmechanismen und Prozesse. Im Projekt Smart Grid Security Guidance – $(SG)^2$ – wurden daher aktuelle Smart-Grid-Technologien in Bezug auf IKT-Sicherheitsaspekte evaluiert und effektive Schutzmaßnahmen vor Cyber-Attacken definiert. Durch Anwendung dieser Maßnahmen können Stromnetzbetreiber ihre Netze besser vor Cyber-Angriffen schützen. Die Ergebnisse leisten somit einen wesentlichen Beitrag zum Schutz unserer Energieversorgung als kritische Infrastruktur. Das Projekt hat zweimal (2013 und 2015) den Smart Grids Award des BMVIT gewonnen, was den Stellenwert der erzielten Ergebnisse verdeutlicht.

Zu Beginn des Projektes wurden nationale sowie internationale Smart-Grid-Pilotprojekte auf ihren Einsatz von IKT-Komponenten und deren Sicherheitsaspekte hin ausgewertet, indem die jeweilige Systemarchitektur auf das von CEN-CENELEC-ETSI entwickelte Smart Grid Architecture Model abgebildet wurde. Aus dieser Analyse heraus wurde ein IKT-Architekturmodell für Smart Grids in Österreich definiert, welches die in den Pilotprojekten vertretenen Komponenten sowie gleichzeitig auch aktuelle bzw. für die nahe Zukunft geplante Systemarchitekturen nationaler Energieversorgungsunternehmen berücksichtigt.

Die Komponenten dieses Architekturmodells wurden anschließend auf theoretische Schwachstellen und Gefährdungen hin analysiert. Ergebnis war ein Bedrohungs- und Risikokatalog für Smart Grids in Österreich mit klarem Fokus auf Energieversorgungsunternehmen. Diejenigen Komponenten des Architekturmodells, welche gemäß diesem Katalog ein besonders hohes Risiko für Cyber-Angriffe aufweisen, wurden in Form zweier Testsysteme (Secure Substation und Smart Meter) einer umfassenden Sicherheitsanalyse unterzogen. Gleichzeitig wurde ein Katalog von Schutzmaßnahmen definiert, welcher die Bedrohungen und Schwachstellen adressiert, die sich aus dem Risikokatalog und der Sicherheitsanalyse ergeben.

Dazu wurden, basierend auf IT-Grundschutz sowie einschlägigen Quellen im Bereich Smart-Grid-Security, technische und organisatorische Schutzmaßnahmen definiert. Durch Umsetzung dieser Maßnahmen können die jeweiligen Cybersecurity-Risiken gemildert werden, indem die Eintrittswahrscheinlichkeit oder die Auswirkungen eines Angriffs reduziert werden. Parallel zu diesen Tätigkeiten wurden über die gesamte Projektlaufzeit hinweg rechtlich-gesellschaftliche Fragestellungen adressiert. So wurden beispielsweise strafrechtliche Fragestellungen rund um das Thema Smart Metering analysiert, und es fand eine sozio-ökonomische Untersuchung der Umsetzbarkeit der vorgeschlagenen Schutzmaßnahmen statt.

Die vorgeschlagenen Sicherheitsmaßnahmen wurden gegen Ende der Projektlaufzeit im Testlabor des Projektpartners Energie AG evaluiert. Dieses Testsystem repräsentiert das Netz in seiner Gesamtheit und erlaubt so Rückschlüsse auf die reale Anwendbarkeit und Effektivität der definierten Schutzmaßnahmen. Zum Teil sind diese Schutzmaßnahmen bereits bei den österreichischen Netzbetreibern umgesetzt. Sofern sie noch nicht implementiert sind, liegt dies vor allem auch an der langen Lebensdauer der im Einsatz befindlichen Komponenten, und der damit verbundenen finanziellen Machbarkeit. So ist beispielsweise ein Austausch der Leitsysteme nur über einen längeren Zeitraum hin finanzierbar. Die jetzt geforderten Sicherheitsmaßnahmen, wie z. B. Verschlüsselung auf Applikationsebene, müssen über einen Lebenszyklus von 20 Jahren und mehr gewährleistet sein; gleichzeitig müssen künftige Systeme flexibel auf neue Anforderungen (z. B. Änderungen des Verschlüsselungssystems) reagieren können. All dies sind wesentliche Herausforderungen, die in Zukunft zu meistern sind.

Die seitens der Energieversorgungsunternehmen tatsächlich zu implementierenden Sicherheitsmaßnahmen müssen aus einer Risikoanalyse heraus definiert werden, die die möglichen Risiken den potenziellen Auswirkungen eines Angriffs sowie dem (Kosten-) Aufwand der entsprechenden Schutzmaßnahmen gegenüberstellt. Bei der Definition der Maßnahmen gilt es zu bedenken, dass sich Sicherheit nur durch eine Kombination von technischen und organisatorischen Maßnahmen erreichen lässt. Rein technische Maßnahmen greifen z. B. bei (absichtlichen oder unabsichtlichen) menschlichen Fehlhandlungen zu kurz. Nach erfolgter Definition der Sicherheitsmaßnahmen muss auch eine kontinuierliche Maßnahmenverfolgung gewährleistet sein: Genau wie die Summe der Betriebsmittel eines Stromnet-

zes kontinuierlicher Erneuerung unterworfen ist, sind auch die Sicherheitsmaßnahmen regelmäßig an die aktuellen Gegebenheiten anzupassen. Nur so kann letztendlich das hohe Maß an Versorgungssicherheit unseres Stromnetzes beibehalten werden.

Teil I: IKT-Architekturmodell

1. Zielsetzung und Vorgehensweise

Basis für die Arbeiten im $(SG)^2$-Projekt sollte ein IKT-Architekturmodell für Smart Grids in Österreich sein, welches es zu Beginn des Projektes zu definieren galt. Dazu wurden zunächst Informationen über laufende sowie abgeschlossene nationale Smart-Grid-Projekte zusammengetragen. Insgesamt 45 Projekte wurden nach Themenbereichen kategorisiert und auf ihre Relevanz für die Aufgabenstellung hin analysiert, um die Auswahl an betrachteten Projekten auf eine sinnvolle Anzahl zu beschränken. Anschließend wurden ergänzend internationale Smart-Grid-Projekte und Entwicklungen betrachtet und ebenfalls kategorisiert sowie auf ihre Relevanz überprüft. Die Ergebnisse aus beiden Schritten wurden mit den Systemarchitekturen der im Projekt vertretenen Netzbetreiber abgeglichen, um nicht nur zukünftige Entwicklungen, sondern auch den Status Quo im Architekturmodell festzuhalten. Aus diesen Vorarbeiten wurde schließlich das IKT-Architekturmodell für das $(SG)^2$-Projekt abgeleitet.

Folgende Kriterien waren für die Auswahl der betrachteten Projekte ausschlaggebend:
1.) Signifikanter IKT-Aspekt: Um in weiterer Folge Aussagen zum Thema Systemarchitektur und IKT-Sicherheit machen zu können, war es nötig, sich von Anfang an auf technisch dimensionierte Projekte zu beschränken, welche eine reale Installation oder eine bereits implementierte IKT-Architektur beinhalten.
2.) Breiter Rollout: Im Hinblick auf die Relevanz der Ergebnisse und die verfügbaren Ressourcen wurden nur Pilotprojekte betrachtet, die eine gewisse Größe aufweisen. Als Untergrenze galt dabei eine Anzahl von mindestens 100 betroffenen Kunden bzw. mehreren Trafostationen.

Als weiteres Ziel sollten die ausgewählten Projekte die aktuelle österreichische Smart-Grid-Landschaft möglichst gut abdecken und somit eine solide Basis für die weiteren Arbeiten im Projekt $(SG)^2$ bilden. Die Auswahl und Priorisierung erfolgte durch die Projektpartner. Dabei war von Vorteil, dass einige Projektpartner auch in vielen Projekten beteiligt sind bzw. waren, bzw. dass durchweg ein gutes Branchen-Know-How vorliegt. Ergänzend wurden Dokumentationen und Berichte aus den einzelnen Projekten ver-

wendet, sowie die online verfügbare Weltkarte mit Smart-Metering-Projekten auf Google Maps[1] .

Nach dem Selektionsschritt waren sieben von 45 Projekten übrig, siehe Tabelle 1. Die sieben ausgewählten Projekte wurden jeweils auf verwendete Technologien und Sicherheitsmechanismen untersucht, auf die Detaildarstellung dieser Ergebnisse verzichten wir an dieser Stelle.

Tabelle 1: Ausgewählte österreichische Smart-Grid-Projekte

Lfd.Nr.	**Kategorie**	**Projektbezeichnung**
1	Smart Metering, Lastmanagement	IEM – Intelligent Energy Management
5	Dezentrale Einspeisung Niederspannung	DG DemoNetz Smart LV Grid
6	Dezentrale Einspeisung Mittelspannung	DG DemoNetz Validierung
7	Dezentrale Einspeisung	SGMS ZUQDE
11	Datenmanagement	SGMS Smart Web Grid
16	E-Mobility	emporA
38	Smart Metering, Lastmanagement	AMIS Smart Metering Rollout

Um ein konsistentes Bild der in jedem Projekt eingesetzten IKT zu gewinnen und eine einheitliche Herangehensweise sicherzustellen, wurde jedes der sieben Projekte anschließend in das Smart Grid Architecture Model eingebettet (siehe Abbildung 1). Hierbei handelt es sich um eine von der CEN-CENELEC-ETSI Smart Grid Coordination Group im Rahmen des M/490-EU-Mandates entwickelte europäische Referenzarchitektur mit den folgenden drei Dimensionen: Die Domänen beschreiben die verschiedenen Stationen der Energieumwandlung von der Energieerzeugung (Generation) über die Übertragung (Transmission) und Verteilung (Distribution) bis hin zu den Verbraucherhaushalten (Customer Premises). Die Zonen stellen die

[1] https://www.google.com/maps/d/viewer?mid=zReklSu043lk.kZ_YiimMzyXc&ie=UTF8&oe=UTF8&msa=0, letzter Zugriff am 17.12.2015

verschiedenen Bereiche des Informationsmanagements dar, welches sich von Prozessen bis hin zu Märkten erstreckt. Domänen und Zonen spannen die Smart-Grid-Plane auf, in der sich veranschaulichen lässt, innerhalb welcher Zonen bestimmte Wechselwirkungen zwischen einzelnen Domänen auftreten. Als dritte Dimension kommen nun noch orthogonal zur Smart-Grid-Plane verschiedene Interoperability Layers hinzu; diese beinhalten Component und Communication Layer sowie Information, Function und Business Layer. Das Modell ermöglicht so die Darstellung von Informationsflüssen zwischen verschiedenen Entitäten eines Smart Grids, und bildet somit eine gute Basis für weitergehende Sicherheitsanalysen.

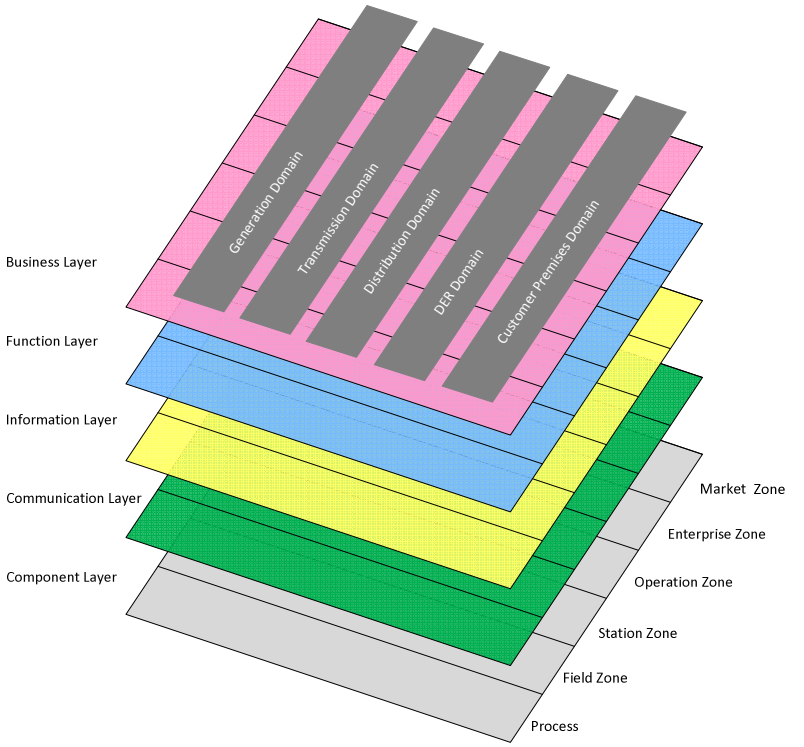


Abbildung 1: Smart Grid Architecture Model gemäß CEN-CENELEC-ETSI (2012)

Die resultierende IKT-Architektur für das $(SG)^2$-Projekt wurde ebenfalls auf SGAM abgebildet, um eine breite Akzeptanz und internationale Vergleichbarkeit zu gewährleisten. Die IKT-Architektur wird im Detail in Abschnitt 2 beschrieben.

2. IKT-Architekturmodell für Smart Grids in Österreich

2.1. Herleitung des Architekturmodells

Die Basis für das IKT-Architekturmodell bildet das Smart Grid Architecture Model oder kurz SGAM (siehe Abbildung 1). Mit Hilfe dieses Modells lassen sich Smart-Grid-Ansätze darstellen und vergleichen, sodass Unterschiede und Gemeinsamkeiten zwischen verschiedenen Paradigmen, Roadmaps und Sichtweisen erkennbar werden. Neben den verschiedenen Domänen der elektrischen Energieversorgung, von der Erzeugung über die Verteilung bis zum Verbraucher, sind auch Service- und Systemdienstleistungen erfasst sowie die Interaktion mit angrenzenden Bereichen wie beispielsweise Haus-, Gebäude- und Industrieautomatisierung und Elektromobilität. Dies führt zu einer Vielzahl von Funktionen, Akteuren und Komponenten, die zusammenspielen müssen, um ein effizientes und sicher funktionierendes System zu gewährleisten. Interoperabilität muss dabei nicht nur im Bereich der Energieerzeugungs- und Energieverteilungsprozesse gewährleistet werden, sondern auch bei den Geschäftsprozessen und der Marktkommunikation der beteiligten Akteure. Dies spiegelt sich auch in der Smart-Grid-Normung mit den verschiedenen direkt oder indirekt involvierten Normungs- und Standardisierungsorganisationen und technischen Komitees wider.

Für das $(SG)^2$-Projekt ist besonders die Smart-Grid-Ebene (im Original „Smart-Grid-Plane“) relevant, die von den Domänen der Energieerzeugungs- und -umwandlungskette sowie den hierarchischen Zonen des Netzmanagements aufgespannt wird. Die Interoperabilität wird von den übereinanderliegenden fünf Modellschichten Component, Communication, Information, Function und Business abgebildet. Die Abbildungen der einzelnen Projekte beschränken sich, ebenso wie das resultierende IKT-Architekturmodell, auf die Ebenen Component und Communication Layer. Grund hierfür ist – neben der hohen Komplexität einer vollständigen Abbildung über alle Ebenen – die Tatsache, dass für die Untersuchungen im $(SG)^2$-Projekt vor allem die Komponenten und ihre Kommunikationsverbindungen relevant waren. Die darüber liegenden Ebenen befassen sich mit Informationsstrukturen bzw. Datenformaten, Funktionen und Business-

Zielen, und sind daher für das Projekt nicht ausschlaggebend.

Folgende Teile wurden im Einzelnen auf SGAM abgebildet, um zum resultierenden IKT-Architekturmodell zu gelangen:

1. IKT-Architekturen relevanter nationaler Projekte,
2. IKT-Architekturen relevanter internationaler Projekte, sowie
3. Aktuelle Systemarchitekturen der im Projekt vertretenen Netzbetreiber.

Die einzelnen Architekturen wurden zusammengeführt und auf den kleinsten gemeinsamen Nenner gekürzt, um eine konsistente Architektur zu erhalten. Unterschiedliche Ausprägungen der verwendeten Kommunikationsprotokolle wurden dabei berücksichtigt.

2.2. Ergebnis

Das resultierende (SG)²-IKT-Architekturmodell ist in Abbildung 2 dargestellt. Das Architekturmodell deckt sechs Zonen (Prozess, Feld, Station, Operation, Enterprise, Markt) sowie drei Domänen (Distribution, DER, Customer) ab, inklusive der eingesetzten Kommunikationstechnologien und Normen.

Für die weitere Verwendung des Architekturmodells im Rahmen der Bedrohungs- und Risikoanalyse in Teil II war eine Zusammenfassung der einzelnen Komponenten zu sogenannten „Komponenten- bzw. Architektur-Clustern“ erforderlich, um zusammengehörige Teile gemeinsam zu betrachten und die Komplexität der Analysen auf ein sinnvolles Maß zu reduzieren. Die Komponenten-Cluster sind in Abbildung 3 dargestellt.

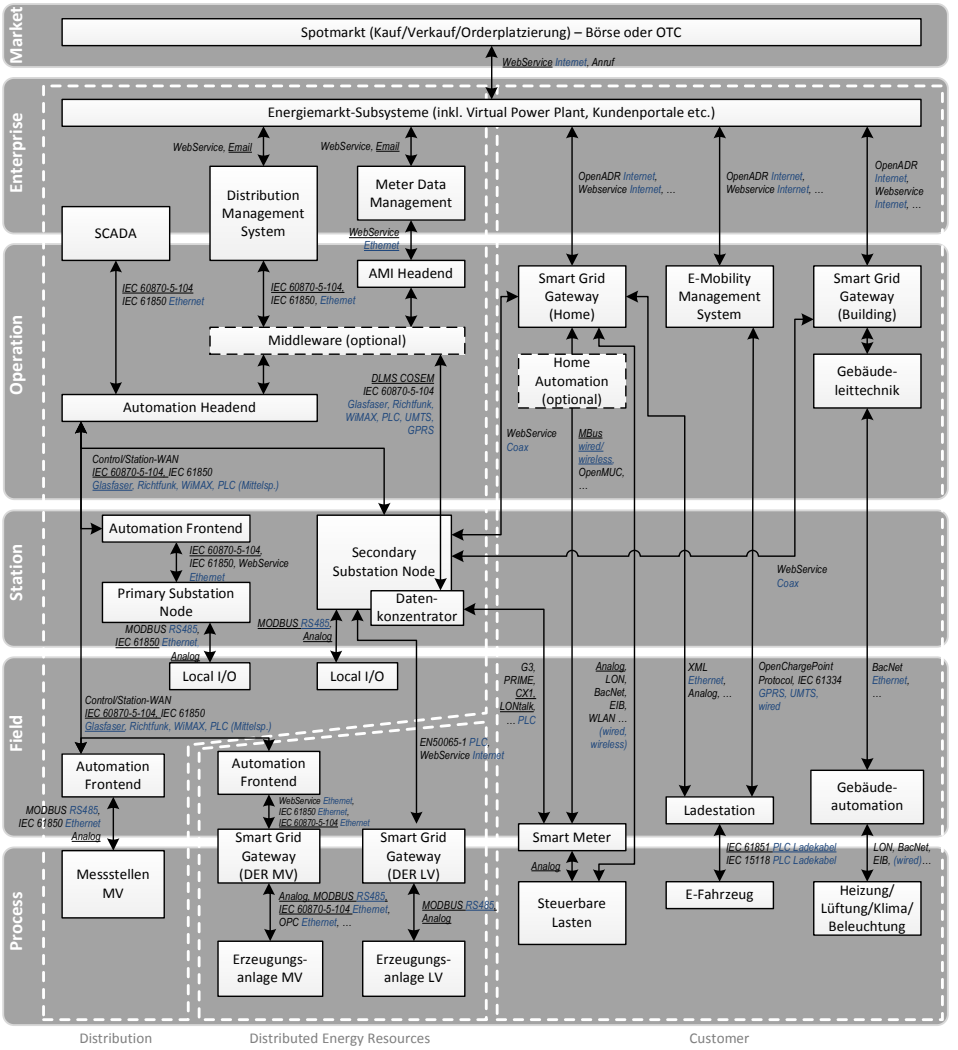


Abbildung 2: IKT-Architekturmodell aus dem Projekt (SG)²

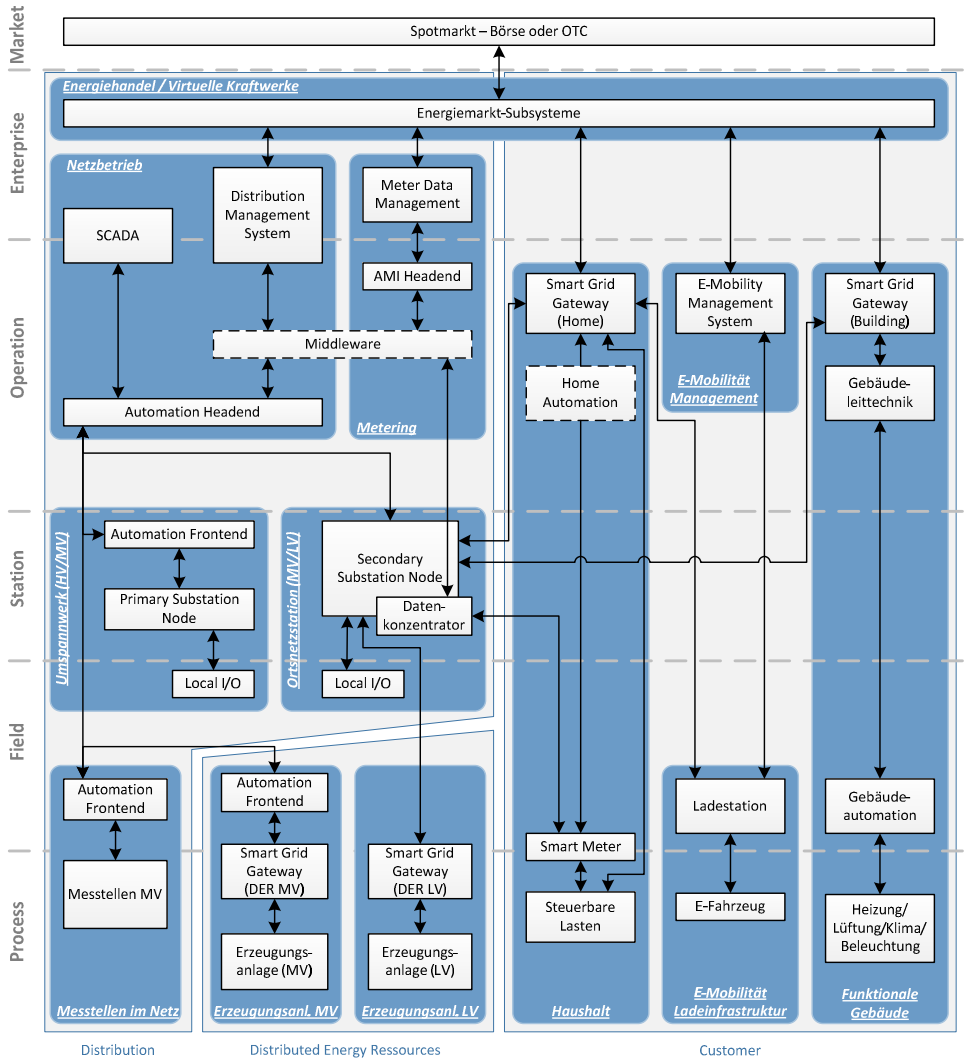


Abbildung 3: Komponenten-Cluster im IKT-Architekturmodell

2.3. Beschreibung der einzelnen Architekturkomponenten

Die folgenden Tabellen enthalten eine Beschreibung der Funktionalität der einzelnen Komponenten des Architekturmodells und der Kommunikation, die zwischen diesen stattfindet.

Tabelle 2: Komponenten-Cluster "funktionale Gebäude"

Komponente	**Beschreibung**
Smart Grid Gateway (Building)	Schnittstelle zwischen Netzbetreiber, ggf. Energiemarktplattformen und Gebäudebetreiber mit Hauptfunktion Lastmanagement (Customer Energy Management System); empfängt von Secondary Substation Node Lastprofilvorgaben und gibt diese nach unten an Gebäudeleittechnik weiter; umgekehrt werden Vorhersagen zum Energieverbrauch bzw. Potential für steuerbare Lasten sowie Rückmeldungen bzgl. der vorgegebenen Betriebsmodi an Secondary Substation Node übermittelt; Internetanbindung an Energiemärkte zwecks Preisabfrage zur lokalen Optimierung von Verbrauch und Erzeugung
Gebäudeleittechnik	Benutzerschnittstelle zur Gebäudeautomation (d.h. Management-Ebene und Visualisierung der technischen Vorgänge innerhalb des Gebäudes und Möglichkeit der Einstellung einzelner Parameter)
Gebäudeautomation	beinhaltet Überwachungs-, Steuer-, und Optimierungseinrichtungen für das Gebäude (d.h. hier findet die eigentliche Laststeuerung statt); empfängt Lastprofilvorgaben von der Gebäudeleittechnik
Heizung / Lüftung / Klima / Beleuchtung	steuerbare Lasten im Gebäude (Heizung, Lüftung, Klimatisierung, Beleuchtung)

Tabelle 3: Komponenten-Cluster "E-Mobilität"

Komponente	**Beschreibung**
E-Mobility Management System	Steuerung der Ladestationen; Abrechnung des Ladevorgangs; Internetanbindung an Energiemärkte zwecks Preisabfrage zur lokalen Optimierung von Verbrauch und Erzeugung
Ladestation	Stromtankstelle für (meist kabelgebundenes) Laden von E-Fahrzeugen; besitzt eindeutige ID zur Verrechnung; kann öffentlich oder privat betrieben werden
E-Fahrzeug	mit elektrischer Energie angetriebenes Fahrzeug; enthält aufladbaren Akku

Tabelle 4: Komponenten-Cluster "Haushalt"

Komponente	**Beschreibung**
Smart Grid Gateway (Home)	Schnittstelle zwischen Netzbetreiber, ggf. Virtuellen Kraftwerken oder Aggregatoren und Haushalt mit Hauptfunktion Lastmanagement (Home Energy Management System); abstrahiert die Haushaltsdaten und macht diese nach außen hin verfügbar; empfängt Lastmanagementvorgaben von Secondary Substation Node; Internetanbindung an Energiemärkte zwecks Preisabfrage zur lokalen Optimierung von Verbrauch und Erzeugung
Home Automation	Gebäudeautomation für Privathaushalte
Smart Meter	Zähler zum Messen der verbrauchten Energiemenge in Haushalten oder Gebäuden; typischerweise im 1h oder 1/4h-Raster, kann Teil des Smart Grid Gateways sein
Steuerbare Lasten	steuerbare Lasten im Haushalt, z. B. weiße Ware, Wärmepumpe

Tabelle 5: Komponenten-Cluster "Erzeugungsanlage LV"

Komponente	**Beschreibung**
Smart Grid Gateway (DER LV)	Schnittstelle zwischen LV-Erzeugungsanlage und Secondary Substation Node (SSN); kommuniziert die Einspeise-Vorgaben der SSN an die Erzeugungsanlage und meldet ggf. die eingespeiste Energiemenge oder andere Prozessparameter an die SSN zurück
Erzeugungsanlage (LV)	Dezentrale Erzeugungsanlage im Niederspannungsnetz, z. B. Photovoltaikanlage

Tabelle 6: Komponenten-Cluster "Erzeugungsanlage MV"

Komponente	**Beschreibung**
Automation Front-end	Schnittstelle zwischen Fernwirknetz und Automationssystem der MV-Erzeugungsanlage
Smart Grid Gateway (DER MV)	Schnittstelle zwischen Netzbetreiber und Erzeugungsanlage; gibt Vorgaben an die MV-Erzeugungsanlage gemäß der Einspeise-Vorgaben aus dem Netzbetrieb bzw. dem Umspannwerk und meldet ggf. die eingespeiste Energiemenge oder andere Prozessparameter zurück
Erzeugungsanlage (MV)	Dezentrale Erzeugungsanlage im Mittelspannungsnetz, z. B. Windkraftanlage

Tabelle 7: Komponenten-Cluster "Messstellen im Netz"

Komponente	**Beschreibung**
Automation Front-end	Schnittstelle zwischen Messstellen und Fernwirknetz; übermittelt Messwerte aus Mittelspannungsnetz in regelmäßigen Abständen an Primary Substation Node bzw. Netzbetrieb; keine Verbindung zur Erzeugungsanlage
Messstellen (MV)	Messstellen im Mittelspannungsnetz (im Architekturmodell separat dargestellt, da die Positionen der Messstellen nicht unbedingt mit den MV-Erzeugungsanlagen oder Primary Substation übereinstimmen); messen aktuelle Stromstärken- und Spannungswerte und melden diese über Automation Frontend an den Netzbetrieb; führen Plausibilitätschecks durch (Fehler der Sensoren berücksichtigt)

Tabelle 8: Komponenten-Cluster "Umspannwerk (HV/MV)"

Komponente	**Beschreibung**
Automation Front-end	Schnittstelle des Umspannwerks nach unten zum Prozess-Bus (Schaltanlagen, Schutz) und nach oben zur Operations-Ebene (Netzbetrieb, Endpunkt des IPSec-Tunnels); überträgt Messwerte und Schaltbefehle; besitzt selbst keine „Intelligenz“, abstrahiert nur die Datenformate (d.h. packt aus und wieder ein)
Primary Substation Node	IT-Komponente des Umspannwerks zur automatisierten Steuerung und Regelung; verarbeitet Messwerte aus der Station und ggf. im Netz und ermittelt Sollwertvorgaben für Komponenten in der Station (z. B. Stufentrafo) oder auch außerhalb (z. B. Erzeugungsanlagen)
Local I/O	Sensoren und Aktuatoren innerhalb des Umspannwerks

Tabelle 9: Komponenten-Cluster "Ortsnetzstation (MV/LV)"

Komponente	**Beschreibung**
Datenkonzentrator	Sammelt die Metering-Daten seines Einzugsgebietes und sendet diese gebündelt ans Zentralsystem (Meter Data Management); ggf. nicht in Ortsnetzstation verbaut sondern außerhalb angebracht (zwecks direkten Zugangs der Messstellenbetreiber)
Secondary Substation Node	IT-Komponente der Ortsnetzstation zur automatisierten Steuerung und Regelung; verarbeitet Messwerte aus der Station und ggf. im Netz und ermittelt Sollwertvorgaben für Komponenten in der Station (z. B. Stufentrafo) oder auch außerhalb (z. B. Erzeugungsanlagen)
Local I/O	Sensoren und Aktuatoren innerhalb der Ortsnetzstation

Tabelle 10: Komponenten-Cluster "Netzbetrieb"

Komponente	**Beschreibung**
SCADA	zentrale Steuerungseinheit und Benutzerschnittstelle für den Verteilernetzbetrieb (Schaltpläne); Entscheidungen über Netzkonfiguration und Zu- bzw. Abschalten von Netzsegmenten (Lastschätzung findet eher im SCADA-System des Übertragungsnetzes statt)
Distribution Management System	unterstützt SCADA mit Lastmodellierung und Assistenzfunktionen; berechnet die erforderliche Regelung auf Basis der SCADA-Daten (State Estimation); meist redundant aufgebaut (hot standby)

Automation Headend	Schnittstelle zum Fernwirknetz; Endpunkt für IPSec-Tunnel ins Fernwirknetz
Middleware	aus OpenNode-Projekt; Software, die Protokolle umsetzt und Daten aus mehreren Secondary Substation Nodes aggregiert (diese Aufgabe kann z. T. auch von SCADA- oder DMS-Systemen übernommen werden)

Tabelle 11: Komponenten-Cluster "Metering"

Komponente	**Beschreibung**
Meter Data Management	zentrales System, das Metering-Daten aufbereitet, speichert und auswertet und für andere Komponenten (z. B. Rechnungserstellung) bereitstellt
AMI Headend	Schnittstelle zwischen Meter Data Management und den Komponenten, die darauf zugreifen (z. B. Datenkonzentrator oder Distribution Management System)
Middleware	siehe Cluster „Netzbetrieb“

2.4. Bewertung der Ergebnisse

Bei Betrachtung der analysierten Projekte fällt auf, dass diese bei Einordnung in das SGAM-Modell fast ausschließlich den rechten unteren Quadrant belegen. Dieser Bereich entspricht den Domänen Distribution, DER und Customer Premises, sowie den Zonen Process, Field und Station. Dies ist darauf zurückzuführen, dass die Anlagen und Vermögenswerte der anderen Domänen und Zonen des SGAM-Modells (Generation und Transmission bzw. Market, Enterprise und Operation) seit jeher besser automatisiert waren, obwohl hier zum Teil noch alte Technologien eingesetzt werden. Die Auswirkungen der Einführung von Smart Grids zeigen sich somit deutlicher im Mittel- und Niederspannungsnetz sowie bei der verteilten Erzeugung. Als Sicherheitsmechanismen werden in den untersuchten Projekten bei Standardkomponenten wie Netzwerken, Servern, etc. die in der IKT bekannten Mechanismen eingesetzt. Manche Smart-Grid-

Komponenten weisen jedoch proprietäre Lösungen auf, welche zum Teil im Rahmen der Sicherheitsanalyse in Teil IV untersucht wurden.

Das eigentliche Ziel von Projektanalyse und Einbettung in das SGAM-Modell war es, Erkenntnisse im Hinblick auf eine generische Smart-Grid-IKT-Architektur für den österreichischen Markt zu gewinnen, die gleichzeitig als Basis für alle weiteren Tätigkeiten im Projekt (SG)² geeignet ist. Die Auswertung der sieben Modellprojekte im Rahmen der SGAM-Referenzarchitektur hat gezeigt, dass dieses europäische Modell auch gut zur Darstellung der Architektur von Pilotprojekten in Österreich geeignet ist. Um das Bild noch weiter zu vervollständigen, wurden zusätzlich auch die Systemarchitekturen nationaler EVUs auf SGAM abgebildet, wobei neben dem Status quo auch bereits absehbare Entwicklungen berücksichtigt werden. Ergebnis ist letztendlich eine in SGAM eingebettete IKT-Architektur für Smart Grids in Österreich, die alle relevanten Systeme (sowohl im Ist- als auch im „smarten" Soll-Zustand) berücksichtigt.

Teil II: Bedrohungs- und Risikoanalyse

1. Zielsetzung und Vorgehensweise

Das Ziel von Bedrohung- und Risikoanalyse im Projekt (SG)[2] war es, Methoden und Richtlinien zu entwickeln bzw. anzuwenden, um Bedrohungen, Verwundbarkeiten und Risiken für Smart Grids in Österreich einheitlich darzustellen und besser zu verstehen. Besonderer Fokus lag dabei auf dem Zusammenspiel zwischen traditionellen Energiesteuerungs-Systemen der Netzbetreiber und neu aufkommenden IKT-Strukturen in Smart Grids.

Ausgangpunkt für die Bedrohungsanalyse war das in Teil I dargestellte IKT-Architekturmodell (siehe Abbildung 2), wobei hier der Fokus auf aktuellen bzw. in naher Zukunft verfügbaren Smart-Grid-Implementierungen lag. Für die Bedrohungsanalyse maßgeblich relevant waren vor allem die eingesetzten Übertragungskanäle und -technologien, deren Exponiertheit sowie die Kommunikationsverbindungen zwischen den einzelnen Komponenten im Smart Grid.

Bei der Erarbeitung relevanter Bedrohungen wurde primär auf die IT-Grundschutz-Kataloge[2] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gesetzt. Andere etablierte Quellen wie die Smart-Metering-Schutzprofile oder das Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“[3] inkl. der Ausführungshinweise von Österreichs Energie, sowie die Smart-Metering-Schutzprofile des BSI für das Smart Meter Gateway[4] und das Smart Meter Security Module[5] wurden ebenso berücksichtigt.

---

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kataloge, siehe http://www.bsi.bund.de/gshb.

[3] Bundesverband der Energie- und Wasserwirtschaft (BDEW): Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme, Version 1.0, Juni 2008.

[4] BSI: Protection Profile for the Gateway of a Smart Metering System (BSI-CC-PP-0073), 2013.

[5] BSI: Protection Profile for the Security Module of a Smart Metering System (Security Module PP, BSI-CC-PP-0077), 2013.

2. IKT-Bedrohungen im Smart Grid

2.1. Betrachtung von allgemeinen Bedrohungen im Smart-Grid-Kontext

Während die beschriebenen Bedrohungen aus den Schutzprofilen des BSI sowie aus dem Whitepaper[6] des BDEW schon Smart-Grid-spezifisch sind, so beinhalten sie im Kontext des zugrundeliegenden IKT-Architekturmodells nur eine geringe Anzahl an möglichen Bedrohungen. Eine gesamtheitliche Betrachtung kann erst durch Berücksichtigung der großen Anzahl möglicher Bedrohungen in den IT-Grundschutz-Katalogen erfolgen. Gleichermaßen handelt es sich hier jedoch um generische Bedrohungen, die noch keinen direkten Bezug zum Smart Grid haben.

Die IT-Grundschutz-Kataloge bestehen aus fünf sogenannten Gefährdungskatalogen:

G1 Höhere Gewalt
G2 Organisatorische Mängel
G3 Menschliche Fehlhandlungen
G4 Technisches Versagen
G5 Vorsätzliche Handlungen

In einem ersten Schritt wurden unter Berücksichtigung aller IT-Grundschutz-Kataloge sowie der anderen angeführten Quellen insgesamt 483 mögliche Bedrohungen gesammelt. Nachdem im Projekt jedoch der Fokus auf den technischen Bedrohungen und Risiken lag, wurden nichttechnische Bedrohungen wie z. B. höhere Gewalt nicht weiterbetrachtet.

Die verbleibenden Bedrohungen wurden nun jeweils einzeln auf ihre Relevanz im Smart-Grid-Kontext überprüft. Zu diesem Zweck wurden sämtliche gesammelte Protokolle und Übertragungstechnologien in den einzelnen

[6] Bundesverband der Energie- und Wasserwirtschaft (BDEW): Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme, Version 1.0, Juni 2008.

Domänen des (SG)²-Architekturmodells betrachtet und in Bezug auf die möglichen Ausgangsbedrohungen im Smart-Grid-Kontext geprüft. Für alle Bedrohungen wurden zudem Begründungen formuliert, weshalb diese im Kontext des Projektes relevant sind oder nicht.

So ist beispielsweise die Bedrohung „G02.147 - Fehlende Zentralisierung durch Peer-to-Peer" auch im Smart-Grid-Kontext zu beachten, da etwa die besonders im Smart-Metering-Bereich eingesetzten PLC-Netze Peer-to-Peer-ähnliche Architekturen wie etwa Mesh Networks besitzen können und dadurch ein Kontrollverlust durch mangelnde Zentralisierung entstehen kann. Andere Bedrohungen wie etwa „G04.015 – Fehlerhafte Faxübertragung" sind hingegen nicht relevant, da im (SG)²-Architekturmodell keine Faxverbindungen zwischen den einzelnen Komponenten eingesetzt werden.

Das Resultat dieses Arbeitsschritts ergab schließlich 261 Bedrohungen, die unter Beachtung des (SG)²-Architekturmodells im Smart-Grid-Kontext relevant sind.

2.2. Granularität und Konsolidierung von Bedrohungen

Die Granularität der Bedrohungen aus den IT-Grundschutz-Katalogen ist zum Teil sehr unterschiedlich. So existieren sehr detaillierte Bedrohungen wie etwa „G02.043 - Migration von Novell Netware 3.x nach Novell Netware Version 4" sowie gleichermaßen auch sehr generisch gehaltene Bedrohungen wie z. B. „G01.002 - Ausfall von IT-Systemen". Um die Bedrohungen mit Hinblick auf Smart Grids und das (SG)²-Architekturmodell auch praktisch betrachten zu können, ist die Granularität jedoch ausschlaggebend. Sie stellt einen Kompromiss zwischen der praktischen Anwendbarkeit und der Feinheit der Betrachtung dar. Sind die Bedrohungen zu fein definiert (etwa wie am Beispiel der Bedrohung G02.043" oben), so ist die praktische Anwendbarkeit auf einzelne Smart-Grid-Komponenten oder Domänen im (SG)²-Architekturmodell nicht mehr gegeben. Gleichermaßen dürfen die Bedrohungen jedoch ebenso wenig zu generisch sein, da durch den damit einhergehenden Informationsverlust möglichweise wichtige Bedrohungen nicht länger berücksichtigt werden könnten.

Im (SG)²-Projekt wurde mit Hinblick auf die Granularität des erstellten

Architekturmodells und der praktischen Anwendbarkeit (etwa durch Netzbetreiber) über eine Konsolidierungsphase ein sorgsamer Kompromiss zwischen der Anwendbarkeit und der Feinheit der Betrachtungsweise von Bedrohungen getroffen. Die 261 Bedrohungen, welche innerhalb des im (SG)²-Architekturmodell modellierten Smart Grid relevant sind, wurden zuerst in die folgenden sechs Kategorien aufgeteilt:

1. Mangelnde Authentifizierung / Autorisierung
2. Mangelnde Kryptografie / Vertraulichkeit
3. Mangelnde Integrität / Verfügbarkeit
4. Fehlende / falsche Sicherheitsmechanismen
5. Sicherheitsprobleme bei internen und externen Schnittstellen
6. Mangelnde Wartung / Instandhaltung

Anschließend wurde die Granularität vereinheitlicht sowie auf die Anwendung im (SG)²-Risikokatalog angepasst. So lassen sich etwa die Grundschutz-Bedrohungen

- G01.010 Ausfall eines Weitverkehrsnetzes
- G01.017 Ausfall oder Störung eines Funknetzes
- G04.004 Leitungsbeeinträchtigung durch Umfeldfaktoren
- G04.004 Übersprechen
- G04.031 Ausfall oder Störung von Netzkomponenten
- G04.031 Nicht-Verfügbarkeit des Mobilfunknetzes
- G04.075 Störung der Netzinfrastruktur von Virtualisierungsumgebungen

in die kumulierte Bedrohung „Ausfall oder Störung von Netzwerken oder Netzwerkkomponenten“ zusammenfassen und der Kategorie „Mangelnde Integrität / Verfügbarkeit“ zuordnen.

2.3. Bedrohungskatalog

Die Anpassung der Granularität und die Konsolidierungsphase ergab schließlich eine praktisch anwendbare Liste von 31 Smart-Grid-spezifischen Bedrohungen und damit den (SG)²-Bedrohungskatalog. Im Folgenden sind die Bedrohungen aus den einzelnen Kategorien zusammengefasst.

Kategorie „Mangelnde Authentifizierung / Autorisierung“

- Fehlerhafte oder fehlende Authentifizierung oder ungeeigneter Umgang mit Authentifizierungsdaten
- Fehlerhafte Autorisierung

Kategorie „Mangelnde Kryptografie / Vertraulichkeit“

- Vertraulichkeitsverlust schutzbedürftiger Daten
- Unzureichendes Schlüsselmanagement
- Einsatz unsicherer Verschlüsselungsverfahren bzw. unsicherer Verschlüsselungsparameter

Kategorie „Mangelnde Integrität / Verfügbarkeit“

- Ausfall oder Störung von IT-Systemen
- Ausfall oder Störung von Netzwerken oder Netzwerkkomponenten
- Ausfall oder Störung von Versorgungsnetzen
- Datenverlust oder -verfälschung durch physische (Umfeld-) Faktoren
- Datenverlust oder -verfälschung durch Fehlbedienung oder Fahrlässigkeit
- Mutwillige Manipulation von Geräten
- Mutwillige Manipulation von Daten
- Gebührenbetrug

Kategorie „Fehlende / falsche Sicherheitsmechanismen“

- Verwendung unsicherer Protokolle
- Fehlende oder unzureichende Sicherheitsmechanismen von Software-Produkten
- Fehlende oder unzureichende Sicherheitsmechanismen in Netzwerken
- Ausfall oder Störung vorhandener Sicherungseinrichtungen (Safety-Maßnahmen)
- Software-Schwachstellen oder -Fehler

Kategorie „Sicherheitsprobleme bei internen und externen Schnittstellen“

- Unzulässige logische Schnittstellen
- Unzulässige physische Schnittstellen
- Inkompatibilität von Systemen und Netzwerkkomponenten

Kategorie „Mangelnde Wartung / Instandhaltung“

- Fehlende oder unzureichende Wartung
- Mangelnde Anomalieerkennung
- Mangelnde Monitoring- und Eingriffsmöglichkeit
- Falsche Dimensionierung
- Sicherheitsprobleme bei Software-Migration
- Betreiben von nicht angemeldeten, unsicheren Komponenten oder Komponenten mit unnötig breitem Funktionsumfang
- Fehlerhafte Nutzung bzw. Administration von IT-Systemen
- Fehlerhafte Zeitsynchronisation
- Fehler bei der Synchronisation von Datenbeständen
- Unkontrollierte Kaskadeneffekte

2.4. Bedrohungsmatrix

Auf Basis des Bedrohungskatalogs (siehe Abschnitt 2.3) wurden nun sämtliche Komponenten-Cluster im (SG)²-Architekturmodell (siehe Abbildung 3) auf ihre Gefährdungen durch die im Katalog definierten Bedrohungen hin analysiert. Davon ausgenommen war der Energiemarkt, da es zum Zeitpunkt der Analyse noch keine speziellen IT-Technologien oder -Systeme in diesem Bereich eingesetzt wurden (Abwicklung des Energiehandels weitestgehend über Telefonanrufe zwischen dafür Verantwortlichen). Ergebnis war eine Matrix aus den zehn verbleibenden Smart-Grid-Domänen und den 31 Smart-Grid-Bedrohungen lt. Bedrohungskatalog. Sie definiert, welche Einzelbedrohungen für die einzelnen Domänen betrachtet werden müssen und dient als Ausgangspunkt für den (SG)²-Risikokatalog. Die detaillierten Ergebnisse und Inhalte der Bedrohungsmatrix sind vertraulich und daher nicht Teil dieser Publikation.

2.5. Abstimmung mit Herstellern und Netzbetreibern in den Entwicklungsphasen

Im Zuge mehrerer Workshops mit Geräteherstellern und Netzbetreibern wurden diese in die Erstellung des (SG)²-Bedrohungskatalogs sowie der Bedrohungsmatrix mit eingebunden. Durch diesen Schritt wurde sichergestellt, dass bestehende Erfahrungen berücksichtigt und die Bedrohungsmatrix möglichst realitätsnah werden.

Während der Entwicklung des (SG)²-Bedrohungskatalogs wurde dieser jeweils vor den Workshops an Gerätehersteller und Netzbetreiber ausgesendet. Auf diese Weise konnten Kommentare hinzugefügt und später berücksichtigt werden. Zudem konnten jeweils individuell Bedrohungen, Begründungen oder technische Annahmen auf Relevanz beurteilt werden. Die Ergebnisse dieser Feedback-Runden wurden anschließend in den Workshops gemeinsam diskutiert und im Bedrohungskatalog berücksichtigt.

Zusätzlich zu den Feedback-Runden und den Workshops wurde ein Detailfragenkatalog für die jeweiligen Smart-Grid-Domänen aus dem (SG)²-Architekturmodell ausgearbeitet und an Hersteller sowie an Netzbetreiber geleitet. Auf diese Weise konnten bei Bedarf notwendige Zusatzinformationen zu Übertragungstechniken, Protokollen, Systemen oder Systemauswirkungen in Erfahrung gebracht werden, ohne die die Betrachtung von allgemeinen Bedrohungen im Smart-Grid-Kontext sowie die anschließende Konsolidierungsphase nicht realistisch umsetzbar gewesen wären. Die gewonnenen Erkenntnisse wurden ebenso in den abgehaltenen Workshops gemeinsam mit Gerätehersteller, Netzbetreiber und den Konsortialpartnern diskutiert und jeweilige Änderungen im Bedrohungskatalog berücksichtigt.

3. Risikomatrix

3.1. Bewertung

Auf Basis der Bedrohungsmatrix (d.h. der Anwendung der Bedrohungen auf das (SG)²-Architekturmodell, siehe Abschnitt 2.4) fand anschließend eine Risikobewertung statt. Dazu wurden sämtliche Bedrohungen innerhalb der jeweiligen Smart-Grid-Cluster bzgl. ihrer Eintrittswahrscheinlichkeit und möglicher Auswirkungen bewertet. Verwendet wurde jeweils eine Skala von 1 bis 5. Durch Multiplikation der beiden Werte ergab sich das jeweilige Risikopotential. Bei der Vorgehensweise wurde unter Berücksichtigung der praktischen Anwendbarkeit der Ergebnisse die bestehende Systematik eines der Netzbetreiber im Konsortium angewandt. Die Definitionen der Skala für die Eintrittswahrscheinlichkeit bzw. die Auswirkungen finden sich in Tabelle 12 bzw. Tabelle 13.

Tabelle 12: Skala für die Bewertung der Eintrittswahrscheinlichkeit

5	Sehr hoch; Auftreten des Ereignisses häufiger als 1 Mal pro Jahr
4	Hoch; Auftreten des Ereignisses 0.5-1 Mal pro Jahr (d.h. alle 1-2 Jahre)
3	Mittel; Auftreten des Ereignisses 0.2-0.5 Mal pro Jahr (d.h. alle 2-5 Jahre)
2	Gering; Auftreten des Ereignisses 0.1-0.2 Mal pro Jahr (d.h. alle 5-10 Jahre)
1	Vernachlässigbar; Auftreten des Ereignisses seltener als 0.1 Mal pro Jahr (d.h. seltener als alle 10 Jahre)

Tabelle 13: Skala für die Bewertung der Auswirkungen

5	Massive Auswirkungen auf die Organisation (Verlust > 1 EGT[7] p.a.), die eine mit der Geschäftsführung und den Eigentümern abgestimmte Reaktion erfordern
4	Große Auswirkungen auf die Organisation (Verlust ca. 1 EGT p.a.), die eine mit der Geschäftsführung abgestimmte Reaktion erfordern; werden in der überregionalen Öffentlichkeit bemerkt oder haben kritische Auswirkungen auf die Geschäftskontinuität
3	Moderate Auswirkungen auf die Organisation (Verlust ca. 0.5 EGT p.a.), die von der Bereichsleitung definierte Reaktion erfordern; werden in der regionalen Öffentlichkeit bemerkt, haben regionale politische Auswirkungen oder Auswirkung auf die Zahl der Aufträge
2	Geringe Auswirkungen auf die Organisation (Verlust ca. 0.2 EGT p.a.), die keine Reaktion erfordern; werden in der Öffentlichkeit kaum bemerkt, haben nur lokale Auswirkungen und nur moderate

[7] Ergebnis der gewöhnlichen Geschäftstätigkeit

	Auswirkung auf die Aufträge
1	Nicht relevante Auswirkungen auf die Organisation, Behebung im Rahmen des täglichen Betriebs, geringe Auswirkungen auf die Aufträge

Mittels der vorgestellten Systematik konnte nun das Risikopotential innerhalb des IKT-Architekturmodells unter Berücksichtigung aktuell verwendeter oder in naher Zukunft verwendeter Smart-Grid-Technologien berechnet werden. Ergebnis war die $(SG)^2$- Risikomatrix, welche je Bedrohung und Architektur-Cluster das Risiko eines erfolgreichen Angriffs darstellt. Die Risikomatrix wurde in mehrmaligen Feedbackrunden und Workshops konsolidiert. Sie ist aufgrund der Kritikalität der enthaltenen Informationen nicht Teil dieser Publikation.

3.2. Visualisierung

Zur Visualisierung wurde das Risikopotential in die Stufen niedrig (grün), mittel (gelb) und hoch (rot) wie folgt unterteilt:

Tabelle 14: Einstufung Risikopotential

Kriterium Risikopotential (RP)	**Bewertung**
1 <= RP < 5	Niedriges Risiko
5 <= RP < 12	Mittleres Risiko
12 <= RP <= 25	Hohes Risiko

Dadurch kann man auf den ersten Blick erfassen, wo innerhalb der Risikomatrix welches Risiko gegeben ist. Bereiche, die ein besonders hohes Risiko aufweisen, können so rasch identifiziert werden. Insgesamt gab es 159 Zellen (d.h. Einträge in der Risikomatrix, definiert durch Bedrohung und Architektur-Cluster) mit niedrigem Risikopotential, 123 mit mittlerem und sieben mit hohem Risikopotential.

3.3. Auswertung

Tendenziell lässt sich sagen, dass die Eintrittswahrscheinlichkeit eines erfolgreichen Angriffs in den oberen Zonen des IKT-Architekturmodells (SGAM-Zonen „Operation“ und „Enterprise“, vgl. Abbildung 1) verhältnismäßig gering ist, da es hier nur relativ wenige Komponenten gibt, die aufgrund ihrer Kritikalität gut abgesichert sind und über entsprechende Redundanzen verfügen. In der Regel hat der Angreifer hier auch keinen physischen Zugang. Wenn er sich jedoch erfolgreich Zugriff auf die kritischen Systeme verschafft, sind die Auswirkungen umso stärker (z. B. Stromausfall in ganzen Stadtteilen bei Ausfall eines Umspannwerkes).

In den unteren Zonen des IKT-Architekturmodells (SGAM-Zonen „Process“ und „Field“, vgl. Abbildung 1) verhält es sich genau umgekehrt: Hier können sich Angreifer leicht Zugang verschaffen, da die Geräte zum Teil in Kundenhaushalten verbaut sind (z. B. Smart Meter) und damit außerhalb des unmittelbaren Einflussbereiches des Netzbetreibers liegen. Die Auswirkungen sind hier auf den ersten Blick relativ gering und nur auf einen kleinen Bereich beschränkt (z. B. Manipulation einzelner Smart Meter); dies kann sich jedoch dramatisch ändern, sobald Angriffsmuster beispielsweise über das Internet veröffentlicht und damit der breiten Masse bekannt werden. Daher können auch die Sicherheitsvorkehrungen in den unteren Zonen nicht vernachlässigt werden. Ein zusätzlicher ungünstiger Faktor ist hier der herrschende Kostendruck und die politische Forderung nach einer raschen, breit angelegten Ausrollung von Smart Metern; beides begünstigt tendenziell einen Einsatz unausgereifter Smart Meter mit unentdeckten Sicherheitslücken.

4. Fazit

Die (SG)²-Risikomatrix hat den Anspruch, Netzbetreibern einen Überblick über die gängigen IKT-bedingten Risiken im Stromnetz zu geben und Anhaltspunkte für Bereiche mit hohem Risikopotential zu geben. Die Risikomatrix ersetzt jedoch keine klassische Risiko*analyse*: Im Gegensatz zur Methodologie bei der Erstellung der (SG)²-Risikomatrix muss bei einer individuellen Risikoanalyse stets eine sehr genaue Betrachtung der individuellen Implementierung erfolgen, d.h. die Granularität der Analyse muss entspre-

chend höher sein. Das Ergebnis der individuellen Risikoanalyse entspricht somit der individuellen Implementierung sowie Konfiguration und ist daher nicht aussagekräftig für andere Implementierungen oder Konfigurationen.

Für die $(SG)^2$-Risikomatrix wurde dagegen eine niedrigere Granularität gewählt, damit eine Aussagekraft für das gesamte, durch das IKT-Architekturmodell definierte Smart Grid ermöglich wird, mit einem Fokus auf aktuelle und in naher Zukunft eingesetzte Technologien. Gleichzeitig hilft die Risikomatrix jedoch auch bei einer individuellen Risikoanalyse im Rahmen einer Voreinschätzung der allgemeinen Risiken, und kann somit als Basis für ebendiese dienen.

Teil III: Rechtliche und gesellschaftliche Aspekte

1. Einleitung

Dieser Teil der Arbeiten umfasste die begleitende Untersuchung rechtlicher und sozio-ökonomischer Gesichtspunkte. Dazu wurden ausgewählte Bedrohungsszenarien im Smart Grid strafrechtlich untersucht, wie beispielsweise die Szenarien Stromdiebstahl, Abrechnungsbetrug, Hacken eines Smart Meters, sowie Ausspähen oder Manipulation von Metering-Daten (siehe Abschnitt 2). Parallel dazu wurden gesellschaftliche Aspekte von IKT-Sicherheit und Datenschutz in intelligenten Stromnetzen untersucht und mit Resultaten aus anderen Projekten abgeglichen, und es erfolgte eine Analyse der gesellschaftlichen Auswirkungen der in Teil V vorgeschlagenen Sicherheitsmaßnahmen (siehe Abschnitt 3).

In zahlreichen Unionsrichtlinien wird die Installation von intelligenten Messgeräten (sog. Smart Meter) unter gewissen Voraussetzungen gefordert.[8] Unter einem „intelligenten Verbrauchserfassungssystem" versteht die EnEff-RL 2012 ein elektronisches System zur Messung des Energieverbrauchs, wobei mehr Informationen angezeigt werden als bei einem herkömmlichen Zähler[9] und Daten auf einem elektronischen Kommunikationsweg übertragen und empfangen werden können.[10] Das ElWOG 2010[11] definiert das "intelligente Messgerät" als technische Einrichtung, die den tatsächlichen Energieverbrauch und Nutzungszeitraum zeitnah misst und

---

8 z.B. in der Richtlinie 2012/27/EU des Europäischen Parlaments und des Rates vom 25.10.2012 zur Energieeffizienz, zur Änderung der Richtlinien 2009/125/EG und 2010/30/EU und zur Aufhebung der Richtlinien 2004/8/EG und 2006/32/EG, Abl. L 315/2012, 1 (EnEff-RL 2012) und in der Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates vom 13.07.2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG, Abl. L 211/2009, 55 (EltRL 2009).

9 Zähler in der Standardeinstellung zeigt nur den aktuellen Zählerstand. Es können aber auf Wunsch des Kunden Anzeigebereiche freigeschaltet werden.

10 Art. 2 Z 28 EnEff-RL 2012.

11 Bundesgesetz, mit dem die Organisation auf dem Gebiet der Elektrizitätswirtschaft neu geregelt wird (Elektrizitätswirtschafts- und -organisationsgesetz 2010 – ElWOG 2010), BGBl. I 2013/174.

über eine fernauslesbare, bidirektionale Datenübertragung verfügt.[12] Diese neuen Stromzähler haben den Sinn, den tatsächlichen Energieverbrauch sowie die damit verbundenen Kosten des Endkunden[13] genau widerzuspiegeln.[14] Mittels einer solchen direkten Rückmeldung über die Auswirkungen von Investitionen in die Energieeffizienz und von Änderungen hinsichtlich des Stromverbrauchs sollen weitere Anreize für Netzbenutzer zu Energieeinsparungen geschaffen werden.

Da die im Rahmen der EltRL 2009[15] vorgesehene Durchführung der Kosten-Nutzen-Analyse hinsichtlich der Einführung von intelligenten Messgeräten in Österreich positiv ausgefallen ist, hat sich der österreichische Verordnungsgeber auf der Ermächtigungsgrundlage des § 83 Abs. 1 ElWOG 2010 dafür entschieden, dass jeder Netzbetreiber im Rahmen der technischen Machbarkeit bis Ende 2019 sukzessive grds. min. 95 % seiner angeschlossenen Zählpunkte mit intelligenten Messgeräten auszustatten hat (§ 1 Abs. 1 Z 3 IME-VO[16]). Damit ist Österreich über die unionsrechtlichen Vorgaben hinausgegangen, die eine Ausstattung von min. 80 % der Verbraucher bis 2020 vorsehen.[17]

2. Strafrechtliche Untersuchung ausgewählter Bedrohungsszenarien im intelligenten Stromnetz

Mit der breitflächigen Einführung von Smart Metern wächst jedoch die Gefahr verschiedener Angriffsmöglichkeiten auf die gesamte Elektrizitätsinfrastruktur, im speziellen aber auch auf die Smart Meter, also die intelligenten Stromzähler, selber. Daher sollen in diesem Kapitel einige Szenarien dahingehend untersucht werden, ob diese bereits durch das sog. Computer-

12 § 7 Abs. 1 Z 31 ElWOG 2010.

13 Aus Gründen der besseren Lesbarkeit werden personenbezogene Bezeichnungen im folgenden Gutachten überwiegend in männlicher Form angeführt. Sie beziehen sich jedoch auf Frauen und Männer in gleicher Weise.

14 Derzeit werden Viertelstundenwerte einmal am Tag übertragen.

15 Anhang I Abs. 2 EltRL 2009.

16 Verordnung des Bundesministers für Wirtschaft, Familie und Jugend, mit der die Einführung intelligenter Messgeräte festgelegt wird (Intelligente Messgeräte-Einführungsverordnung-IME-VO), BGBl. II 2014/323.

17 Anhang I Abs. 2 EltRL 2009.

strafrecht erfasst sind oder ob in diesem Bereich noch Strafbarkeitslücken bestehen, die mittels Gesetzesänderungen bzw. -ergänzungen geschlossen werden sollten.[18] Bei der Untersuchung werden die Rechtswidrigkeit und Schuld des Täters vorausgesetzt und daher nicht geprüft.

2.1. Vorab: Übereinkommen des Europarates über Computerkriminalität vom 23.11.2001

In dem Übereinkommen über Computerkriminalität[19], das auch Cybercrime Convention" (CCC) genannt wird, werden sowohl materielle Straftatbestände (z. B. das „Hacking"), als auch strafprozessuale Vorgaben rund um das Computerstrafrecht zusammengetragen, die durch die unterzeichnenden Staaten in nationales Recht umzusetzen sind. Wie die Umsetzung im österreichischen Strafrecht erfolgt ist, wird im Rahmen der folgenden Untersuchung dargestellt.

2.2. Vorab: Rahmenbeschluss 2005/222/JI des Rates über Angriffe auf Informationssysteme

Ziel dieses Rahmenbeschlusses über Angriffe auf Informationssysteme[20] war es, die Strafvorschriften der einzelnen Mitgliedsstaaten im Rahmen der Angriffe auf Informationssysteme anzugleichen sowie die Zusammenarbeit der zuständigen Behörden in diesem Bereich zu verbessern. Auf die Darstellung dieses Beschlusses wird jedoch an dieser Stelle verzichtet, da die Umsetzung im österreichischen Strafrecht schon aufgrund der CCC weitgehend erfolgt ist und zudem der Rahmenbeschluss mittlerweile durch die Richtlinie über Angriffe auf Informationssysteme[21] ersetzt worden ist, die am Ende der strafrechtlichen Untersuchung zusammengefasst wird.

---

18 Die Ausarbeitung der strafrechtlichen Untersuchung im Rahmen des Projektes (SG)² wurde im Frühjahr 2015 abgeschlossen. Daher konnte das Strafrechtsänderungsgesetz 2015 auch in der vorliegenden Veröffentlichung nicht berücksichtigt werden.

19 SEV-Nr. 185.

20 Rahmenbeschluss 2005/222/JI des Rates vom 24.02.2005 über Angriffe auf Informationssysteme, Abl. L 69/2005, 67.

21 Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12.08.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl. L 218/2013, 8.

2.3. Szenario 1: Stromdiebstahl

Zu untersuchen ist zunächst, ob der Diebstahl von Elektrizität strafbar ist, wenn der Täter z. B. eine Freileitung bzw. die Leitung eines Nachbarn widerrechtlich nutzt, um auf diesem Wege an Elektrizität zu gelangen.

2.3.1. Diebstahl gem. § 127 StGB

Möglicherweise macht sich der Täter durch die Entwendung der Elektrizität eines Diebstahls nach § 127 StGB[22] strafbar. Dies setzt voraus, dass er eine fremde bewegliche Sache einem anderen mit dem Vorsatz wegnimmt, sich oder einen Dritten durch deren Zueignung unrechtmäßig zu bereichern. Problematisch ist allerdings, ob es sich beim Strom um eine Sache handelt. Unter einer Sache versteht man körperliche Gegenstände, an denen Eigentum erworben werden kann, unabhängig von ihrem wirtschaftlichen Wert und ihrem Aggregatzustand.[23] Zwar ist der Aggregatzustand gleichgültig, sodass auch Gase, Flüssigkeiten und Dämpfe erfasst werden, nicht jedoch Elektrizität (es sei denn, die Elektrizität ist z. B. in einer Batterie gespeichert).[24] Dies liegt daran, dass Elektrizität mangels fassbarer Abgrenzbarkeit keinen körperlichen Gegenstand und damit keine Sache darstellt. Folglich scheidet eine Strafbarkeit des Täters wegen Diebstahls der Elektrizität nach § 127 StGB aus.

2.3.2. Entziehung von Energie gem. § 132 StGB

Allerdings kommt eine Strafbarkeit wegen Entziehung von Energie, also der sog. „Stromdiebstahl", nach § 132 Abs. 1 StGB in Betracht. Den Tatbestand erfüllt, wer vorsätzlich aus einer Anlage, die der Gewinnung, Umformung, Zuführung oder Speicherung von Energie dient, Energie entzieht, um sich oder einen Dritten unrechtmäßig zu bereichern.

Unter Energie wird in diesem Sinne auf jeden Fall elektrische Energie ver-

---

22 Bundesgesetz vom 23.01.1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB), BGBl. I 2014/106.

23 *Wegscheider*, Strafrecht BT, S. 185; *Wessels/Hillenkamp*, Strafrecht BT II, S. 35.

24 Vgl. RGSt 29, 111; 32, 165; *Joecks*, Studienkommentar, vor § 242 Rz. 8 f.; WK-StGB, *Bertel*,
§ 132 Rz. 1.

standen. Der Straftatbestand wurde geschaffen, um Strafbarkeitslücken zu schließen, da – wie bereits in Abschnitt 2.3.1 ausgeführt – Strom im Gegensatz zu Gas und Warmwasser keinen körperlichen Gegenstand und damit keine Sache darstellt, sodass der Straftatbestand des Diebstahls nach § 127 StGB nicht einschlägig ist.

Die Anlage, der die elektrische Energie entzogen wird, muss deren Gewinnung, Umformung, Zuführung oder Speicherung dienen. Darunter fallen somit z. B. Kraftwerke, Generatoren, Akkumulatoren, Transformatoren, Batterien sowie das gesamte Stromnetz, nicht jedoch Telefon- und Kabelfernsehleitungen.[25] Freileitungen des Netzbetreibers bzw. die Hausleitungen des Nachbarn unterfallen zweifelsohne dem Anlagenbegriff des § 132 StGB, da sie Strom zuführen.

Als Tathandlung muss der Täter die elektrische Energie dieser Anlage entziehen. Unter Entziehung versteht man jeglichen Energieverbrauch ohne Zustimmung des Berechtigten.[26] Das bedeutet, dass der Energieverlust des Berechtigten zum Zufluss beim Täter führen muss. Mögliche Tathandlungen sind somit der unberechtigte Anschluss eines eigenen stromverbrauchenden Gerätes an eine fremde Leitung[27], die Verbindung eines gesperrten Stromanschlusses mit einem nicht gesperrten Stromkreis des Täters[28] sowie die Umgehung bzw. Überbrückung des Stromzählers.[29] Nicht tatbestandsmäßig i.S.v. § 132 StGB ist hingegen die Manipulation von Stromzählern mit Magneten oder auf andere Weise, sodass die Zähler nicht mehr ordnungsgemäß funktionieren. Indem der Täter z. B. Freileitungen bzw. Leitungen des Nachbarn „anzapft", entzieht er diesen Anlagen elektrische Energie.

Wenn somit der Täter einem anderen, also dem Erzeuger, Versorgungs-

---

25 OGH 05.12.1985, 12 Os 156/85; *Fischer*, StGB-Kommentar, § 248c Rz. 2; Salzburger Kommentar, *Triffterer/Rosbaud/Hinterhofer*, § 132 Rz.14; WK-StGB, *Bertel*, § 132 Rz. 1; *Bertel/Schwaighofer*, Strafrecht BT I, § 132 Rz. 1.

26 *Wegscheider*, Strafrecht BT, S. 198. Dazu auch Salzburger Kommentar, *Triffterer/Rosbaud/Hinterhofer*, § 132 Rz. 11 f.

27 WK-StGB, *Bertel*, § 132 Rz. 2.

28 OLG Celle 13.02.1969, 1 Ss 488/68, MDR 1969, 597.

29 RGSt 42, 19, 21; OLG Hamburg 13.12.1967, 1 Ss 141/67, MDR 1968, 257; OLG Celle 13.02.1969, 1 Ss 488/68, MDR 1969, 597; WK-StGB, *Bertel*, § 132 Rz. 2.

unternehmen oder berechtigten Bezieher die Energie entzieht, ohne selber ein Recht zur Entnahme zu haben, hat er den objektiven Tatbestand des § 132 Abs. 1 StGB erfüllt.

Allerdings muss der Täter zudem noch den subjektiven Tatbestand erfüllen. Das bedeutet im Rahmen von § 132 Abs. 1 StGB, dass er bei der Tathandlung nicht nur den Vorsatz hinsichtlich der Verwirklichung der objektiven Tatbestandsmerkmale haben, sondern darüber hinaus auch den Vorsatz haben muss, sich oder einen Dritten damit unrechtmäßig zu bereichern. Das beinhaltet, dass der Täter sein Vermögen bzw. das eines Dritten mittels der entzogenen Energie vermehren und somit die Kosten die Strombeziehung ersparen möchte[30], was im vorliegenden Szenario des „Anzapfens" fremder Leitungen i.d.R. der Fall ist.

Folglich macht sich der Täter durch das unberechtigte Nutzen einer Leitung (z. B. einer Freileitung bzw. der Hausleitung des Nachbarn) wegen Entziehung von Energie nach § 132 Abs. 1 StGB strafbar.

Die Qualifikation des § 132 Abs. 2 StGB erfüllt der Täter darüber hinaus dann, wenn er vorsätzlich Energie entzieht, deren Wert 3.000 € bzw. 50.000 € überschreitet.[31]

Werden nicht sämtliche Tatbestandsvoraussetzungen von § 132 Abs. 1 und evtl. von § 132 Abs. 2 StGB durch den Täter verwirklicht, so macht er sich der versuchten Entziehung elektrischer Energie nach §§ 132 Abs. 1, 15 StGB (evtl. in Verbindung mit § 132 Abs. 2 StGB) strafbar.

2.3.3. Ergebnis zu Szenario 1, dem Stromdiebstahl

Während ein klassischer Diebstahl der Elektrizität nach § 127 StGB aufgrund der fehlenden Sachqualität ausscheidet, wenn der Täter z. B. eine Freileitung bzw. die Leitung eines Nachbarn widerrechtlich nutzt, ist jedoch eine Strafbarkeit des Täters wegen Entziehung von Energie nach § 132 Abs.1 StGB (evtl. in Verbindung mit § 132 Abs. 2 StGB) einschlägig. Bei fehlender Verwirklichung sämtlicher objektiver Tatbestandsvorausset-

30 Salzburger Kommentar, *Triffterer/Rosbaud/Hinterhofer*, § 132 Rz. 23 f.

31 Diesen Grenzwert wird jedoch ein Privathaushalt nicht erreichen.

zungen kann das Verhalten als versuchte Entziehung von Energie strafbar sein.

2.4. Szenario 2: Abrechnungsbetrug

Im Rahmen des zweiten Szenarios ist zu untersuchen, ob sich der Täter strafbar macht, der manipulativ – insbesondere durch das Anbringen eines sog. „Supermagneten" am Stromzähler oder durch die Installation eines Computerprogrammes – auf die Funktionsweise seines ihm zugeordneten eigenen[32] Stromzählers einwirkt, was zu einer vom Täter bezweckten geringeren Stromrechnung[33] durch den Netzbetreiber bzw. den Stromlieferanten[34] führt.[35]

2.4.1. Urkundenfälschung gem. § 223 StGB

Fraglich ist zunächst, ob sich der Täter, der zum Zwecke einer niedrigeren Stromrechnung seinen Stromzähler manipuliert, einer Urkundenfälschung nach § 223 Abs. 1 2. Var. StGB strafbar macht. Dazu müsste er eine echte Urkunde mit dem Vorsatz verfälschen, sie im Rechtsverkehr zum Beweis eines Rechts oder einer Tatsache zu gebrauchen.

Das setzt zunächst voraus, dass die Anzeige des Stromzählers eine Urkunde darstellt. Unter einer Urkunde versteht man eine schriftlich fixierte Gedankenerklärung (Perpetuierungsfunktion), die den Aussteller erkennen

---

32 Der Stromzähler steht allerdings im Eigentum des jeweiligen Netzbetreibers, während der Kunde für dessen Nutzung ein Entgelt für Messleistungen im Rahmen der Systemnutzungsentgelte zu entrichten hat.

33 Unter einer Stromrechnung ist sowohl die Abrechnung der Netznutzung als auch die der reinen Energie (sowie Steuern und Abgaben) zu verstehen.

34 Möglich ist zum einen, dass der Kunde eine Rechnung vom Netzbetreiber hinsichtlich der Systemnutzungsentgelte und eine Rechnung vom Stromlieferanten über den reinen Energiepreis erhält und zum anderen ist möglich, dass der Kunde sich für das sog. Vorleistungsmodell, also eine integrierte Rechnungslegung, entscheidet, sodass ihm nicht nur der reine Energiepreis, sondern auch das Systemnutzungsentgelt durch den Stromlieferanten in einem in Rechnung gestellt werden (in diesem Fall begleicht der Stromlieferant sodann das Systemnutzungsentgelt an den Netzbetreiber).

35 Das bedeutet, der Stromzähler misst weniger, als der Täter tatsächlich an Strom bezieht.

lässt (Garantiefunktion) und geeignet und bestimmt ist, im Rechtsverkehr Beweis zu erbringen (Beweisfunktion).[36] Das bedeutet, dass in der Urkunde als Schriftstück der Gedankeninhalt des Ausstellers dauerhaft verkörpert sein muss. Bei der Darstellung der Stromverbrauchswerte im Strommessgerät handelt es sich jedoch weder um ein Schriftstück (auch sind die Verbrauchswerte nicht in einem selbstständig verkörperten, vom Gerät abtrennbaren Stück enthalten) noch um eine menschliche Gedankenerklärung des Ausstellers. Eine solche setzt nämlich voraus, dass die betroffene Person frei über den Inhalt ihrer Erklärung entscheiden kann und somit die Aussageherrschaft hat.[37] Dies ist aber beim Stromzähler gerade nicht der Fall, selbst wenn die betroffene Person weiß, dass sie durch ihr Verhalten den Stromzähler in Gang setzt. Allerdings kann sie nicht beeinflussen, was genau aufgezeichnet wird; sie kann also nicht erwirken, dass der Zähler ein anderes Stromverhalten misst, als sie verbrauchsmäßig an den Tag legt, sodass ihr die Aufzeichnung nicht als eigene Erklärung zugerechnet werden kann. Es steht jedoch der Aussageherrschaft der erklärenden Person nicht entgegen, wenn sie sich bei der Erstellung ihrer Erklärung z. B. eines Computers bedient, solange sie durch die Eingabe der Zeichen ihre Erklärung frei bestimmen kann.[38] Zudem fehlt es vorliegend an einer dauerhaften verkörperten Darstellung dieser technischen Anzeige, da der aktuelle Stromverbrauchswert fortlaufend überschrieben wird. Damit ist die Darstellung der Verbrauchswerte auf dem Stromzähler (egal, ob Smart Meter oder Ferraris-Zähler) bereits mangels schriftlich fixierter menschlicher Gedankenerklärung keine Urkunde.

Selbst wenn der Stromzähler mittels einer Plombe verschlossen ist, die der Täter zunächst verletzen muss, so enthält auch diese keine über die Sicherung hinausgehende Gedankenerklärung und stellt somit keine Urkunde, sondern nur ein qualifiziertes Augenscheinobjekt dar, das anzeigen soll, ob

---

36 *Fischer*, StGB Kommentar, § 267 Rz. 2 m.w.N.; WK-StGB, *Kienapfel/Schroll*, § 223 Rz. 7 ff. m.w.N.; *Wegscheider*, Strafrecht BT, S. 362.

37 Ausführlich dazu: NK-StGB, *Puppe*, § 267 Rz. 29.

38 NK-StGB, *Puppe*, § 267 Rz. 29; Schönke/Schröder, StGB, *Heine/Schuster*, § 267 Rz. 4.

der Stromzählerkasten geöffnet wurde oder eben nicht.[39]

Durch die Manipulation seines Stromzählers zum Zwecke einer niedrigeren Stromrechnung macht sich der Täter somit nicht wegen einer Urkundenfälschung nach § 223 Abs. 1 2. Var. StGB strafbar.

2.4.2. Schwerer Betrug gem. §§ 146, 147 StGB (beim klassischen Stromzähler)

In Betracht kommt jedoch eine Strafbarkeit des Täters wegen schweren Betrugs nach §§ 146, 147 Abs. 1 und Abs. 2 StGB gegenüber einem Mitarbeiter des Netzbetreibers und zu Lasten des Netzbetreibers bzw. des Stromlieferanten durch die Manipulation des Stromzählers zum Zwecke einer niedrigeren Stromrechnung.

2.4.2.1. Grundtatbestand des § 146 StGB

Beim Betrug handelt es sich um ein sog. „Selbstschädigungsdelikt", bei dem der Täter vorsätzlich durch Täuschung über Tatsachen auf die Vorstellung einer anderen natürlichen Person derart einwirkt, dass bei dieser ein Irrtum entsteht, wodurch sie zu einer Vermögensverfügung, also zu einer Handlung, Duldung oder Unterlassung, veranlasst wird, die sich wiederum bei ihr selber oder einem Dritten vermögensmindernd auswirkt. Dabei ist es der Wille des Täters, sich oder einen Dritten durch diese Verfügung der getäuschten Person rechtswidrig zu bereichern.

Die Tathandlung des Grunddelikts von § 146 StGB stellt die Täuschung über Tatsachen dar. Tatsachen sind sämtliche Umstände, die objektiv bestimmbar und dem Beweis zugänglich sind, unabhängig davon, ob sie in der Gegenwart oder in der Vergangenheit liegen.[40] Unter einer Täuschung versteht man jede intellektuelle Einwirkung auf das Vorstellungsbild eines

---

39 So auch RGSt 64, 48, 49; *Fischer*, StGB Kommentar, § 267 Rz. 6 m.w.N.; Schönke/Schröder, StGB, *Heine/Schuster*, § 267 Rz. 26a. A.A. für elektrische Zähler, RGSt 50, 191; *Rengier*, Strafrecht BT II, S. 282 Rz. 14, sofern der verplombte Zähler für den angezeigten Verbrauch maßgeblich sein soll.

40 NK-StGB, *Kindhäuser*, § 263 Rz. 73 m.w.N.; WK-StGB, *Kirchbacher*, § 146 Rz. 31; *Birklbauer/Hilf/Tipold*; Strafrecht BT I, S. 354 Rz. 7.

anderen Menschen zum Zwecke der Irreführung über Tatsachen.[41] Getäuscht werden können somit im Rahmen des § 146 StGB ausschließlich andere Personen.[42] Problematisch an dieser Stelle ist jedoch, dass bei der Manipulation des Smart Meters kein anderer Mensch getäuscht wird, der sich irren kann. Beim Smart Meter handelt es sich nämlich um einen kleinen Computer, der mittels Funk, Powerline oder anderer Leitungen durch einen Konzentrator als Schnittstelle mit Netzwerken des Netzbetreibers direkt verbunden ist und auf diesem Wege die abrechnungsrelevanten Stromverbrauchswerte[43] täglich erfasst und an den Netzbetreiber sendet, der sie sodann (u.a. zum Zwecke des Vergleichs mit dem historischen Verbrauchsverhalten) speichert.[44] Auch in weiterer Folge ist grds. kein Mensch[45] mehr hinsichtlich der schädigenden Vermögensverfügung eingebunden, da die Stromverbrauchswerte, nach der elektronischen Übermittlung durch den Netzbetreiber an den jeweiligen Stromlieferanten, automatisch zur Stromrechnung verarbeitet werden.[46] Damit scheidet bei der Manipulation eines Smart Meters zum Zwecke einer niedrigeren Stromrechnung aufgrund mangelnder menschlicher Täuschung ein Betrug nach § 146 StGB aus.

Anders liegt der Fall hingegen bei den (in diesem Projekt nicht relevanten) klassischen Ferraris-Zählern[47], die keine Computer darstellen. Zum Zwecke der Abrechnung muss entweder der Kunde den Wert des gesamten Stromverbrauchs zu einem bestimmten Stichtag in ein Formular eintragen und dem Netzbetreiber zusenden oder der Stromverbrauch wird beim Kunden vor Ort durch einen Mitarbeiter des Netzbetreibers ausgelesen. Damit sind

---

41 *Fischer*, StGB Kommentar, § 263 Rz. 14; Schönke/Schröder, StGB, *Cramer/Perron*, § 263 Rz. 11; *Wegscheider*, Strafrecht BT, S. 232.

42 OGH 07.03.2007, 13 Os 2/07d; *Fischer*, StGB Kommentar, § 263 Rz. 66; WK-StGB, *Kirchbacher*, § 146 Rz. 47.

43 Dies sind täglich ein Verbrauchswert sowie sämtliche Viertelstundenwerte.

44 § 84 ElWOG 2010.

45 Es werden Kontrollen durchgeführt (Qualitätsmanagement). Ein System überwacht die Abweichungen beim jährlichen Verbrauch und meldet dies auch. Zudem erfolgen Kontrollablesungen vor Ort am System bei Verdacht.

46 § 84a Abs. 2 i.V.m. § 81 ElWOG. Die Übermittlung der Viertelstundenwerte an den Lieferanten ist jedoch nur nach ausdrücklicher Zustimmung des Kunden bzw. zur Erfüllung vertraglicher Pflichten zulässig, § 84a Abs. 2 ElWOG 2010.

47 Ausführlich dazu: *Kudlich/Oglakcioglu*, Strom-„Diebstahl", in: FS Imme Roxin, S. 265 ff.

im Gegensatz zum Smart Meter grds. noch „täuschungsfähige" Menschen in den Ablauf eingebunden.

Die Täuschung der anderen Person kann dabei sowohl durch ein Tun als auch durch ein Unterlassen begangen werden, wobei die aktive Täuschung wiederum ausdrücklich oder konkludent, also schlüssig, erfolgen kann. Eine aktive Täuschung setzt eine mündliche oder schriftliche Erklärung gegenüber der getäuschten Person voraus.[48] Dies ist in der Variante einschlägig, in der der Täter seine Stromverbrauchswerte in eine Postkarte des Netzbetreibers einträgt und diese sodann an den Netzbetreiber zurück sendet, sofern die Karte anschließend von einem Mitarbeiter des Netzbetreibers eigenhändig ausgewertet wird. Mit dem Eintragen der Stromwerte erklärt der Täter zugleich, dass er diese von einem nicht manipulierten Zähler abgelesen hat. Damit täuscht er eine andere Person bei der Auswertung der Karte zum Zwecke der Erstellung der Stromrechnung darüber, dass sein Stromverbrauch im abrechnungsrelevanten Zeitraum wesentlich geringer war, als es objektiv der Fall ist und stellt somit eine nicht bestehende Tatsache als gegeben dar. Mit diesem ausdrücklichen Verhalten ruft der Täter einen täuschungsbedingten Irrtum[49] bei der auswertenden Person hervor. Problematisch ist hingegen der Fall, in dem der Täter seine Stromverbrauchswerte in das Formular einträgt und an den Netzbetreiber versendet, dieses jedoch nicht von einem Mitarbeiter des Netzbetreibers ausgewertet wird, sondern lediglich eingescannt und sodann automatisch weiterverarbeitet wird. Da der Mitarbeiter des Netzbetreibers das Formular nur einscannt, ohne sich mit den Verbrauchswerten zu beschäftigen, findet keine Einwirkung auf sein Vorstellungsbild und damit keine Täuschung eines anderen Menschen statt. Die Auswertung wird anschließend maschinell vorgenommen, sodass sich quasi der Computer täuscht, nicht aber ein anderer Mensch. Daher scheidet bei dieser elektronischen Form der Weiterverarbeitung der eingetragenen Stromverbrauchswerte des Täters ein

---

48 WK-StGB, *Kirchbacher*, § 146 Rz. 20; *Birklbauer/Hilf/Tipold*; Strafrecht BT I, S. 355 Rz. 9. Nach *Fischer*, StGB Kommentar, § 263 Rz. 18 sind im deutschen Strafrecht ausdrückliche Erklärungen in jeglicher Form, also auch Gesten und Zeichen, umfasst.

49 Unter einem Irrtum versteht man jede Vorstellung, die von der Wirklichkeit abweicht, WK-StGB, *Kirchbacher*, § 146 Rz. 44; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 357 Rz. 16.

Betrug nach § 146 StGB aus.[50]

Wieder anders könnte die weitere Variante zu beurteilen sein, in der der Stromverbrauch durch einen Mitarbeiter des Netzbetreibers vor Ort, also direkt am Zähler des Täters, abgelesen wird. Hier fehlt es nämlich an einer ausdrücklichen schriftlichen bzw. mündlichen Erklärung des Täters. In Betracht käme daher eine konkludente Täuschung durch den Täter. Dies ist der Fall, wenn dem Gesamtverhalten des Täters ein entsprechender (stillschweigender) Erklärungswert nach den Regeln des redlichen Geschäftsverkehrs und unter Beachtung der Verkehrsauffassung zukommt.[51] Das bedeutet, dass der Täter nicht ausdrücklich, aber dennoch schlüssig etwas Unwahres vorspiegelt. Allerdings reichen bloße Tatsachenveränderungen, also die Manipulation des Stromzählers, alleine grds. nicht für eine Täuschung aus (sie stellen nur die Vorbereitung für die Täuschung dar); dies ändert sich jedoch in den Fällen, in denen diese Tatsachenveränderungen konkludente Erklärungen enthalten bzw. diese nachfolgen und der Täter diese Information zur Irreführung nutzt.[52] Hier erklärt der Täter zwar nicht expressis verbis etwas Unwahres – er nennt also nicht ausdrücklich die unrichtigen Stromverbrauchswerte, sondern lässt diese den Mitarbeiter des Netzbetreibers selber ablesen – erklärt aber konkludent durch sein Verhalten bei der Vorführung seines Stromzählers, dass dieser ordnungsgemäß und einwandfrei funktioniert, also nicht von ihm manipuliert wurde, und die Stromverbrauchswerte somit objektiv richtig gemessen wurden. Beim Ablesen des Stromverbrauchs wird der Mitarbeiter sodann über die Tatsache des objektiv richtigen Stromverbrauchs getäuscht. Folglich kommt dem Verschweigen durch den Täter ein Erklärungswert zu, das einem aktiven

---

50 OGH 03.04.1990, 15 Os 25/90. Diese Variante ist somit nach § 148a StGB strafbar, da das Ergebnis des automationsunterstützten Datenverarbeitungsvorgangs aufgrund der Eingabe unrichtiger Daten beeinflusst und somit falsch ist. Zum Computerbetrug ausführlich s. Punkt 1.1.4.3.

51 *Lackner/Kühl*, StGB Kommentar, § 263 Rz. 7; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 359 f. Rz. 10.

52 So auch *Fischer*, StGB Kommentar, § 263 Rz. 15 m.w.N; NK-StGB, *Kindhäuser*, § 263 Rz. 100 m.w.N. A.A. *Lackner/Kühl*, StGB Kommentar, § 263 Rz. 8, die eine irreführende Veränderung (also eine Manipulation) an Stromzählern sogar für ein ausdrückliches Vorspiegeln ausreichen lassen, da eine Äußerung dafür nicht zwingend sei, sofern der Täter das Bewusstsein hat, dass zwischen dem inszenierten Sachverhalt und der Wirklichkeit eine Diskrepanz besteht.

Tun gleichwertig ist.[53] Wird die auslesende Person aus irgendwelchen Gründen beim Auslesen der Stromdaten stutzig und schließt vielleicht sogar zu Kontrollzwecken ein eigenes Messgerät an, so bleibt der Betrug im (ebenfalls strafbaren) Versuchsstadium stecken. Macht er dies nicht, hat der Täter einen täuschungsbedingten Irrtum bei dem Mitarbeiter des Netzbetreibers hinsichtlich der ordnungsgemäßen Funktionstüchtigkeit des Messgerätes und der richtigen Stromverbrauchswerte hervorgerufen.

In beiden Varianten, bei denen Menschen in den Auswertungsvorgang eingebunden sind, täuscht der Täter somit durch aktives Tun: Einmal ausdrücklich (wenn der Täter objektiv unrichtige Stromverbrauchswerte in die Karte einträgt und an den Netzbetreiber versendet) und einmal konkludent (wenn der Netzbetreiber die Stromverbrauchswerte des Täters selber bei diesem am Zähler abliest). Erfasst sind somit nicht nur Manipulationen an Kilometerzählern an Autos[54] sondern auch Manipulationen an Verbrauchsmessern, worunter neben Gas- und Wasseruhren auch Stromzähler fallen.[55]

Hinsichtlich des kausalen Irrtums genügt bloßes Mitbewusstsein in der Hinsicht, dass der Getäuschte denkt, alles sei in Ordnung.[56] Es reicht somit aus, dass der Getäuschte davon ausgeht, dass die eingetragenen bzw. abgelesenen Stromverbrauchswerte objektiv richtig zustande gekommen sind. Dabei schließen nach h.M. Zweifel des Getäuschten an der Wahrheit einen Irrtum nicht aus.[57] Dieser Irrtum tritt somit beim Netzbetreiber ein. In weiterer Folge müsste dieser Irrtum über die objektiv richtigen Stromverbrauchswerte zu einer Vermögensverfügung[58] in Form einer „zu niedrigen"

---

53 So auch WK-StGB, *Kirchbacher*, § 146 Rz. 22; A.A. *Kudlich/Oglakcioglu*, Strom-„Diebstahl", in: FS Imme Roxin, S. 271, denen es an dem für den Betrug typischen kommunikativen Zusammenwirkens fehlt.

54 OGH 16.11.2010, 11 Os 133/10h; *Bertel/Schwaighofer*, Strafrecht BT I, § 146 Rz. 8, 27.

55 *Lackner/Kühl*, StGB Kommentar, § 263 Rz. 8.

56 *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 357 Rz. 17.

57 *Fischer*, StGB Kommentar, § 263 Rz. 55 m.w.N.; Schönke/Schröder, StGB, *Cramer/Perron*,
§ 263 Rz. 40 m.w.N.; WK-StGB, *Kirchbacher*, § 146 Rz. 45.

58 Eine Vermögensverfügung ist jede Handlung, Duldung oder Unterlassung, die sich beim Getäuschten oder einem Dritten unmittelbar vermögensmindernd auswirkt, WK-StGB, *Kirchbacher*, § 146 Rz. 53.

Stromrechnung, also in der unterlassenen Geltendmachung der kompletten Forderung, führen. Problematisch ist jedoch an dieser Stelle, dass diese Vermögensverfügung in der Regel (auf Antrag des Kunden) nicht durch den Netzbetreiber, also der Stelle, die den Stromzähler abgelesen hat, sondern durch den Stromlieferanten vorgenommen wird. Allerdings ist der Netzbetreiber, nach Auslesung der Stromverbrauchswerte, verpflichtet, diese zwecks Abrechnung an den Stromlieferanten weiterzuleiten.[59] Über diese Vorgehensweise wird der Kunde auch im Rahmen der Allgemeinen Geschäftsbedingungen des Netzbetreibers sowie des Stromlieferanten informiert. Das bedeutet, dass sich der Irrtum des Netzbetreibers über die objektiven, richtigen Verbrauchswerte des Täters aufgrund der Weitergabe dieser Verbrauchswerte beim Stromlieferanten fortsetzt. Es handelt sich damit beim Stromlieferanten um eine Person, die nicht unmittelbar durch den Täter selber, sondern aufgrund einer gesetzlich vorgesehenen Weitergabe der tatsachenwidrigen Behauptung getäuscht wurde.[60] Es ist in diesem Fall die dispositionskausale Täuschung einer Person als ausreichend anzusehen.[61]

Diese irrtumsbedingte Vermögensverfügung durch den Stromlieferanten bedingt hier sodann einen Vermögensschaden sowohl beim Netzbetreiber (hinsichtlich der Systemnutzungsentgelte bzw. muss der Netzbetreiber die Netzverluste selber decken) als auch beim Stromlieferanten (hinsichtlich der reinen Energiekosten). Der Vermögensschaden ermittelt sich aufgrund eines Vergleichs der Vermögenslage vor und nach der durch die Täuschung bewirkten Vermögensverfügung im Wege einer Gesamtsaldierung, wobei es auf die der geschädigten Person zustehenden wirtschaftlichen Werte (z. B. aus Forderungen) ankommt.[62] Folglich geht das österreichische Strafrecht von einer wirtschaftlichen Betrachtungsweise aus, sodass nur der direkt aufgrund der Vermögensverfügung des Getäuschten entstandene Schaden, also der effektive Verlust an Vermögenssubstanz, erfasst wird.[63] Die zu geringe Stromrechnung (die sowohl die Netzentgelte als auch den Energiepreis beinhaltet) bzw. die zu geringe Abbuchung vom Konto des

---

59 § 84a Abs. 2 ElWOG 2010.

60 WK-StGB, *Kirchbacher*, § 146 Rz. 8.

61 WK-StGB, *Kirchbacher*, § 146 Rz. 8.

62 *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 359 Rz. 23.

63 *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 359 Rz. 23; *Wegscheider*, Strafrecht BT, S. 233.

Täters stellt einen realen Vermögensverlust des Netzbetreibers und des Stromlieferanten dar, da die durch den Stromlieferanten vom Täter eingeforderte Gegenleistung wirtschaftlich nicht der tatsächlichen Vorleistung des Netzbetreibers und des Stromlieferanten entspricht. Die Stromrechnung bleibt somit objektiv hinter dem eigentlich Geschuldeten zurück, sodass Leistung und Gegenleistung nicht gleichwertig sind. Diese Differenz stellt den wirtschaftlichen Vermögensschaden des Netzbetreibers und des Stromlieferanten dar.

Für den subjektiven Tatbestand muss der Täter nicht nur mit Schädigungsvorsatz, sondern auch mit rechtswidriger Bereicherungsabsicht handeln. Die Tat muss folglich subjektiv auf die Erlangung eines rechtswidrigen Vermögensvorteils für den Täuschenden oder einen Dritten gerichtet sein. An der Bereicherungsabsicht fehlt es, wenn der Täter nur darauf abzielt, einem Dritten Aufwand, Unruhe oder Unannehmlichkeiten zu bereiten, da es dem Täter beim Betrug explizit darum gehen muss, sich oder einem Dritten einen Vermögensvorteil zu verschaffen.[64] Rechtswidrig ist dieser Vermögensvorteil dann, wenn der Täter keinen Rechtsanspruch hinsichtlich dieses Vorteils hat. Im vorliegenden Fall geht es dem Täter ausschließlich darum, eine geringe Stromrechnung als objektiv erforderlich vom Stromlieferanten zu erhalten. Folglich möchte er sich auf Kosten des Netzbetreibers und des Stromlieferanten unrechtmäßig bereichern. Diese beabsichtigte Ersparnis als Vorteil des Täters entspricht auf der Gegenseite als unmittelbare Folge der täuschungsbedingten Verfügung genau dem Verlust, also dem Schaden des Netzbetreibers und des Stromlieferanten. Somit ist auch der subjektive Tatbestand des § 146 StGB erfüllt.

Mit der Manipulation des klassischen Stromzählers und der damit verbundenen ausdrücklichen bzw. konkludenten Täuschung über seinen tatsächlichen Stromverbrauch macht sich der Täter eines Betruges nach § 146 StGB gegenüber einem Mitarbeiter (sofern dieser die Stromwerte auswertet bzw. abliest) des Netzbetreibers und aufgrund der Weitergabe der Stromwerte auch gegenüber dem Stromlieferanten und zu Lasten des Netzbetreibers und des Stromlieferanten strafbar.[65] Hat er hingegen nicht alle objektiven

---

64 *Fischer*, StGB Kommentar, § 263 Rz. 186 ff.

65 Gleichzeit begeht er u.U. auch eine Sachbeschädigung nach § 125 StGB am Stromzähler, der im Eigentum des Netzbetreibers steht.

Tatbestandsmerkmale verwirklicht, so ist der versuchte Betrug gem. § 146 i.V.m. § 15 StGB einschlägig. Sofern jedoch das ausgefüllte Formular des Täters von einem Mitarbeiter des Netzbetreibers nur eingescannt, nicht aber ausgewertet wird, scheidet ein Betrug nach § 146 StGB mangels menschlicher Täuschung aus.

2.4.2.2. Qualifikation des § 147 StGB

Fraglich ist, ob der Täter bei der Manipulation seines klassischen Stromzählers zum Zwecke einer niedrigeren Stromrechnung auch einen schweren Betrug nach § 147 StGB verwirklichen kann.

In Betracht kommt dabei zunächst der Messbetrug nach § 147 Abs. 1 Z 1 5. Var. StGB. Dies ist dann der Fall, wenn der Täter zur Täuschung ein unrichtiges Messgerät verwendet. Messgeräte sind dabei sämtliche Vorrichtungen, die dazu bestimmt sind, im Rechtsverkehr zum Wiegen, Zählen oder Messen verwendet zu werden und das Ergebnis anzuzeigen, unabhängig davon, ob sie geeicht sind oder nicht und unabhängig von der technischen Beschaffenheit.[66] Darunter fallen neben Waagen, Kilometerzählern von Fahrzeugen, Gas- und Wasserzählern u.a. auch Stromzähler und andere Energiemessvorrichtungen.[67] Unrichtig ist das Messgerät, also auch der klassische Stromzähler, dann, wenn es aufgrund einer Manipulation am Gerät selbst falsche Messergebnisse liefert.[68] Dabei ist es unerheblich, ob durch die Manipulation nur ein einziger Messvorgang beeinflusst wird oder sämtliche Messvorgänge ab der Manipulation dauerhaft zu falschen Ergebnissen führen, da allein die Veränderung der Messeinrichtung maßgeblich ist.[69] Durch die Installation eines sog. „Supermagneten“[70] wird nämlich das Messverhalten des Gerätes bei ordnungsgemäßem Gebrauch verändert,

66 WK-StGB, *Kirchbacher*, § 147 Rz. 46; *Birkelbauer/Hilf/Tipold*, Strafrecht BT I, S. 370 Rz. 59.

67 Ebenda.

68 WK-StGB, *Kirchbacher*, § 147 Rz. 47 m.w.N; *Bertel/Schwaighofer*, Strafrecht BT I, S. 271 Rz. 5.

69 Dazu: OGH 22.04.1993, 12 Os 25/93; OGH 15.02.2007, 15 Os 137/06w.

70 Oder durch die Beeinflussung der Eichsoftware.

sodass der Zähler falsche Messergebnisse liefert.[71] Ausschlaggebend ist somit beim Messbetrug, dass aufgrund der Manipulation des Stromzählers die Messung als solche nicht funktioniert und daher falsche Werte errechnet werden, die sodann der ablesenden Person des Netzbetreibers zugänglich gemacht werden. Somit ist die Qualifikation des § 147 Abs. 1 Z 1 5. Var. StGB in dem Fall erfüllt, in dem der Täter den Ferraris-Zähler vorsätzlich derart manipuliert, dass dieser falsche Messergebnisse liefert und der Täter diese Ergebnisse gegenüber der stromauslesenden Person des Netzbetreibers zu Täuschungszwecken benützt, also verwendet.

Anders liegt der Fall hingegen, wenn der Täter nicht den Stromzähler als solchen manipuliert, sodass dieser ordnungsgemäß weiter arbeitet, jedoch die richtig ermittelten Stromverbrauchswerte anschließend in der Anzeige verändert bzw. zurückdreht oder die Stromanzeige austauscht. [72] Diese Vorgehensweise unterfällt nicht dem Messbetrug nach § 147 Abs. 1 Z 1 5. Var. StGB, denn wer bloß auf die Anzeige eines richtig ermittelten Messergebnisses im Nachhinein einwirkt und dieses zur Täuschung verwendet, handelt nicht tatbestandlich.[73]

Zu untersuchen ist daher, ob das Zurückdrehen oder der Austausch des Zählers nach erfolgreichem Messvorgang einem anderen Qualifikationstatbestand des Betrugs unterfallen. In Betracht käme die Benützung verfälschter Daten zu Täuschungszwecken nach § 147 Abs. 1 Z 1 3. Var. StGB. Daten sind nach der Legaldefinition des § 74 Abs. 2 StGB sowohl personenbezogene und nicht personenbezogene Daten als auch Programme. Allerdings werden von diesem Qualifikationstatbestand nur Daten geschützt, die automationsunterstützt erfasst werden.[74] Damit unterfällt der manipulierte Ferraris-Zähler nicht dem Qualifikationstatbestand des § 147

---

71 Zudem bewirkt dieser Supermagnet, dass der Zähler auch nach Entfernung als defekt auszuscheiden ist. Das gleiche würde für einen Smart Meter gelten. Bei manueller Beschädigung oder einem Eingriff in den Eichteil müsste dieser auszuscheiden sein.

72 OGH 23.10.2003, 12 Os 43/03; OGH 16.11.2010, 11 Os 133/10h; dazu auch *Hoffer*, Der Kilometerzähler, JBl 2011, 542 f.

73 WK-StGB, *Kirchbacher*, § 147 Rz. 47; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 367 Rz. 60.

74 WK-StGB, *Kirchbacher*, § 147 Rz. 28b; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 367 Rz. 51 jeweils m.w.N.

Abs. 1 Z 1 3. Var. StGB, da hierbei die Stromwerte nicht in computertechnisch bearbeitbarer Form vorliegen und der Täter diese nicht selbst durch Eingabe in ein Computersystem in eine Form bringt, die eine unmittelbare automationsunterstützte (Weiter-) Verarbeitung erlaubt.[75]

Zu prüfen bleibt schließlich, ob es sich beim Zurückdrehen oder Austauschen der Stromverbrauchswerte um einen Beweismittelbetrug nach § 147 Abs. 1 Z 1 4. Var. StGB handelt. Dies setzt die Benützung eines anderen solchen Beweismittels zur Täuschung voraus. Dieser Qualifikationsvariante, die die Verwendung eines falschen oder verfälschten Beweismittels sanktioniert, kommt eine gewisse Auffangfunktion v.a. gegenüber dem Urkunden- und Messbetrug zu.[76] Fraglich ist, was genau unter einem Beweismittel zu verstehen ist und wie weit dieser Begriff geht. Die Rechtsprechung vertritt einen weiten prozessualen Beweismittelbegriff, der alles umfasst, was geeignet ist, jemanden von der Wahrheit oder Unwahrheit einer Behauptung zu überzeugen.[77] Nach dieser Ansicht würde auch das Zurückdrehen und das Austauschen von Zähleruhren unter diesen Begriff fallen, sofern nicht der speziellere Messbetrug nach § 147 Abs. 1 Z 1 5. Var. StGB einschlägig ist. Die Literatur möchte dieses weite Begriffsverständnis dahingehend reduzieren, dass die Beweismittel mit einer falschen bzw. verfälschten Urkunde gleichwertig sein müssen, sodass bloße Augenscheinobjekte wie Bremsspuren oder beschädigte Sachen ausscheiden.[78] Legt man somit den Begriff des Beweismittels restriktiv aus, so werden nur solche Objekte erfasst, die den anderen, ausdrücklich genannten rechtsgeschäftlichen Gewährschaftsträgern (Urkunden, unbare Zahlungsmittel, urkundenähnliche Daten und Messgeräte) gleichwertig sind und im Rechtsverkehr eine ähnliche Funktion erfüllen.[79] Es wäre folglich sinnwidrig, einen zurückgedrehten Stromzähler nicht unter diesen Qualifikationstatbestand zu subsumieren, zumal § 147 Abs. 1 Z 1 4. Var. StGB eine Auffangfunktion zukommt und der Erfolg, nämlich das Vorzeigen unrichtiger Stromwerte, der gleiche ist, wie beim Messbetrug. Somit ist auch ein nach-

---

75 WK-StGB, *Jerabek/Reindl-Krauskopf/Schroll*, § 74 Rz. 65.
76 So auch *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 368 Rz. 55.
77 OGH 08.04.1976, 9 Os 132/75; OGH 08.05.2001, 14 Os 2/01.
78 WK-StGB, *Kirchbacher*, § 147 Rz. 34 m.w.N.
79 OGH 15.12.2010, 15 Os 127/10f., JBl 2011, 666.

träglich zurückgedrehter, also verfälschter[80] Stromzähler geeignet, jemanden in qualifizierter Weise zu täuschen. Anders sieht dies hingegen nach h.M. beim Austauschen der Stromanzeige aus, wenn also der Täter nicht manipulativ auf die objektiv richtige Stromanzeige selber einwirkt, sondern diese lediglich mit einer anderen überdeckt bzw. gegen eine andere (mit niedrigeren Stromverbrauchswerten) austauscht. Das bloße Unterschieben eines Gegenstandes zum Bezugsobjekt (z. B. das Vertauschen oder Überkleben von Preisetiketten) stellt kein Fälschen oder Verfälschen und somit keinen qualifizierten Betrug dar, da nur noch die „neue" Stromanzeige als Beweismittel dient.[81] Sie selber ist jedoch weder falsch, da der Täter sie nicht herstellt, noch ist sie verfälscht, da der Täter diese nicht manipuliert. Somit erfüllt der Täter in der Variante des Austauschens der Stromanzeige nur den Grundtatbestand des § 146 StGB. Während folglich das Zurückdrehen des Stromzählers einen Beweismittelbetrug darstellt, ist das beim Austauschen der Anzeigentafel nicht der Fall.

Der Täter begeht aber auch in dem Fall einen schweren Betrug, wenn der Schaden 3.000 € bzw. 50.000 € übersteigt, § 147 Abs. 2 und Abs. 3 StGB.

Sofern der Täter in der beschriebenen Weise vorsätzlich einen Qualifikationstatbestand des § 147 StGB erfüllt, begeht er einen schweren Betrug.

2.4.2.3. Zwischenergebnis

Im Rahmen des manipulierten Smart Meters ist der klassische Betrug nach § 146 StGB mangels Täuschung eines anderen Menschen nicht einschlägig. Das gleiche gilt für den klassischen Stromzähler, sofern der Täter objektiv unrichtige Stromverbrauchswerte in ein Formular einträgt, was dann von einem Mitarbeiter des Netzbetreibers nur eingescannt, nicht jedoch ausgewertet wird, da dies automatisch erfolgt. Diese Fälle unterfallen dem betrügerischen Datenverarbeitungsmissbrauch nach § 148a StGB.[82]

---

80 Verfälscht ist ein Beweismittel dann, wenn es derart verändert wird, dass dadurch der Schlussfolgerung eine andere Richtung gegeben wird, WK-StGB, *Kirchbacher*, § 147 Rz. 39.

81 OGH 16.11.2010, 11Os133/10h; WK-StGB, *Kirchbacher*, § 147 Rz. 40; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 369 Rz. 56.

82 Dazu ausführlich s. Punkt 1.1.4.3.

Im Rahmen des klassischen Stromzählers gibt es jedoch auch Varianten, in denen ein Betrug nach § 146 StGB einschlägig ist: Dies ist dann der Fall, wenn der Täter einen klassischen Stromzähler (z. B. mit einem sog. „Supermagneten") manipuliert, um anschließend eine niedrigere Stromrechnung zu erwirken und in das Abrechnungsprocedere (sei es durch Auswertung einer Karte oder durch das Ablesen der Stromwerte des Täters vor Ort) noch täuschungsfähige Menschen involviert sind. Unter bestimmten Voraussetzungen begeht der Täter sogar einen qualifizierten Betrug. Dies ist z. B. dann der Fall, wenn der Täter den Stromzähler derart manipuliert, dass dieser falsch misst (Messbetrug i.S.v. § 147 Abs. 1 Z 1 5. Var. StGB) oder wenn der Täter den Stromzähler nach objektiv richtiger Messung zurückdreht (Beweismittelbetrug i.S.v. § 147 Abs. 1 Z 1 4. Var. StGB) bzw. wenn der Schaden des Netzbetreibers 3.000 € bzw. 50.000 € übersteigt (§ 147 Abs. 2 und Abs. 3 StGB).

Rechtspolitisch unbefriedigend ist hingegen, dass der Austausch der richtigen Stromwertedarstellung gegen eine neue (geringere) Stromwertedarstellung keinem Qualifikationstatbestand unterfällt. Die kriminelle Energie dürfte die gleiche sein, wie beim Zurückdrehen des objektiv richtigen Messergebnisses, sodass es ratsam erscheint, diese Variante ebenfalls aufgrund einer Gesetzesergänzung als qualifizierten Betrug zu werten.

2.4.3. Betrügerischer Datenverarbeitungsmissbrauch gem. § 148a StGB

Möglicherweise kommt jedoch eine Strafbarkeit des Täters wegen betrügerischen Datenverarbeitungsmissbrauchs nach § 148a Abs. 1 StGB (dies entspricht Art. 8 CCC) bei der Manipulation seines Smart Meters zum

Zwecke des Abrechnungsbetrugs in Betracht.[83]

Den Tatbestand des betrügerischen Datenverarbeitungsmissbrauchs erfüllt, wer vorsätzlich das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs beeinflusst und dadurch einen anderen am Vermögen schädigt, um sich selbst oder einen Dritten unrechtmäßig zu bereichern. Der Tatbestand des betrügerischen Datenverarbeitungsmissbrauchs wurde nachträglich ins StGB eingeführt, um auch derartige Betrugsfälle erfassen zu können, in denen kein Mensch, sondern eine Maschine getäuscht wird.[84] Tathandlung ist in diesem Fall, dass das Ergebnis eines vollautomatisierten Datenverarbeitungsvorgangs beeinflusst wird (dies ersetzt die Erfordernisse von Irrtum und Vermögensverfügung durch eine Person beim klassischen Betrug nach § 146 StGB), wodurch ein anderer an seinem Vermögen geschädigt wird.

Unter Daten versteht man nach der Legaldefinition des § 74 Abs. 2 StGB sowohl personenbezogene und nicht personenbezogene Daten als auch Programme. Dies ist bei den Stromverbrauchswerten der Fall, da es sich dabei um personenbezogene Daten handelt. Diese Daten müssen im Bereich des betrügerischen Datenverarbeitungsmissbrauchs elektronisch,

---

83 Wenn der Täter im Zusammenhang mit dem klassischen Stromzähler zum Zwecke einer niedrigeren Stromrechnung objektiv unrichtige Stromverbrauchswerte in ein Formular einträgt und an den Netzbetreiber versendet, unterfällt dies mangels menschlicher Täuschung nicht dem Betrug nach § 146 StGB, sofern das Formular nur eingescannt und anschließend nicht persönlich, sondern automatisch, weiterverarbeitet wird. Diese Vorgehensweise unterliegt der Strafbarkeit des betrügerischen Datenverarbeitungsmissbrauchs nach § 148a StGB und zwar in Form der Input-Manipulation, da das automatische Verarbeitungsergebnis aufgrund der Eingabe unrichtiger Daten beeinflusst und verfälscht wird und somit materiell falsch ist. Dies führt – nach Übersendung der Daten an den Stromlieferanten – in Folge zu einer schädigenden Vermögensdisposition durch das Computersystem des Stromlieferanten, da automatisch zu wenig vom Konto des Täters abgebucht bzw. ihm zu wenig in Rechnung gestellt wird, was zu einem Vermögensschaden beim Netzbetreiber und auch beim Stromlieferanten führt. Dadurch erwirkt der Täter eine beabsichtigte unrechtmäßige Bereicherung.

84 Anders als beim Betrug handelt es sich beim betrügerischen Datenverarbeitungsmissbrauch nicht um ein Selbstschädigungsdelikt, sondern um ein Fremdschädigungsdelikt.

magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sein oder übermittelt werden.[85] Die Datenverarbeitung wiederum meint alle automatisierten Vorgänge, bei denen durch Aufnahme von Daten und ihre Verknüpfung nach Programmen Arbeitsergebnisse erzielt werden.[86] Bei der Verarbeitung dieser Daten kommt es somit darauf an, dass dies auf elektronischem Wege erfolgt. Beim Smart Meter handelt es sich um einen kleinen Computer, der z. B. über Funkverbindungen, Infrarot, Powerline oder leitungsgebundene Verbindungen wie DSL die entsprechenden (Verbrauchs-) Daten[87] an den Netzbetreiber übermittelt. Dieser macht sodann wiederum dem Kunden seine Verbräuche in einem bestimmten Portal zugänglich, sodass der Kunde animiert wird, Strom zu sparen. Somit handelt es sich beim Stromzähler in Form eines Smart Meters (im Gegensatz zum klassischen Ferraris-Zähler) um einen Computer mit Mess- und Kommunikationsaufgaben, der automationsunterstützt die jeweiligen Stromverbrauchswerte verarbeitet.[88]

In der ersten Alternative müsste der Täter gestalterisch auf den Programmablauf einwirken. Dies kann im Bereich des Smart Meters vor allem durch die sog. **Programm-Manipulation**, also die Manipulation an Softwareprodukten, erfolgen und zwar in der Weise, dass entweder von vorneherein das Programm[89] fehlerhaft gestaltet wird oder nachträglich Verfälschungen mittels Veränderungen (z. B. Löschen, Hinzufügen, Überschreiben) bei den einzelnen Ablaufschritten vorgenommen werden.[90] Durch diesen Eingriff in die Verarbeitungsphase resultiert, dass, anders als vom Netzbetreiber als Verfügungsberechtigten vorgesehen, Daten im nicht eichpflichtigen Teil des Smart Meters nicht oder unrichtig verarbeitet oder falsche Daten erzeugt werden, sodass das Ergebnis inhaltlich objektiv unrichtig ist, da sich

85 NK-StGB, *Kindhäuser*, § 263a Rz. 10.

86 NK-StGB, *Kindhäuser*, § 263a Rz. 12 m.w.N.; *Rengier*, Strafrecht BT I, S. 302 Rz. 3.

87 Bei den durch den Smart Meter erfassten Stromverbrauchsdaten handelt es sich um personenbezogene Daten.

88 *Cyber Security Austria*, Smart Metering, S. 1.

89 Unter einem Programm versteht man die in Form von Daten fixierte Steuerung der einzelnen Ablaufschritte der Datenverarbeitung, NK-StGB, *Kindhäuser*, § 263a Rz. 13.

90 NK-StGB, *Kindhäuser*, § 263a Rz. 13.

der Computer quasi „täuscht".[91] In der Praxis ist davon auszugehen, dass der Täter mittels eines Computerprogramms erreicht, dass der Smart Meter andere, also geringere Stromverbrauchswerte errechnet, als sie der Wirklichkeit entsprechen, sodass inhaltliche Darstellung verfälscht wird. Ebenfalls darstellbar ist allerdings auch die Variante der **Datenmanipulation**, wobei eine Entscheidung hinsichtlich der genauen Begehungsform aufgrund der Gleichwertigkeit der Alternativen dahinstehen kann.

Die durch die Tathandlung resultierende „Täuschung des Smart Meters" muss das Ergebnis der automationsunterstützten Datenverarbeitung derart beeinflussen, dass infolge dessen automatisch eine Vermögensverschiebung zum Nachteil eines anderen erfolgt.[92] Das Ergebnis des Datenverarbeitungsvorgangs ist dann beeinflusst, wenn es sich durch die Programm- bzw. Daten-Manipulation abweichend zum ordnungsgemäßen Programmablauf darstellt und somit eine Vermögensdisposition (eine sog. „Computerverfügung") auslöst, die sich unmittelbar vermögensmindernd auswirkt.[93] An einer manipulierten Vermögensverschiebung fehlt es dann, wenn es dem Täter ausschließlich darum geht, die regelgerechte Aufzeichnung der Stromverbrauchswerte zu unterbinden. Vorliegend ist es so, dass der Smart Meter aufgrund der Manipulation objektiv unrichtige Stromverbrauchswerte, die nicht der Wirklichkeit entsprechen, an den Netzbetreiber sendet, wodurch sodann in Folge der Stromlieferant automatisch eine zu geringe Stromrechnung (die beim sog. Vorleistungsmodell sowohl die Systemnutzungsentgelte als auch den reinen Energiepreis beinhaltet) erstellt bzw. zu wenig vom Konto des Täters abbucht.

Zudem muss der manipulierte Datenverarbeitungsvorgang kausal für die Vermögensverschiebung sein, sodass die Vermögensverfügung unmittelbar durch die Aktion des Computers vorgenommen wird. Das bedeutet, dass es zum einen keiner weiteren Zwischenschritte des Täters bedarf und zum

---

91 *Fischer*, StGB Kommentar, § 263a Rz. 6; Schönke/Schröder, StGB, *Perron*, § 263a Rz. 5; *Wessels/Hillenkamp*, Strafrecht BT II, S. 309 Rz. 609 m.w.N.; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 391 Rz. 6.

92 *Fischer*, StGB Kommentar, § 263a Rz. 20; NK-StGB, *Kindhäuser*, § 263a Rz. 31 m.w.N.; *Wegscheider*, Strafrecht BT, S. 241.

93 Schönke/Schröder, StGB, *Perron*, § 263a Rz. 18 ff.; NK-StGB, *Kindhäuser*, § 263a Rz. 32; *Rengier*, Strafrecht BT I, S. 303 Rz. 4; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 156 Rz. 521 m.w.N.

anderen keine verfügungsbefugte Person auf Seiten des Geschädigten in das Geschehen eingebunden werden darf.[94] Allerdings genügt es, dass der Datenverarbeitungsvorgang nur ein Teilstück einer mehraktigen Verfügung darstellt: So kann diese z. B. durch eine Person **ohne** Inhaltskontrolle umgesetzt werden[95] oder in eine weitere Computeranlage eingespeichert werden, die sodann die Vermögensverfügung endgültig durchführt.[96] So werden auch automatische Abbuchungen oder Ausdrucke in Form von (zu niedrigen) Rechnungen erfasst. Dies trifft selbst dann noch zu, wenn diese Ausdrucke regelmäßig bzw. stichprobenartig hinsichtlich ihres Inhalts überprüft werden, da sie dennoch eine konkrete Vermögensgefährdung darstellen und nicht garantiert ist, dass die Programmmanipulation tatsächlich erkannt wird.[97] Die Vermögensverfügung, also der Abbuchungsvorgang beim Täter, wird auf der Basis der vom Smart Meter übermittelten Stromverbrauchswerte an den Netzbetreiber automatisch durch den Stromlieferanten vorgenommen, sodass die erforderliche Kausalität gegeben ist. Selbst wenn die Abbuchung bzw. Rechnungslegung durch den Stromlieferanten nicht unmittelbar nach Erhalt der Stromwerte erfolgt, da dies grds. nur monatlich bzw. jährlich stattfindet[98], so reicht es dennoch als Zwischenerfolg aus, wenn das manipulierte Ergebnis einer automationsunterstützten Datenverarbeitung inhaltlich vom objektiv richtigen Ergebnis abweicht. Auf Basis dieses Zwischenerfolgs nimmt der Stromlieferant nämlich sodann die Abrechnung, also die Vermögensverfügung, vor.[99]

Das Ergebnis des manipulierten Datenverarbeitungsprozesses, also die „Computerverfügung" führt schließlich, wie beim Betrug auch, zum Vermögensschaden eines anderen.[100] Wenn der Täter somit den Datenverarbeitungsvorgang seines Smart Meters bei der Aufzeichnung und Verarbeitung der Stromverbrauchswerte derart manipuliert, dass dieser objektiv unrichti-

---

94 NK-StGB, *Kindhäuser*, § 263a Rz. 33 ff.; WK-StGB, *Kirchbacher/Presslauer*, § 148a Rz. 7.

95 Wird in den Vermögensverfügungsvorgang eine Person mit Kontrollfunktion eingebunden, liegt ein Betrug nach § 146 StGB vor, OGH 03.04.1990, 15 Os 25/90.

96 Schönke/Schröder, StGB, *Perron*, § 263a Rz. 21.

97 *Lackner/Kühl*, StGB, § 263a Rz. 18.

98 Der Kunde hat nach § 81 Abs. 6 ElWOG 2010 das diesbezügliche Wahlrecht, wenn er über einen Smart Meter verfügt.

99 Salzburger Kommentar, *Triffterer*, § 148a Rz. 37 ff.

100 Dazu ausführlich beim Betrug s. Punkt 1.1.4.2.

ge Werte aufzeichnet und an den Netzbetreiber versendet, wodurch der Stromlieferant nach Erhalt der Daten durch den Netzbetreiber automatisch eine zu geringe Stromrechnung erstellt bzw. Abbuchung vornimmt, hat der Täter den objektiven Tatbestand des § 148a Abs. 1 StGB erfüllt, zumal er mit diesem Verhalten den Netzbetreiber und den Stromlieferanten an ihrem Vermögen schädigt, da die Rechnung an den Täter wertmäßig hinter der Leistung des Netzbetreiber und des Stromlieferanten zurück bleibt. Der Vermögensschaden der beiden Unternehmer stellt aufgrund der Beeinflussung der automationsunterstützten Datenverarbeitung eine dem Täter objektiv zurechenbare Folge dar.[101]

Dabei ist es im subjektiven Tatbestand erforderlich, dass der Täter mit Vorsatz hinsichtlich des objektiven Tatbestands (also sowohl des Zwischen- als auch des Enderfolgs) handelt und darüber hinaus den Willen hat, sich selber durch das Ergebnis des manipulierten Datenverarbeitungsprozesses unrechtmäßig zu bereichern.[102] Seine Bereicherungsabsicht ist dann rechtswidrig, wenn er auf den angestrebten Vermögensvorteil keinen Rechtsanspruch hat, was vorliegend der Fall ist. Genauso ist sein Vorteil die Kehrseite, des Vermögensschadens, da sie als unmittelbare Folge auf der täuschungsbedingten Verfügung beruht.[103]

Über das Grunddelikt des § 148a Abs. 1 StGB hinaus, verwirklicht der Täter einen qualifizierten betrügerischen Datenverarbeitungsmissbrauch nach § 148a Abs. 2 StGB, sofern er vorsätzlich einen Schaden von über 3.000 € bzw. über 50.000 € herbeiführt.

Hat der Täter den objektiven Tatbestand nicht verwirklicht, weil z. B. der Netzbetreiber die Manipulation des Smart Meters bemerkt, so ist nach § 148a StGB i.V.m. § 15 StGB zumindest der versuchte betrügerische Datenverarbeitungsmissbrauch strafbar.

---

101 Salzburger Kommentar, *Triffterer*, § 148a Rz. 48.

102 Dazu ausführlich beim Betrug s. Punkt 1.1.4.2.1.

103 *Fischer*, StGB Kommentar, § 263 Rz. 187.

2.4.4. Zwischenergebnis

Manipuliert der Täter zum Zwecke einer niedrigeren Stromrechnung das Programm seines Smart Meters im nicht eichpflichtigen Teil derart, dass dieser objektiv unrichtige Stromverbrauchswerte aufzeichnet und sodann an den Netzbetreiber versendet, woraufhin der Stromlieferant in Folge automatisch „zu wenig" vom Konto des Täters abbucht, macht sich dieser eines betrügerischen Datenverarbeitungsmissbrauchs nach § 148a Abs. 1 StGB strafbar. Darüber hinaus erfüllt er den Qualifikationstatbestand des § 148a Abs. 2 StGB, sofern der Schaden einen Wert von 3.000 € bzw. von 50.000 € übersteigt. Kommt ein vollendeter betrügerischer Datenverarbeitungsmissbrauch nicht in Betracht, liegt zumindest ein versuchter betrügerischer Datenverarbeitungsmissbrauch vor.

2.4.5. Widerrechtlicher Zugriff auf ein Computersystem gem. § 118a StGB

Der Täter, der seinen eigenen Smart Meter für einen Abrechnungsbetrug manipuliert, könnte sich auch wegen widerrechtlichen Zugriffs auf ein Computersystem nach § 118a Abs. 1 StGB, der Art. 2 CCC innerstaatlich umsetzt, strafbar machen. Den Straftatbestand des § 118a Abs. 1 StGB erfüllt, wer sich oder einem anderen Unbefugten vorsätzlich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezielle Sicherheitsvorkehrungen des Computersystems überwindet. Dabei muss der Täter zunächst die Absicht haben, sich oder einem Dritten Kenntnis von den dort gespeicherten und für ihn nicht bestimmten Daten zu verschaffen, um sie sodann entweder selbst zu benützen, einem anderen Unbefugten zugänglich zu machen bzw. zu veröffentlichen und um sich oder einem Dritten einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen. § 118a StGB schützt die Daten im Computersystem selber und damit sowohl die Privatsphäre als auch das Verfügungsrecht über die eigenen Daten und dient der Bekämpfung der Computerkriminalität.

Die Prüfung und die Verwirklichung des objektiven Tatbestandes kann jedoch an dieser Stelle dahinstehen, da die Strafbarkeit des Täters in diesem Fall am subjektiven Tatbestand scheitert. Der Täter handelt bei der Manipulation seines eigenen Smart Meters nämlich nicht in der Absicht, sich

von den im Computersystem gespeicherten Daten widerrechtlich Kenntnis zu verschaffen. Sinn und Zweck des Smart Meters ist es gerade, dass sich der Nutzer fortlaufend über seinen eigenen Stromverbrauch informieren kann, mit dem Ziel, diesen (auf legale Weise) zu senken. Somit will der Täter seine eigenen Stromverbräuche nicht ausspionieren.

Folglich macht sich der Täter bei der Manipulation seines eigenen Smart Meters nicht des widerrechtlichen Zugriffs auf ein Computersystem nach § 118a Abs. 1 StGB strafbar.

2.4.6. Missbräuchliches Abfangen von Daten gem. § 119a StGB

Ebenfalls nicht in Betracht kommt ein missbräuchliches Abfangen von Daten nach § 119a Abs. 1 StGB[104] bei der Manipulation des eigenen Smart Meters. Dies würde voraussetzen, dass der Täter vorsätzlich eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benutzt oder die elektromagnetische Abstrahlung eines Computersystems auffängt, in der Absicht, sich oder einem Dritten Kenntnis von den übermittelten und für ihn nicht bestimmten Daten zu verschaffen, um sie sodann entweder selbst zu benützen, einem anderen Unbefugten zugänglich zu machen bzw. zu veröffentlichen und um sich oder einem Dritten einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, sofern die Tat nicht nach § 119 StGB[105] mit Strafe bedroht ist. Geschützt wird mit diesem Straftatbestand das formelle Geheimhaltungsinteresse an der Nichtöffentlichkeit der Kommunikation mit elektronischen Mitteln.

Auch wenn es dem Täter darum geht, sich mittels einer objektiv unrichtigen Stromrechnung einen Vermögensvorteil zu verschaffen, so manipuliert der Täter zum einen seinen eigenen Smart Meter vor Ort und liest die Daten nicht auf ihrem Weg der Übermittlung zum Netzbetreiber aus und zum anderen darf und soll der Täter Kenntnis von seinen eigenen Stromverbrauchswerten haben.

---

104 Dieser setzt Art. 3 CCC in nationales Recht um.

105 Verletzung des Telekommunikationsgeheimnisses.

2.4.7. Sachbeschädigung gem. § 125 StGB

Fraglich ist, ob der Täter durch die Manipulation seines eigenen Smart Meters eine Sachbeschädigung nach § 125 StGB begeht. Eine Strafbarkeit nach § 125 StGB begeht, wer eine fremde Sache zerstört, beschädigt, verunstaltet oder unbrauchbar macht. Zwar tauscht der Netzbetreiber den Smart Meter nach einer entdeckten Manipulation der Stromverbrauchswerte aus, allerdings kann an dieser Stelle nicht generell beantwortet werden, ob der Smart Meter selber, also die Hardware[106], durch die Manipulation auch tatsächlich beschädigt oder zerstört ist, sodass eine Beurteilung der Strafbarkeit wegen Sachbeschädigung nach § 125 StGB an dieser Stelle nicht abschließend geklärt werden kann.[107]

2.4.8. Datenbeschädigung gem. § 126a StGB

Möglich erscheint jedoch, dass sich der Täter wegen einer Datenbeschädigung nach § 126a Abs. 1 StGB (in Umsetzung von Art. 4 CCC) strafbar macht, wenn er den nicht eichpflichtigen Teil seines Smart Meters derart manipuliert, dass dieser objektiv unrichtige Stromwerte errechnet. Danach macht sich der Täter strafbar, wenn er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst unbrauchbar macht bzw. unterdrückt und dadurch einen anderen schädigt. Zweck dieses Straftatbestandes ist es zum einen, fremdes Vermögen und zum anderen, das Interesse an der Verfügbarkeit der Daten und deren Fortbestand zu schützen.[108] Mit der Schaffung dieser Norm wurde eine Strafbarkeitslücke geschlossen, da Daten keinen körperlichen Gegenstand darstellen und somit nicht dem Schutzbereich der Sachbeschädigung nach § 125 StGB unterfallen.[109] Folg-

---

106 Bei den Daten innerhalb des Smart Meters handelt sich nicht um Sachen, sodass eine evtl. Strafbarkeit diesbezüglich ausscheidet.

107 In den meisten Fällen wird der Täter wohl die Kontakte anlöten usw. Das bedeutet, der Zähler ist zwar nicht physisch zerstört, aber wohl beschädigt (ähnlich einem Schrank, der eine Beschädigung aufweist welche nicht die Benutzung beeinträchtigen muss).

108 *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 256 f. Rz. 1; *Schuh*, Computerstrafrecht, S. 104.

109 *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 256 Rz. 1; *Reindl-Krauskopf*, Computerstrafrecht, S. 19.

lich werden von § 126a StGB die Daten selber (vor Zerstörung) und nicht das Speichermedium, dieses unterfällt § 125 StGB, geschützt.

Bei den mittels des Smart Meters errechneten Stromverbrauchswerten müsste es sich um Daten i.S.v. § 74 Abs. 2 StGB handeln, was der Fall ist. Unter einem Verarbeiten versteht man nach § 4 Z 9 DSG 2000[110] das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (§ 4 Z 11 DSG 2000), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns (§ 4 Z 12 DSG 2000) von Daten. Auch dies ist vorliegend gegeben, da der Smart Meter in Abhängigkeit des Verbrauchsverhaltens des Täters dessen Stromwerte automatisch ermittelt, aufzeichnet, für eine gewisse Zeit speichert und sodann an den Netzbetreiber weitersendet. Die Verarbeitung muss zudem automationsunterstützt, also maschinell oder programmgesteuert erfolgen[111], was im Rahmen der Stromwerte der Fall ist. Über diese Stromverbrauchsdaten müsste der Täter entweder gar nicht oder zumindest nicht alleine verfügen dürfen. Verfügungsbefugt über die Daten sind nur die Personen, die die Daten hergestellt haben oder denen eine Verfügungsbefugnis eingeräumt worden ist, was z. B. für den Systembetreiber gilt.[112] Dabei ist nicht das zivilrechtliche Eigentum bzw. die Fremdheit dieser Daten maßgeblich, sondern ausschließlich das Alleinverfügungsrecht über diese Daten.[113] Dem Täter steht jedoch keinesfalls das Alleinverfügungsrecht über diese Daten zu, auch wenn sie sein Verbrauchsverhalten darstellen und in seinem Eigentum stehen, sondern (zumindest auch) dem Netzbetreiber und dem Lieferanten, die auf die objektiv richtigen Verbrauchswerte zum Zwecke der Übermittlung bzw. Abrechnung angewiesen sind, sodass sich auch der Täter als Kunde vertraglich im Rahmen der Allgemeinen Bedingungen verpflichtet hat, nicht manipulativ auf seinen Stromzähler einzuwirken[114], zumal sein Vertrag ansonsten aufgrund des missbräuchli-

---

110 Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000-DSG 2000), BGBl. I 2013/83.

111 Salzburger Kommentar, *Komenda/Madl*, § 126a Rz. 21 m.w.N.

112 *Beer*, Convention on Cybercrime, S. 144 f.

113 *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 257 Rz. 5.

114 So z.B. die Allgemeinen Bedingungen der Netz Oberösterreich GmbH, S. 19, abrufbar unter: http://strom.netzgmbh.at/eag_at/resources/284094835607631929_1028631756552887790_4K7KgkNN.pdf.

chen Verhaltens ohne Mahnverfahren gekündigt werden kann[115]. Dass der Täter über seine im Smart Meter aufgezeichneten Stromverbrauchswerte kein (Allein-)Verfügungsrecht hat, deckt sich auch mit dem Schutzzweck der Norm, die unrechtmäßige Eingriffe in den Datenbestand sanktionieren und somit auch das Interesse am (richtigen) Fortbestand sowie an der Verfügbarkeit dieser Daten bewahren will.[116]

Diese Daten müsste der Täter verändern, löschen, sonst unbrauchbar machen oder unterdrücken. Diese Tathandlungen überschneiden sich teilweise, sodass eine genaue Abgrenzung nicht möglich ist. Ergebnis sämtlicher Begehungsvarianten ist jedoch, dass der rechtmäßige Dateninhaber keinen Zugriff auf den originären und damit objektiv richtigen Dateninhalt mehr hat.[117] Daher ist es der Sinn und Zweck dieser Norm, einen umfassenden Schutz vor Beeinträchtigungen zu erreichen und Strafbarkeitslücken zu vermeiden.[118] Bei der Manipulation des eigenen Smart Meters zum Zwecke einer niedrigeren Stromrechnung kommt die Variante des Veränderns als Unterfall des Unbrauchbarmachens in Betracht. Unter einem Verändern versteht man die Herstellung eines neuen Informationsgehaltes bzw. neuen Dateninhalts, z. B. durch inhaltliche Umgestaltung, durch teilweise Löschung oder durch eine veränderte Verknüpfung mit anderen Daten, sodass der ursprüngliche Verwendungszweck dadurch beeinträchtigt bzw. nicht mehr durchführbar ist.[119] Indem der Täter das ursprüngliche Programm innerhalb des nicht eichpflichtigen Teils des Smart Meters z. B. durch die Einführung eines Trojaners oder Virenprogramms derart verändert, dass der Smart Meter niedrigere Stromverbräuche aufzeichnet, als dies objektiv der Fall ist, beeinträchtigt er den ursprünglichen Verwendungszweck dieses Messgerätes, also die Aufzeichnung der richtigen Stromverbräuche zur korrekten Auslesung und Verrechnung durch den Netzbetreiber und Lieferanten.

Der Täter gibt der Datenaufzeichnung folglich einen neuen, also falschen, Informationsgehalt, sodass der Netzbetreiber grds. nicht seinen be-

115 § 82 Abs. 4 ElWOG 2010.
116 Salzburger Kommentar, *Komenda/Madl*, § 126a Rz. 27.
117 *Sonntag*, Internetrecht, S. 360.
118 Schönke/Schröder, StGB, *Stree/Hecker*, § 303a Rz. 4.
119 *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 258 Rz. 6; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 178 Rz. 594; *Reindl-Krauskopf*, Computerstrafrecht, S. 22.

zweckten objektiv richtigen Dateninhalt durch den Smart Meter übermittelt bekommt, den er sodann an den Lieferanten weiterleiten kann.

Durch die Tathandlung müsste der Täter das Vermögen eines anderen schädigen. Der Vermögensschaden ist darin begründet, dass der Geschädigte Daten übermittelt bekommt, die in ihrem Vermögenswert nachhaltig durch den Täter verändert worden sind und somit nicht mehr den objektiv richtigen Vermögenswert beinhalten. Maßgeblich für die Schadensberechnung im Rahmen des § 126a Abs. 1 StGB ist allein der unmittelbare Schaden an den Daten selber, also die Summe, die der Geschädigte dafür aufwenden muss, seinen ursprünglichen Datenbestand wiederzubeschaffen (Wiederbeschaffungs- bzw. Wiederherstellungssaufwand).[120] Mittelbare Folgeschäden, wie entgangene Gewinne oder Imageschäden, werden bei der Schadensberechnung hingegen nicht berücksichtigt, selbst wenn die Handlung des Täters diesbezüglich ebenfalls kausal ist.[121] Vorliegend ist es in der Praxis so, dass der Netzbetreiber ein großes Interesse an den objektiv richtigen Daten hat. Daher verfügt der Smart Meter zusätzlich zu dem manipulierbaren Teil über einen eichfähigen Teil, auf den hingegen durch den Täter nicht zugegriffen werden kann und der somit immer die korrekten, also objektiv richtigen, Stromwerte aufzeichnet. Diese objektiv richtigen Zählwerte werden sodann aufgrund der gesetzlichen Vorgaben 60 Tage im eichpflichtigen Teil des Smart Meters gespeichert (§ 83 Abs. 2 ElWOG 2010 und § 3 Z 3 IMA-VO 2011[122]). Nach Ablauf dieser 60 Tage werden die Daten jedoch wieder überschrieben und sind somit nicht mehr verfügbar[123] und auch nicht rekonstruierbar. Entdeckt der Netzbetreiber somit aufgrund der Manipulationserkennung[124] innerhalb des Smart Meters innerhalb dieser 60 Tage die Manipulation muss unterschieden werden: Kann der Netzbetreiber auf diesen eichpflichtigen Teil des Smart Meters, also auf die objektiv richten Stromwerte, in der Weise (z. B. online) zugreifen, dass

120 Salzburger Kommentar, *Komenda/Madl*, § 126a Rz. 50; WK-StGB, *Bertel*, § 126a Rz. 5; *Reindl-Krauskopf*, Computerstrafrecht, S. 23; *Sonntag*, Internetrecht, S. 361.

121 *Reindl-Krauskopf*, Computerstrafrecht, S. 24.

122 Verordnung der E-Control, mit der die Anforderungen an intelligente Messgeräte bestimmt werden (Intelligente Messgeräte-AnforderungsVO 2011-IMA-VO 2011), BGBl. II 2011/339.

123 Erläuterungen zur IMA-VO 2011, S. 4.

124 Nach § 3 Z 10 IMA-VO 2011 muss der Smart Meter mit einer solchen Manipulationserkennung ausgestattet sein.

ihm – wie bei der Bereithaltung einer Sicherheitskopie – kein Wiederherstellungsaufwand entsteht, ist der Tatbestand des § 126a StGB mangels Schadens nicht erfüllt.[125] Muss der Netzbetreiber hingegen die objektiv richtigen Stromwerte (vor Ort) aus dem eichpflichtigen Teil des Smart Meters auslesen und den manipulierten Teil des Smart Meters wieder mit diesen richtigen Daten überspielen bzw. einen neuen Datenträger installieren oder den Smart Meter neu eichen[126], liegt sehr wohl ein Schaden vor. Für die Schadensberechnung sind dabei die notwendigen Auslagen für diese Wiederherstellung entscheidend (Aufwand für die Rekonstruktion der Daten im manipulierten Teil des Smart Meters, Kosten für IT-Experten, Eichung, etc.).[127] Nach Ablauf dieser 60 Tage, wenn also die manipulierten Daten nicht mehr mittels des objektiv richtigen eichpflichtigen Teils wiederhergestellt werden können, bedarf es der Installation eines neuen Smart Meters (inkl. einer neuen Software). Der Schaden bemisst sich sodann nach dem Marktpreis.[128]

Da an dieser Stelle nicht generell gesagt werden kann, ob der Netzbetreiber noch innerhalb der 60 Tagesfrist die Manipulation bemerkt und ob ihm dann ein Wiederherstellungsaufwand entsteht oder nicht, kann eine endgültige Entscheidung hinsichtlich einer Strafbarkeit des Täters nach § 126a StGB nicht generell getroffen werden, wobei wohl eher davon auszugehen ist.
Sofern der finanzielle Schaden an den Daten über 3.000 € bzw. über 50.000 € liegen sollte, so würde der Täter über den Grundtatbestand hinaus zudem eine Qualifikation nach § 126a Abs. 2 StGB erfüllen.
Da von einem vorsätzlichen Verhalten des Täters auszugehen ist, würde § 126a StGB, sofern er einschlägig ist, in Tateinheit mit dem betrügerischen Datenverarbeitungsmissbrauch nach § 148a StGB stehen.

---

125 WK-StGB, *Bertel*, § 126a Rz. 6; *Beer*, Convention on Cybercrime, S. 147; *Sonntag*, Internetrecht, S. 361.

126 In der Praxis ist es zumeist so, dass im Falle einer Manipulation ein neuer Smart Meter installiert wird, da nicht nur die richtigen Stromwerte aus dem eichfähigen Teil des Smart Meters ausgelesen werden müssen, sondern der manipulierte Smart Meter sodann auch neu geeicht werden müsste.

127 Salzburger Kommentar, *Komenda/Madl*, § 126a Rz. 52; WK-StGB, *Bertel*, § 126a Rz. 5.

128 Salzburger Kommentar, *Komenda/Madl*, § 126a Rz. 52; WK-StGB, *Bertel*, § 126a Rz. 5.

Die einschränkende Regelung, wonach die Strafbarkeit des Täters trotz Veränderung von Daten davon abhängt, dass dem Opfer ein Wiederherstellungsaufwand entstehen muss, erscheint im Rahmen des § 126a StGB allerdings rechtspolitisch problematisch. Dieser Wiederherstellungsaufwand entsteht dem Geschädigten nämlich nur in dem Fall, wenn er z. B. keine Sicherungskopie dieser Daten zur Hand hat und somit die objektiv richtigen Daten wiederherstellen muss. Nur in diesem Fall ist also eine Strafbarkeit des Täters gegeben. Hat der Geschädigte hingegen die Daten noch an einem anderen Ort gespeichert, hat er daher zumeist keinen Wiederherstellungsaufwand und die Strafbarkeit des Täters entfällt. Es scheint allerdings nicht sachgerecht, die Strafbarkeit des Täters von den zuvor getätigten Schutz- und Sicherungsmaßnahmen des Geschädigten abhängig zu machen, da derartige Schutz- und Sicherungsmaßnahmen zu einer Privilegierung dieses Täters führen würden.[129] Ferner ist der Schutzzweck der Norm darin zu sehen, das Interesse an der Verfügbarkeit der konkreten Daten und deren Fortbestand zu schützen, ohne dass es auf den Wert oder die Wiederherstellbarkeit ankommen sollte. Daher scheint im Vergleich die Regelung im deutschen StGB (auch vor dem Hintergrund des Opferschutzes) sinnvoller zu sein, wonach sich strafbar macht, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert (§ 303a StGB), ohne dass es auf einen darüberhinausgehenden wirtschaftlichen Wiederherstellungsschaden des Opfers ankommt. Diesbezüglich wäre eine gesetzliche Änderung anzudenken, die auch mit Art. 4 CCC vereinbar wäre.

2.4.9. Störung der Funktionsfähigkeit eines Computersystems gem. § 126b StGB

Es ist nunmehr zu prüfen, ob sich der Täter aufgrund der Manipulation seines eigenen Smart Meters wegen Störung der Funktionsfähigkeit eines Computersystems nach § 126b Abs. 1 StGB strafbar macht, mit dem Art. 5 CCC umgesetzt wird. Eine Strafbarkeit nach § 126b Abs. 1 StGB setzt voraus, dass der Täter die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt und diese Tat nicht bereits nach § 126a StGB strafbar ist. Damit stellt § 126b StGB einen Auffangtatbestand für § 126a StGB dar. Mittels § 126b StGB werden Computersysteme zur Gän-

129 So auch *Schuh*, Computerstrafrecht, S. 106.

ze und nicht nur einzelne Daten geschützt.

Unter einem Computersystem versteht man nach der Legaldefinition des § 74 Abs. 1 Z 8 StGB sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen. Somit unterfallen dieser Begriffsbestimmung nicht nur Computernetzwerke, sondern z. B. auch einzelne EDV-Geräte, Handys, Smartcards, Software[130] oder eben auch Smart Meter. Auch wenn der Smart Meter im Haus des Täters installiert ist und ausschließlich dessen Stromverbräuche aufzeichnet, so darf der Täter dennoch nicht allein über diesen und dessen Aufzeichnungen verfügen, da dies Sache des Netzbetreibers ist, zumal der Smart Meter, also das Computersystem selber, in dessen Eigentum steht.

Als Tathandlung müsste der Täter in dieses Computersystem Daten eingeben oder übermitteln. In diesem Sinne sind z. B. die Einführung von Computerviren, Computerwürmern oder sog. Trojaner bzw. große Datenmengen vorstellbar, die Auswirkungen auf das Computersystem haben.[131] Vorliegend ist die Tathandlung des Täters die, dass er z. B. Daten in Form eines Trojaners in sein Smart Meter-System eingibt, um dessen Stromaufzeichnung zu manipulieren.

Der Taterfolg müsste sich sodann unmittelbar in einer schweren Störung der Funktionsfähigkeit des Computersystems niederschlagen, ohne dass dies mit einem Vermögensschaden wie bei § 126a Abs. 1 StGB verbunden sein muss.[132] Der Angriff stellt dann eine schwere Störung dar, wenn das Computersystem bzw. bestimmte Dienste vollkommen lahmgelegt oder so verlangsamt sind, dass der verbleibende Gebrauchswert dieses Computer-

---

130 Salzburger Kommentar, *Daxecker*, § 126b Rz. 21; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 261 Rz. 4.

131 *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 261 Rz. 5.

132 Allerdings wird die Ansicht vertreten, dass die systematische Stellung des § 126b StGB bei den Vermögensdelikten nahelege, dass sich die schwere Störung auch anhand der finanziellen Aufwendungen zu orientieren habe, die notwendig sei, um die Funktionsfähigkeit des Computersystems wiederherzustellen, WK-StGB, *Reindl-Krauskopf*, § 126b Rz. 12; *dies.,* Computerstrafrecht, S. 33.

systems für den Betroffenen quasi gleich Null ist.[133] Ebenfalls maßgeblich sollte in diesem Zusammenhang die Dauer der Störung sein.[134] Problematisch ist, dass das Computersystem in Form des Smart Meters durch die Eingabe des Trojaners bzw. Virenprogramms grds. nicht stillgelegt sein wird, da es weiterhin die Stromverbrauchswerte des Täters an den Netzbetreiber übermittelt, nur eben in manipulierter und damit nicht in objektiv richtiger Form. Aber auch wenn der Smart Meter durch die Manipulation weder vollkommen lahm gelegt noch erheblich verlangsamt worden ist, so funktionieren dennoch bestimmte wesentliche Dienste und Funktionen nicht mehr oder falsch, da die Berechnung und die Übermittlung manipulierter Daten in Form der Stromverbräuche aufgrund der objektiven Unrichtigkeit gerade nicht dem Willen des Netzbetreibers entsprechen wird, sodass der Gebrauchswert des Smart Meters, dessen vordringlicher Sinn die Erfassung und Übermittlung objektiv richtiger Stromverbrauchswerte liegt, für den Netzbetreiber gegen Null laufen dürfte. Die Intention des Netzbetreibers wird durch die Übersendung der manipulierten Daten genauso wenig erfüllt, als wenn der Smart Meter gar keine Stromdaten schicken würde. Damit liegt eine schwere mechanische Störung des Smart Meter-Systems des Täters vor, da die Stromverbrauchsermittlung nicht mehr korrekt bzw. falsch funktioniert. Aus diesem Grund ist wohl folgende Definition passender: Eine schwere Störung ist jede negative Abweichung vom ordnungsgemäßen und bestimmungsgemäßen Verarbeitungsablauf.[135]

Dabei handelt der Täter auch vorsätzlich. Der Täter, der sein Smart Meter zum Zwecke einer niedrigeren Abrechnung manipuliert, hat nämlich v.a. Schädigungsvorsatz und nimmt dabei auch die Störung des Computersystems billigend in Kauf.

Sofern eine Strafbarkeit des Täters nach § 126b StGB einschlägig ist, steht § 126b StGB in Tateinheit zu § 148a StGB. Allerdings muss zuvor beachtet werden, dass, sobald – wovon in diesem Szenario auszugehen ist – eine Datenbeschädigung nach § 126a StGB einschlägig ist, § 126b StGB dahin-

---

133 EB zur RV 11666 BlgNR XXI.GP 28; Salzburger Kommentar, *Daxecker*, § 126b Rz. 3; WK-StGB, *Reindl-Krauskopf*, § 126b Rz. 10; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 262 Rz. 6 m.w.N.

134 *Beer*, Convention on Cybercrime, S. 153.

135 *Beer*, Convention on Cybercrime, S. 153.

ter zurücktritt. Wurde jedoch § 126a mangels Wiederherstellungsaufwands ausnahmsweise nicht verwirklicht, kommt § 126b StGB als Auffangtatbestand aufgrund der schweren mechanischen Störung zur Anwendung.

2.4.10. Zwischenergebnis

Mit der Manipulation des eigenen Smart Meters zum Zwecke der Aufzeichnung niedrigerer Stromverbrauchswerte ist es sehr wohl vorstellbar, dass sich der Täter wegen Datenbeschädigung nach § 126a Abs. 1 StGB strafbar macht. Eine Ausnahme ist nur dann gegeben, wenn dem Netzbetreiber aufgrund der für 60 Tage im eichpflichtigen Teil des Smart Meters vorhandenen objektiv richtigen Stromverbrauchswerte kein Wiederherstellungsaufwand und damit auch kein Schaden entsteht. Darüber hinaus kommt u.U. in Abhängigkeit der Schadenshöhe zudem die Verwirklichung der Qualifikation nach § 126a Abs. 2 StGB in Betracht. Für den Fall, dass § 126a StGB ausnahmsweise nicht einschlägig sein sollte, kommt § 126b StGB als Auffangtatbestand wegen Störung der Funktionsfähigkeit eines Computersystems zur Anwendung. Sofern im konkreten Fall sowohl § 126a StGB als auch § 126b StGB einschlägig sind, tritt § 126b aufgrund einer gesetzlichen Subsidiarität hinter § 126a StGB zurück. Sowohl § 126a als auch § 126b stehen in Tateinheit mit dem betrügerischen Datenverarbeitungsmissbrauch nach 148a StGB.

2.4.11. Missbrauch von Computerprogrammen gem. § 126c StGB

Ferner stellt sich die Frage, ob sich der Täter im Rahmen seiner Manipulationen auch wegen Missbrauchs von Computerprogrammen oder Zugangsdaten nach § 126c Abs. 1 StGB (in Umsetzung von Art. 6 CCC) strafbar macht. Das setzt voraus, dass er ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a StGB), einer Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB), eines missbräuchlichen Abfangens von Daten (§ 119a StGB), einer Datenbeschädigung (§ 126a StGB), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a StGB) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung (Z 1) oder ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein

Computersystem oder einen Teil davon ermöglichen (Z 2), mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, es zur Begehung einer der in Z 1 genannten strafbaren Handlungen zu gebrauchen. § 126c StGB sanktioniert als abstraktes Gefährdungsdelikt somit die Vorbereitungshandlungen zu den in § 126c Abs. 1 Z 1 StGB explizit aufgezählten Computerstraftatbeständen als Hauptdelikte. Ziel ist es, der Computerkriminalität bereits im Vorfeld zu begegnen.[136]

Als Tatmittel werden allerdings nicht sämtliche Computerprogramme erfasst, sondern nur solche, die explizit für derartige kriminelle Verwendungszwecke im oben genannten Sinne geschaffen worden sind.[137] Umfasst sind somit u.a. typische Hackerprogramme zum Einstieg in fremde Computer, Trojaner, Keylogger, Computerviren bzw. schädliche Programme, um Daten zu verändern oder zu löschen.[138] Diese Computerprogramme müssen für die deliktischen Zwecke entweder geschaffen oder adaptiert worden sein. Das heißt, sie müssen entweder bereits ursprünglich zu diesen Zwecken hergestellt, also programmiert, worden sein oder diese „kriminelle" Eigenschaft muss den fertigen Computerprogrammen im Nachhinein dazu programmiert worden sein.[139] Ebenfalls kommen vergleichbare Vorrichtungen zur Begehung der aufgezählten Delikte tatbestandlich in Betracht. Dies sind sämtliche notwendige Gerätschaften, v.a. Hardware.[140] Schließlich sind auch die Zugangsdaten nach § 126c Abs. 1 Z 2 StGB umfasst, sofern sie den Zugriff auf ein Computersystem bzw. einen Teil dessen ermöglichen können (z. B. Passwörter, Zugangscodes). Hinsichtlich der Manipulation der Smart Meter sind nur derartige Computerprogramme gemeint, die in der Lage sind, die Aufzeichnung der Stromverbrauchswerte in der Weise zu stören, dass regelmäßig niedrigere Stromverbrauchswerte gemessen und an den Netzbetreiber versendet werden, was z. B. bei Trojanern oder Computerviren der Fall ist.

Als Tathandlungen kommen hinsichtlich der Manipulation der Smart Me-

136 NK-StGB, *Kargl*, § 202c Rz. 3; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 263 Rz. 1.
137 BVerfG 18.05.2009, 2 BvR 2233/07, 2 BvR 1151/08, 2 BvR 1524/08.
138 WK-StGB, *Reindl-Krauskopf*, § 126c Rz. 8.
139 *Beer*, Convention on Cybercrime, S. 184.
140 *Schuh*, Computerstrafrecht, S. 129.

ter-Daten das Herstellen, Einführen, Verschaffen und Besitzen der jeweiligen Tatmittel in Betracht. Das Herstellen meint jede Art der gebrauchsfertigen Produktion dieser Tatmittel (u.a. die Fertigung von Softwareprodukten und die Generierung von Sicherheitscodes).[141] Unter dem Einführen ist der Import nach Österreich gemeint.[142] Das Sich-Verschaffen setzt voraus, dass der Täter das Tatmittel in seine Verfügungsgewalt bringt.[143] Das Besitzen stellt einen Auffangtatbestand dar, da der, der das Tatmittel hat, dieses zuvor hergestellt bzw. sich verschafft haben muss.[144] Egal, ob der Täter das Programm zur Manipulation seines Smart Meters selber herstellt oder sich dieses verschafft: Vor der Einführung in das Computersystem zu seinen Zwecken wird er es auf jeden Fall besitzen, sodass zumindest diese Tathandlung erfüllt sein wird und er damit den objektiven Tatbestand verwirklicht.

Im subjektiven Tatbestand muss der Täter neben dem üblichen Vorsatz (hier in Form des dolus eventualis) einen erweiterten (Gebrauchs-)Vorsatz dahingehend aufweisen, dass er die Tathandlung nur deshalb ausführt, um sodann mit den Tatmitteln eines der aufgelisteten Delikte zu begehen. Das heißt, der Täter muss bereits bei der Vorbereitungshandlung eine weitere Computerstraftat i.S.v. § 126b Abs. 1 Z 1 StGB im Blick haben. Vorliegend kommt es dem Täter darauf an, den eigenen Smart Meter hinsichtlich seiner tatsächlichen Stromverbräuche zu täuschen, um eine niedrigere Stromrechnung vom Netzbetreiber bzw. Stromlieferanten zu erhalten. Damit ist der Besitz des Computerprogramms nur ein notwendiger Zwischenschritt des Täters auf dem Weg zum betrügerischen Datenverarbeitungsmissbrauch nach § 148a StGB. Folglich handelt der Täter auch mit einem erweiterten Gebrauchsvorsatz.

Vollendet ist die Tat bereits dann, wenn der Täter das Computerprogramm z. B. besitzt, um es für eine der aufgelisteten Straftaten zu verwenden. Auf die tatsächliche Ausführung der dabei beabsichtigten Haupttat kommt es hingegen nicht an.

---

141 NK-StGB, *Kargl*, § 202c Rz. 9; WK-StGB, *Reindl-Krauskopf*, § 126c Rz. 11; *Gercke/Brunst*, Internetstrafrecht, S. 77 Rz. 123.

142 WK-StGB, *Reindl-Krauskopf*, § 126c Rz. 11.

143 NK-StGB, *Kargl*, § 202c Rz. 9.

144 So auch *Schuh*, Computerstrafrecht, S. 132.

Aufgrund des Besitzens des zur Manipulation des Smart Meters geeigneten Computerprogramms macht sich der Täter nach § 126c Abs. 1 StGB strafbar, da es ihm vorliegend explizit darum geht, es v.a. für den betrügerischen Datenverarbeitungsmissbrauch nach § 148a StGB einzusetzen, um seine Stromrechnung zu reduzieren. Dabei tritt jedoch die Strafbarkeit dieses Vorbereitungsdelikts nach § 126c Abs. 1 StGB aufgrund stillschweigender Subsidiarität hinter § 148a StGB und § 126a StGB bzw. § 126b StGB zurück.[145]

2.4.12. Datenfälschung gem. § 225a StGB

Hinsichtlich der Manipulation des eigenen Smart Meters zum Zwecke des Abrechnungsbetrugs kommt schließlich noch eine Strafbarkeit nach § 225a StGB, also wegen Datenfälschung, in Betracht, womit Art. 7 CCC umgesetzt wird. Das erfordert, dass der Täter durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten falsche Daten mit dem Vorsatz herstellt oder echte Daten mit dem Vorsatz verfälscht, dass sie im Rechtsverkehr zum Beweis eines Rechts, Rechtsverhältnisses oder einer Tatsache gebraucht werden. Während § 223 StGB dem Schutz der Urkunden dient, ist es Sinn und Zweck von § 225a StGB, die Echtheit der Daten abzusichern.[146]

Vorliegend könnte das Verfälschen echter Daten, also die Manipulation der objektiv richtigen Stromverbrauchswerte im Smart Meter, durch Eingabe bzw. Veränderung von Daten einschlägig sein, sodass ein falscher Ausstelleranschein erweckt wird.[147] Das bedeutet, dass der Eindruck entstehen soll, dass die manipulierten Stromverbrauchswerte objektiv richtig sind und in dieser Form vom Netzbetreiber aufgezeichnet worden sind. Allerdings sind derartige Stromwerte nicht in der Lage, den zu beweisenden Gedankeninhalt längerfristig zu verkörpern[148], da diese ständig überschrieben werden und sich somit fortlaufend ändern. Zudem scheitert die Strafbarkeit nach dieser Vorschrift spätestens im subjektiven Tatbestand, sodass der objektive Tatbestand an dieser Stelle dahinstehen kann. Der erweiterte

145 Salzburger Kommentar, *Daxecker*, § 126c Rz. 38.
146 *Wegscheider*, Strafrecht BT, S. 372; *Hinterhofer/Rosbaud*, Strafrecht BT II, S. 207 Rz. 1.
147 *Hinterhofer/Rosbaud*, Strafrecht BT II, S. 209 Rz. 5.
148 Salzburger Kommentar, *Thiele,* § 225a Rz. 20 m.w.N.

Vorsatz geht nämlich dahin, diese Fälschung zum Beweis einer Tatsache einzusetzen (Gebrauchsvorsatz). Diese Art Täuschungsvorsatz muss jedoch darauf gerichtet sein, einen anderen Menschen durch Vorlage dieser Täuschung in die Irre zu führen, sodass der Getäuschte veranlasst wird, dem Begehren des Täters nachzukommen.[149] Zwar geht es dem Täter darum, mittels der manipulierten Stromverbrauchswerte eine niedrigere Stromrechnung zu erreichen, jedoch täuscht er dafür keinen Menschen, sondern, im Fall des Smart Meters, einen nicht täuschungsfähigen Computer. Damit entfällt der erforderliche Täuschungsvorsatz und der Täter macht sich nicht der Datenfälschung nach § 225a StGB strafbar.

2.4.13. Ergebnis zu Szenario 2, dem Abrechnungsbetrug

Manipuliert der Täter zum Zwecke einer niedrigeren Stromrechnung seinen klassischen Stromzähler, so macht er sich eines Betruges nach § 146 StGB strafbar, sofern in die Abrechnungserstellung (sei es durch Auswertung einer Karte oder durch das Ablesen der Stromwerte des Täters vor Ort) täuschungsfähige Menschen involviert sind. Unter Umständen begeht der Täter sogar einen qualifizierten Betrug im Sinne des Messbetrugs (§ 147 Abs. 1 Z 1 5. Var. StGB) oder Beweismittelbetrugs (§ 147 Abs. 1 Z 1 4. Var. StGB) bzw. wenn durch seine Tathandlung eine gewisse Schadensgrenzen überschritten wird (§ 147 Abs. 2 und Abs. 3 StGB).

Ist in das Abrechnungsprocedere des klassischen Stromzählers hingegen keine täuschungsfähige Person mehr eingebunden, da die Rechnung automatisch erstellt wird, so macht sich der Täter eines betrügerischen Datenverarbeitungsmissbrauchs nach § 148a Abs. 1 StGB strafbar. Das gleiche gilt für den Fall, dass der Täter nicht seinen klassischen Stromzähler, sondern das Programm seines Smart Meters zum Zwecke einer niedrigeren Stromrechnung derart manipuliert, dass objektiv unrichtige Stromverbrauchswerte aufgezeichnet und sodann an den Netzbetreiber versendet werden, woraufhin der Stromlieferant nach Weiterleitung der Daten durch den Netzbetreiber, automatisch „zu wenig" beim Täter abbucht. Darüber hinaus erfüllt der Täter den Qualifikationstatbestand des § 148a Abs. 2 StGB, sofern der Schaden des Netzbetreibers einen Wert von 3.000 € bzw.

---

149 *Hinterhofer/Rosbaud*, Strafrecht BT II, S. 209 Rz. 9; *Reindl-Krauskopf*, Computerstrafrecht, S. 67.

50.000 € übersteigt. Die Delikte der Datenbeschädigung gem. § 126a Abs. 1 StGB (evtl. in Verbindung mit § 126a Abs. 2 StGB) bzw. die Störung der Funktionsfähigkeit eines Computersystems gem. § 126b StGB stehen dazu in Tateinheit, während der Missbrauch von Computerprogrammen nach § 126c StGB kraft stillschweigender Subsidiarität dahinter zurücktritt. Die Frage, ob der Smart Meter (Hardware) durch die Manipulation i.S.v. § 125 StGB beschädigt oder zerstört wird, muss vorliegend offenbleiben.

2.5. Szenario 3: Pures Hacken eines fremden Smart Meters

Fraglich ist, ob sich der Täter, dem es ausschließlich darauf ankommt, z. B. mittels eines Trojaners in das Computersystem eines fremden Smart Meters (z. B. den Smart Meter des Nachbarn) einzudringen, dieses also zu „hacken“[150], strafbar macht.

2.5.1. Widerrechtlicher Zugriff auf ein Computersystem gem. § 118a StGB

In Betracht kommt in dieser Hinsicht eine Strafbarkeit nach § 118a Abs. 1 StGB[151] wegen widerrechtlichen Zugriffs auf ein Computersystem. Danach macht sich strafbar, wer sich oder einem anderen Unbefugten vorsätzlich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezielle Sicherheitsvorkehrungen des Computersystems überwindet. Dabei muss der Täter die Absicht haben, sich oder einem Dritten Kenntnis von den dort gespeicherten und für ihn nicht bestimmten Daten zu verschaffen, um sie sodann entweder selbst zu benützen, einem anderen Unbefugten zugänglich zu machen bzw. zu veröffentlichen und um sich oder einem Dritten einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen.

Jedoch kann an dieser Stelle dahinstehen, wie sich der Täter Zugang zu dem Computersystem verschafft, da die Strafbarkeit aufgrund der erforderlichen dreifachen überschießenden Innentendenz im subjektiven Tatbestand scheitert, die vorliegend durch den Täter nicht erfüllt wird. So geht es

---

150 Ausführlich dazu: *Beer*, Convention on Cybercrime, S. 39; *Reindl-Krauskopf*, Computerstrafrecht, S. 10 f.

151 Damit erfolgt die Umsetzung von Art. 2 CCC in nationales Recht.

dem Hacker im Zeitpunkt der Tathandlung weder darum, sich Kenntnis von den Daten in Form der Stromverbrauchswerte zu verschaffen noch möchte er diese benützen und er möchte sich schließlich auch nicht bereichern.

Sofern der Täter in diesem Fall lediglich seine computertechnischen Fähigkeiten testen möchte, ohne Daten ausspionieren zu wollen und ohne, dass eine erforderliche Bereicherungs- oder Schädigungsabsicht bei ihm gegeben ist, scheidet eine Strafbarkeit des Hackers wegen widerrechtlichen Zugriffs auf ein Computersystem nach § 118a Abs. 1 StGB aus.

Dieses Ergebnis scheint jedoch rechtspolitisch unbefriedigend zu sein, da diese Strafbestimmung, die gerade für das Hacken geschaffen wurde, die Strafbarkeit erheblich einschränkt und damit der Bekämpfung von wohl künftig eher zunehmenden Hackerangriffen nicht gerecht wird. Dies liegt neben dem Erfordernis im objektiven Tatbestand, dass der Täter eine spezifische Sicherheitsvorkehrung im Computersystem selber überwinden muss, vor allem an den zu hohen Voraussetzungen im subjektiven Tatbestand in Form einer dreifachen Absichtserfordernis (Datenspionage, Datenverwendung und Bereicherung oder Schädigung). Damit wird ein umfänglicher Schutz der (in anderen Bereichen oft auch sensiblen) Daten nicht erreicht, zumal insbesondere das sog. Hacking, bei dem es dem Täter nur darum geht, die Sicherheitsvorrichtungen im Computersystem zu überwinden, ohne dass er eine Bereicherungs- oder Schädigungsabsicht hat, sowie das bloße Lesen und Auskundschaften nicht sanktioniert werden.[152] § 118a StGB schützt die Privatsphäre sowie das Verfügungsrecht über die eigenen Daten. Diese Schutzgüter sind jedoch bereits dann verletzt, wenn der Täter unberechtigterweise vorsätzlich in das gesicherte Computersystem eindringt.[153] Das Eindringen gibt dem Täter sodann objektiv die Möglichkeit, Kenntnis von den geschützten Daten zu erlangen oder diese z. B. zu verändern oder zu löschen.[154] Es erscheint allerdings nicht sachgerecht, die Strafbarkeit derartiger Vorgehensweisen, also z. B. dem Einführen von Trojanern, von weiteren Absichten des Täters abhängig zu ma-

---

152 So auch *Reindl-Krauskopf*, Computerstrafrecht, S. 25; *Schuh*, Computerstrafrecht, S. 83; *Salimi*, Daten und Geheimnisschutz, ÖJZ 2012/115, 998 ff.

153 Dieser stellt quasi einen elektronischen Hausfriedensbruch dar.

154 So auch *Gercke/Brunst*, Internetstrafrecht, S. 69 Rz. 97.

chen, zumal in diesem Bereich auch die Beweisführung recht schwierig sein dürfte, da die Absichtserfordernisse in der Realität nur sehr schwer nachweisbar sein dürften.[155] Zudem wird auch nicht sanktioniert, wer die weitere Verwendungs- und Schädigungsabsicht erst fasst, nachdem er die Daten ausgelesen hat, da diese Absichten bereits bei der eigentlichen Tatbegehung vorliegen müssen. Vor diesem Hintergrund wäre es anzudenken, eine gesetzliche Änderung in der Weise zu erreichen, dass hinsichtlich des objektiven Tatbestandes bedingter Vorsatz ausreichend ist, ohne dass es weiterer Absichten des Täters bei der Tatbegehung bedarf wie es auch in Art. 2 CCC als Möglichkeit vorgesehen und im deutschen Strafrecht der Fall ist.[156] Ziel sollte sein, bereits das schlichte Hacken eines fremden Computersystems unter Überwindung der speziellen Sicherheitsvorkehrung unter Strafe zu stellen.

2.5.2. Missbräuchliches Abfangen von Daten gem. § 119a StGB

Möglich erscheint jedoch eine Strafbarkeit des Täters nach § 119a Abs. 1 StGB, womit Art. 3 CCC umgesetzt wird. Dies setzt voraus, dass der Täter vorsätzlich eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde benutzt oder die elektromagnetische Abstrahlung eines Computersystems auffängt, in der Absicht, sich oder einem Dritten Kenntnis von den übermittelten und für ihn nicht bestimmten Daten zu verschaffen, um sie sodann entweder selbst zu benützen, einem anderen Unbefugten zugänglich zu machen bzw. zu veröffentlichen und um sich oder einem Dritten einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, sofern die Tat nicht nach § 119 StGB[157] mit Strafe bedroht ist. Allerdings hackt der Täter den Smart Meter selber und liest die Daten nicht auf ihrem Übertragungsweg aus. Ferner scheidet aus dem gleichen Grund wie bei § 118a Abs. 1 StGB, also mangels Erfüllung des erweiterten Vorsatzes, eine Strafbarkeit des Täters wegen missbräuchlichen Abfangens von Daten nach § 119a StGB aus.

---

155 So auch *Schuh*, Computerstrafrecht, S. 202, 206; *Salimi*, Daten und Geheimnisschutz, ÖJZ 2012/115, 998, 1000 f.

156 Vgl. § 202a Abs. 1 StGB.

157 Verletzung des Telekommunikationsgeheimnisses.

2.5.3. Datenbeschädigung gem. § 126a StGB

Fraglich ist, ob sich der Täter einer Datenbeschädigung nach § 126a StGB[158] bei seinem Hackerangriff strafbar macht. Dies setzt voraus, dass der Täter automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst unbrauchbar macht bzw. unterdrückt und dadurch einen anderen schädigt. Der Schutzzwecke der Norm liegt darin, Daten vor Zerstörung, nicht aber vor dem reinen Auslesen zu schützen.

Bei den mittels des Smart Meters errechneten Stromverbrauchswerten handelt es sich um automationsunterstützte verarbeitete Daten i.S.v. § 74 Abs. 2 StGB i.V.m. § 4 Z 9 DSG 2000, über die der Täter auch nicht verfügen darf, zumal es sich in diesem Fall sogar um einen fremden Smart Meter und damit auch um fremde Stromverbrauchsdaten handelt. Problematisch ist jedoch, ob der Täter beim reinen Hacken dieses fremden Computersystems die darin enthaltenen Daten verändert. Unter einem Verändern von Daten versteht man die Herstellung eines neuen Informationsgehaltes, z. B. durch inhaltliche Umgestaltung, durch teilweise Löschung oder durch eine veränderte Verknüpfung mit anderen Daten, sodass der ursprüngliche Verwendungszweck dadurch beeinträchtigt bzw. nicht mehr durchführbar ist.[159] Bei der Eingabe von schädigenden Datencodes zum Zwecke des Hackens, also z. B. von Viren oder Trojanern, kann es durchaus sein, dass die Daten und auch die Software verändert werden, da eine Datenmodifizierung stattfindet. [160] Möglich wäre jedoch auch die Variante des sonst Unbrauchbarmachens, sofern die Daten aufgrund der Einwirkung in sonstiger Weise nicht mehr bestimmungsgemäß verwendet werden können.[161] Eine abschließende Entscheidung kann jedoch an dieser Stelle nicht vorgenommen werden, da die Veränderung der Daten eine Frage des jeweiligen Einzelfalls ist.

Durch die Tathandlung müsste der Täter das Vermögen eines anderen

158 Dies dient der Umsetzung von Art. 4 CCC in nationales Recht.

159 *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 258 Rz. 6; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 178 Rz. 594; *Reindl-Krauskopf*, Computerstrafrecht, S. 22.

160 Salzburger Kommentar, *Daxecker*, § 126a Rz. 60 ff.; *Beer*, Convention on Cybercrime, S. 142.

161 *Beer*, Convention on Cybercrime, S. 145.

schädigen. Der Vermögensschaden ist darin begründet, dass der Geschädigte möglicherweise Daten übermittelt bekommt, die in ihrem Vermögenswert nachhaltig durch den Täter verändert worden sind und somit nicht mehr den objektiv richtigen Vermögenswert beinhalten. Maßgeblich für die Schadensberechnung im Rahmen des § 126a Abs. 1 StGB ist allein der unmittelbare Schaden an den Daten selber, also die Summe, die der Geschädigte dafür aufwenden muss, seinen ursprünglichen Datenbestand wiederzubeschaffen (Wiederbeschaffungs- bzw. Wiederherstellungssaufwand).[162] Mittelbare Folgeschäden, wie entgangene Gewinne oder Imageschäden, werden bei der Schadensberechnung hingegen nicht berücksichtigt, selbst wenn die Handlung des Täters diesbezüglich ebenfalls kausal ist.[163] Vorliegend ist es in der Praxis so, dass der Netzbetreiber ein großes Interesse an objektiv richtigen Daten hat. Daher verfügt der Smart Meter zusätzlich zu dem manipulierbaren bzw. hackbaren Teil über einen eichfähigen Teil, auf den hingegen durch den Täter nicht zugegriffen werden kann und der somit immer die korrekten, also objektiv richtigen, Stromwerte aufzeichnet. Diese objektiv richtigen Zählwerte werden sodann aufgrund der gesetzlichen Vorgaben 60 Tage im eichpflichtigen Teil des Smart Meters gespeichert (§ 83 Abs. 2 ElWOG 2010 und § 3 Z 3 IMA-VO 2011). Nach Ablauf dieser 60 Tage werden die Daten jedoch wieder überschrieben und sind somit nicht mehr verfügbar[164] und auch nicht rekonstruierbar. Entdeckt der Netzbetreiber somit aufgrund der Manipulationserkennung innerhalb des Smart Meters innerhalb dieser 60 Tage die Manipulation muss unterschieden werden: Kann der Netzbetreiber auf diesen eichpflichtigen Teil des Smart Meters, also auf die objektiv richten Stromwerte, in der Weise (z. B. online) zugreifen, dass ihm – wie bei einer Sicherheitskopie – kein Wiederherstellungsaufwand entsteht, ist der Tatbestand des § 126a StGB mangels Schadens nicht erfüllt.[165] Muss der Netzbetreiber hingegen (vor Ort) nachsehen, ob der Hackerangriff auf den Smart Meter gleichzeitig auch zugleich zu einer Datenbeschädigung geführt hat und diese sodann evtl. wieder beheben[166], liegt ein Schaden vor, für dessen Berechnung die

---

162 Salzburger Kommentar, *Komenda/Madl*, § 126a Rz. 50; WK-StGB, *Bertel*, § 126a Rz. 5; *Reindl-Krauskopf*, Computerstrafrecht, S. 23; *Sonntag*, Internetrecht, S. 361.

163 *Reindl-Krauskopf*, Computerstrafrecht, S. 24.

164 Erläuterungen zur IMA-VO 2011, S. 4.

165 WK-StGB, *Bertel*, § 126a Rz. 6; *Beer*, Convention on Cybercrime, S. 147; *Sonntag*, Internetrecht, S. 361.

166 In der Praxis ist es jedoch zumeist so, dass im Falle eines Hackerangriffs ein neuer

notwendigen Auslagen für diese Wiederherstellung entscheidend sind (Aufwand für die Rekonstruktion der Daten im gehackten Teil des Smart Meters, Kosten für IT-Experten, Eichung, etc.).[167] Nach Ablauf dieser 60 Tage, wenn also nicht mehr festgestellt werden kann, ob der Hackerangriff auch zu einer Datenbeschädigung geführt hat und die evtl. beschädigten Daten nicht mehr mittels des objektiv richtigen eichpflichtigen Teils wiederhergestellt werden können, bedarf es der Installation eines neuen Smart Meters (inkl. einer neuen Software). Der Schaden bemisst sich sodann nach dem Marktpreis.[168]

Somit macht sich der Täter, der einen fremden Smart Meter hackt, möglicherweise nach § 126a StGB strafbar, wenn es dabei tatsächlich auch zu einer Beschädigung der Daten kommt (Schutzweck der Norm ist nämlich die Datenzerstörung, nicht hingegen der Schutz vor reinem Auslesen). Im Rahmen des Vorsatzes ist davon auszugehen, dass der Täter beim Hacken die Beschädigung der Daten zumindest billigend in Kauf nehmen wird. Konkret kann diese Frage allerdings nur nach den Umständen des Einzelfalls beantwortet werden.

Sofern der finanzielle Schaden an den Daten über 3.000 € bzw. über 50.000 € liegen sollte, so erfüllt der Täter über den Grundtatbestand hinaus zudem eine Qualifikation nach § 126a Abs. 2 StGB.

2.5.4. Störung der Funktionsfähigkeit eines Computersystems gem. § 126b StGB

In Betracht käme allerdings eine Strafbarkeit wegen Störung der Funktionsfähigkeit eines Computersystems nach § 126b StGB. Dies setzt voraus, dass der Täter die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt und diese Tat nicht bereits nach § 126a StGB strafbar ist.

Smart Meter installiert wird, da der gehackte ansonsten auch wieder neu geeicht werden müsste.

167 Salzburger Kommentar, *Komenda/Madl*, § 126a Rz. 52; WK-StGB, *Bertel*, § 126a Rz. 5.

168 Salzburger Kommentar, *Komenda/Madl*, § 126a Rz. 52; WK-StGB, *Bertel*, § 126a Rz. 5.

Unter einem Computersystem versteht man nach der Legaldefinition des § 74 Abs. 1 Z 8 StGB sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen. Somit unterfallen dieser Begriffsbestimmung nicht nur Computernetzwerke, sondern z. B. auch einzelne EDV-Geräte, Handys, Smartcards, Software[169] oder eben auch Smart Meter. Über einen fremden Smart Meter ist der Täter auch keineswegs verfügungsbefugt.

Als Tathandlung müsste der Täter in dieses Computersystem Daten eingeben oder übermitteln. In diesem Sinne sind z. B. die Einführung von Computerviren, Computerwürmern oder sog. Trojaner bzw. große Datenmengen vorstellbar, die Auswirkungen auf das Computersystem haben.[170] Vorliegend ist die Tathandlung des Täters die, dass er z. B. Daten in Form eines Trojaners in das fremde Smart Meter-System eingibt, um in dieses zu gelangen.

Der Taterfolg müsste sich sodann unmittelbar in einer schweren Störung der Funktionsfähigkeit des Computersystems niederschlagen, ohne dass dies mit einem Vermögensschaden wie bei § 126a Abs. 1 StGB verbunden sein muss.[171] Der Angriff stellt dann eine schwere Störung dar, wenn das Computersystem bzw. bestimmte Dienste vollkommen lahmgelegt oder so verlangsamt sind, dass der restliche Gebrauchswert dieses Computersystems für den Betroffenen quasi gleich Null ist.[172] Ebenfalls maßgeblich sollte in diesem Zusammenhang die Dauer der Störung sein.[173] Fraglich ist, ob das Computersystem in Form des Smart Meters durch die Eingabe des Trojaners bzw. Virenprogramms zum Zwecke des reinen Hackens vollkommen stillgelegt sein wird bzw. ob auch eventuelle rechtliche Störungen

---

169 Salzburger Kommentar, *Daxecker*, § 126b Rz. 21; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 261 Rz. 4.

170 *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 261 Rz. 5.

171 Allerdings wird die Ansicht vertreten, dass die systematische Stellung des § 126b StGB bei den Vermögensdelikten nahelege, dass sich die schwere Störung auch anhand der finanziellen Aufwendungen zu orientieren habe, die notwendig sei, um die Funktionsfähigkeit des Computersystems wiederherzustellen, WK-StGB, *Reindl-Krauskopf*, § 126b Rz. 12; *dies.,* Computerstrafrecht, S. 33.

172 EB zur RV 11666 BlgNR XXI.GP 28; Salzburger Kommentar, *Daxecker*, § 126b Rz. 3; WK-StGB, *Reindl-Krauskopf*, § 126b Rz. 10; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 262 Rz. 6 m.w.N.

173 *Beer*, Convention on Cybercrime, S. 153.

(z. B. Verwendungsverbot aus eichrechtlichen Gründen) vom Tatbestand umfasst sind. Dies zu beantworten wird eine Frage des jeweiligen Einzelfalls sein, da es sicher reine Hackerprogramme gibt, die eine schwere (mechanische) Störung der Funktionsfähigkeit des Computersystems bedingen, während andere dies unter Umständen nicht tun.[174]

Problematisch wird beim reinen Hacken auch sein, den Vorsatz des Täters, selbst wenn dieser nur in Form von dolus eventualis vorliegen muss, nachzuweisen, wobei davon auszugehen ist, dass der Täter Störungen des Computersystems billigend in Kauf nehmen wird.

Die Strafbarkeit des reinen Hackers nach § 126b StGB kann an dieser Stelle nicht eindeutig beantwortet werden, da es sich um eine Frage des Einzelfalls handelt und die Strafbarkeit nach § 126b auch davon abhängt, ob bereits eine solche nach § 126a StGB gegeben ist, weil § 126b StGB diesbezüglich subsidiär ist.

2.5.5. Missbrauch von Computerprogrammen oder Zugangsdaten gem. § 126c StGB

Möglicherweise macht sich der Täter im Rahmen seiner Hackerattacke wegen Missbrauchs von Computerprogrammen oder Zugangsdaten nach §126c Abs. 1 StGB (in Umsetzung von Art. 6 CCC) strafbar. Das setzt voraus, dass er ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a StGB), einer Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB), eines missbräuchlichen Abfangens von Daten (§ 119a StGB), einer Datenbeschädigung (§ 126a StGB), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a StGB) geschaffen oder adaptiert worden ist oder eine vergleichbare solche Vorrichtung (Z 1) oder ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen (Z 2), mit dem Vorsatz herstellt, einführt, vertreibt, veräußert,

---

174 Das Hacken eines Smart Meters kann unter Umständen die Unterbindung oder Einschränkung der Kommunikation anderer Smart Meter und eine unzureichende oder nichterfolgte zur Verfügung Stellung von Verbrauchsdaten anderer Kunden zu Folge haben.

sonst zugänglich macht, sich verschafft oder besitzt, es zur Begehung einer der in Z 1 genannten strafbaren Handlungen zu gebrauchen. § 126c StGB sanktioniert als abstraktes Gefährdungsdelikt somit die Vorbereitungshandlungen zu den in § 126c Abs. 1 Z 1 StGB explizit aufgezählten Computerstraftatbeständen als Hauptdelikte. Ziel dabei ist es, der Computerkriminalität bereits im Vorfeld zu begegnen.[175]

Hinsichtlich des objektiven Tatbestands sei an dieser Stelle auf die Ausführungen in Abschnitt 2.4.11 verwiesen.

Im subjektiven Tatbestand muss der Täter neben dem üblichen Vorsatz (hier in Form des dolus eventualis) einen erweiterten (Gebrauchs-)Vorsatz dahingehend aufweisen, dass er die Tathandlung nur deshalb ausführt, um sodann mit den Tatmitteln eines der aufgelisteten Delikte zu begehen. Das heißt, der Täter muss bereits bei der Vorbereitungshandlung eine weitere Computerstraftat i.S.v. § 126b Abs. 1 Z 1 StGB im Blick haben. Im vorliegenden Fall kommt es dem Täter darauf an, einen fremden Smart Meter zu überlisten und diesen zu hacken, also seine Computerfähigkeiten zu testen. Damit ist z. B. der Besitz des Computerprogramms oder anderer Daten, mit denen er den fremden Smart Meter hacken, möchte nur ein notwendiger Zwischenschritt eben zu weiteren Computerstrafbarkeiten. Folglich handelt der Täter auch mit einem erweiterten Gebrauchsvorsatz. Vollendet ist die Tat bereits dann, wenn der Täter das Computerprogramm z. B. besitzt, mit dem Willen, es für eine der aufgelisteten Straftaten zu verwenden. Auf die tatsächliche Ausführung der dabei beabsichtigten Haupttat kommt es hingegen nicht an.[176]
Da § 126c StGB bereits die Vorbereitung unter Strafe stellt, macht sich der Täter aufgrund des Besitzens des zum Hacken eines fremden Smart Meters geeigneten Computerprogramms nach § 126c Abs. 1 StGB strafbar. Ob eines der in § 126c Abs. 1 StGB aufgelisteten Delikte aufgrund der jeweiligen Begehungsweise im Rahmen der Ausführung des Täters sodann tatsächlich verwirklicht wird, ist für eine Strafbarkeit nach § 126c unerheblich. Es reicht aus, wenn der Täter das Tatmittel zum Zeitpunkt des sich Verschaffens bzw. Besitzens für eines der taxativ aufgelisteten Delikte verwenden möchte. Da es in weiterer Folge unerheblich ist, ob diese Tat tatsäch-

175 NK-StGB, *Kargl*, § 202c Rz. 3; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 263 Rz. 1.
176 Salzburger Kommentar, *Daxecker*, § 126c Rz. 29 m.w.N.

lich ausgeführt wird, kann auch dahinstehen, ob einer der Tatbestände im Rahmen der Ausführung tatsächlich verwirklicht wurde.

2.5.6. Datenverwendung in Gewinn- oder Schädigungsabsicht, § 51 DSG 2000

Neben dem StGB finden sich auch Strafbestimmungen im DSG 2000. Nach § 51 Abs. 1 DSG 2000 ist – sofern die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist – zu bestrafen, wer in der Absicht, sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, personenbezogene Daten, die ihm ausschließlich aufgrund seiner beruflichen Stellung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, benützt, insbesondere einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat.

Die Verwirklichung dieses Tatbestands scheitert jedoch einerseits am Benützen. Dies würde voraussetzen, dass der Täter die Daten für einen speziellen Zweck verwenden möchte. Dies ist hier jedoch gerade nicht der Fall, da es dem Täter nur darum geht, seine computerspezifischen Fähigkeiten zu testen, indem er in das Computersystem selber gelangen möchte. Die Daten selber sind hingegen für ihn in diesem Fall ohne Interesse. Aus diesem Grund liegt andererseits auch keine Bereicherungsabsicht, die auf einen Vermögensvorteil gerichtet ist, vor, da er die Daten nicht veräußert und eine Schädigungsabsicht kann ebenfalls nicht nachgewiesen werden. Selbst wenn es der Täter für möglich hält, dass er durch seine Handlung die Geheimhaltungsinteressen der Betroffenen verletzt (dolus eventualis), so ist dies jedoch nicht sein erklärtes Ziel, sodass keine Form der Absicht gegeben ist.

Eine Strafbarkeit des Täters wegen Datenverwendung in Gewinn- oder Schädigungsabsicht nach § 51 DSG 2000 scheidet somit aus.

2.5.7. Ergebnis zu Szenario 3, dem puren Hacken eines fremden Smart Meters

Wer ein fremdes Computersystem (hier in Form eines Smart Meters) einfach nur überlisten, also hacken bzw. Sicherheitslücken aufspüren, möchte, geht unter Umständen weitgehend straflos aus, was man an dieser Stelle rechtspolitisch als unbefriedigend empfinden mag. Dieses Defizit des öster-

reichischen Strafrechts liegt vor allem an der gesetzlichen Ausgestaltung des § 118a StGB. Allerdings gilt das gleiche für § 119a StGB, der ebenfalls das Geheimhaltungsinteresse des Verfügungsberechtigten schützen sollte und diese Strafbarkeit auch von einem weiten subjektiven Tatbestand abhängig macht. Ob eine Strafbarkeit nach § 126a bzw. § 126b StGB gegeben ist, ist eine Frage des jeweiligen Einzelfalls und kann an dieser Stelle nicht beantwortet werden. Unabhängig davon scheint es nicht sinnvoll zu sein, die Strafbarkeit nach § 126a StGB von einem wirtschaftlichen Wiederherstellungsschaden des Opfers abhängig zu machen, da dieses Erfordernis dazu führt, dass eine Strafbarkeit von vorgenommenen Vorsichtsmaßnahmen des Opfers abhängt. Von einer Strafbarkeit nach § 126c Abs. 1 StGB ist hingegen auszugehen.

2.6. Szenario 4: „Ausspähen" von Daten fremder Smart Meter bzw. des Konzentrators für kriminelle Zwecke

Zu untersuchen ist an dieser Stelle die Strafbarkeit des Täters, der die Daten aus fremden Smart Metern bzw. Konzentratoren ausliest bzw. diese auf ihrem Übermittlungsweg zum Netzbetreiber abfängt und anschließend zum Zwecke krimineller Handlungen (z. B. Einbrüche, organisierten Handel mit den Daten, Erpressung, Terrorismus) verwenden möchte.

2.6.1. Widerrechtlicher Zugriff auf ein Computersystem gem. § 118a StGB

In Betracht kommt dabei zunächst ein widerrechtlicher Zugriff auf ein Computersystem nach § 118a StGB, der Art. 2 CCC umsetzt. Danach macht sich strafbar, wer sich oder einem anderen Unbefugten vorsätzlich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezielle Sicherheitsvorkehrungen des Computersystems überwindet. Dabei muss der Täter zunächst die Absicht haben, sich oder einem Dritten Kenntnis von den dort gespeicherten und für ihn nicht bestimmten Daten zu verschaffen, um sie sodann entweder selbst zu benützen, einem anderen Unbefugten zugänglich zu machen bzw. zu veröffentlichen und um sich oder einem Dritten einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen. § 118a StGB schützt die Daten im Computersystem selber und damit sowohl die Privatsphäre als auch das Verfügungsrecht

über die eigenen Daten und dient der Bekämpfung der Computerkriminalität.

Tatobjekt ist somit ein Computersystem bzw. zumindest ein Teil dessen, über das der Täter nicht alleine verfügen darf. Unter einem Computersystem versteht man nach der Legaldefinition in § 74 Abs. 1 Z 8 StGB sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen. Neben der vorhandenen Hardware (inkl. Drucker, Bildschirm, Maus, Handy etc.) ist somit auch die Software (wie z. B. System- und Programmdateien und andere gespeicherte Daten) erfasst, da sie der automationsunterstützenden Datenverarbeitung dient.[177] Damit stellen sowohl der Smart Meter als auch der Konzentrator geeignete Tatobjekte dar, da sie beide Computersysteme sind.

Über dieses Computersystem bzw. Teile dessen, zu dem sich der Täter Zugang verschafft, darf er nicht alleine verfügungsbefugt sein, da das Handeln bei alleiniger Verfügungsbefugnis nicht tatbestandsmäßig wäre. Um ein Ausufern des Tatbestandes in den weitvernetzten Systemen der Computerwelt allerdings zu unterbinden, kommt es entscheidend darauf an, ob der Täter die alleinige Verfügungsbefugnis über das spezielle Computersystem hat, zu dem er sich Zugang verschaffen möchte, wobei die Eigentumsverhältnisse irrelevant sind.[178] Die alleinige Verfügungsbefugnis steht im Rahmen von § 118a StGB demjenigen zu, der das Computersystem verwendet und gestaltet.[179] Hat auch nur eine weitere Person das Nutzungsrecht an diesem Computersystem, so ist der Täter nicht alleine darüber verfügungsbefugt. Auch wenn die aus dem Smart Meter resultierenden Daten im Eigentum des jeweiligen Kunden stehen, steht der Smart Meter, also das Computersystem selber im Eigentum des Netzbetreibers, der auch die Verfügungsbefugnis darüber innehat, da er das System gestaltet, ausliest, etc. Die Verfügungsbefugnis über einen fremden Smart obliegt jedoch keinesfalls dem Täter. Gelangt der Täter somit in ein derartiges Computersystem, also in einen fremden Smart Meter bzw. in den Konzentrator, so

---

177 WK-StGB, *Jerabek/Reindl-Krauskopf/Schroll*, § 74 Rz. 58 f.; *Reindl-Krauskopf*, Computerstrafrecht, S. 12; *Beer*, Convention on Cybercrime, S. 118.

178 *Fischer*, StGB Kommentar, § 202a Rz. 7a; WK-StGB, *Jerabek/Reindl-Krauskopf/Schroll*, § 118a Rz. 13; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 221.

179 *Reindl-Krauskopf*, Computerstrafrecht, S. 13.

macht er sich, sofern die weiteren Tatbestandsvoraussetzungen ebenfalls erfüllt werden, strafbar.

Die Tathandlung besteht darin, dass sich der Täter Zugang zu diesem Computersystem verschafft, indem er spezifische Sicherheitsvorkehrungen überwindet. Der Täter verschafft sich dann Zugang zum Computersystem bzw. Verfügungsgewalt über dieses, wenn er tatsächlich – egal, ob online (z. B. per E-Mail) oder real (also vor Ort) – dermaßen auf den Computer zugreift, dass er innerhalb dessen Systems tätig werden kann, indem er z. B. dort vorhandene Daten liest, verändert oder kopiert.[180] Sofern der Täter also die Daten des Smart Meters / Konzentrators[181] auslesen kann, hat er sich Zugang zu diesen Systemen verschafft. Jedoch reicht diese bloße Zugriffsmöglichkeit auf das Computersystem alleine nicht aus, da der Täter vor dem Zugang zu dem Computersystem noch eine spezifische Sicherheitsvorkehrung überwunden haben muss, da der Tatbestand nur gesicherte Systeme schützt. Um die kriminelle Energie des Täters zu manifestieren, bedarf es nach dem Wortlaut der Norm einer Überwindung eines speziellen Schutzes im Computersystem selber, sodass z. B. das Aufbrechen einer Haus- oder Zimmertüre sowie das Knacken eines Laptopschlosses oder das Rausnehmen einer normalen Tastensperre nicht ausreichen.[182] Als spezifische Computersicherung kommen jedoch u.a. individuell gestaltete Passwörter oder Zugangscodes, eine Firewall bzw. biometrische Sicherungen in Betracht.[183] Diese Sicherungen überwindet der Täter, indem er Handlungen setzt, die geeignet sind, die jeweilige Sicherung auszuschalten, indem er z. B. das richtige Passwort (widerrechtlich) erlangt, „bösartige" Computerprogramme, also z. B. Trojaner oder Viren per E-Mail versendet bzw. installiert oder eine sog. Brute-Force-Attacke durchführt.[184] Dabei

---

180 WK-StGB, *Reindl-Krauskopf*, § 118a Rz. 20; *Gercke/Brunst*, Internetstrafrecht, S. 69 Rz. 97; *Reindl-Krauskopf*, Computerstrafrecht, S. 14; *Beer*, Convention on Cybercrime, S. 120.

181 Über den Konzentrator kommt man nicht an die Daten eines einzelnen Kunden heran, da eine Kundenzuordnung an dieser Stelle nicht möglich ist.

182 WK-StGB, *Reindl-Krauskopf*, § 118a Rz. 23; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 221; *Sonntag*, Internetrecht, S. 354.

183 NK-StGB, *Kargl*, § 202a Rz. 10; WK-StGB, *Reindl-Krauskopf*, § 118a Rz. 25; *Reindl-Krauskopf*, Computerstrafrecht, S. 15.

184 *Fischer*, StGB Kommentar, § 202a Rz. 11b; WK-StGB, *Reindl-Krauskopf*, § 118a Rz. 26; *Beer*, Convention on Cybercrime, S. 122; *Reindl-Krauskopf*, Computerstrafrecht, S. 16.

muss sich der Überwindungsvorgang nicht notwendigerweise direkt gegen die Sicherung als solche richten, sondern diese kann auch schlicht umgangen werden.[185] Im Gegensatz zum Konzentrator ist der Smart Meter mit einer derartigen computerspezifischen Sicherung ausgestattet. Diese kann der Täter jedoch z. B. mit der Einführung eines Trojaners überwinden, wodurch es ihm ermöglich wird, die im Smart Meter enthaltenen Daten zu lesen. Der Schutz des § 118a StGB kommt somit nur speziell gesicherten Computersystemen zu Gute. Da der Konzentrator wohl nicht über eine derartige Sicherung verfügt, die der Täter überwinden muss, scheidet in diesem Fall eine Strafbarkeit an dieser Stelle aus.

In subjektiver Hinsicht muss der Täter den objektiven Tatbestand zunächst vorsätzlich in Form des dolus eventualis erfüllen. Darüber hinaus setzt § 118a Abs. 1 StGB einen dreifach erweiterten Vorsatz in Form der Absicht des Täters voraus: So muss es dem Täter zunächst darauf ankommen, sich oder einem anderen Unbefugten Kenntnis von den Daten des Smart Meters zu verschaffen. Das bedeutet, dass die Kenntnis der speziellen Daten das vordringliche Ziel des Täters sein muss. Ferner muss er die Absicht haben, diese Daten sodann entweder selber zu benutzen, einem anderen Unbefugten zugänglich zu machen oder sie zu veröffentlichen. Schließlich setzt der subjektive Tatbestand zwingend voraus, dass der Täter die Absicht hat, durch die vorherige Verwendungsabsicht der Daten sich oder einem Dritten einen Vermögensvorteil zukommen zu lassen bzw. einem anderen einen Nachteil zuzufügen. Diese Voraussetzungen müssen im Zeitpunkt der Begehung der Tat zwingend vorliegen. Begeht der Täter somit die Tat, verschafft er sich also die Daten, um sie hinterher selber oder mit einem Dritten für weitere kriminelle Handlungen (Erpressung des Netzbetreibers, Einbrüche in Privathaushalten, Handel mit den Daten, etc.) zu verwenden, womit er einem anderen schaden will, so macht er sich nach § 118a StGB strafbar. Dies ist vorliegend der Fall, da der Täter nur deshalb auf den Smart Meter zugreift, um sich die Daten in Form der Stromverbrauchswerte zu verschaffen, die er sodann für kriminelle Zwecke verwenden möchte, womit auch ein Schaden des Netzbetreibers verbunden ist.

Während sich der Täter durch das Ausspähen der Daten aus dem Smart Meter zum Zwecke krimineller Handlungen nach § 118a Abs. 1 StGB

185 *Schuh*, Computerstrafrecht, S. 76.

strafbar macht, ist dies im Falle eines Konzentrators mangels Überwindung einer spezifischen Sicherungsvorkehrung nicht der Fall. Allerdings muss beachtet werden, dass die Strafverfolgung eine Ermächtigung durch den Verletzten voraussetzt (§ § 118a Abs. 2 StGB).

2.6.2. Verletzung des Telekommunikationsgeheimnisses gem. § 119 StGB

Fraglich ist, ob der Täter beim Zugriff auf die Daten des Smart Meters bzw. Konzentrators auch das Telekommunikationsgeheimnis nach § 119 Abs. 1 StGB (Umsetzung von Art. 3 CCC) verletzen kann. Dies ist u.a. dann der Fall, wenn der Täter vorsätzlich eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benutzt, in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer über das Computersystem übermittelten Nachricht, die nicht für ihn bestimmt ist, Kenntnis zu verschaffen. Die Neufassung der Norm beinhaltet somit, dass nunmehr auch Computersysteme erfasst werden. Geschütztes Rechtsgut ist der Inhalt von Nachrichten auf ihrem Weg der Übertragung von einem Computersystem zum anderen (also nicht der Inhalt der Nachricht, die im Computer abgespeichert ist wie bei § 118a StGB).[186] Sanktioniert wird somit das Abfangen der Nachrichten.

Zunächst müsste der Täter eine Vorrichtung, die an einem Computersystem angebracht ist, benutzt haben. Unter einem Computersystem versteht man nach § 74 Abs. 1 Z 8 StGB einzelne oder mehrere untereinander vernetzte Anlagen zur Datenverarbeitung, was auch die Datenübermittlung beinhaltet. Davon ist somit auch der Smart Meter bzw. der Konzentrator umfasst, da diese beiden Einheiten zwecks Datenweiterleitung zum Netzbetreiber verbunden sind. An diesem Computersystem müsste eine Vorrichtung angebracht oder sonst empfangsbereit gemacht worden sein. Als Vorrichtungen kommen sämtliche Einrichtungen in Betracht, die eigens zum Zwecke des Abhörens hergestellt bzw. diesbezüglich adaptiert worden sind, egal, ob es sich um körperliche Gegenstände wie Wanzen oder Mikrofone handelt oder um spezielle Computerprogramme (sog. Schnüffelsoftware).[187] Dabei ist es irrelevant, von wem diese Vorrichtung angebracht

---

186 *Bertel/Schwaighofer*, Strafrecht BT I, § 119 Rz. 1.

187 WK-StGB, *Reindl-Krauskopf*, § 119a Rz. 4; *Reindl-Krauskopf*, Computerstrafrecht, S. 29; *Sonntag*, Internetrecht, S. 357.

worden ist und ob dies rechtmäßig oder rechtswidrig erfolgt ist.[188] Das bedeutet, dass der Täter diese entsprechende Vorrichtung auch extra zum Zwecke der Tat an dem Smart Meter/Konzentrator anbringen bzw. einführen kann. Jedoch genügt das bloße Anbringen der Vorrichtung alleine nicht, sondern es bedarf nach dem Wortlaut der Norm darüber hinaus auch ihrer Benutzung, also ihrer konkreten Verwendung. Verwendet der Täter somit ein spezielles Computerprogramm, um an die übermittelten Daten zu gelangen, erfüllt er diese Tatbestandsvoraussetzung des § 119 Abs. 1 StGB.

Tatobjekt von § 119 StGB sind Nachrichten, die mittels eines Computersystems verschickt werden. Bei den Nachrichten muss es sich um Mitteilungen mit eigenem gedanklichem Inhalt handeln (z. B. E-Mails).[189] Dabei ist es unerheblich, ob der Inhalt dieser Nachricht geheim ist oder nicht, da mittels § 119 Abs. 1 StGB lediglich die Möglichkeit geschützt werden soll, dass eine gewisse Anzahl an Personen mittels eines Computersystems miteinander kommunizieren können, gleichgültig, ob dies leitungsgebunden oder drahtlos verläuft.[190] Problematisch ist vorliegend jedoch, dass nur Menschen in der Lage sind, Gedanken zu äußern, nicht jedoch Computersysteme. Zwar werden im Rahmen der aufgezeichneten Stromwerte menschliche Verhaltensweisen im Zusammenhang mit ihrem Stromverbrauch wieder gespiegelt, jedoch kann der Mensch nicht wirklich Einfluss auf die Aufzeichnung und damit den Inhalt nehmen. Damit stellen die Stromwerte keine Mitteilungen mit gedanklichem Inhalt dar. Zudem findet bei der Übermittlung der Stromwerte durch den Smart Meter über den Konzentrator zum Netzbetreiber keine Kommunikation im eigentlichen Sinne statt, da diese Übermittlung zum einen nicht von Personen ausgeht (der Smart Meter versendet diese Werte automatisch) und zum anderen nicht auf Gegenseitigkeit, in Form eines Hin und Her, ausgerichtet ist.

Somit scheidet eine Strafbarkeit des Täters wegen Verletzung des Telekommunikationsgeheimnisses nach § 119 Abs. 1 StGB aus.

---

188 WK-StGB, *Lewisch*, § 119 Rz. 8; *Bertel/Schwaighofer*, Strafrecht BT I, § 119 Rz. 1.

189 Salzburger Kommentar, *Thiele*, § 119 Rz. 34 m.w.N.; *Reindl-Krauskopf*, Computerstrafrecht, S. 30.

190 *Fischer*, StGB Kommentar, § 202b Rz. 3; *Reindl-Krauskopf*, Computerstrafrecht, S. 30.

2.6.3. Missbräuchliches Abfangen von Daten gem. § 119a StGB

Allerdings kommt subsidiär, also als Auffangtatbestand zu § 119 Abs. 1 StGB, eine Strafbarkeit des Täters wegen missbräuchlichen Abfangens von Daten nach § 119a Abs. 1 StGB in Betracht, der ebenfalls den Übermittlungsweg, hier allerdings von Daten, schützt. Danach macht sich strafbar, wer vorsätzlich eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benutzt oder die elektromagnetische Abstrahlung eines Computersystems auffängt, in der Absicht, sich oder einem Dritten Kenntnis von den über ein Computersystem übermittelten und für ihn nicht bestimmten Daten zu verschaffen, um sie sodann entweder selbst zu benützen, einem anderen Unbefugten zugänglich zu machen bzw. zu veröffentlichen und um sich oder einem Dritten einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, sofern die Tat nicht nach § 119 StGB mit Strafe bedroht ist. Geschützt wird mit diesem Straftatbestand das formelle Geheimhaltungsinteresse an der Nichtöffentlichkeit der Kommunikation mit elektronischen Mitteln.

So setzt der objektive Tatbestand zunächst voraus, dass der Täter eine Vorrichtung, die an einem Computersystem angebracht wurde, benutzt, also in Gang setzt. Unter einer solchen Vorrichtung versteht man sämtliche Einrichtungen, die speziell zum Zwecke des Abfangens von Daten im Zeitraum ihrer Übertragung hergestellt oder eigens dafür adaptiert wurden.[191] Obwohl diese Vorrichtung sowohl körperlicher als auch nicht körperlicher Natur sein kann, wird wohl die Verwendung eines speziellen Computerprogramms am wahrscheinlichsten sein. Der Täter wird ein entsprechend gestaltetes Computerprogramm verwenden, das es ihm ermöglicht, die gewünschten Stromdaten abzufangen. Diese Vorrichtung muss am Computersystem angebracht sein oder zumindest empfangsbereit gemacht worden sein, was im vorliegenden Fall durchaus möglich erscheint. Der objektive Tatbestand setzt schließlich voraus, dass der Täter diese Vorrichtung auch tatsächlich benutzt, also verwendet, um auf die Übermittlung der Daten zuzugreifen.
Alternativ sieht § 119a StGB jedoch auch die Möglichkeit des Auffangens elektromagnetischer Abstrahlungen des Computersystems vor. Darunter

191 *Beer*, Convention on Cybercrime, S. 132.

versteht man u.a. die elektromagnetischen Strahlen beim Arbeitsprozess durch den Bildschirm oder die Signale der Funktastatur, mit denen Dateninhalte rekonstruiert werden können, wobei es entscheidet auf das Auffangen der Daten an sich, nicht hingegen um die tatsächliche Rekonstruktion ankommt.[192] Maßgeblich ist jedoch, dass die Daten (egal, ob verschlüsselt oder nicht, wobei die Stromdaten in der Praxis verschlüsselt übermittelt werden) während des Abstrahlungsvorgangs abgefangen werden (was technisch vorliegend durchaus möglich ist, wenn der Täter z. B. direkt am Kabel steht), da gespeicherte Daten von § 118a Abs. 1 StGB geschützt werden.[193] Fraglich ist, ob die Datenübertragung mittels WLAN/Funk (die Daten werden dabei mittels elektromagnetischer Wellen übertragen) ebenfalls tatbestandsmäßig erfasst ist.[194] Während der Täter bei § 119a Abs. 1 1. Var. StGB eine spezielle Vorrichtung am Computersystem (z. B. in Form eines speziellen Computerprogramms) zur Datenspionage benutzen muss, ist diese „Hürde" in § 119a Abs. 1 2. Var. StGB nicht vorgesehen, da lediglich das Auffangen einer elektromagnetischen Abstrahlung des Computersystems gefordert wird. Der Wortlaut umfasst somit auch die Abstrahlung von Daten, die mittels Funk in einem kabellosen Netzwerk erfolgt.[195] Allerdings ist laut *Reindl-Krauskopf* die Abstrahlung kein Synonym für die Übertragung und sprachlich auch nicht mit dieser gleichzusetzen.[196] Dieses Argument kann an dieser Stelle nicht nachvollzogen werden, zumal eine Gleichsetzung dieser beiden Tatbestandsvoraussetzungen auch gar keinen Sinn machen würde. Ziel des § 119a StGB ist es, das missbräuchliche Abfangen von Daten zu unterbinden. Dabei soll sanktioniert werden, wer sich durch ein Computersystem übermittelte Daten entweder dadurch verschafft, dass er dafür eine am Computer angebrachte Vorrichtung zu Spionagezwecken verwendet oder diese Daten mittels elektromagnetischer Ab-

---

192 WK-StGB, *Reindl-Krauskopf*, § 119a Rz. 10; *Bertel/Schwaighofer*, Strafrecht BT I, § 119a Rz. 2 m.w.N.; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 225 m.w.N.

193 *Fischer*, StGB Kommentar, § 202b Rz. 3; NK-StGB, *Kargl*, § 202b Rz. 4; *Rengier,* Strafrecht BT II, S. 270 Rz. 35 f. Anders sieht dies *Reindl-Krauskopf*, in: WK-StGB, § 119a Rz. 10, wonach das Übertragungsgeheimnis nicht verletzt sei, da der Eingriff nicht am Übertragungsweg ansetze. Jedoch sei dennoch die Privatsphäre desjenigen betroffen, dessen Tätigkeit am Computer aufgrund der Abstrahlung rekonstruiert werden könne.

194 Verneinend *Bertel/Schwaighofer*, Strafrecht BT I, § 119a Rz. 2 m.w.N.

195 So auch: WK-StGB, *Reindl-Krauskopf*, § 119a Rz. 10.

196 WK-StGB, *Reindl-Krauskopf*, § 119a Rz. 10.

strahlung abfängt. Bei der ersten Alternative ist es notwendig, dass der Täter dafür eine Vorrichtung (z. B. ein Programm) benutzt, egal, ob diese bereits am Computer vorhanden ist oder ob er diese erst noch selber anbringen muss. Bei der zweiten Alternative wird hingegen die elektromagnetische Abstrahlung eines Computersystems sanktioniert. Auch wenn bei der ersten Variante eine spezielle Abhöreinrichtung verwendet wird, so bedürfen beide Vorgehensweisen der Aufbringung des gleichen Maßes an krimineller Energie.[197] Mit dem Auffangtatbestand des § 119a Abs. 1 StGB sollen alle Formen nichtöffentlicher, elektronischer Datenübertragung (z. B. E-Mail, Fax, Telefon) erfasst werden und zwar unabhängig davon, ob diese leitungsgebunden, drahtlos oder innerhalb privater Netzwerke erfolgt (z. B. Intranet, WLAN, VPN-Übermittler).[198] Folglich sind auch die kabelgebundenen Netzwerke nicht weniger geschützt als die kabellosen.[199] Einer Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem bedarf es im Gegensatz zu § 118a Abs. 1 StGB hingegen nicht.

Geschützt sind bei § 119a Abs. 1 StGB nicht nur Nachrichten, sondern Daten aller Art i.S.v. § 74 Abs. 2 StGB. Unter Daten fallen personen- und nichtpersonenbezogene Daten sowie Programme, sodass das Kommunikationsgeheimnis umfassend geschützt ist. Der Schutzbereich ist somit weiter gefasst als bei § 119 Abs. 1 StGB der nur Nachrichten erfasst. Während die Nachricht einen Gedankeninhalt beinhaltet, kommt es auf einen solchen bei den Daten nicht an, sodass auch PIN-Codes oder Kreditkartennummern sowie generell Computerdaten umfasst werden.[200] Die im Smart Meter aufgezeichneten Stromverbrauchswerte unterfallen, im Gegensatz zum Begriff der Nachrichten, zweifelsohne dem Begriff der (personenbezogenen) Daten. Diese Daten werden im Wege eines Computersystems übermittelt, also vom Smart Meter des Kunden (Speicherort) über übergeordnete technische Einheiten wie den Datenkonzentrator oder Transaktionsserver zum Netzbetreiber (Zielort). Geschützt sind die Daten somit in diesem Falle nur während des Übertragungs- bzw. Abstrahlungsvorgangs. Diese „fremden" Stromwerte sind auch nicht für den Täter bestimmt.

---

197 A.A. *Reindl-Krauskopf*, in: WK-StGB, § 119a Rz. 10.

198 *Fischer*, StGB Kommentar, § 202b Rz. 3; NK-StGB, *Kargl*, § 202b Rz. 4, *Rengier,* Strafrecht BT II, S. 270 Rz. 35 f.; *Sonntag,* Internetrecht, S. 358; Vgl. auch Salzburger Kommentar, *Thiele*, § 119a Rz. 29.

199 A.A. WK-StGB, *Reindl-Krauskopf*, § 119a Rz. 10.

200 WK-StGB, *Reindl-Krauskopf*, § 119a Rz. 8.

Allerdings ist im Gegensatz zu § 119 Abs. 1 StGB der subjektive Tatbestand enger gefasst, indem er neben dem üblichen Vorsatz eine dreifache überschießende Innentendenz erfordert. So muss sich der Täter nicht nur mittels des Abfangens in der Übermittlungsphase unberechtigterweise Kenntnis von den Daten verschaffen wollen, wie in § 119 Abs. 1 StGB, sondern darüber hinaus auch noch bezwecken, mittels eigener Benutzung, Zugänglichmachen für andere Unbefugte oder Veröffentlichen der Daten sich oder einem anderen einen Vermögensvorteil zu erbringen bzw. einem anderen einen Nachteil zuzufügen (wie in § 118a StGB). Diese Daten muss der Täter somit ausspionieren wollen. An die Spionageabsicht schließt sich die Verwendungsabsicht dieser Daten sowie die Schädigungsabsicht an, wovon im vorliegenden Fall auszugehen ist. Ob der Täter diese Absicht auch wirklich in die Tat umsetzt, ist für die Strafbarkeit nicht relevant, da es lediglich auf die Absicht zum Zeitpunkt der Begehung der Tat ankommt.

Wenn man davon ausgeht, dass der Täter die Daten nicht direkt im Smart Meter oder Konzentrator ausspioniert, sondern erst auf dem Weg ihrer Übertragung (also entweder vom Smart Meter zum Konzentrator/Transaktionsserver bzw. von diesem zum Netzbetreiber) abfängt, um sie sodann für weitere kriminelle Handlungen (wie Erpressung des Netzbetreibers, Einbrüche, Handel mit diesen Daten) verwenden zu wollen, macht sich dieser nach § 119a StGB strafbar, wobei die Tat nur auf Ermächtigung des Verletzten erfolgt (§ 119a Abs. 2 StGB).

Problematisch ist jedoch an § 119a StGB, genau wie bei § 118a StGB, der dreifach erweiterte Vorsatz, der die Strafbarkeit erheblich einengt und unter beweisrechtlichen Gesichtspunkten erschwert. Die mit § 119a StGB bezweckte Vertraulichkeit der Datenübertragung ist bereits bei Kenntniserlangung durch einen Unberechtigten verletzt, wie dies auch bei § 119 StGB der Fall ist. Daher wäre vor dem Hintergrund umfassenden Datenschutzes eine gesetzliche Änderung anzuraten, die auch von Art. 3 CCC gedeckt wäre.

2.6.4. Datenbeschädigung gem. § 126a StGB

Der Täter könnte sich zudem einer Datenbeschädigung nach § 126a Abs. 1 StGB strafbar machen, sofern er beim Zugriff auf das fremde Computersystem Daten beschädigt. Danach macht sich strafbar, wer automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst unbrauchbar macht bzw. unterdrückt und dadurch einen anderen schädigt. Der Tatbestand ist eine besondere Form der Sachbeschädigung, die deshalb nachträglich ins StGB eingeführt wurde, da es sich bei den Daten[201] nicht um körperliche Gegenstände handelt, sodass eine Strafbarkeit nach § 125 StGB ausscheidet. Der Schutzzwecke der Norm liegt somit darin, Daten vor Zerstörung, nicht aber vor dem reinen Auslesen zu schützen.

Bei den Stromwerten, die in dem fremden Smart Meter gespeichert sind, handelt es sich um automationsunterstützt verarbeitete Daten, über die der Täter nicht verfügen darf. Fraglich ist allerdings, ob der Täter durch das reine Auslesen der Stromwerte diese Daten im Smart Meter oder Konzentrator verändert, löscht oder sonst unbrauchbar macht. Der Täter muss auch für das reine Auslesen dieser Daten heimlich, also ohne Einwilligung des Berechtigten, also des Netzbetreibers, z. B. eine Software installieren[202] (damit der fremde Smart Meter mit seinem Computer zum Zwecke der Auslesung kommunizieren kann, wodurch auch die Daten verändert werden). Diese könnte u.U. die Variante der Veränderung bewirken, auch wenn sie keine Funktionsbeeinträchtigung des Smart Meters erfordert, da durch den Übertragungsvorgang die Datenstruktur der Festplatte mit dem Speichervorgang verändert wird.[203] Ansonsten käme jedoch auch die Variante des sonst Unbrauchbarmachens in Betracht, da die Daten möglicherweise aufgrund der Einwirkung in sonstiger Weise nicht mehr bestimmungsgemäß verwendet werden können.[204]

---

201 Gemeint ist somit der Inhalt der Daten und nicht das Medium, auf dem die Daten gespeichert sind.

202 Es gibt in dieser Hinsicht auch andere Möglichkeiten und Vorgehensweisen.

203 *Gercke/Brunst*, Internetstrafrecht, S. 81 Rz. 180.

204 *Beer*, Convention on Cybercrime, S. 145.

Hinsichtlich der weiteren Ausführungen sei auf Abschnitt 2.4.8 und 2.5.3 verwiesen.

Somit macht sich der Täter, der die Daten eines fremden Smart Meter für kriminelle Zwecke ausliest, möglicherweise nach § 126a StGB strafbar, wenn es dabei tatsächlich auch zu einer Beschädigung der Daten und zu einem Wiederherstellungsaufwand für den Netzbetreiber kommt, da die Norm nur vor Zerstörung der Daten, nicht aber vor dem reinen Auslesen schützt. Im Rahmen des Vorsatzes ist davon auszugehen, dass der Täter, auch wenn er die richtigen Stromdaten ausspähen möchte, dabei die Beschädigung der Daten zumindest billigend in Kauf nehmen wird. Konkret kann diese Frage allerdings nur nach den Umständen des Einzelfalls beantwortet werden.

Sofern der finanzielle Schaden an den Daten über 3.000 € bzw. über 50.000 € liegen sollte, so erfüllt der Täter über den Grundtatbestand hinaus zudem eine Qualifikation nach § 126a Abs. 2 StGB.

2.6.5. Störung der Funktionsfähigkeit eines Computersystems gem. § 126b StGB

Fraglich ist, ob sich der Täter beim Auslesen der Daten nach § 126b Abs. 1 StGB strafbar macht. Dies ist dann der Fall, wenn er die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt. Allerdings setzt die Strafbarkeit eine schwere Störung der Funktionsfähigkeit des Computersystems voraus. Genauso wie bei 2.5.4 kann an dieser Stelle nicht beantwortet werden, ob das im Einzelfall durch den Täter verwendete Programm zum Ausspähen der Daten tatsächlich eine schwere Störung der Funktionsfähigkeit des Computersystems, also des Smart Meters/des Konzentrators bedingt, selbst wenn der Netzbetreiber z. B. den Smart Meter möglicherweise austauscht, sobald er von einem solchen Angriff Kenntnis erlangt. Ebenfalls problematisch ist der Nachweis des Vorsatzes des Täters. Sofern eine Strafbarkeit nach § 126a StGB gegeben ist, scheidet eine solche nach § 126b StGB ohnehin aus.

2.6.6. Missbrauch von Computerprogrammen oder Zugangsdaten gem. § 126c StGB

In Betracht kommt ebenfalls eine Strafbarkeit nach § 126c Abs. 1 StGB durch den Täter, womit Art. 6 CCC umgesetzt wird. Dies setzt voraus, dass er ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich u.a. zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a StGB), einer Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB), eines missbräuchlichen Abfangens von Daten (§ 119a StGB) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a StGB) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung (§ 126c Abs. 1 Z 1 StGB) oder ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen (§ 126c Abs. 1 Z 2 StGB) mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Z 1 genannten strafbaren Handlungen gebraucht werden.

An dieser Stelle soll auf die Ausführungen in Abschnitt 2.5.5 verwiesen werden. Es ist davon auszugehen, dass der Täter, der sich vorsätzlich ein spezielles Computerprogramm, das ihm entweder direkten Zugang zum Computersystem ermöglicht (§ 118a StGB) bzw. zum Abfangen von Daten geeignet ist (§ 119a StGB), verschafft, um sich widerrechtlich Kenntnis von den gespeicherten oder übermittelten Stromdaten zu verschaffen, sich wegen des Missbrauchs von Computerprogrammen nach § 126c Abs. 1 StGB strafbar macht, zumal auch der Vorsatz gegeben ist.

2.6.7. Datenverwendung in Gewinn- oder Schädigungsabsicht gem. § 51 DSG 2000

Schließlich kommt zudem eine Strafbarkeit wegen Datenverwendung in Gewinn- oder Schädigungsabsicht nach § 51 DSG 2000 aufgrund des Auslesens fremder Smart Meter-Daten zu kriminellen Zwecken in Betracht. Nach § 51 Abs. 1 DSG 2000 ist – sofern die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist – mit Freiheitsstrafe bis zu einem Jahr zu bestrafen, wer mit dem Vorsatz, sich oder einen Dritten unrechtmäßig zu bereichern oder mit der Absicht, einen anderen in seinem von § 1 Abs. 1 DSG 2000 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich aufgrund seiner beruflichen Stellung anvertraut oder zugänglich geworden sind oder die er sich wider-

rechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat.
Dafür müsste es sich im Rahmen des objektiven Tatbestandes bei den auszulesenden Smart Meter Daten zunächst um personenbezogene Daten handeln. Bei personenbezogenen Daten handelt es sich nach § 4 Z 1 DSG 2000 um solche Angaben über Betroffene, durch die deren Identität bestimmt oder bestimmbar ist. Darunter fallen z. B. Name, Geburtsdatum, Postanschrift, E-Mailadresse, Kontonummer und biometrische Daten, über die der Betroffene zu identifizieren ist.[205] Fraglich ist, ob dies auch bei den Daten des Smart Meters der Fall ist. Der Smart Meter erfasst zunächst den jeweiligen Stromverbrauch und gibt somit Aufschluss darüber, wieviel Strom über diesen Zählpunkt bezogen wird. Diese Stromverbrauchswerte werden sodann für 60 Tage im Gerät selber abgespeichert.[206] Da die Stromverbrauchswerte Rückschlüsse über die Lebensgewohnheiten des Anschlussinhabers ermöglichen[207], ist auch die Identität des Betroffenen über den Zählpunkt zumindest bestimmbar, sodass es sich bei den Verbrauchsdaten um personenbezogene Daten handelt.[208] Daran ändert auch die Tatsache nichts, dass z. B. mehrere Personen in der Wohnung leben und somit alle den Elektrizitätsanschluss nutzen.[209] Dies ist vergleichbar mit einer Telefonnummer, die auch von mehreren genutzt werden kann und dennoch als personenbezogenes Datum gilt.[210]

An diesen personenbezogenen Daten müsste der Betroffene ein schutzwürdiges Geheimhaltungsinteresse haben. Ein schutzwürdiges Geheimhaltungsinteresse ist nach § 1 Abs. 1 S. 2 DSG 2000 dann nicht gegeben, wenn die Daten entweder allgemein verfügbar sind oder nicht zur Rückführbarkeit auf den Betroffenen geeignet sind. Da die durch den Smart Meter aufgezeichneten Verbrauchswerte nicht veröffentlicht werden, sind sie auch nicht für jedermann bzw. die Allgemeinheit bekannt. Zudem können über

---

205 *Jahnel*, Datenschutzrecht, S. 127 f.

206 Ausführlich dazu: *Markl*, Smart Metering und Datenschutz, in: Steinmüller/Hauer/Schneider, Jahrbuch Energiewirtschaft 2011, S. 37 ff.

207 So z.B. wie viele Personen leben im Haushalt? Wann sind diese anwesend?

208 *Buschmann/Motyka*, Energieeffizienz, wbl 2011, 11, 16.

209 Anders ist das jedoch der Fall, wenn der Stromverbrauch von mehreren Wohneinheiten bzw. ganzer Straßenzüge zusammengefasst wird.

210 Datenschutzbehörde 09.08.2006, K121.109/0006-DSK/2006.

die jeweiligen Stromverbrauchswerte die Betroffenen zumindest bestimmt werden. Dieses Geheimhaltungsinteresse an den Daten hat jedoch nicht nur der jeweilige Kunde, sondern ebenfalls der Netzbetreiber[211], der auch als Betroffener i.S.v. § 4 Z 3 DSG 2000 anzusehen ist, da mittels der Daten auch auf die bestehende Kundenbeziehung geschlossen werden kann.[212]

Der Täterkreis ist eingegrenzt: Entweder müssen die Daten dem Täter aufgrund seiner beruflichen Stellung anvertraut bzw. zugänglich gemacht worden sein, wovon hier nicht ausgegangen wird, oder aber der Täter müsste sich die Daten widerrechtlich verschafft haben. Unter ein widerrechtliches Verschaffen fallen sämtliche rechtswidrige Vorgehensweisen, durch die der Täter an die Daten gelangt.[213] Vorliegend gelangt der Täter an die Daten fremder Smart Meter, indem er entweder widerrechtlich auf dieses Computersystem in Form des Hackens nach § 118a StGB zugreift oder aber, indem er die Daten missbräuchlich auf ihrem Übermittlungsweg nach § 119a StGB abfängt. Folglich hat der Täter aktiv und widerrechtlich gehandelt, um an die Daten zu gelangen. Diese müsste er in Folge auch benützen. Das Benützen stellt im Rahmen der Legaldefinition des § 4 Z 9 DSG 2000 einen Unterfall des Verarbeitens von Daten dar, während das Verarbeiten wiederum einen Unterfall des Verwendens (§ 4 Z 8 DSG 2000), also jede Art der Handhabung der Daten, darstellt. Dem Täter kommt es in diesem Szenario darauf an, die Daten auszulesen, um sie sodann für weitere kriminelle Zwecke (sei es Erpressung, Einbrüche oder dergleichen) zu verwenden. Dabei ist es nicht notwendig, dass der Täter in irgendeiner Weise auf die Daten selber einwirkt, relevant ist nur, dass er sich den Inhalt der Daten für seine weiteren kriminellen Aktivitäten (mit Außenwirkung) zu eigen macht.[214] Dies ist hier der Fall, sodass der Täter den objektiven Tatbestand erfüllt.

Der subjektive Tatbestand setzt eine Bereicherungs- bzw. Schädigungsabsicht voraus. Die Bereicherungsabsicht bezweckt einen Vermögensvorteil, also eine Vermögensvermehrung, aufgrund der Verwendung der

211 Nach § 4 Z 3 DSG 2000 werden auch Daten von juristischen Personen geschützt.
212 *Leissler*, Hackattacken, in: Jahnel, Jahrbuch Datenschutzrecht 2012, S. 170.
213 *Salimi*, Daten- und Geheimnisschutz, ÖJZ 2012/115, 998, 1002.
214 *Salimi*, Daten- und Geheimnisschutz, ÖJZ 2012/115, 998, 1002.

Daten.[215] Dies könnte z. B. dann der Fall sein, wenn der Täter die widerrechtlich erlangten Smart Meter-Daten dazu verwendet, den Netzbetreiber zu erpressen. Nicht eindeutig zu beantworten ist die Alternative der Schädigungsabsicht des Täters, die darauf abzielt, einen anderen in seinen Geheimhaltungsinteressen zu schädigen. Da der Wortlaut der Norm explizit Absicht erfordert, muss es dem Täter primär auf die Verletzung dieser Geheimhaltungsinteressen ankommen. Dies wird vorliegend jedoch wohl eher nicht der Fall sein, da es dem Täter in erster Linie darum geht, die ausgelesenen Daten in weiterer Folge für andere kriminelle Zwecke zu verwenden, sodass die Daten lediglich „Mittel zum Zweck" sind.[216] Da die Vorsatzform des dolus eventualis in diesem Zusammenhang nicht ausreichend ist, erscheint nur die Vorgehensweise möglich, dass der Täter die ausgelesenen Daten absichtlich veröffentlicht, um damit nicht nur die Geheimhaltungsinteressen der jeweiligen gehackten Kunden, sondern v.a. die des Netzbetreibers zu verletzen, worum es im wohl vordringlich gehen wird. In diesem Fall wird auch der Netzbetreiber zum Betroffenen eines solchen Angriffs. Der Personenbezug der Stromverbrauchswerte ist dabei darin zu sehen, dass diese Aufschluss über die Geschäftsbeziehung zwischen den Kunden und dem Netzbetreiber geben.[217] Somit ist auch der subjektive Tatbestand erfüllt, sodass sich der Täter wegen Datenverwendung in Gewinn- oder Schädigungsabsicht nach § 51 DSG 2000 strafbar macht.

Allerdings ist die in § 51 DSG 2000 verankerte Subsidiaritätsklausel zu berücksichtigen. Sofern also neben § 51 DSG 2000 noch andere Strafbestimmungen einschlägig sind, kommt es auf das jeweilige Strafmaß an. Da für sämtliche in diesem Szenario (möglicherweise) verwirklichte Delikte (§§ 118a, 119a, 126a, 126b, 126c StGB) nach der aktuellen Rechtslage jedoch nur eine Freiheitsstrafe von höchstens sechs Monaten vorgesehen ist, greift die Subsidiaritätsklausel nicht ein. Das hat zur Folge, dass der Täter diese Delikte in Tateinheit begeht und der Strafrahmen von bis zu einem Jahr Freiheitsstrafe gem. § 51 DSG 2000 zur Anwendung kommt.[218]

---

215 *Jahnel*, Datenschutzrecht, S. 546.
216 *Leissler*, Hackattacken, in: Jahnel, Jahrbuch Datenschutzrecht 2012, S. 169.
217 *Leissler*, Hackattacken, in: Jahnel, Jahrbuch Datenschutzrecht 2012, S. 170.
218 *Leissler*, Hackattacken, in: Jahnel, Jahrbuch Datenschutzrecht 2012, S. 170.

2.6.8. Ergebnis zu Szenario 4, dem Ausspähen von Daten

Liest der Täter die Stromdaten direkt am fremden Smart Meter aus, um diese Daten anschließend für kriminelle Zwecke weiter zu verwenden, macht er sich des widerrechtlichen Zugriffs auf ein Computersystem nach § 118a StGB strafbar, wobei die Tat nur mit Ermächtigung des Verletzten erfolgt. In Tateinheit dazu steht die Strafbarkeit wegen Datenverwendung in Gewinn- oder Schädigungsabsicht gem. § 51 DSG 2000, wobei der höhere Strafrahmen von einem Jahr zur Anwendung kommt. Im Gegensatz zu § 118a StGB handelt es sich bei § 51 DSG 2000 um ein Offizialdelikt.

Werden die Stromwerte hingegen nicht direkt am Smart Meter selber ausgelesen, sondern auf ihrem Übermittlungsweg zum Zwecke weiterer krimineller Handlungen abgefangen, steht das missbräuchliche Abfangen dieser Daten nach § 119a StGB unter Strafe. Zur Verfolgung dieser Tat bedarf es (wie bei § 118a StGB auch) einer Ermächtigung des Verletzten. In Tateinheit dazu steht die Strafbarkeit wegen Datenverwendung in Gewinn- oder Schädigungsabsicht gem. § 51 DSG 2000, wobei der höhere Strafrahmen von einem Jahr zur Anwendung kommt. Im Gegensatz zu § 118a StGB handelt es sich bei § 51 DSG 2000 um ein Offizialdelikt.

Ebenfalls in Tateinheit dazu steht jeweils der Straftatbestand der Datenbeschädigung nach § 126a StGB bzw. der Störung der Funktionsfähigkeit eines Computersystems gem. § 126b StGB. Verwendet der Täter für dieses Auslesen bzw. Abfangen ein geeignetes Computerprogramm, so tritt die Strafbarkeit wegen Missbrauchs von Computerprogrammen nach § 126c kraft stillschweigender Subsidiarität dahinter zurück.

2.7. Szenario 5: Manipulation der Daten fremder Smart Meter / des Konzentrators für kriminelle Zwecke

Schließlich soll die Strafbarkeit des Täters untersucht werden, der die Daten eines fremden Smart Meters / Konzentrators nicht nur ausliest, sondern diese Daten für kriminelle Zwecke (z. B. Angriff auf das Elektrizitätsnetz – u.a. zwecks Vorspiegelung einer hohen/niedrigen Last im Netz, Erpressung, Terrorismus) manipuliert.

2.7.1. Widerrechtlicher Zugriff auf ein Computersystem gem. § 118a StGB

Der Täter könnte sich zunächst wegen des widerrechtlichen Zugriffs auf ein Computersystem nach § 118a Abs. 1 StGB strafbar machen. Dies ist dann der Fall, wenn er sich oder einem anderen Unbefugten vorsätzlich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezielle Sicherheitsvorkehrungen des Computersystems überwindet. Dabei muss der Täter zunächst die Absicht haben, sich oder einem Dritten Kenntnis von den dort gespeicherten und für ihn nicht bestimmten Daten zu verschaffen, um sie sodann entweder selbst zu benützen, einem anderen Unbefugten zugänglich zu machen bzw. zu veröffentlichen und um sich oder einem Dritten einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen.

An dieser Stelle sei auf die Ausführungen in Abschnitt 2.6.1 verwiesen. Der einzige Unterschied ist hier, dass der Täter, nachdem er sich den Zugang zu dem Computersystem, dem Smart Meter (der Konzentrator ist mangels spezifischer Sicherungsvorkehrung vom Schutz des § 118a StGB ausgenommen), verschafft hat, die hinterlegten Daten nicht nur ausliest, sondern diese auch verändert, also manipuliert.

Der Täter macht sich durch die Manipulation eines fremden Smart Meters vor dem Hintergrund krimineller Absichten wegen widerrechtlichen Zugriffs auf ein Computersystem nach § 118a Abs. 1 StGB strafbar. Aufgrund von § 118a Abs. 2 StGB wird die Tat allerdings nur mit der Ermächtigung des Verletzten verfolgt.

2.7.2. Verletzung des Telekommunikationsgeheimnisses gem. § 119 StGB

Fraglich ist, ob zugleich eine Strafbarkeit nach § 119 StGB in Betracht kommt. Dies ist u.a. dann der Fall, wenn der Täter vorsätzlich eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benutzt, in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer über das Computersystem übermittelten Nachricht, die nicht für ihn bestimmt ist, Kenntnis zu verschaffen. Allerdings scheidet eine Strafbarkeit wegen Verletzung des Telekommunikationsgeheimnisses nach § 119 StGB vor allem aus dem Grund aus, da es sich bei

den Stromwerten nicht um Nachrichten handelt und der Täter die Stromwerte nicht auf dem Weg ihrer Übertragung manipuliert, sondern direkt am Smart Meter bzw. Konzentrator.

2.7.3. Missbräuchliches Abfangen von Daten gem. § 119a StGB

Eine Strafbarkeit nach § 119a StGB scheidet ebenfalls aus. Danach macht sich nämlich strafbar, wer vorsätzlich eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde benutzt oder die elektromagnetische Abstrahlung eines Computersystems auffängt, in der Absicht, sich oder einem Dritten Kenntnis von den über ein Computersystem übermittelten und für ihn nicht bestimmten Daten zu verschaffen, um sie sodann entweder selbst zu benützen, einem anderen Unbefugten zugänglich zu machen bzw. zu veröffentlichen und um sich oder einem Dritten einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, sofern die Tat nicht nach § 119 StGB mit Strafe bedroht ist. Der Täter manipuliert jedoch die Stromdaten nicht auf ihrem Weg der Übermittlung zum Netzbetreiber, sondern direkt im fremden Smart Meter bzw. Konzentrator.

2.7.4. Datenbeschädigung gem. § 126a StGB

Aufgrund der Manipulation der Smart Meter Daten (z. B. mittels Computerviren) könnte sich der Täter in Umsetzung von Art. 4 CCC einer Datenbeschädigung nach § 126a StGB strafbar machen. Dies ist dann der Fall, wenn er einen anderen dadurch schädigt, dass er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht alleine verfügen darf, verändert, löscht oder sonst unbrauchbar macht oder unterdrückt.

Unter Daten versteht man nach der Legaldefinition in § 74 Abs. 2 StGB sowohl personenbezogene wie nicht personenbezogene Informationen als auch Programme. Damit handelt es sich bei den Angaben des Smart Meters bzw. des Konzentrators zweifelsohne um Daten, die automatisch verarbeitet werden. Über diese Daten darf der Täter nicht oder nicht alleine verfügen dürfen. Dabei kommt es nicht auf das zivilrechtliche Eigentum son-

dern auf das Alleinverfügungsrecht über die Daten an.[219] Der Täter hat keinesfalls das (Allein-) Verfügungsrecht über die Daten fremder Smart Meter bzw. über Konzentratoren, da dieses dem Netzbetreiber zusteht. Diese Daten müsste der Täter verändern, löschen oder sonst unbrauchbar machen bzw. unterdrücken. Es ist durchaus möglich, dass sich die einzelnen Handlungsalternativen überschneiden, um Strafbarkeitslücken auszuschließen.[220] Allerdings muss sich die Handlung des Täters nachteilig auswirken, sodass Beeinträchtigungen, die sich ohne weiteres beseitigen lassen, nicht tatbestandsmäßig sind.[221] In Betracht käme vorliegend das Verändern. Verändert werden die Daten dann, wenn sie durch eine Handlung des Täters einen neuen Informationsgehalt bekommen und der ursprüngliche Verwendungszweck dadurch beeinträchtigt wird (z. B. das inhaltliche Umgestalten der Daten).[222] Aufgrund der Manipulation z. B. mittels Computerviren durch den Täter sollen die Daten einen neuen Informationsgehalt dahingehend bekommen, dass die Stromwerte z. B. wesentlich höher ausfallen, als es der Realität entspricht.

Durch die Tathandlung müsste der Täter das Vermögen eines anderen schädigen. In dieser Hinsicht sei auf die Ausführungen in 2.4.8 und 2.5.3 verwiesen.

Da der Vorsatz des Täters, der die Stromwerte zu kriminellen Zwecken verändert, zweifelsohne gegeben ist, macht sich dieser wegen Datenbeschädigung nach § 126a Abs. 1 StGB strafbar, wenn dem Netzbetreiber (wovon auszugehen ist) dadurch auch ein Wiederherstellungsaufwand entsteht.

Sofern der finanzielle Schaden an den Daten über 3.000 € bzw. über 50.000 € liegen sollte, so erfüllt der Täter über den Grundtatbestand hinaus zudem eine Qualifikation nach § 126a Abs. 2 StGB.

---

219 *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 257.

220 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 176 Rz. 589.

221 Ebenda.

222 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 178 Rz. 594.

2.7.5. Störung der Funktionsfähigkeit eines Computersystems gem. § 126b StGB

Fraglich ist, ob der Täter bei der Manipulation der fremden Stromwerte innerhalb eines fremden Smart Meters auch eine Störung der Funktionsfähigkeit eines Computersystems nach § 126b StGB (Art. 5 CCC) bewirkt. Dies ist dann der Fall, wenn er die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt. Damit stellt § 126b StGB einen Auffangtatbestand für § 126a StGB dar. Mittels § 126b StGB werden Computersysteme zur Gänze und nicht nur einzelne Daten geschützt.

Unter einem Computersystem versteht man nach der Legaldefinition des § 74 Abs. 1 Z 8 StGB sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen. Somit unterfallen dieser Begriffsbestimmung nicht nur Computernetzwerke, sondern z. B. auch einzelne EDV-Geräte, Handys, Smartcards, Software[223] oder eben auch Smart Meter. Über einen fremden Smart Meter/Konzentrator ist der Täter auch keineswegs verfügungsbefugt.

Hinsichtlich der weiteren Ausführungen sei auf Abschnitt 2.4.9 verwiesen.

Da der Täter vorsätzlich handelt, also zumindest mit dolus eventualis, hat er den Tatbestand des § 126b Abs. 1 StGB erfüllt. Allerdings scheidet vorliegend eine Strafbarkeit wohl aus, da § 126b StGB gegenüber 126a Abs. 1 StGB subsidiär ist.

2.7.6. Missbrauch von Computerprogrammen oder Zugangsdaten gem. § 126c StGB

Zu untersuchen ist, ob der Täter aufgrund der Manipulation der Stromdaten ein Computerprogramm i.S.v. § 126c StGB missbraucht. Dies setzt voraus, dass er ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich u.a. zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a StGB), einer Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB), eines missbräuchlichen Abfangens von Daten (§ 119a StGB) oder eines betrügerischen Datenverarbeitungs-

223 Salzburger Kommentar, *Daxecker*, § 126b Rz. 21; *Birklbauer/Hilf/Tipold*, Strafrecht BT I, S. 261 Rz. 4.

missbrauchs (§ 148a StGB) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung (§ 126c Abs. 1 Z 1 StGB) oder ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen (§ 126c Abs. 1 Z 2 StGB) mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Z 1 genannten strafbaren Handlungen gebraucht werden.
An dieser Stelle sei auf die Ausführungen zu Abschnitt 2.4.11 verwiesen.

Da sich der Täter eines schädlichen Computerprogramms bedienen wird, um sich zu manipulativen Zwecken in das Computersystem einzuhacken, macht er sich wegen Missbrauchs von Computerprogrammen nach § 126c Abs. 1 StGB strafbar, zumal auch hier der erweiterte Vorsatz erfüllt ist.

2.7.7. Datenverwendung in Gewinn- oder Schädigungsabsicht gem. § 51 DSG 2000

Schließlich könnte sich der Täter wegen Datenverwendung in Gewinn- oder Schädigungsabsicht nach § 51 DSG 2000 aufgrund der Manipulation fremder Smart Meter Daten zu kriminellen Zwecken strafbar gemacht haben. Nach § 51 Abs. 1 DSG 2000 ist – sofern die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist – mit Freiheitsstrafe bis zu einem Jahr bestrafen, wer mit dem Vorsatz, sich oder einen Dritten unrechtmäßig zu bereichern oder mit der Absicht, einen anderen in seinem von § 1 Abs. 1 DSG 2000 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich aufgrund seiner beruflichen Stellung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat.

Hinsichtlich der ausführlichen Prüfung sei auf Abschnitt 2.6.7 verwiesen.

Der Täter macht sich auch hier wegen Datenverwendung in Gewinn- oder Schädigungsabsicht nach § 51 DSG 2000 strafbar.

2.7.8. Ergebnis zu Szenario 5, der Manipulation der Daten fremder Smart Meter / des Konzentrators zwecks Störung Netzsteuerung durch den Netzbetreiber

Sofern der Täter in einen fremden Smart Meter eindringt, um dessen Stromwerte zwecks krimineller Vorhaben zu manipulieren, macht er sich wegen eines widerrechtlichen Zugriffs auf ein Computersystem nach § 118a StGB in Tateinheit mit der Datenverwendung in Gewinn- oder Schädigungsabsicht nach § 51 DSG 2000 strafbar, wobei der höhere Strafrahmen von einem Jahr zur Anwendung kommt. Während es sich bei § 118a StGB um ein Ermächtigungsdelikt handelt, stellt § 51 DSG 2000 ein Offizialdelikt dar. Die wohl erfüllte Datenbeschädigung nach § 126a Abs. 1 StGB (evtl. in Verbindung mit § 126a Abs. 2 StGB)[224] steht dazu ebenfalls in Tateinheit, der Missbrauch von Computerprogrammen gem. § 126c StGB tritt hingegen kraft stillschweigender Subsidiarität dahinter zurück.

2.8. Ausblick: Geplante Strafrechtsnovelle

2.8.1. Inhaltliche Zusammenfassung der Richtlinie über Angriffe auf Informationssysteme

Mit der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12.08.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (Cybercrime-RL), die auf dem Übereinkommen des Europarates über Computerkriminalität (CCC) aufbaut und die bis zum 04.09.2015 in nationales Recht umzusetzen ist, sollen die strafrechtlichen Bestimmungen der einzelnen Mitgliedstaaten hinsichtlich der Angriffe auf Informationssysteme angeglichen werden, indem Mindestvorschriften zur Festlegung von Straftaten und einschlägigen Strafen festgelegt werden. Zudem soll die Zusammenarbeit und der Informationsaustausch innerhalb der Mitgliedstaaten in diesem Bereich verbessert werden.[225]

Die Erwägungsgründe der Richtlinie lassen sich folgendermaßen zusam-

---

224 Ansonsten die Störung der Funktionsfähigkeit eines Computersystems nach § 126b StGB.

225 Erwägungsgrund 1 der Richtlinie.

menfassen: Die Informationssysteme sind für die politische, gesellschaftliche und wirtschaftliche Interaktion in der Union unverzichtbar, da die Gesellschaft in hohem Maße von diesen Systemen abhängig ist. Daher sollte auch ein angemessenes Schutzniveau dieser Informationssysteme gewährleistet werden.[226] Angriffe auf die Informationssysteme (auch terroristischer Natur) werden nicht nur in der Union, sondern weltweit zunehmend als Bedrohung angesehen, zumal diese mit immer ausgefeilteren Methoden begangen werden (z. B. Botnetze). Besonders die Störung bzw. Zerstörung kritischer Infrastrukturen (z. B. Kraftwerke, Verkehrsnetze, staatliche Netze) hätte erhebliche grenzüberschreitende Auswirkungen. Zudem ist der wirtschaftliche Schaden durch die Störung der Informationssysteme und der Kommunikation sowie der Verlust oder die Veränderung vertraulicher Informationen oder anderer Daten erheblich. Daher bedarf es der Vereinheitlichung der Straftatbestände für den rechtswidrigen Zugang zu Informationssystemen, den rechtswidrigen Systemeingriff, den rechtswidrigen Eingriff in Daten und das rechtswidrige Abfangen von Daten. Dabei sollten z. B. schwere Strafen vorgesehen werden, wenn die Taten von kriminellen Vereinigungen begangen werden, wenn bei groß angelegten Cyberangriffen eine beträchtliche Anzahl von Informationssystemen beeinträchtigt wird, wenn schwere Schäden verursacht oder ein Botnetz verwendet wird und wenn sich der Angriff gegen eine kritische Infrastruktur richtet. Allerdings soll eine Strafbarkeit ausgeschlossen sein, wenn die Instrumente, also die Hard- und Software, für rechtmäßige Zwecke hergestellt und in den Verkehr gebracht worden sind. Die Strafbarkeit setzt somit den Vorsatz voraus, diese Instrumente für Straftaten verwenden zu wollen. Zum Zwecke der Bekämpfung der Cyberkriminalität sollten die Mitgliedstaaten die erforderlichen Maßnahmen treffen, um die Informationssysteme und die dazugehörigen Daten der kritischen Infrastruktur zu schützen, wobei der Aufwand und die Kosten für einen solchen Schutz im angemessenen Verhältnis zu einem möglichen Schaden stehen müssen.

Die Cybercrime-RL versteht nach **Art. 2 lit. a** unter einem Informationssystem eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung von Compu-

---

226 Dabei muss jede Verarbeitung von Daten dem einschlägigen Unionsrecht über Datenschutz entsprechen.

terdaten durchführen, sowie die von ihr oder ihnen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten, abgerufenen oder übertragenen Computerdaten.

Art. 3 der Cybercrime-RL will zunächst den vorsätzlichen unbefugten Zugang zu einem Informationssystem unter Strafe stellen, wenn dieser unter Verletzung von Sicherheitsmaßnahmen erfolgt und kein leichter Fall vorliegt.

Mittels **Art. 4** der Cybercrime-RL soll die vorsätzliche und unbefugte schwere Behinderung oder Störung des Betriebs eines Informationssystems durch Eingeben von Computerdaten, durch Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern und[227] Unterdrücken von Computerdaten und[228] durch Unzugänglichmachen von Computerdaten bestraft werden, wenn kein leichter Fall vorliegt. Der Versuch soll ebenfalls strafbar sein.

Art. 5 der Cybercrime-RL sieht eine Strafbarkeit für das vorsätzliche und unbefugte Löschen, Beschädigen, Beeinträchtigen, Verändern und Unterdrücken von Computerdaten eines Informationssystems bzw. das Unzugänglichmachen solcher Daten vor, sofern kein leichter Fall vorliegt. Der Versuch soll ebenfalls strafbar sein.

Aufgrund von **Art. 6** der Cybercrime-RL gilt es, das vorsätzliche und unbefugte, mit technischen Hilfsmitteln bewirkte Abfangen nichtöffentlicher Computerdatenübermittlungen an ein Informationssystem, aus einem Informationssystem oder innerhalb eines Informationssystems einschließlich elektromagnetischer Abstrahlungen aus einem Informationssystem zu bestrafen, wenn kein leichter Fall vorliegt.

Aufgrund von **Art. 7** der Cybercrime-RL soll das vorsätzliche und unbefugte Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachung folgender Instrumente, mit der Absicht, eine Straftat im Sinne der Art. 3 bis 6 zu begehen, pönalisiert werden, wenn kein leichter Fall vorliegt: Ein Computerprogramm, das v.a.

---

227 Das „und" sollte wohl als „oder" gelesen werden.

228 Das „und" sollte wohl als „oder" gelesen werden.

dafür hergestellt wurde, diese Straftaten zu begehen sowie ein Computerpasswort, ein Zugangscode oder ähnliche Daten, die den Zugang zu einem Informationssystem ermöglichen.

Die Anstiftung und Beihilfe zu den dargestellten Delikten soll ebenfalls strafbar sein, **Art. 8** der Cybercrime-RL.

Nach **Art. 9** der Cybercrime-RL ist es die Aufgabe der Mitgliedstaaten, die in den Art. 3 bis 8 aufgelisteten Straftaten mit wirksamen, angemessenen und abschreckenden Strafen zu ahnden. So sollen die Straftaten im Sinne der Art. 3 bis 7 der Cybercrime-RL dann mit Freiheitsstrafen im Höchstmaß von mindestens zwei Jahren bestraft werden, wenn kein leichter Fall vorliegt. Straftaten gem. Art. 4 und 5 der Cybercrime-RL sollen mit Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden, sofern eine beträchtliche Anzahl von Informationssystemen beeinträchtigt und dafür ein Instrument i.S.v. Art. 7 verwendet wird. Angriffe nach Art. 4 und 5 der Cybercrime-RL, die im Rahmen einer kriminellen Vereinigung begangen werden, die einen schweren Schaden anrichten oder sich gegen eine kritische Infrastruktur (z. B. Kraftwerk oder Stromnetz) richten, werden in Zukunft mit einer Freiheitsstrafe im Höchstmaß von mindestens fünf Jahren geahndet.

Schließlich sieht **Art. 10** der Cybercrime-RL vor, dass auch juristische Personen für Straftaten im Sinne von Art. 3 bis 8 verantwortlich sein sollen, wenn diese Straftat zu Gunsten der juristischen Person entweder durch eine Führungsperson oder durch eine unterstellte Person aufgrund mangelnder Überwachung oder Kontrolle begangen wurde.

2.8.2. Zwischenergebnis

Um kritische Infrastrukturen, wozu auch Stromnetze und Kraftwerke gehören, besser zu schützen, werden derartige Cyberangriffe künftig härter bestraft. Da solche Angriffe zumeist landesübergreifende Auswirkungen haben, scheint es sinnvoll, ein einheitliches Strafmaß zu finden, sowie die Zusammenarbeit der Mitgliedstaaten in diesem Bereich zu verbessern.

2.8.3. Konsequenzen der unionsrechtlichen Vorgaben für das bestehende österreichische Strafrecht

Um u.a. die Cybercrime-RL umzusetzen, gibt es nunmehr einen Entwurf zum Strafrechtänderungsgesetz 2015, dessen wesentlichen Änderungen im Hinblick auf die projektrelevanten Delikte an dieser Stelle kurz dargestellt werden sollen (ohne jedoch auf die Anhebung der Wertgrenzen einzugehen).

2.8.3.1. Widerrechtlicher Zugriff auf ein Computersystem gem. § 118a StGB

In Umsetzung von Art. 3 der Cybercrime-RL sollen die zu hohen Voraussetzungen im subjektiven Tatbestand in Form einer dreifachen Absichtserfordernis (Datenspionage, Datenverwendung und Bereicherung oder Schädigung) überarbeitet werden. Somit soll künftig nach § 118a Abs.1 Z 1 des Entwurfs bestraft werden, wer sich unbefugt durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem, Zugang zu diesem verschafft, in der Absicht, sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt. Zwar wurde mit diesem Entwurf im Rahmen des Vorsatzes die Absicht der Datenverwendung (zumindest in Abs. 1 Z 1) und Bereicherung bzw. Schädigung gestrichen[229], aber in vielen Fällen (wie vorliegend das Szenario 3) dürfte das pure Hacken fremder Computersysteme weiterhin schwer nachweisbar sein, sodass immer noch Strafbarkeitslücken bestehen. Dies betrifft gerade die Fälle, in denen es dem Täter ausschließlich darum geht, seine Computerfähigkeiten unter Beweis zu stellen und zu testen, ob er das Computersystem überlisten, also hacken kann. Dabei kommt es ihm jedoch gar nicht auf die Kenntniserlangung der in dem jeweiligen Computersystem gespeicherten Daten an, sodass der Nachweis der erforderlichen Absicht (dolus eventualis reicht somit nicht aus), kaum zu erbringen sein wird. Vor diesem Hintergrund wäre es sinnvoll gewesen, bereits den schlichten unbefugten Zugang zu Daten in einem Computersystem unter Überwindung einer speziellen Sicherheitsvorkehrung unter Strafe zu stellen, wie es auch Art. 3 der

229 Auch für § 119a StGB hätte sich eine Überarbeitung des dreifach erweiterten Vorsatzes angeboten.

Cybercrime-RL vorgesehen und z. B. im deutschen Strafrecht (§ 202a StGB) verankert ist. Mit § 118 Abs. 1 Z 2 des Entwurfs soll bestraft werden, wer die Daten oder das Computersystem zum Nachteil eines anderen verwendet. Dies würde, wie jedoch die aktuelle Regelung auch, das Szenario 5 erfassen.

Neu verankert werden soll in § 118a Abs. 2 des Entwurfs die erhöhte Strafbarkeit des Täters, sofern das Computersystem einen wesentlichen Bestandteil einer kritischen Infrastruktur i.S.v. § 74 Abs. 1 Z 11 des Entwurfs darstellt.

2.8.3.2. Datenbeschädigung gem. § 126a StGB

In Anlehnung an Art. 9 Abs. 3 der Cybercrime-RL soll in § 126a Abs. 3 des Entwurfs ein neuer Qualifikationstatbestand in der Form eingeführt werden, dass durch die Tat viele Computersysteme unter Verwendung eines Computerprogramms, eines Computerpasswortes, Zugangscodes oder vergleichbarer Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, sofern diese Mittel nach ihrer besonderen Beschaffenheit ersichtlich dafür geschaffen oder adaptiert wurden, beeinträchtigt oder schwer gestört werden.

Zudem wurde aufgrund von Art. 9 Abs. 4 der Cybercrime-RL ein weiterer Qualifikationstatbestand in § 126a Abs. 4 Z 2 StGB geschaffen, wenn durch die Tat wesentliche Bestandteile der kritischen Infrastruktur beeinträchtigt werden.

Im Rahmen des Entwurfs bleibt jedoch § 126a Abs. 1 StGB unverändert. In Übereinstimmung mit Art. 5 der Cybercrime-RL wäre es jedoch sinnvoll gewesen, das Erfordernis des Schadens in Form eines Wiederherstellungsaufwandes zu streichen. Dieser Wiederherstellungsaufwand entsteht dem Geschädigten nämlich nur dann, wenn er z. B. keine Sicherungskopie dieser Daten zur Hand hat und diese somit wiederherstellen muss. Nur in diesem Fall ist also eine Strafbarkeit des Täters gegeben. Hat der Geschädigte hingegen die Daten noch an einem anderen Ort gespeichert, hat er daher zumeist keinen Wiederherstellungsaufwand und die Strafbarkeit des Täters entfällt. Es scheint allerdings nicht sachgerecht, die Strafbarkeit des Täters von den zuvor getätigten Schutz- und Sicherungsmaßnahmen des

Geschädigten abhängig zu machen, da derartige Schutz- und Sicherungsmaßnahmen zu einer Privilegierung dieses Täters führen würden.[230] Ferner ist der Schutzzweck der Norm darin zu sehen, das Interesse an der Verfügbarkeit der konkreten Daten und deren Fortbestand zu schützen, ohne dass es auf den Wert oder die Wiederherstellbarkeit ankommen sollte. Daher scheint im Vergleich die Regelung im deutschen StGB (auch vor dem Hintergrund des Opferschutzes) sinnvoller zu sein, wonach sich strafbar macht, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert (§ 303a StGB), ohne dass es auf einen darüberhinausgehenden wirtschaftlichen Wiederherstellungsschaden des Opfers ankommt.

2.8.3.3. Störung der Funktionsfähigkeit eines Computersystems gem. § 126b StGB

Es wurden bei § 126b mit dem Entwurf die gleichen Qualifikationen wie bei § 126a StGB vorgeschlagen.

2.8.4. Auswirkungen der geplanten Strafrechtsnovelle auf die Ergebnisse der Begutachtung

An dieser Stelle soll kurz aufgezeigt werden, an welchen Stellen der Begutachtung die Strafrechtsnovelle zu anderen Ergebnissen führen würde.

2.8.4.1. Szenario 1: Stromdiebstahl

- Entziehung von Energie gem. § 132 StGB
  Die Wertgrenzen im Rahmen der Qualifikation des § 132 Abs. 2 StGB sollen von 3.000 € bzw. 50.000 € auf 5.000 € bzw. 500.000 € angehoben werden.

2.8.4.2. Szenario 2: Abrechnungsbetrug

- Schwerer Betrug gem. § 147 StGB
  Auch hier sollen die Wertgrenzen nach § 147 Abs. 2 und Abs. 3 StGB von 3.000 € bzw. 50.000 € auf 5.000 € bzw. 500.000 € angehoben werden.
- Betrügerischer Datenverarbeitungsmissbrauch gem. § 148a StGB

---

230 So auch *Schuh*, Computerstrafrecht, S. 106.

Im Rahmen der Qualifikation des § 148a Abs. 2 StGB ist ebenfalls eine Anhebung der Wertgrenzen von 3.000 € bzw. 50.000 € auf 5.000 € bzw. 500.000 € angedacht.

- Datenbeschädigung gem. § 126a StGB
  Auch hier käme die Anhebung der Wertgrenze auf 5.000 € bzw. 500.000 € zum Tragen.

2.8.4.3. Szenario 3: Pures Hacken eines fremden Smart Meters

- Datenbeschädigung gem. § 126a StGB
  Es käme auch hier die Anhebung der Wertgrenze auf 5.000 € bzw. 500.000 € zur Anwendung.

2.8.4.4. Szenario 4: „Ausspähen" von Daten fremder Smart Meter bzw. des Konzentrators für kriminelle Zwecke

- Widerrechtlicher Zugriff auf ein Computersystem gem. § 118a StGB
  Möglicherweise käme hier zusätzlich die neu zu schaffende Qualifikation zur Anwendung, wenn der Smart Meter als Computersystem ein wesentlicher Bestandteil einer kritischen Infrastruktur ist.
- Datenbeschädigung gem. § 126a StGB
  Es käme auch hier möglicherweise die Anhebung der Wertgrenze auf 5.000 € bzw. 500.000 € zur Anwendung.
- Störung der Funktionsfähigkeit eines Computersystems gem. § 126b StGB
  Sofern eine Strafbarkeit an diesem Punkt nach § 126b StGB überhaupt in Betracht kommt, könnte möglicherweise auch die neue Qualifikation nach § 126b Abs. 4 Z 2 StGB greifen, da die Tat gegen ein Computersystem verübt wird, das möglicherweise ein wesentlicher Bestandteil der kritischen Infrastruktur ist.

2.8.4.5. Szenario 5: Manipulation der Daten fremder Smart Meter / des Konzentrators zwecks Störung der Netzsteuerung durch den Netzbetreiber

- Widerrechtlicher Zugriff auf ein Computersystem gem. § 118a StGB
  Hier ist wohl von davon auszugehen, dass der neu zu schaffende Qualifikationstatbestand nach § 118a Abs. 2 StGB einschlägig wäre,

da es sich bei dem Smart Meter als Computersystem um einen wesentlichen Bestandteil der kritischen Infrastruktur handelt, sodass eine Freiheitsstrafe bis zu zwei Jahren vorgesehen ist.

- Datenbeschädigung gem. § 126a StGB
  Es käme auch hier möglicherweise die Anhebung der Wertgrenze auf 5.000 € bzw. 500.000 € zur Anwendung.
- Datenverwendung in Gewinn- oder Schädigungsabsicht gem. § 51 DSG 2000
  Da vorliegend die neue Qualifikation des § 118a Abs. 2 StGB einschlägig sein dürfte und von einer Ermächtigung des Verletzten ausgegangen wird, greift aufgrund der höheren Strafandrohung die Subsidiaritätsklausel des § 51 DSG 2000.

3. Gesellschaftliche Aspekte

3.1. Privacy in der ökonomischen Literatur

Die ökonomische Literatur beschäftigte sich gerade in jüngerer Zeit intensiv mit der Thematik nutzenbeeinflussender Aspekte von *Privacy* und *Security*. Gerade in Zeiten digitaler Vernetzung und der vermehrt auftretenden Fragestellungen, wie mit privaten Daten auch aus wohlfahrtstheoretischer Sicht umzugehen ist, sind Erkenntnisse dahingehend neben den evidenten sozialen Aspekten auch von zunehmendem wirtschaftlichen Interesse. Dahingehend sind auch theoretische sowie empirische Erkenntnisse aus vorangegangenen Forschungsansätzen von besonderem Wert. So geht die als Informationsökonomie bekannte Wissenschaftsdisziplin auf Autoren wie Hayek (1945), Stigler (1961); und Arrow (1962) zurück, die sich mit der Thematik von Wissen und dessen Entstehung als Innovationsbestandteil auseinandersetzten.

Kritisch ist insbesondere in der Informationsgesellschaft sowie im Energiebereich eine substantielle Informationsasymmetrie, die dann vorherrscht, wenn Konsumenten im Glauben an abgesicherte Datenakquise, -speicherung und -übermittlung entsprechend agieren (siehe auch die Grundsatzforschung asymmetrischer Information von Akerlof, 1970). Dies ist vor allem in Hinblick auf die Detailgenauigkeit und Zuordenbarkeit von

in 15-Minuten-Intervallen gemessenen Stromverbrauchsdaten relevant. Doch auch die für soziale Medien – wie facebook, twitter, etc. – öfters angeführten Aspekte der freiwilligen Informationsausgabe sind für energiewirtschaftliche Fragestellungen von Relevanz. Aus ökonomischen Sicht wurden diese sowohl auf Basis einer theoretischen Fundierung als auch im Hinblick auf dessen empirische Evidenz eingehend untersucht (siehe bspw. Grossman, 1981; Milgrom, 1981 sowie in jüngerer Vergangenheit Acquisti et al., 2015, die insbesondere auf die Problematik der unterschiedlichen Bewertung von *Privacy* hinweisen[231]).

Es gibt aus Sicht der Endkunden im Hinblick auf die betrachteten energiewirtschaftlichen Fragestellungen sowohl Situationen, in denen der Schutz der Privatsphäre zu einer Nutzenoptimierung führen kann, als auch Situationen, respektive Allokationen, in denen dieses Optimum bereits erreicht und überschritten wird. In diesem Fall sind zusätzliche finanzielle Aufwendungen für Sicherheit, Information und Partizipation sowie für technische Lösungen zur Erhöhung des Niveaus an *Privacy* bzw. *Security* nicht mehr zielführend. Diesen *threshold* gilt es aus sozio-ökonomischer Sicht festzustellen und entsprechende Schutzmaßnahmen dahingehend zu verbessern, um dieser Präferenzlage gerecht zu werden.

Dafür ist auf Konsumentenseite jedoch eine intensive Beschäftigung mit dem Thema *Privacy* notwendig. Dies ist auch auf neue (technologische) Entwicklungen zurückzuführen, wie das Beispiel der sozialen Medien eindrucksvoll unter Beweis stellt. So wird in Zukunft der Verbraucher noch besser über die Fähigkeit verfügen müssen, fundierte Entscheidungen über seine Privatsphäre betreffende Aktivitäten treffen zu können. Dies ist vielfach noch kaum oder nicht möglich, da eine intensive Beschäftigung mit dem Thema in den seltensten Fällen erfolgte. Auf Seite der Betreiber von Smart-Grid-Applikationen ist andererseits mittels legistischer bzw. regulatorischer Rahmenbedingungen sicherzustellen, dass es keine asymmetrischen sowie unvollkommenen kommunizierten Informationen gibt. Die Kenntnis der Stromverbrauchsmuster darf beispielsweise nicht zum Nachteil der Konsumenten führen.

---

231 Diese Autoren prägten auch den Ausspruch: "Privacy is difficult to define. It means different things to different people (Solove, 2006)".

Grundsätzlich ist *Privacy* ein schwer zu definierendes Gut. Es wurde vielfach als individuelle Fähigkeit von Personen beschrieben, einen definierten, rein persönlichen, Rückzugsraum zu wahren (Warren und Brandeis, 1890). Darin spielt auch die Kontrolle über und Schutz der persönlichen Daten (Westin, 1967) eine entscheidende Rolle, gerade für Smart Grids der Zukunft. Es stellen sich beispielsweise folgende Fragen:

- Verletzt beispielsweise bereits die Kenntnis der Verbrauchsmuster Aspekte der menschlichen Würde?
- Ist die Autonomie und letztlich die menschliche Freiheit (Schoeman, 1992) höher zu bewerten als die möglichen Effizienzgewinne sowohl in ökonomischer wie auch ökologischer Hinsicht, die gerade Smart Meter in vielfacher Ausführung versprechen (siehe dazu auch Acquisti et al., 2015)?

Ziel dieses und der folgenden Abschnitte ist es nicht, darauf abschließende Antworten zu geben, jedoch auf die zu klärenden Aspekte hinzuweisen. Wichtig ist es festzuhalten, dass in der gesamten Debatte monokausale Ansätze dieser – sehr wichtigen – Thematik keine allumfassenden Lösungen darstellen können und die Einbeziehung interdisziplinärer Forschungsansätze, Politik, Wirtschaft und Endkunden voraussetzt. Es zeigt sich, dass eine umfassendere wissenschaftliche Auseinandersetzung mit der Thematik im Lichte substantieller volkswirtschaftlicher Kosten von Versorgungsunterbrechungen (siehe Reichl et al. 2013) sowie der nicht gänzlich geklärten regulatorischen und gesellschaftspolitischen Aspekte von Smart Grids zu erfolgen hat. Wirtschaftswissenschaftliche Erkenntnisse können dabei unterstützend wirken, jedoch ist eine umfassende Analyse sämtlicher Einflussbereiche vor Festlegung von *privacy*-beeinflussenden Sicherheitsstandards durchzuführen.

3.2. Cybersecurity und Individuum

Dem einzelnen Bürger kommen im Zusammenhang mit Cybersecurity unterschiedliche Rollen zu. Einerseits *fordert* der Einzelne Cybersecurity, also die Sicherheit seiner Daten und der für ihn direkt oder indirekt relevanten und über IKT laufenden Prozesse. In diesem Zusammenhang steht Cybersecurity für eine notwendige Systemeigenschaft von Smart Grids, und damit für eine Leistung des Smart Grids *für* das Individuum. Die essentielle

Bedeutung von Cybersecurity wird im Rahmen der vorliegenden Arbeit postuliert, wobei festzuhalten ist, dass Cybersecurity wie viele Eigenschaften und Bedingungen komplexer Systeme nie entweder *vorhanden* oder *nicht vorhanden* ist. Vielmehr ist die eigentliche Herausforderung, möglichst genau jenes Niveau an Cybersecurity im System Smart Grid zu gewährleisten, das am besten den Trade-off zwischen gewähltem Sicherheitsniveau und Kosten für die Bereitstellung dieses Sicherheitsniveaus ökonomisch effizient abbildet. Daraus leitet sich wiederum ab, dass die Kenntnis über den Wert des Gutes Cybersecurity Voraussetzung ist, um darauf aufbauend Maßnahmen zur Erreichung bestimmter Sicherheitsniveaus und deren Kosten besser einordnen zu können. Der Wert des Gutes Cybersecurity ist nicht direkt aus vorhandenen Daten zu berechnen und bedarf einer gesonderten Betrachtung. Dieser Fragestellung widmet sich ab Juli 2015 eine Arbeitsgruppe im Rahmen der Forschungsinitiative *Referenzarchitektur für sichere Smart Grids in Österreich* (RASSA). Im Rahmen der Tätigkeit dieser Arbeitsgruppe wird international erstmals versucht, die möglichen negativen Auswirkungen durch unzureichende Maßnahmen für eine Smart Grids Cybersecurity auf Haushaltsebene zu erheben und für eine umfassende Vergleichbarkeit zu monetarisieren. Im Rahmen dieses Berichts wird deshalb nicht näher auf die Bedeutung von Cybersecurity und Datensicherheit eingegangen.

Sowie der Einzelne Security als Eigenschaft eines Systems nachfragt, ist Security immer auch vom Verhalten des Einzelnen abhängig, der im Rahmen seiner Interaktion mit der IKT, beruflich oder privat, Einfluss auf die Security des Systems nimmt. Beispielsweise richten sich einige der klassischen Maßnahmen im Security-Bereich auf Zugangsbeschränkungen zu sensiblen Gebäuden oder Gebäudebereichen. Die Einhaltung dieser Zutrittsbeschränkungen ist häufig auch abhängig von der Disziplin des Personals bei der Einhaltung gewisser Abläufe, und wenn die Zugangsbeschränkung für IKT-relevante Gebäudebereiche vom Protokoll abweicht, ist dadurch letztendlich auch die Cybersecurity betroffen. Auf Seiten des Konsumenten besteht jedoch ebenfalls zumindest Restverantwortung, der Einzelne wird unweigerlich Teil der Cybersecurity und bestimmt deren Qualität mit. So hat er im Smart Grid über das Onlineportal seines Netzbetreibers (meist) Zugang zu seinen Lastgängen, für die Sicherheit der Zugangsdaten zu sorgen obliegt aber vollständig dem Einzelnen.

3.3. Cybersecurity durch das Individuum

Entsprechend der Zielsetzung der begleitenden Betrachtung Individuumsspezifischer Co-Determinanten von Cybersecurity im Smart Grid mit den im Projekt evaluierten technischen Maßnahmen, sollen zunächst die im Kontext als zentral erscheinenden Schnittstellen besprochen werden. Dabei wird davon ausgegangen, dass die jeweils relevanten technischen Systeme einwandfrei funktionieren, und dass eine fehlerfreie Bedienung bzw. Wartung sicher hergestellt wurde. Im Besonderen sollen Schnittstellen und mögliche Schwachstellen betrachtet werden, die auf der Haushaltsebene angesiedelt sind und damit nicht unmittelbar *innerhalb* des technischen Systems liegen. Dabei stellen sich vor allem regulatorische sowie gesellschaftspolitisch relevante Problemfelder dar.

3.2.1. Der Haushalt als technische Schnittstelle

Zahlreiche Smart-Grid-Komponenten inkl. ihrer IKT-Anbindung sind vor Ort bei Haushalten installiert. Die Verbreitung von Smart Metern ist entsprechend rechtlicher Vorgaben auf das Niveau von annähernd 100%[232] im Jahr 2020 zu heben. Smart Meter liefern gemessene Energieverbrauchsdaten an den Netzbetreiber, und können im Gegenzug Steuersignale erhalten, wie etwa das Abschalten der Stromversorgung des betroffenen Haushalts[233]. Dementsprechend ist durch technische und administrative Maßnahmen sicherzustellen, dass Steuersignale ausschließlich durch autorisiertes Personal und nach entsprechenden Prüfroutinen abgesetzt werden können. Die in Teil V beschriebenen Maßnahmen zielen unter anderem auf die Sicherstellung entsprechender Systemintegrität.

Insbesondere in den folgenden Punkten unterscheiden sich Bedrohungsszenarien zukünftiger Smart Grids von jenen traditioneller Versorgungskonzepte:

---

232 DAVID-VO 2012 der E-Control, BGBl. II Nr. 313/2012.

233 Anderson, R. and Fuloria, S. 2010. Who controls the off switch? Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on (2010), 96-101.

1. Bedrohungspotential aufgrund systemübergreifender negativer Effekte ausgehend von einer Zugriffsmöglichkeit über konsumentenseitige Smart-Grid-Komponenten (bspw. Smart Meter) auf übergelagerte Infrastrukturen.
2. Innovationen durch Öffnung des Systems *Elektrizitätsmarkt* für eine Vielzahl heterogener Konsumenten (bspw. Haushalte) mit verschiedenen Vorkenntnissen, Einstellungen zur Thematik und Akzeptanz von Energieinfrastrukturen.

Um ein „smartes" Stromnetz der Zukunft bestmöglich auszugestalten, ist es daher unumgänglich, insbesondere folgende Aspekte von kundenseitigen Smart-Grid-Komponenten proaktiv anzudenken und im Gleichklang mit der technischen Implementierung umzusetzen:

- Verhinderung fortschreitender Systemverletzungen (Kaskadeneffekte) von unteren Ebenen auf übergelagerte Infrastrukturen.

Die Möglichkeit auf die kleinste Einheit intelligenter Netzinfrastrukturen – typischerweise Smart Meter – zuzugreifen und in weiterer Folge Zugriff auf andere Smart-Grid-Komponenten, wie Kleinspeicher und Verbrauchsanlagen, zu erhalten, ist mittels systemimmanenter Sicherheitsmechanismen zu verhindern. Gerade die Anfälligkeit der Kategorie menschliches Verhalten ist systemimmanent. Daher gilt es insbesondere ein Versagen in kleinteilig vermaschten Strukturen zu verhindern und technische Lösungen so auszugestalten, dass Manipulationshandlungen nicht systemgrenzenübergreifende Auswirkungen nach sich ziehen können. Diese Sicherheit muss daher systemimmanent sein, da – auch im besten Wissen durchgeführte und somit ohne adverse Vorsätze getätigte – menschliche Aspekte schwer beeinflusst werden können. Wird beispielsweise durch Vorschützen einer vertrauenswürdigen Handlung durch eine Person (was im Zuge einer traditionellen Ablesung den meisten Konsumenten vertraut sein dürfte) Schadsoftware von Dritten im System implementiert, muss ein physischer Zugriff auf übergelagerte Strukturen rein technisch verhindert werden. Gerade das Vorschützen einer vertrauenswürdigen Institution ist aufgrund der langjährigen Kunden-EVU-Beziehung als potenzielle Schwachstelle zu verhindern.

Entsprechend muss die haustechnische Installation und sämtliche Anwendungen, welche durch Smart Meter und Haushalts-IKT steuerbar sind,

dahingehend optimiert werden, dass niemals Gefahr für übergeordnete Systeme bestehen kann. Die daraus abzuleitende Empfehlung ist es, den individuellen Haushalt nicht in die – dennoch vordergründig notwendigen – Sicherheitskonzepte zu integrieren.

- Soziale Medien – insbesondere Facebook und andere „real-time" Applikationen – stellen eine Gefahr für absichtlich herbeigeführte, jedoch nicht primär als schadhaft klassifizierte Handlungen dar.

Wird beispielsweise über koordinierte Aktionen ein „Smart Grid Mob" (in Anlehnung an das vermehrt auftretende Phänomen der Flash Mobs) über Online-Medien verbreitet, kann dies unter Extremverhältnissen zu starken Beeinträchtigungen führen. So kann eine koordinierte positive wie negative Lastveränderung (etwa durch das online koordinierte gleichzeitige Einschalten laststarker Verbrauchsgeräte) Auswirkungen für darauf nicht vorbereitete Netze haben.[234] Als informative Maßnahme muss auf die Bedeutung einer gesicherten Versorgungslage für jeden individuellen Haushalt vermehrt hingewiesen werden. Dies ist in Anbetracht der möglichen sozialen Implikationen von großer Bedeutung.

- Geringe Akzeptanz innovativer Technologien und notwendiger Ausbau- und Sicherheitsmaßnahmen für ein Stromnetz der Zukunft.

Gerade in Hinblick auf die gesellschaftliche Wahrnehmung von Maßnahmen zur Aufrechterhaltung hoher Sicherheits- und Datenintegritätsstandards ist eine proaktive Informationsdissemination von großer Bedeutung. Die, auch in anderen Mitgliedsländern der Europäischen Union beobachtbare, hohe Ablehnungsraten intelligenter Strommess- und -übertragungseinrichtungen stellt auch für die notwendige Bereitstellung entsprechender Sicherheitsmaßnahmen ein großes Hindernis dar.

Wichtig sind jene über alle technischen und organisatorischen Lösungsan-

---

234 Dies beinhaltet – hypothetische – Aktionen wie die Vereinbarung an einem bestimmten Tag um 12 große Verbraucher, wie Backrohr, Klimaanlagen und elektrische Geräte einzuschalten um diese genau 60 Sekunden später wieder vom Netz zu nehmen.

sätze gleichermaßen gültigen Kriterien für die bestmögliche Dissemination der Vor- und Nachteile entsprechender Lösungen.[235] Dies bedingt neben einer vertrauenswürdigen Vorgangsweise eine für den Endkunden möglichst unauffällige Implementierung zur Vermeidung von Nutzeneinbußen. Dies kann beispielsweise in der Sicherstellung rascher Installationszeiten, in der Wahrung der IKT-Kommunikationsqualität und der Vermeidung anderer Einbußen des persönlichen Wohlbefindens sein.

- Gewährleistung von Privacy auf allen Ebenen.

Datenintegrität und -sicherheit ist ein zentraler Baustein erfolgreicher Smart-Grid-Implementierungsstrategien. Ohne die Sicherstellung und Kommunikation der erfolgreichen Aufrechterhaltung sämtlicher Datenstandards ist eine Umsetzung der – sehr ehrgeizigen – Roll-out-Pläne nicht umsetzbar. Verschiedene europäische Forschungsstrategien haben dieses Thema aufgegriffen. Gerade die Geistes-, Kultur- und Sozialwissenschaften sind gefordert, die sozio-ökonomischen Aspekte holistisch zu analysieren um die technischen Lösungsansätze an die gesellschaftliche Wahrnehmung abzustimmen.

- Vermeidung von Service- und Qualitätseinbußen.

Die Frage der gesellschaftlichen Akzeptanz ist entscheidend für den Erfolg geplanter Smart-Grid-Implementierungsstrategien. Insbesondere die Sicherstellung des gewohnten Systemumfelds, geringen Wartungsaufwänden sowie eines hohen Service- und Bedienkomforts sind entscheidend für gesellschaftlich weithin akzeptierte Umsetzungsstrategien. So ist beispielsweise die Möglichkeit der Fernablesung von Zählerständen als positive Verbesserung entsprechend zu kommunizieren. Dennoch sind Sicherheitsstandards entsprechend hoch zu halten, da insbesondere Haushalte aufgrund ihrer Heterogenität besonderen Gefährdungssituationen ausgesetzt sind. Dementsprechend sind neben der technischen Implementierung entsprechende *Awareness*-Kampagnen durchzuführen. Dies soll beispielsweise verhindern, dass sich Dritte Zugang zu sensiblen Schnittstellen u.d.g.

---

235 Siehe diesbezüglich Cohen, Reichl and Schmidthaler (2014). *Re-focussing research efforts on the public acceptance of energy infrastructure: A critical review. Energy – The International Journal Vol. 76. P 4-6.*

verschaffen, indem sie Haushaltskunden fälschlich eine Zugehörigkeit zu einem Netzbetreiber bzw. EVU suggerieren. Die substantiellen Vorteile von integrierten Smart-Grid-Ansätzen sind demnach nur unter Sicherstellung entsprechender technischer sowie verhaltensbezogener (*behavioral)* Begleitmaßnahmen im Bereich Security/Privacy nutzbar.

- Verantwortungsvermeidung in Hinblick auf Haushaltskunden (Netzebene 6 und 7).

Integraler Bestandteil der Umsetzungsstrategie Smart Meter 2020 muss die weitgehende Entlastung von Haushaltskunden sein. So ist eine Übernahme von zusätzlichen Verantwortungen – beispielsweise in Hinblick auf Updates und Interaktionsnotwendigkeiten – weitestgehend zu vermeiden. Dies bezieht sich auf etwaige Pflichten, welche in Verbindung mit intelligenten Zählertechnologien einhergehen können. Entsprechende Realisierungsstrategien müssen dahingehend optimiert werden.

- Berücksichtigung der Kosten für Security- und Privacy-Maßnahmen sowie der volkswirtschaftlich relevanten Vorteile von sicheren, smarten und nachhaltigen Stromnetzen.

Die Vorteile intelligenter Netz- und Messtechnologien sind weitgehend bekannt. Um den Endkunden noch zielgruppengerechter zu adressieren, ist es notwendig, die Vor- und Nachteile auch auf individueller Ebene zu erheben sowie diese sachlich zu kommunizieren. Dies ist insbesondere im Hinblick auf die notwendige Abgeltung sicherheitsbezogener Systemkosten für Netzbetreiber von großer Bedeutung. Eine objektive Erhebung von Kosten und Nutzen entsprechender Technologien muss daher neben den projektspezifischen Aufwendungen (wie etwa moderne Zählertechnologie, Sicherheitsarchitekturen und physische Systemeinrichtungen) auch die Vorteile entsprechend abbilden und den relevanten Entscheidungsträgern zur Verfügung stehen. Insbesondere die Bewertung der als Opportunitätskosten zu kategorisierenden Vorteile von Nicht-Ausfällen der Stromversorgung sowie der Wahrung der Datenintegrität und Persönlichkeitsrechte ist als zentrale Zielsetzung in Implementierungsstrategien vorzusehen. Nur durch die Darstellung etwaiger Nutzen (wie jene der gesicherten Versorgung, einer umfassenden Wahrung von Datenintegrität und -sicherheit, etc.) ist es möglich, Aufwendungen in Sicherheitsmaßnahmen für Politik

und Regulator sichtbar zu machen.[236] Diese können entstehen und der Regulator muss über deren Notwendigkeit entscheiden. Sie werden aber in vielen Fällen negativ auf die Akzeptanz des Smart Grids wirken.

[236] Eine dahingehende Analysemethode liefert beispielsweise die Software www.blackout-simulator.com.

Teil IV: Sicherheitsanalyse

1. Zielsetzung

Ziel dieses Teiles der Arbeiten war die Analyse der Sicherheitseigenschaften von technischen Kernkomponenten aktueller sowie zukünftiger Smart Grids als Basis für die Einschätzung von Bedrohungslagen und Bewertung des Risikos beim Einsatz derartiger Komponenten. Inhaltlich konzentriert sich diese Arbeit auf (i) die Erarbeitung von aktuellen und zukünftigen Angriffsvektoren für Smart-Grid-Infrastrukturkomponenten; (ii) die gezielte Überprüfung ausgewählter Angriffsszenarien in einen Blackbox-Ansatz (d.h. ohne Zusatzinformationen über Komponentendetails wie z. B. Konfiguration und Source-Code); bzw. Glassbox-Ansatz (d.h. mit Zusatzinformationen über Komponentendetails wie z. B. Konfiguration und Source-Code); und (iii) die Konsolidierung der Ergebnisse in einem Analysebericht zu weiteren Bearbeitung im Gesamtprojekt. Wo notwendig, wurden für die Analyse entsprechende Tools und Mechanismen entwickelt, um die speziellen Komponenten in diesem Umfeld ausreichend testen zu können.

2. Vorgehensweise

Nachdem ein vollständiger sowie tiefgehender Security Audit aller Smart-Grid-Komponenten aufgrund des dafür notwendigen finanziellen wie auch zeitlichen Aufwands nicht möglich war, musste in einem ersten Schritt eine gezielte Einschränkung vorgenommen werden. Es wurde bestimmt, welche Systeme des innerhalb des (SG)²-Projektes eingebundenen Herstellers (Siemens) für einen repräsentativen Smart-Grid-Testaufbau herangezogen werden können sowie einem Security Audit zu unterziehen sind. Hierzu wurde das IKT-Architekturmodell (siehe Abschnitt 2.2 in Teil I) sowie die Bedrohungsmatrix (siehe Abschnitt 2.4 in Teil II) herangezogen, sodass Komponenten mit hohem Risiko besonders beachtet und in die Auswahl mit aufgenommen werden können. In mehreren Konsortialsitzungen wurde zudem das gesamte (SG)²-Konsortium inkl. Hersteller und Netzbetreiber in die Auswahl einbezogen, um einen realistischen sowie praktisch rele-

vanten Testaufbau zu erhalten.
Die Auswahlkriterien waren somit im Wesentlichen:

1. Verfügbarkeit der Systeme (Projektpartner Siemens)
2. Kritikalität der Systeme lt. Bedrohungsmatrix
3. Typische Exponiertheit, Zugänglichkeit und potenzielle Auswirkungen der konkreten Systeme bei einem erfolgreichen Angriff bei den Netzbetreibern im Konsortium

In Abbildung 4 ist die Auswahl der entsprechenden Teststellungen als Abbildung auf das IKT-Architekturmodell ersichtlich, wobei die Smart-Grid-Systeme in eine Smart-Metering-Teststellung (AMIS-System des Projektpartners Siemens, in grün dargestellt) und in eine „Secure Substation Automation"-Teststellung (in rot dargestellt) unterteilt wurden. Die Unterteilung erfolgte aus mehreren Gründen. Zum einen konnte so die parallele Durchführbarkeit ermöglicht werden: Während der Projektpartner SEC Consult die Sicherheitstests auf der Smart-Metering-Teststellung durchführte, konnten parallel dazu die Sicherheitstests der Smart-Grid-Komponenten in der „Secure Substation Automation"-Teststellung vom Projektpartner TU Wien (Secure Systems Lab an der Automation Systems Group) übernommen werden. Zum anderen waren die abgebildeten Systeme zur Netzsteuerung („Secure Substation Automation") auch bei den Netzbetreibern im Konsortium stets physisch von den Smart-Metering-Systemen getrennt, sodass die Separierung der Systeme auch der real im Feld umgesetzten Konfiguration entspricht. Die Smart-Metering-Teststellung wurde als portabler „Testkoffer" konzipiert, während die größere „Secure Substation Automation"-Teststellung in Form eines 19"-Racks realisiert wurde.

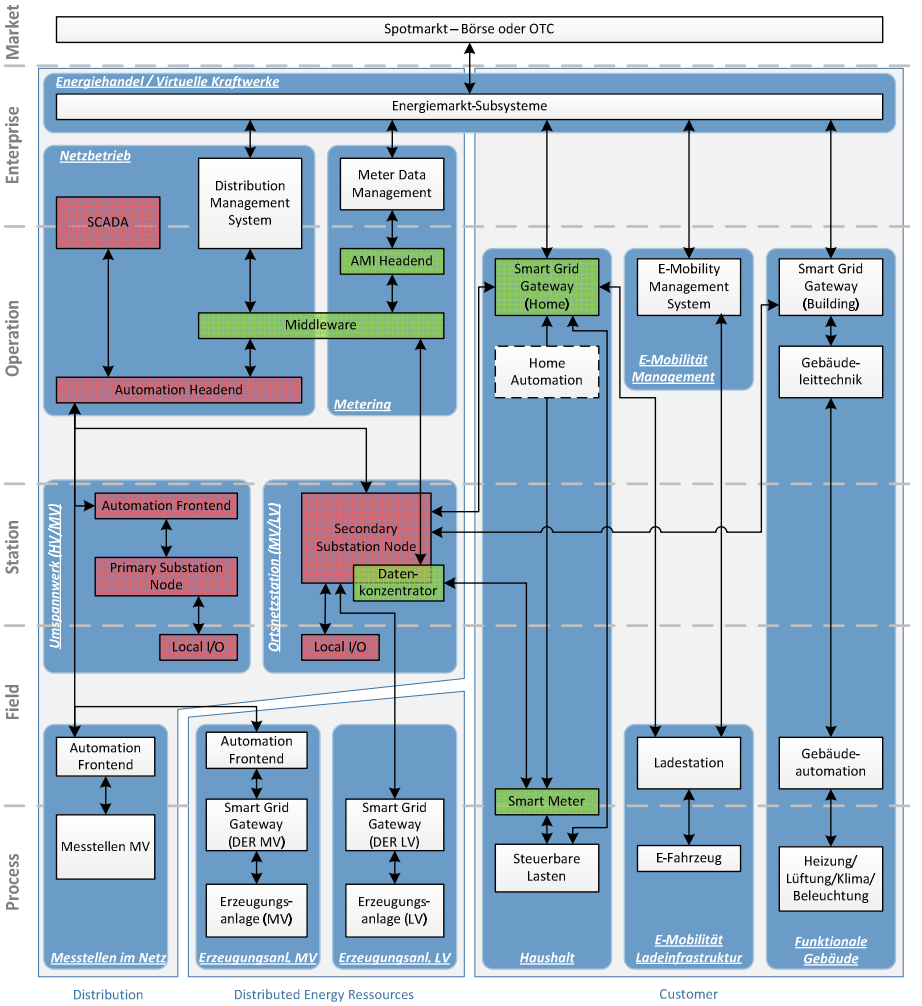


Abbildung 4: Mapping der Teststellungen auf das IKT-Architekturmodell: „Secure Substation Automation“ (rot) und „Smart Metering“ (grün)

Die Teststellungen dienten in weiterer Folge als Ausgangspunkt für die Sicherheitstests an den jeweiligen Smart-Grid-Komponenten. Ein hoher Realitätsbezug wurde sichergestellt, indem bei den Komponenten eine vergleichbare Konfiguration (Firmware, Geräteparametrierung, Verschaltung, etc.) vorhanden war, wie sie auch bei den Netzbetreibern im Konsortium vorhanden ist. Im Rahmen der Sicherheitstests wurden nicht nur die ein-

zelnen Komponenten auf Schwachstellen hin geprüft, sondern auch das Gesamtsystem analysiert. Im Rahmen der Security Audits wurden etwa reale Kommunikationsvorgänge zwischen den Komponenten nachgestellt und diese gleichzeitig mit entsprechenden Sniffing-Werkzeugen aufgezeichnet und anschließend in einem Protokollanalysator analysiert. Die gesammelten Daten dienten in weiterer Folge als Input-Daten für typische Security-Tests wie etwa Fuzz-Tests oder Replay-Angriffe mit manueller Datenmanipulation bei gleichzeitiger Analyse des Geräte- und Firmwareverhaltens auf den Smart-Grid-Komponenten (z. B. über Debug-Schnittstellen wie JTAG).

2.1 Analysearten

Nachdem es aufgrund der im Projekt limitieren Ressourcen nicht möglich war, alle in den beiden Teststellungen enthaltenen Systeme tiefgehend auf ihre Sicherheit hin zu analysieren, wurden zwei unterschiedliche Security-Analyse-Strategien mit unterschiedlicher Analysetiefe definiert:

1. Oberflächenanalyse
2. Tiefenanalyse

Bei der Oberflächenanalyse liegt der Fokus auf den Kommunikationsvorgängen und -schnittstellen zwischen den zu auditierenden Smart-Grid-Komponenten. Auf diese Weise lassen sich etwa Schwachstellen in den eingesetzten Protokollen oder den Mechanismen zum Schutz der Vertraulichkeit, Authentizität oder Integrität identifizieren. Maßgeblich für die Umsetzung der Oberflächenanalysen war es, technische Methoden und Tools zu entwickeln, mit welchen Kommunikation auf den eingesetzten Schnittstellen nicht nur transparent mitgeschnitten sowie analysiert, sondern auch beliebige Nachrichten in die Kommunikation eingeschleust werden können. Im Gegensatz zur sehr aufwändigen Tiefenanalyse wird jedoch bei der Oberflächenanalyse nicht die Firmware auf den Geräten selbst analysiert, um etwa genau herausfinden zu können, wie die Gerätefirmware kritische Vorgänge wie die Authentifizierung oder Verschlüsselung abwickelt. Dies beinhaltet auch Abstürze der Firmware oder Ähnliches. Werden etwa im Zuge von Fuzz-Tests Paketdaten gefunden, die einen Absturz auf dem Gerät verursachen, so kann durch eine Oberflächenanalyse allein nicht herausgefunden werden, warum das Gerät abstürzt bzw. ob sich die

Schwachstelle auch für die Ausführung von eigenem Code (Arbitrary Code Execution) verwenden lässt. Gleichermaßen sind bloße Oberflächenanalysen beim Einsatz von Verschlüsselung im Protokoll nur sehr begrenzt zielführend, ohne weitere Erkenntnisse aus Tiefenanalysen nutzen zu können. Zusammenfassend wurden im Zuge der Oberflächenanalysen folgende Tests durchgeführt:

- Aktive und passive Port Scans
- Protocol Sniffing mit anschließenden Protokollanalysen
- Fuzz Tests
- Manuelles Testing auf Basis von aufgezeichneter Kommunikation (z. B. für Replay Attacks)

Die Tiefenanalyse versteht sich als ergänzender Schritt zur Oberflächenanalyse. Sie umfasst etwa das Extrahieren der Firmware aus den Geräten sowie die statische wie auch dynamische Code-Analyse in einem Disassembler bzw. Debugger. Üblicherweise wurden die Firmwares derartiger Geräte von den Herstellern über viele Jahre hin entwickelt und besitzen daher nicht nur einen großen Umfang, sondern auch eine erhebliche Komplexität. Dies ist auch einer der Gründe, weshalb Tiefenanalysen derart aufwändig sind und somit im $(SG)^2$-Projekt nur bei wenigen Komponenten möglich waren. Die durchgeführten Tiefenanalysen umfassten je nach Analyseanforderungen unter anderem folgende Punkte:

- Analyse des Hardware-Aufbaus
- Extraktion der Firmware
- Disassemblierung der Firmware
- Aufbau einer Debug-Umgebung zur dynamischen Firmware-Analyse in einem Debugger (z. B. mittels JTAG Dongles und geeignetem Software Setup sowie eigens entwickelter Software/Scripts)
- Debugging der Firmware in Kombination mit Fuzz Tests und manuellem Generieren von Test-Stimuli (manuelles Testing)

Die Umsetzung eines Glassbox-Ansatzes war zudem nicht möglich, da der Hersteller keine internen Informationen (wie Quellcode oder Entwickler-Dokumentation) zur Verfügung stellen konnte. Sämtliche Analysen muss-

ten daher weitestgehend über einen Blackbox-Ansatz durchgeführt werden, wobei jedoch die Zugangsdaten oder allgemeine Betriebsinformationen (Bedienungsanleitung) zu den jeweiligen Systemen zur Verfügung gestellt wurden (Greybox).

2.2. Einzelrisikobewertung

Alle gefundenen Sicherheitsrisiken wurden entsprechend der existierenden Methodik des Projektpartners SEC Consult mit einem Risk-Score bewertet. Dieser Risk-Score wird in einer Matrix ermittelt, die sich aus Wahrscheinlichkeit und Schwere der Auswirkungen zusammensetzt (siehe Tabelle 15). Die Wahrscheinlichkeit bezeichnet dabei die Erfolgswahrscheinlichkeit, mit der ein Angreifer den Fehler findet und ausnutzen kann. Die Schwere bezieht sich auf den Schweregrad der Lücke und ihre Auswirkungen. Da der Schweregrad das Risiko wesentlich stärker beeinflusst als die Wahrscheinlichkeit, fließt er quadriert in die Gleichung ein. Durch die Multiplikation von Wahrscheinlichkeit und Quadrat der Schwere ergibt sich der Risk-Score, der eine sehr differenzierte Einschätzung des Risikos, das durch eine Sicherheitslücke entsteht, erlaubt.

Tabelle 15: Einfluss von Wahrscheinlichkeit und Schwere der Auswirkungen auf den Risk-Score

Schwere / **Wahrscheinlichkeit**	**1**	**4**	**9**	**16**	**25**
1	1	4	9	16	25
2	2	8	18	32	50
3	3	12	27	48	75
4	4	16	36	64	100
5	5	20	45	80	125

Um eine einfache textuelle Beschreibung des Risikos zu ermöglichen, wurden die Risk-Scores in vier Kategorien unterteilt (siehe Tabelle 16).

Tabelle 16: Kategorien Risk-Score

Risk-Score	Bewertung
1 – 10	gering
11 – 24	mittel
25 – 60	groß
61 – 125	kritisch

3. Analyse von Smart-Grid-Systemen

3.1. Übersicht der analysierten Komponenten

Vom Konsortialpartner Siemens wurde die „Secure Substation Automation"-Teststellung in Form eines 19" Racks zur Verfügung gestellt, siehe Abbildung 5.

Abbildung 5: „Secure Substation Automation"-Teststellung (SCADA System nicht abgebildet)

Die Teststellung beinhaltete folgende Komponenten:

- Siemens SICAM AK1703 Stationsleitgerät
- Siemens SICAM BC Feldleitgerät
- Siemens SICAM TM Fernwirkgerät mit abgesetzten Peripheriegeräten
- Siemens SICAM CMIC Verteilnetzautomatisierung
- Siemens SIPROTEC 7SJ801 Schutzgerät
- RuggedCom RX1512 Router/Firewall für Datenverkehr im
- Umspannverkehr
- Cisco 2901-SEC/K9 Router/Firewall für Datenverkehr via VPN zur übergeordneten Leittechnik (z. B. Lastverteiler)
- Fujitsu Celsius W420 Leittechnikrechner im Umspannwerk
- Siemens Toolbox, Version 5.10 Projektierung SICAM – Produkte
- Siemens DIGSI, Version 4.87 Projektierung SIPROTEC Schutzgeräte
- Siemens SICAM 230, Version 7 Leittechnik Visualisierung

3.2. Topologie der Komponenten

In Abbildung 6 ist die Topologie für die „Secure Substation Automation"-Teststellung ersichtlich. Symbolisch über dem Bereich „Umspannungswerk" ist die SCADA Umgebung „Control Center" dargestellt. Von ihr aus wird über einen Cisco 2901 Router/Firewall eine VPN Verbindung zum Umspannwerk aufgebaut.

Der RuggedCom-Router im Bereich „Umspannwerk" nimmt die gesicherte VPN-Verbindung entgegen und ermöglicht über die Routing-Funktionalität den Zugriff auf die einzelnen Smart-Grid-Komponenten dahinter. Dies sind im Einzelnen die für das Fernwirken notwendigen Systemkomponenten (TM 1703 mit Aktuatoren/Sensoren), die Systemkomponenten für die Ortsnetz-Automatisierung (CMIC über AK1703 Stationsleitgerät) sowie die äußerst kritischen Schutzsysteme (SIPROTEC Schutzgerät über BC1703 Feldleitgerät).

Zur lokalen Steuerung sowie zur Parametrierung existiert ein lokaler Leittechnikrechner mit NTP Server zur Zeitsynchronisation, SICAM 230 SCADA Software zur Steuerung sowie der SICAM Toolbox II und DIGSI

Software zur Parametrierung der Smart-Grid-Komponenten.

Aus topologischer Sicht sind der RuggedCom-Router sowie die SICAM-CMIC-Komponente besonders gefährdet, da sie für externe Angreifer leichter zugänglich sind als die geschützten Komponenten hinter dem Router bzw. innerhalb des Umspannwerks.

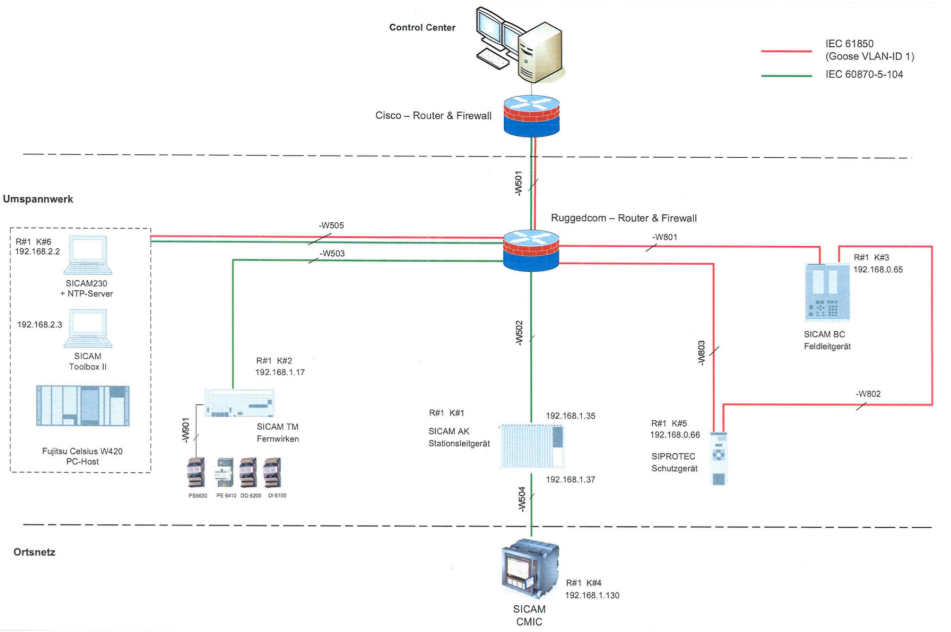


Abbildung 6: Topologieübersicht „Secure Substation Automation"-Teststellung

4. Analyse von Smart-Metering-Systemen

4.1. Übersicht der analysierten Komponenten

Von der Firma Siemens AG wurden zwei identische Testkoffer (siehe Abbildung 7) mit folgenden Komponenten zur Verfügung gestellt:

- Siemens AMIS Smart Meter TD-3510
- Siemens AMIS Datenkonzentrator CP-3410
- Siemens AMIS TM 1703 ACP
- Siemens AMIS Transaktionsserver

Abbildung 7: Testkoffer für die Analyse von Smart-Metering-Systemen

4.2. Topologie der Komponenten

Die Topologie der Testkoffer ist in Abbildung 8 dargestellt.

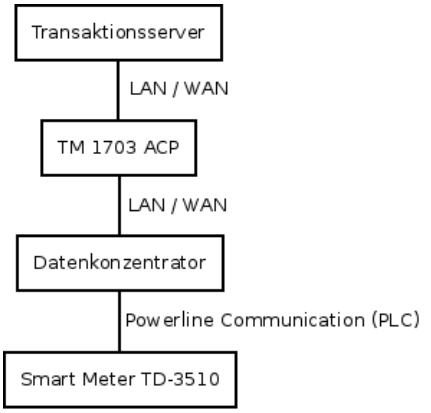


Abbildung 8: Topologie der Teststellung „Smart Metering“

Abbildung 9 zeigt einen typischen Aufbau eines Smart-Metering-Systems. Zusätzlich ist der physische Standort der Komponenten angeführt.

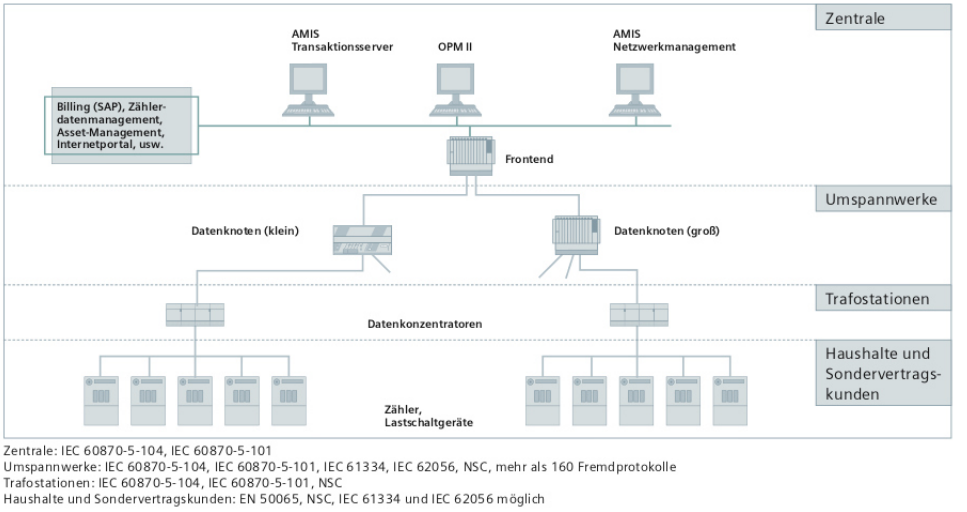


Abbildung 9: Typischer Aufbau eines Smart-Metering-Systems

5. Analyse McAfee Application Control

5.1. Übersicht der analysierten Software

McAfee Application Control ist ein Produkt zur Umsetzung des Sicherheitskonzepts Application Whitelisting. Dieses Konzept wird eingesetzt, um die Sicherheit von Systemen mit hohen Sicherheitsanforderungen in kritischen Infrastrukturen zu erhöhen. Hierbei wird eine Liste von erlaubten Programmen erzeugt, welche nur Programme enthält, die auf dem System ausgeführt werden dürfen. Im Falle eines Angriffs kann dies die Ausführung von Programmen eines Angreifers (Viren, Malware, diverse Hackerprogramme, etc.) verhindern, da diese nicht in der Whitelist enthalten sind.

McAfee Application Control wird eingesetzt, um die Sicherheit von SCADA-Leitständen zu erhöhen. Diese weisen einen sehr hohen Schutzbedarf auf, da ein Angreifer bei einer Kompromittierung dieser Systeme einen hohen Schaden anrichten kann. Aus diesem Grund wurde die Software McAfee Application Control in die Sicherheitsanalyse aufgenommen.
Abbildung 10 zeigt die Ausführung des Befehls „sadmin solidify“, welcher eine Whitelist sämtlicher Programme auf dem System erstellt.

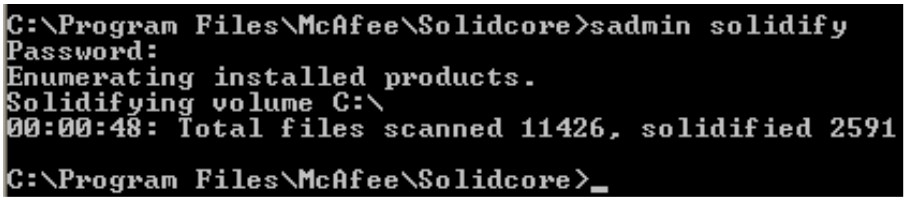


Abbildung 10: Erstellung einer Whitelist auf einem System

Sobald der Schutzmechanismus aktiviert wird, können nur noch Programme, welche in der Whitelist enthalten sind, aufgerufen werden. Abbildung 11 und Abbildung 12 zeigen Fehlermeldungen, welche angezeigt werden, wenn ein Benutzer versucht, ein Programm zu starten, welches nicht in der Whitelist enthalten ist.

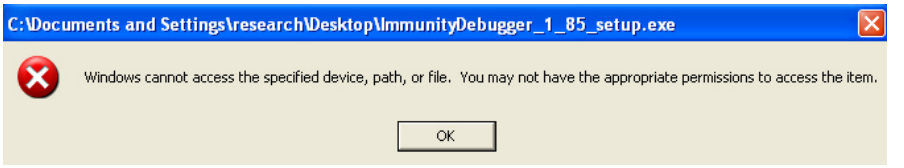


Abbildung 11: Programmausführung wird verhindern, da das Programm nicht in der Whitelist enthalten ist

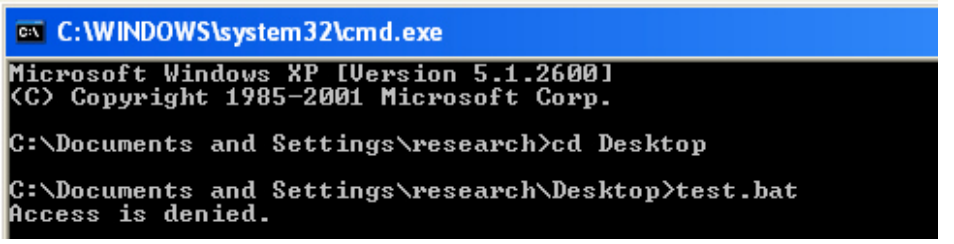


Abbildung 12: Skriptausführung wird verhindert, da das Skript nicht in der Whitelist enthalten ist

McAfee Application Control wurde auf diversen Testsystemen mit unterschiedlichen Betriebssystemen (Microsoft Windows XP, Microsoft Windows 7 sowie Microsoft Windows 8.1) sowie Architekturen (32-bit sowie 64-bit) getestet. Weiters wurden die entsprechenden Server-Versionen der Software getestet. Da diese allerdings mit den Client-Versionen übereinstimmen, wird nicht näher darauf eingegangen.

5.2. Durchgeführte Testklassen

Im Rahmen der Analyse wurde geprüft, ob die Schutzfunktionen durch gezielte Angriffe umgangen werden können. Dies betraf insbesondere die Überprüfung der nachfolgenden Punkte:

1. Analyse der Kommunikation der einzelnen Komponenten.
   McAfee Application Control besteht aus mehreren Teilkomponenten, welche untereinander kommunizieren. Der Endanwender arbeitet mit dem Konsolenprogramm „sadmin.exe“. Über dieses Programm werden sämtliche Befehle eingegeben um beispielsweise Programme zur Whitelist hinzuzufügen oder den Schutz zu aktivieren oder zu deaktivieren. Das Programm fragt ebenfalls den Benut-

zer nach dem Passwort, falls eines gesetzt wurde. Die Komponente „sadmin.exe“ überträgt sämtliche Daten per IPC (Interprozesskommunikation) zum Service „scsrv.exe“. Dieser Service ist für die Umsetzung der einzelnen Befehle verantwortlich. Beispielsweise modifiziert dieser Service die Whitelist-Datenbank, um neue Programme in der Whitelist aufzunehmen. Die tatsächliche Umsetzung der einzelnen Schutzmechanismen wird mittels des Kernel-Treibers „swin1.sys“ durchgeführt. Dieser stellt beispielsweise sicher, dass nur Programme, welche in der Whitelist enthalten sind, vom Benutzer ausgeführt werden können. Weiters wird die Lese-Beschränkung umgesetzt (ein Benutzer kann beispielsweise nicht die Datei mit dem Passwort-Hashwert auslesen) sowie die Schreib-Beschränkung (ein Benutzer kann keine vorhandenen Programme oder die Whitelist verändern). Die Kommunikation zwischen dem Service und dem Treiber erfolgt über IOCTL- Anfragen (Device Input and Output Control).

Sowohl die Kommunikation zwischen der Konsolenanwendung und dem Service, als auch die Kommunikation zwischen Service und Treiber wurde im Detail analysiert. Hierzu wurden die übertragenen Daten per Hand analysiert und modifiziert. Dies erlaubte eine Prüfung, ob an korrekter Stelle das Passwort überprüft wird und das Programm korrekt mit manipulierten Daten umgeht. Weiters wurde das Übertragungsprotokoll analysiert.

2. Analyse des technischen Designs der Software und daraus resultierender Schwachstellen.
   Sämtliche der bereitgestellten Schutzfunktionen (Application Whitelisting, Lese- sowie Schreibschutz, usw.) können auf mehrere Arten umgesetzt werden. Jede dieser Implementierungen bietet gewisse Vor- und Nachteile. Die Wahl dieser Implementierungen und deren Zusammenspiel wurde bewertet, um resultierende Schwachstellen im Aufbau der Software zu identifizieren.

3. Überprüfung der Software auf typische Programmierfehler, welche von Angreifern missbraucht werden können.
   Die Auswahl der gängigsten Programmierfehler bei einer Software hängt stark von der verwendeten Programmiersprache ab. In die-

sem Fall wurde eine Programmiersprache gewählt, bei welcher der Programmierer selbst die Speicherverwaltung übernehmen muss. Daher wurde gezielt nach Schwachstellen in der Speicherverwaltung gesucht, da diese meist zu einer direkten Übernahme der Software führen. Dies betraf insbesondere das Auffinden von Buffer-Overflows, Integer-Overflows, Format-String- sowie Use-After-Free-Schwachstellen. Neben diesen wurde nach weiteren gängigen Schwachstellen gesucht wie beispielsweise Command-Execution- oder Denial-of-Service-Schwachstellen.

4. Auffinden von Möglichkeiten zum Umgehen der Standardschutzmechanismen der Software.
   Das Auffinden von Methoden zum Umgehen der Hauptfunktionalität der Software (Application Whitelisting) war ein integraler Bestandteil der Analyse. Des Weiteren wurden Methoden zum Umgehen der zusätzlichen Schutzmechanismen (Lese- sowie Schreibschutz, Schutz vor Speicherverwaltungs-Schwachstellen, usw.) gesucht.

5. Analyse von Drittsoftware, welche von der Software installiert und verwendet wird.
   Da während der Installation von McAfee Application Control zusätzlich Drittsoftware installiert wird, wurde untersucht, ob diese Software die Grundsicherheit des Betriebssystems oder von McAfee Application Control gefährdet.

6. Analyse von gängigen Angriffsszenarien und ob diese trotz McAfee Application Control durchgeführt werden können.
   Schwachstellen in den oben angeführten Testklassen wären für einen Angreifer nicht wertvoll, wenn der Angreifer diese Schwachstellen nicht tatsächlich ausnutzen könnte. Daher wurden während der Analyse die gängigsten Angriffsszenarien überprüft, sowie ob diese trotz einer Installation von McAfee Application Control zu einer Kompromittierung des Systems führen. Diese Angriffsszenarien werden zurzeit in der realen Welt bei tatsächlichen Angriffen eingesetzt um Systeme zu übernehmen. Die Analyse umfasste insbesondere den Punkt, ob ein Angreifer unter Ausnutzung dieser Angriffsszenarien die Hauptfunktionalität (Application Whitelis-

ting) umgehen und somit einen Virus in das System einschleusen kann. Insbesondere wurden die Angriffsszenarien Java Applet, Office-Dokument mit Macros, Programm mit einem Speicherverwaltungsfehler (z. B. Buffer Overflow), Webseite mit einem Programmierfehler, USB-Stick, Pass-the-Hash-Angriff sowie Übertragung einer bösartigen E-Mail überprüft.

6. Ergebnisse

In der Sicherheitsüberprüfung wurde eine Vielzahl von Schwachstellen mit großem und kritischem Risiko festgestellt, welche sich in folgende Bereiche einteilen lassen:

Einsatz von Klartextprotokollen ohne Möglichkeit der Authentifizierung.
Werden Datenströme zwischen den einzelnen Endpunkten unverschlüsselt (zum Beispiel: ohne TLS) übertragen, kann der Datenverkehr in den Netzwerksegmenten aller beteiligten Endpunkte mit- bzw. abgehört und in weiterer Folge missbraucht werden. Sofern möglich, sollten alle Services verschlüsselte Kanäle zumindest unterstützten. Sensible Informationen sollten niemals unverschlüsselt über nicht vertrauenswürdige Netzwerke übertragen werden.

Sowohl im Hardware-Design, als auch im Software-Design der Komponenten wurde die Exponiertheit nicht berücksichtigt.
Im Zuge des Entwicklungs- und Designprozess von Hardware und Software muss das Einsatzgebiet, der Standort und die physische Exponiertheit gegenüber Angreifern berücksichtigt werden. Je nachdem können Hardware und Software ausschließlich auf Funktionalität und Safety, oder aber zusätzlich auf strenge Security-Anforderungen ausgelegt sein.

Komponenten und Services entsprechen nicht dem Minimalprinzip.
Entsprechen Konten und Einstellungen von Services nicht dem Minimalprinzip, kann ein potenzieller Angreifer diese missbrauchen und seine Rechte auf den verschiedenen Komponenten eskalieren.
Benutzerkonten, Services und ihre Berechtigungen müssen dem Minimalprinzip entsprechen. Das heißt, dass jede Komponente und jedes Objekt

nur über die für den Betrieb unbedingt notwendigen Rechte verfügen darf.

Fehlendes Patch- und Vulnerability-Management.
Nicht implementierte Sicherheitspatches und Softwareupgrades sind einer der Hauptgründe für kompromittierte Systeme. Bekannte Sicherheitslücken in Serversoftware und Anwendungen können automatisiert identifiziert und genutzt werden. In den meisten Fällen ist kein zusätzliches Know-How notwendig, um diese Fehlerklasse zu missbrauchen. Aus diesem Grund ist ein gut funktionierendes Patch- und Vulnerability-Management für exponierte Systeme eines der wichtigsten Instrumente, um den Sicherheitslevel eines Unternehmens anzuheben.

Umgehungsmöglichkeit des Application Whitelisting.
Application Whitelisting wird auf Systemen mit fehlendem oder schlechtem Patch-Management eingesetzt, um deren Sicherheit trotzdem zu gewährleisten. Das eingesetzte Produkt McAfee Application Control kann allerdings von Angreifern mittels diversen Techniken umgangen werden, um nicht erlaubte Programme dennoch auszuführen. Weitere mitgelieferte Schutzfunktionen wie beispielsweise Lese- bzw. Schreibschutz sowie „Buffer Overflow Protections“ können von einem Angreifer ebenfalls umgangen werden. Aufgrund von diversen Implementierungsfehlern kann die Software missbraucht werden, um die Verfügbarkeit der Systeme anzugreifen. Es wird daher empfohlen, die Grundsicherheit von Systemen mittels Patch-Management und sicherer Konfiguration zu gewährleisten und Application Whitelisting nur als zusätzliche Schutzmaßnahme einzusetzen. Dabei darf das eingesetzte Produkt nicht die Sicherheit des Grundsystems aufgrund von Software-Fehlern gefährden.

Eine detaillierte Darstellung der gefundenen Schwachstellen und Angriffsmöglichkeiten ist aufgrund der Kritikalität der enthaltenen Informationen nicht Teil dieser Publikation.

Teil V: Maßnahmenkatalog und Tool-Implementierung

1. Zielsetzung und Vorgehensweise

Ziel der in diesem Teil des Projektes durchgeführten Arbeiten war es, Sicherheitsmaßnahmen zu definieren, welche Netzbetreiber und andere Smart-Grid-Stakeholder nutzen können, um ihre Netzinfrastrukturen gegen die in Teil II identifizierten Bedrohungen und Risiken abzusichern.

Basis für die Entwicklung des Maßnahmenkatalogs waren die Normen ISO/IEC 27002 und ISO/IEC 27019, die BSI-Schutzprofile[237,238], sowie die durch die ENISA definierten Sicherheitsmaßnahmen für Smart Grids[239]. Der Maßnahmenkatalog baut auf folgenden Vorarbeiten innerhalb des Projektes auf:

- IKT-Architekturmodell aus Teil I
- Bedrohungskatalog und Risikomatrix aus Teil II

Die Erarbeitung des Maßnahmenkatalogs erfolgte in mehreren Schritten, welche nachfolgend als Übersicht aufgeführt sind:

1. Definition generischer Maßnahmen (je Bedrohung) und spezifischer Maßnahmen (je Bedrohung und Architektur-Cluster)
2. Einschränkung auf diejenigen Bedrohungen, bei welchen das Risikopotential als hoch bewertet wurde
3. Erweiterung auf übergeordnete Maßnahmen, um sinnvolle Auswertung zu ermöglichen
4. Priorisierung dieser übergeordneten Maßnahmen durch Bestimmung ihrer Anzahl über den gesamten Maßnahmenkatalog

[237] BSI: Protection Profile for the Gateway of a Smart Metering System (BSI-CC-PP-0073), 2013.

[238] BSI: Protection Profile for the Security Module of a Smart Metering System (Security Module PP, BSI-CC-PP-0077), 2013.

[239] European Union Agency for Network and Information Security (ENISA): Appropriate security measures for smart grids. Dezember 2012.

hinweg
5. Ideale Umsetzungsszenarien inkl. Definition der verantwortlichen Stakeholder
6. Konkrete Umsetzungsbeispiele

In weiterer Folge werden die einzelnen Schritte, welche zur Erstellung des Maßnahmenkatalogs geführt haben, dargestellt. Der einfacheren Lesbarkeit halber werden die (Zwischen-) Ergebnisse der einzelnen Schritte jeweils direkt nach der Beschreibung der Vorgehensweise aufgeführt.

Der Maßnahmenkatalog wurde auch als Tool implementiert, um eine möglichst einfache und effiziente Verwendung zu ermöglichen. Die Implementierung ist im Open-Source-ISMS-Tool „Verinice" erfolgt. Details zur Verwendung der Tool-Implementierung finden sich in Abschnitt 4.

2. Herleitung der Sicherheitsmaßnahmen

2.1. Definition generischer und spezifischer Maßnahmen

Die Sicherheitsmaßnahmen wurden aufbauend auf dem Risikokatalog aus Teil II zunächst für jede der 31 identifizierten Bedrohungen definiert. Zusätzlich wurden nach Möglichkeit spezifische Maßnahmen je Architektur-Cluster definiert. So wurden beispielsweise folgende generische Maßnahmen zum Schutz vor der Bedrohung „Fehlende oder unzureichende Sicherheitsmechanismen von Software-Produkten" (siehe Abschnitt 2.3) definiert:

- Authentizität & Integrität von Software sicherstellen (Code Signing)
- ggf. im Vorfeld Penetrationstests durchführen
- Internetzugriff nur beschränkt ermöglichen (ausschließlich dort, wo tatsächlich notwendig)
- Access Control
- Fernwartungskommunikation über verschlüsselte Kommunikationstunnel
- lokale Firewalls wo nötig bzw. sinnvoll
- Sicherheitsanforderungen & relevante Standards für Hersteller (bzw. gesamte supply chain) – z. B. bzgl. Tests und Pat-

ches/Upgrades – vertraglich festschreiben und die Umsetzung regelmäßig überprüfen
- Hersteller müssen eventuelle Backdoors oder (Wartungs-)Zugänge offenlegen und diese entsprechend geschützt werden

Neben diesen generischen Maßnahmen wurden beispielsweise für den Architektur-Cluster „Funktionale Gebäude" zusätzlich folgende spezifische Maßnahmen definiert:

- Geräte müssen beide Schnittstellen sicher trennen können, d.h. es darf weder eine Verbindung von der HGA ins Fernwirknetz möglich sein, noch ein Senden von Steuerbefehlen durch das Smart Meter (Nachweis eventuell über Prüfzertifikat)

Der erste Entwurf des Maßnahmenkatalogs enthielt folglich eine Mischung aus generischen Sicherheitsmaßnahmen (je Bedrohung) und spezifischen Maßnahmen (je Bedrohung und Architektur-Cluster). Dieser Entwurf wurde daraufhin dem Konsortium vorgestellt, um Feedback zu erhalten hinsichtlich der weiteren Bearbeitung bzw. Verfeinerung der Sicherheitsmaßnahmen. Folgende Wünsche wurden bei dieser Feedbackrunde seitens der Projektpartner formuliert:

- **Fokussierung der Maßnahmen:** Die generischen Maßnahmen, welche je Bedrohung definiert wurden, waren insgesamt sehr umfangreich. Das Konsortium hat die Befürchtung geäußert, dass hier bei der Anwendung der Maßnahmen „der Wald vor lauter Bäumen" nicht gesehen wird, und es wurde einstimmig gewünscht, dass eine Einschränkung bzw. Fokussierung auf die wichtigsten Maßnahmen stattfindet. Es wurde vorgeschlagen, auf diejenigen Maßnahmen zu fokussieren, welche Bedrohungen mit hohem Risikopotential adressieren, und eine Priorisierung über die Häufigkeit der einzelnen (atomaren) Maßnahmen vorzunehmen.
- **Stakeholderverantwortung:** Das Projektkonsortium war sich einig darüber, dass neben der Definition der Sicherheitsmaßnahmen auch eine Festlegung der Verantwortlichkeiten bzgl. der Umsetzung der Maßnahmen stattfinden sollte. Durch einen klaren Vorschlag hinsichtlich der Zuständigkeit würde der Mehrwert des Maßnahmenkatalogs für die Anwender (v.a. Netzbetreiber) deutlich steigen,

da die praktische Anwendung konkretisiert und somit vereinfacht wird.

- **Best-Practice-Beispiele:** Die Konsortialpartner haben außerdem vorgeschlagen, konkrete Praxisbeispiele für die Umsetzung der Sicherheitsmaßnahmen aufzuführen. Durch die Angabe solcher Best-Practice-Vorschläge bekommen Anwender eine konkrete Vorstellung von den umzusetzenden Maßnahmen und außerdem eine praktische Anleitung, wie die Umsetzung der Sicherheitsmaßnahmen in der Realität aussehen kann.

Alle Vorschläge wurden bei der Überarbeitung des Maßnahmenkatalogs berücksichtigt und umgesetzt. Die einzelnen Schritte vom ersten Entwurf des Maßnahmenkatalogs bis hin zu seiner finalen Form werden im Folgenden genauer beschrieben.

2.2. Einschränkung auf Bedrohungen mit hohem Risikopotential

Um eine Priorisierung und damit eine stärkere Aussagekraft zu erreichen, wurde auf diejenigen Sicherheitsmaßnahmen fokussiert, welche Bedrohungen mit hohem Risikopotential abdecken. Dabei handelt es sich um die folgenden Bedrohungen:

1. Fehlende oder unzureichende Sicherheitsmechanismen von Software-Produkten
2. Fehlende oder unzureichende Sicherheitsmechanismen in Netzwerken
3. Sicherheitsprobleme bei Software-Migration
4. Mutwillige Manipulation von Geräten
5. Unzulässige physische Schnittstellen
6. Ausfall oder Störung vorhandener Sicherungseinrichtungen (Safety-Maßnahmen)

Die Einschränkung auf diese sechs Bedrohungen ergab eine Reduktion auf 36 Maßnahmen, welche in den nächsten Schritten weiterbetrachtet wurden.

2.3. Erweiterung auf übergeordnete Maßnahmen („Maßnahmen-Cluster“)

Um eine sinnvolle Auswertung der Anzahl gleicher Maßnahmen über den

gesamten Katalog hinweg zu ermöglichen, wurden die 36 Maßnahmen aus Schritt 1 in diesem Schritt in ihrer Bedeutung erweitert. Beispiele für diesen Verallgemeinerungsschritt finden sich in Abbildung 13. Ohne diesen Schritt wäre keine sinnvolle Häufigkeitsauswertung möglich gewesen, da sonst aufgrund der hohen Spezialisierung die meisten Maßnahmen mit einer sehr geringen Anzahl aufgetreten wären. Der Verallgemeinerungsschritt erlaubt an dieser Stelle eine aussagekräftige Auswertung.

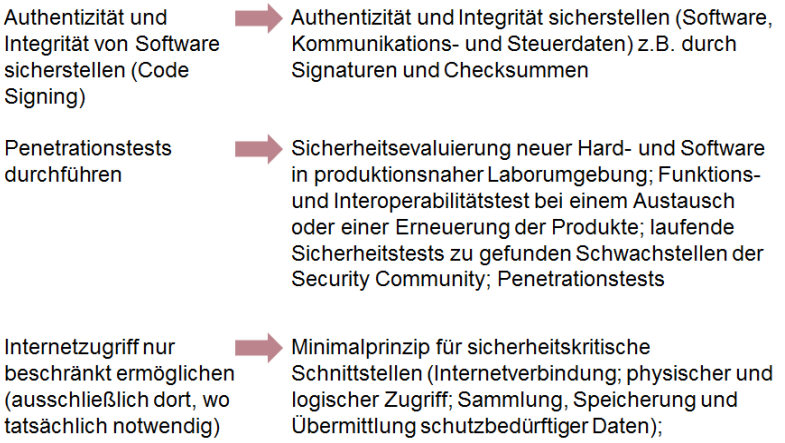


Abbildung 13: Beispiele für den Verallgemeinerungsschritt bei der Definition des Maßnahmenkatalogs

Die verallgemeinerten Maßnahmen wurden daraufhin thematisch zusammengefasst, so dass sich insgesamt folgende zehn übergeordnete Maßnahmen-Cluster ergaben:

1. **Authentizität und Integrität sicherstellen:** Authentizität und Integrität (von Software, Kommunikations- und Steuerdaten) sicherstellen z. B. durch elektronische Signaturen, Software-Zertifikate, Hardware UUIDs, elliptische Kurven Kryptographie, Checksummen
2. **Sicherheitsevaluierung & Funktions-, Interoperabilitäts- und Penetrations-Tests:** Sicherheitsevaluierung neuer Hard- und Software in produktionsnaher Laborumgebung mit einem technischen und physischen Audit; Funktions- und Interoperabilitätstest

bei einem Austausch oder einer Erneuerung der Produkte; laufende Sicherheitstests zu gefundenen Schwachstellen der Security Community; Penetrationstests

3. **Minimalprinzip:** Minimalprinzip für sicherheitskritische Schnittstellen (Internetverbindung; physischer und logischer Zugriff; Sammlung, Speicherung und Übermittlung schutzbedürftiger Daten); Kapselungsprinzip: Schnittstellen sollen nicht direkt, sondern über eine für beide Parteien sichere Umgebung ablaufen und nur funktionsspezifischen Zugang bieten (um eine sichere Funktionserweiterung zu gewährleisten)
4. **Netzwerksegmentierung & Abschottung verschiedener (Sicherheits-) Bereiche:** Netzwerksegmentierung; Abschottung verschiedener (Sicherheits-) Bereiche durch Firewalls (auch intern) und besonderer Schutz für kritische Bereiche (Sandboxing in einer virtuellen Maschine, eigenes virtuelles LAN, IPS/IDS, Firewalls, Zugriff ausschließlich für Administrations- und Wartungspersonal, Access Control)
5. **Schutz von (Fern-) Wartungszugängen & verpflichtende Transparenz seitens der Hersteller:** besonderer Schutz von (Fern-) Wartungszugängen durch verschlüsselte Kommunikationstunnel; verpflichtende Herstellertransparenz zur Offenlegung von möglichen Wartungsschnittstellen; Access Control; Protokollierung von Rollen, Personen, Zeiten und Tätigkeiten; Schulung von Wartungspersonal zur Förderung von Sicherheitsbewusstsein
6. **Sicherheitsanforderungen für Hersteller:** Sicherheitsanforderungen und relevante Standards für Hersteller (bzw. gesamte supply chain) festschreiben und Nachweispflicht einführen; Security-by-Design bei den Komponenten fordern; Nachweis durch Prüfzertifikat oder Auditergebnis
7. **Change Management, Patch Management, Configuration Management:** konsistente Dokumentation von System- und Gerätekonfigurationen sowie von Änderungsanforderungen und tatsächlich durchgeführten Änderungen von Hard- und Software in Produktivsystemen; Festlegung der Rollen & Verantwortlichkeiten; Integrationstests
8. **Physische Sicherheitsmaßnahmen:** physische, möglichst IKT-unabhängige Sicherheitsmaßnahmen (Geräteschutz, Zutrittskontrolle, Schlüsselkartensystem, Änderungsprotokollierung, Dongle-

Systeme, Alarmanlagen)

9. **Incident Management:** Identifizierung, (Fern-) Abschaltung und Austausch von Komponenten mit fehlerhaftem oder schädlichem Verhalten (HW wie SW); Notsignalgebung bei (Verdacht auf) Unregelmäßigkeiten (z. B. Umgehung physischer Zugangs- oder Geräteschutzeinrichtungen, unbekannte SW-Version etc.); Regelwerkerstellung zu Fehlerbehebungsabläufen
10. **Mehrstufiges Sicherheitskonzept:** z. B. Sicherheit auf der Übertragungsebene bei technisch nicht möglicher oder zu aufwendiger Protokollsicherheit; verschlüsselte Datenkommunikation; Anonymisierung und Aggregation von personenbezogenen Daten wo möglich

Diese zehn übergeordneten Maßnahmen wurden als Basis für die darauffolgende Häufigkeitsauswertung herangezogen.

2.4. Priorisierung der Maßnahmen-Cluster

Im nächsten Schritt wurde die Häufigkeit der Maßnahmen-Cluster über den gesamten Maßnahmenkatalog hinweg (d.h. für alle 31 Bedrohungen) bestimmt, um zu einer Aussage hinsichtlich der Wichtigkeit der einzelnen Maßnahmen zu gelangen. Tabelle 17 zeigt das Ergebnis der Auswertung.

Tabelle 17: Häufigkeit der übergeordneten Maßnahmen über den gesamten Maßnahmenkatalog hinweg

Häufigkeit	**Maßnahmen-Cluster**
15	Authentizität und Integrität sicherstellen
13	Sicherheitsevaluierung & Funktions-, Interoperabilitäts- und Penetrations-Tests
11	Change Management, Patch Management, Configuration Management
10	Incident Management
9	Netzwerksegmentierung & Abschottung verschiedener (Sicherheits-) Bereiche
7	Minimalprinzip; Schutz von (Fern-) Wartungszugängen & verpflichtende Transparenz seitens der Hersteller; physische Sicherheitsmaßnahmen
6	Mehrstufiges Sicherheitskonzept
5	Sicherheitsanforderungen für Hersteller

Die drei wichtigsten Maßnahmen-Cluster sind demnach (in dieser Reihenfolge):

1. Authentizität und Integrität sicherstellen
2. Sicherheitsevaluierung & Funktions-, Interoperabilitäts- und Penetrations-Tests
3. Change Management, Patch Management, Configuration Management

Um die Aussagekraft der Häufigkeitsauswertung noch weiter zu erhöhen, wurde in diesem Schritt eine Gewichtung der Maßnahmen-Cluster vorgenommen je nachdem, wie hoch das Risikopotential der einzelnen Bedrohungen ist, welche die Maßnahme jeweils abdeckt. Es wurden folgende Gewichte festgelegt:

- Faktor 0,1 für niedriges Risikopotential
- Faktor 0,5 für mittleres Risikopotential
- Faktor 1,0 für hohes Risikopotential

Die Gewichtung sei beispielhaft mittels der Bedrohung „Ausfall oder Störung von IT-Systemen“ dargestellt: Bei dieser Bedrohung ergab die Risikobewertung insgesamt sechs Architektur-Cluster mit niedrigem Risikopotential, vier mit mittlerem Risikopotential und keinen mit hohem Risikopotential. Somit ergibt sich eine Gewichtung von

$$6*0,1 + 4*0,5 + 0*1,0 = 3,4.$$

Die Maßnahmen, welche für diese Bedrohung definiert wurden, bekamen somit einen Faktor von 3,4 zugewiesen. Diese Faktoren wurden anschließend je Maßnahmen-Cluster addiert, um eine deutlichere Priorisierung zu erreichen. Tabelle 18 zeigt das Ergebnis der gewichteten Auswertung.

Tabelle 18: Gewichtete Häufigkeit der übergeordneten Maßnahmen über den gesamten Maßnahmenkatalog hinweg

Häufigkeit	**Maßnahmen-Cluster**
46	Authentizität und Integrität sicherstellen
36	Sicherheitsevaluierung & Funktions-, Interoperabilitäts- und Penetrations-Tests
34	Change Management, Patch Management, Configuration Management
31	Netzwerksegmentierung & Abschottung verschiedener (Sicherheits-) Bereiche
25	Minimalprinzip
21	Schutz von (Fern-) Wartungszugängen & verpflichtende Transparenz seitens der Hersteller; Incident Management
19	Mehrstufiges Sicherheitskonzept; physische Maßnahmen
18	Sicherheitsanforderungen für Hersteller

Bei den drei häufigsten (und damit wichtigsten) Maßnahmen ergab sich durch die Gewichtung somit keine Änderung der Reihenfolge gegenüber der ungewichteten Auswertung. Allerdings fällt auf, dass sich der Abstand des am häufigsten genannten Maßnahmen-Clusters (Authentizität und Integrität sicherstellen) zu den nachfolgenden Maßnahmen-Clustern weiter

vergrößert. Folglich kann gesagt werden, dass unsere Auswertungen zeigen, dass „Authentizität und Integrität sicherstellen“ die mit Abstand wichtigste Maßnahme für die kommunikationstechnische Absicherung von Smart Grids darstellt.

2.5. Ideale Umsetzungsszenarien inkl. Definition der verantwortlichen Stakeholder

In diesem Schritt wurden zunächst die Stakeholder identifiziert, welche für die Umsetzung der Sicherheitsmaßnahmen (mit-)verantwortlich sind. Die jeweiligen Aufgaben bzw. Verantwortlichkeiten wurden anschließend bei der Entwicklung der Umsetzungsszenarien „ideale Welt“ beschrieben. Folgende Stakeholder wurden bei der Zuordnung in Betracht gezogen (in alphabetischer Reihenfolge):

- Administratoren
- Applikationsentwickler
- Endkunden
- Gerätehersteller
- Netzbetreiber
- Regulierungsbehörden
- Schnittstellendesigner
- Sicherheitsforschungseinrichtungen
- Standardisierungsgremien
- Stromanbieter
- Softwarehersteller bzw. -provider
- Testinstitutionen (unabhängig)
- Wartungspersonal

Anschließend wurde das Szenario einer idealen Umsetzung jedes einzelnen Maßnahmen-Clusters unter Berücksichtigung der für die Umsetzung der einzelnen Aufgaben verantwortlichen Stakeholder beschrieben:

1. Maßnahmen-Cluster: Authentizität und Integrität sicherstellen:
Software-Provider stellt Checksummen auf zertifizierten Online-Quellen zur Verfügung oder erlaubt Verifikation durch UUIDs über einen verschlüsselten Übertragungskanal. Endkunden müssen den Verifikationsprozess vor einer Nutzung des Produktes durchführen. Applikationsentwickler

müssen dafür sorgen, dass Kommunikation innerhalb eines Programms und über Applikationsgrenzen hinweg nach Stand der Technik verschlüsselt erfolgt. Schnittstellendesigner stellen durch zertifizikatsbasierte Authentifizierung (oder ähnliche Techniken) sicher, dass die Identität des Senders und Integrität der Daten beim Empfänger jederzeit gewährleistet ist. Administratoren oder Wartungspersonal prüfen die digitale Signatur des Übertragungskanals und der Software, verifizieren die Checksummen oder leiten eine Verifikation der Software nach Herstelleranleitung ein.

2. Maßnahmen-Cluster: Sicherheitsevaluierung & Funktions-, Interoperabilitäts- und Penetrations-Tests:
Der Gerätehersteller führt ständige Sicherheitsevaluierungen von der Konzeption bis zur Umsetzung der Produkte durch, sowie ein Security Audit vor Auslieferung. Unabhängige Testinstitutionen sowie Sicherheitsforschungseinrichtungen führen Penetrationstests durch und veröffentlichen Systemschwachstellen auf verantwortungsvollen, dafür vorgesehenen Wegen. Netzbetreiber führen Integrationstests neuer Komponenten in einer produktionsnahen Laborumgebung durch. Stromanbieter achten auf durchgeführte Security Audits bei der Wahl der Produkte und lassen für ihr System selbst Penetrationstests durchführen.

Auf Ebene von Österreichs Energie werden im Arbeitskreis Sicherheit derzeit europaweite Gespräche mit Gesellschaften geführt, die für System- und Softwaretests von Komponenten in Frage kommen. Ziel sind herstellerunabhängige Dienstleistungsanbieter für Smart-Meter- bzw. Smart-Grid-Komponententests mit einheitlichen Standards in der Prüfung und Produktfreigabe. Die Verantwortung für und die Tests von einzelnen Komponenten sollte in Zukunft nicht mehr beim Anwender (z. B. Netzbetreiber oder Dienstleister) liegen, sondern beim Hersteller dieser Komponenten.

3. Maßnahmen-Cluster: Minimalprinzip:
Gerätehersteller entwickeln ihre Komponenten bereits nach dem minimalen Kostenprinzip; dies soll auf minimale Schnittstellenangriffsflächen erweitert werden, indem keine nicht notwendigen Verbindungen hergestellt werden, die notwendigen Verbindungen in der Konfiguration standardmäßig verschlüsselt und gesichert ablaufen, und die Authentizität von Kommunikationspartnern stets überprüft wird. Ein Datensicherheitsbeauftragter kann die Rolle der Sicherheitsinnovation, Überprüfung und Kontrolle

übernehmen. Netzbetreiber achten bei der Konfiguration ihres Gesamtsystems darauf, die Angriffsflächen zu minimieren, unnötige Datensammlungen zu vermeiden, Daten stets nach dem aktuellen Stand der Technik zu verschlüsseln und diese auch inhouse verschlüsselt zu übertragen, und durch geeignete Schlüsselsysteme nur befugtem Personal kontrollierten Zugang zu Systemen zu gewähren (need-to-know). Stromanbieter achten in ihrer Produktauswahl und -konfiguration darauf, dass nicht einfach ein größerer Funktionsumfang durch geringe Manipulation freigeschaltet werden kann, dass Firmware nachgeladen werden kann (im Fall von Sicherheitslücken), dass Daten nach Möglichkeit nur lokal und verschlüsselt gespeichert werden. Applikationsentwickler sind bestrebt, Daten lokal zu halten und nur notwendige Daten zu übermitteln, Übermittlungs- und Aufbewahrungswege stets sicher zu wählen, bewährte und getestete Techniken auch für neue Problemstellungen einzusetzen und auf Kapselung, Integrität und Authentizität der Kommunikationspartner zu achten.

4. Maßnahmen-Cluster: Netzwerksegmentierung & Abschottung verschiedener (Sicherheits-) Bereiche:
Gerätehersteller achten bei der Entwicklung ihrer Produkte darauf, dass Arbeitsgeräte nur wenn nötig mit dem Internet verbunden sind, mit allen Sicherheitsupdates ausgestattet sind, Benutzer sich nicht mit einem Administrationsaccount einloggen und arbeiten, Arbeitsgeräte sich hinter gewarteten Firewalls befinden, Arbeit möglichst in virtuellen Maschinen stattfindet und Zugriffskontrollen Änderungen zurückverfolgen lassen. Für Netzbetreiber und Stromanbieter gilt Ähnliches in ihrem System im laufenden Betrieb. Administratoren haben die Aufgabe, auf die Umsetzung der Maßnahmen und die korrekte, lückenlose Durchführung zu achten. Wartungspersonal stellt regelmäßig fest, ob alles erwartungsgemäß verläuft und meldet Auffälligkeiten, wie z. B. das einmalige kurze Flackern eines Programmes am Bildschirm beim Öffnen eines Dokuments, den Absturz eines Programms, Unregelmäßigkeiten in einer der Metriken, die noch keinen automatisierten Alarm ausgelöst haben, usw.

5. Maßnahmen-Cluster: Schutz von (Fern-) Wartungszugängen & verpflichtende Transparenz seitens der Hersteller:
Gerätehersteller achten bei der Entwicklung der Fernwartungsschnittstellen ihrer Produkte auf die Umsetzung von sicheren Kommunikationstunneln, Verschlüsselung der Kommunikation und Daten, Protokollierung, sowie

Sicherstellung der Authentizität der Kommunikationspartner, so dass ein Offenlegen aller vorhandener Wartungsschnittstellen kein Sicherheitsrisiko birgt. Netzbetreiber und Stromanbieter achten beim Kauf von Produkten auf die Offenlegung und sichere Durchführung von Fernwartungsschnittstellen. Administratoren achten bei der Umsetzung von Fernwartungen auf die sichere Durchführung an jedem Systempunkt und die automatisierte Überwachung von Protokollen. Das Wartungspersonal achtet bei der Durchführung von Fernwartungen auf die sichere Umgebung, in der die Wartung erfolgt, hält sich an Vorgaben ihr Arbeitsgerät sowie das fernzuwartende Gerät betreffend, und meldet Unregelmäßigkeiten.

6. Maßnahmen-Cluster: Sicherheitsanforderungen für Hersteller:
Sicherheitsforschungseinrichtungen unterstützen bei der Definition der Sicherheitsanforderungen vor Allem durch Veröffentlichung von Forschungsergebnissen, „Best Practices" und der Mitarbeit in entsprechenden Gremien. Standardisierungsgremien definieren einheitliche Vorgaben, die von Industriepartnerinnen umgesetzt werden können. Regulierungsbehörden setzen die Einhaltung von Standards voraus. Netzbetreiber und Stromanbieter fordern die umgesetzten Standards bei Ausschreibungen ihrer Produkte ein. Gerätehersteller setzen die Anforderungen von Standards um.

In Österreichs Energie existieren verschiedene Arbeitskreise für Netzwerk, Fernwirktechnik, Funk, Smart Meter und andere technische Anforderungen. Sind explizite Anforderungen wie z. B. End-to-End-Security-Anforderungen für Smart Meter für Ausschreibungen oder die Überwachung bestehender Technik erforderlich, so werden Projektgruppen mit externer Begleitung (technikspezialisierte Beratungsunternehmen) mit der Erstellung entsprechender Anforderungen und Dokumente beauftragt. Ein Beispiel dazu ist das Whitepaper[240] von BDEW und Österreichs Energie. Weiters werden mit der E-Control Austria Risikoanalysen des Gas- und Stromnetzes durchgeführt und aus den Ergebnissen dieser Analysen Umsetzungsanforderungen für die gesamte Branche erstellt. Dabei ist die Zusammenarbeit mit den Behörden zur Sicherheit der kritischen Infrastruktur

[240] Österreichs Energie: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme. Ausführungshinweise zur Anwendung des BDEW Whitepaper. Version 1.0, 2012.

unerlässlich.

7. Maßnahmen-Cluster: Change Management, Patch Management, Configuration Management:
Geräte- und Softwarehersteller stellen getestete Patches zur Behebung von Sicherheitslücken über einen sicheren Kanal verifizierbar zur Verfügung. Unter Umständen machen Patches und Konfigurationsänderungen ein neuerliches Security Audit erforderlich. Netzbetreiber oder Stromanbieter führen die eigentlichen Patches aus, verwalten die eingesetzten Konfigurationen in ihren Produkten, führen Integrationstests in echtbetriebähnlicher Laborumgebung durch und dokumentieren Änderungen.

8. Maßnahmen-Cluster: Physische Sicherheitsmaßnahmen:
Gerätehersteller achten bei der Umsetzung ihrer Geräte darauf, dass Unberechtigten der Zugang zu Schnittstellen der Geräte erschwert wird, oder Gegenmaßnahmen wie z. B. eine teilweise Abschaltung vorgenommen werden können, sollte ein fehlerhaftes oder schädliches Verhalten festgestellt werden. Netzbetreiber oder Stromanbieter überwachen ihre Systeme auf Fehlverhalten. Administratoren verwalten und beheben Incidents und veranlassen notwendige Fernabschaltungen im Betrieb.

9. Maßnahmen-Cluster: Incident Management:
Gerätehersteller achten bei der Umsetzung ihrer Geräte darauf, dass schädliches Verhalten der Geräte möglichst lokal erkannt wird, alarmiert wird, oder Gegenmaßnahmen wie z. B. teilweise Abschaltung vorgenommen werden. Netzbetreiber achten bei Ausschreibungen und bei ihrer Anlagenumsetzung auf ausreichende Alarmsysteme, Geräteschutz, Personenschutz, Schließmechanismen, Schlüsselsysteme, IKT-Redundanz (alles nach Stand der Technik). Stromanbieter sorgen in ihren Produkten für das vorhergesehene Verhalten im vorhersehbaren Anwendungsumfeld und protokollieren Änderungen.

10. Maßnahmen-Cluster: Mehrstufiges Sicherheitskonzept:
Netzbetreiber oder Stromanbieter achten im Kontext personengebundener Daten grundsätzlich auf Datenvermeidung und zweckgebundene Datensammlung. Gerätehersteller haben ein mehrstufiges Sicherheitskonzept für jeden Schritt der Produktentwicklung in ihrem Fachgebiet gemäß Stand der Technik erstellt. Applikationsentwickler halten sich in jedem Schritt der

Entwicklung an das Sicherheitskonzept für den jeweiligen Vorgang im Gerät oder System und erhalten damit eine Blaupause, nach der die sicheren Elemente modular in weiteren Produkten wiederverwendet werden können. Netzbetreiber sehen bei mangelnder Protokollsicherheit alternative Sicherheitsmechanismen (z. B. auf Übertragungsebene) vor. Standardisierungsbehörden entwickeln möglichst sichere Protokolle bzw. holen dies bei bereits implementierten Protokollen nach.

2.6. Konkrete Umsetzungsbeispiele

Im letzten Schritt wurden schließlich praxisnahe Umsetzungsbeispiele je Maßnahmen-Cluster beschrieben, die sich zum Teil auch bereits bei den im Konsortium vertretenen Netzbetreibern bewährt haben:

1. Maßnahmen-Cluster: Authentizität und Integrität sicherstellen:
Es sollten Mechanismen genutzt werden, welche die Geräte im Netzwerk bieten (z. B. je Access Port nur ein Gerät zulassen, automatischer Port Shutdown sobald mehrere Geräte zugreifen, Port-Überwachung, evt. Authentifizierung der Netzwerkgerätschaften via Radius). Nach Möglichkeit sollte IPSec zur Absicherung des Netzwerks verwendet werden, auch wenn hier keine Ende-zu-Ende-Verschlüsselung bis zu den Endgeräten möglich ist. Smart Meter bieten bereits Ende-zu-Ende-Verschlüsselung und zertifikatsbasierte Authentifizierung, allerdings sind die aktuell am Markt vorhandenen Systeme nicht dafür ausgelegt, d.h. es muss auch die Frage der Verfügbarkeit am Markt gestellt werden (was wäre wünschenswert vs. was ist erhältlich). Bei größeren Energieversorgungsunternehmen ist eine Ende-zu-Ende-Verschlüsselung mit zertifikatsbasierter Authentifizierung bei Smart Metern zum Teil bereits implementiert.

2. Maßnahmen-Cluster: Sicherheitsevaluierung & Funktions-, Interoperabilitäts- und Penetrations-Tests:
Das Vier-Augen-Prinzip sollte unbedingt eingehalten werden, insbesondere sollte nicht dieselbe Person bzw. Personengruppe für die Entwicklung und zugleich den Test von Smart-Grid-Komponenten verantwortlich sein. Hersteller sollten die durchgeführten Testabläufe offenlegen (Umfang, Art und Ergebnisse der durchgeführten Tests) und sich außerdem laufend (z. B. via Cert) über kritische Schwachstellen informieren, diese Information an ihre Kunden weitergeben sowie zeitnah entsprechend nachrüsten (ggf. ver-

pflichtende Vereinbarung mit Lieferanten). Der Netzbetreiber sollte im Zusammenhang mit einer effizienten Konfiguration und Patch Management auch konsequentes Vulnerability Management betreiben, um sich eventueller Schwachstellen bewusst zu werden und entsprechend handlungsfähig zu sein. Penetrationstests sollten nicht nur externe Angreifer, sondern auch mögliche Innentäter berücksichtigen. Der Softwareentwicklungsprozess sollte nach dem Capability Maturity Model oder einem vergleichbaren Modell optimiert werden; bei den Qualitäts- und Security-Checks sollten sowohl dynamische, als auch statische Tests durchgeführt werden, um ein möglichst umfassendes Bild zu erhalten. Eine verbindliche Gewährleistung dieser Anforderungen kann durch entsprechende Anforderungsdokumente beim Ausschreibungs- und Bestellprozess erfolgen. Nach jedem Test bzw. jeder Systemänderung sollte ein definiertes Freigabeverfahren befolgt werden.

3. Maßnahmen-Cluster: Minimalprinzip:
Insbesondere für sicherheitskritische Schnittstellen sollte das Minimalprinzip strikt befolgt werden, d.h. es sollten nur diejenigen Funktionen und Schnittstellen aktiviert sein, welche auch wirklich benötigt werden. Sämtliche Debug-Funktionalitäten und ungenutzte Code-Teile sind nach der Entwicklungsphase zu entfernen. Weitere Maßnahmen in diesem Bereich sind (dynamisches) Bandbreitenshaping gemäß Normalbetrieb (d.h. ungewöhnlich hohe Bandbreiten werden nicht zugelassen, wobei in diesem Zusammenhang das Risiko von mangelnder Verfügbarkeit und Denial-of-Service-Problemen beachtet werden muss). Hersteller sollten Empfehlungen hinsichtlich eines geeigneten Setups je nach Einsatzzweck geben (Implementationsanleitung für sicheren Betrieb gemäß Minimalprinzip). Systemabhängigkeiten, welche Sicherheitslücken bergen könnten, sind zu vermeiden. Ein physischer Zugriff auf (kritische) Smart-Grid-Komponenten sollte primär mit eigener Infrastruktur des Netzbetreibers (d.h. ohne Internetnutzung) via Lichtwellenleiter erfolgen. Wo dies nicht möglich ist, sollte eine andere leitungsgebundene Infrastruktur verwendet werden; eine unverschlüsselte kabellose Übertragung (z. B. über UMTS o.ä.) ist jedenfalls zu vermeiden.

4. Maßnahmen-Cluster: Netzwerksegmentierung & Abschottung verschiedener (Sicherheits-) Bereiche:

Eine Aufteilung in verschiedene (Sicherheits-) Zonen sollte sowohl auf physikalischer, als auch auf logischer Ebene stattfinden (beispielsweise ein vom Netzbetreiber eigens zur Verfügung gestelltes Gerät für Wartungstechniker). Ausfälle kritischer Komponenten sind durch entsprechende Redundanzen aufzufangen; so sollten beispielsweise Schaltgeräte und Übertragungstechnik im Umspannwerk über eine gesicherte Stromversorgung verfügen (z. B. Batterien). Für den Notbetrieb ist außerdem der Aufbau eines zweiten Kommunikationssystems zur Visualisierung der ferngesteuerten Anlagen empfehlenswert.

Ein Auslösen von Schutzkomponenten über Fernzugriff (Distanz-, Überstrom-, Frequenzschutz, usw.) darf nicht möglich sein. Bei jeder Netzwerkplanung und -Erweiterung ist auf eine entsprechende Netzwerksegmentierung zu achten und es sind entsprechende Firewall-Zonen einzurichten. Die Übergänge zwischen den einzelnen Zonen sind in regelmäßigen Abständen auf Schwachstellen zu prüfen (mindestens jedoch, wenn ein neues Gerät in eine Zone eingebunden wird). Eine Trennung von Smart-Meter-Netzwerken, dem Fernwirknetzwerk und dem allgemeinen Büronetzwerk ist dabei eine der Grundvoraussetzungen. Meldungen aus kritischen Systemzonen (z. B. Umspannwerke) sind über ein zweites, gesondertes Netzwerk in die Energieleitstelle zu übertragen. Eine Notstromversorgung mit ausreichender Reserve (mindestens 24 Stunden) ist bei den für die kritischen Anlagen und deren Betrieb notwendigen Komponenten vorzusehen.

5. Maßnahmen-Cluster: Schutz von (Fern-) Wartungszugängen & verpflichtende Transparenz seitens der Hersteller:

Für Fernwartungstätigkeiten ist ein zeitlich begrenzter Zugang via SSL-VPN zwingend erforderlich (z. B. Fastviewer oder andere als sicher geltende bzw. produktzertifizierte Desktop-Sharing-Systeme). Jeglicher Zugriff muss systemtechnisch überwacht werden, d.h. Zeitpunkt und Aktivitäten müssen zweifelsfrei aufgezeichnet werden. Das Logging sollte auf zertifizierten Systemen erfolgen, welche gegen Manipulation geschützt sind; auch hier sind entsprechende vertragliche Vereinbarungen mit dem Dienstleister angebracht (siehe auch Maßnahmen-Cluster „Sicherheitsevaluierung & Funktions-, Interoperabilitäts- und Penetrations-Tests“).

6. Maßnahmen-Cluster: Sicherheitsanforderungen für Hersteller:
Wie bereits im Maßnahmen-Cluster „Sicherheitsevaluierung & Funktions-, Interoperabilitäts- und Penetrations-Tests" erwähnt, sollten Hersteller die von ihnen durchgeführten Testabläufe offenlegen und verpflichtet werden, bei Bekanntwerden kritischer Schwachstellen ihre Kunden zu informieren und entsprechend nachzurüsten. Neben den unverzichtbaren Tests auf Hersteller- und Netzbetreiberseite sollten unabhängige Prüf- bzw. Zertifizierungsstellen für IKT-Sicherheitsaspekte von Smart-Grid-Komponenten etabliert werden, ähnlich wie sie für Safety-Aspekte bereits existieren. Neben der Prüfung von Einzelkomponenten sollte auch die Systemintegration, d.h. die Wirkung im Gesamtsystem, getestet werden.

Die Überprüfung einzelner Komponenten und ein vorhandenes Prüfzertifikat gibt jedoch noch keine Gewährleistung für hohe Sicherheit. Durch falsche Konfiguration oder Implementierung in den einzelnen Systemen kann es zu neuen Schwachstellen kommen. Jegliche Änderung im System sollte durch neuerliche Penetrationstests überprüft werden (siehe dazu auch den folgenden Maßnahmen-Cluster). Zusätzliche externe Prüfungen ermöglichen es, fehlerhafte Prüfszenarien festzustellen und gleichzeitig eine kontinuierliche Sicherheit des Systems zu gewährleisten. Anforderungen an die kontinuierliche Systemsicherheit sind in den Wartungsverträgen zu vereinbaren. Systemtests, Systemhärtungen, Sicherheitspatches, Updates sollten nur nach vorheriger Absprache und entsprechenden Tests durchgeführt werden. Nach Möglichkeit sollten einzelne Komponenten getestet werden und erst nach einer Überprüfung der jeweiligen einzelnen Komponente das Upgrade ins gesamte System gespielt werden. Ein vorher durchgeführtes Systembackup erleichtert ein Wiederherstellen bei Fehlern auf einen möglichst zeitneutralen Systemletztstand.

7. Maßnahmen-Cluster: Change Management, Patch Management, Configuration Management:
Ein Netzbetreiber sollte zu jedem Zeitpunkt ein umfassendes Bild über alle eingesetzten Systeme und deren (Wartungs-) Zustand haben, um bei Sicherheitsvorfällen rasch reagieren zu können. Beispielsweise sollte eine Dokumentation der gesamten verwendeten Software-Versionsstände vorliegen, damit bei Meldungen von Softwarebugs sofort ein Überblick über die Bedrohungen vorhanden ist und entsprechend reagiert werden kann. Die vorhandenen Softwareversionen sollten regelmäßig überprüft und –

soweit das System dies erlaubt – aktualisiert werden; bei bekannten Softwarebugs sollten (wenn notwendig) andere Schutzmechanismen angewendet werden, damit das Schutzziel erreicht werden kann. Nach jeder Systemänderung (z. B. Austausch von Komponenten oder Software-Versionen) sollten System- und Sicherheitstests stattfinden, nach größeren Systemänderungen entsprechend umfassende Tests des Gesamtsystems und zusätzlich Penetrationstests. In diesem Zusammenhang ist eventuell die Einführung einer Policy-Matrix sinnvoll, um zu definieren, welche Änderungskonstellationen jeweils zu welchen Penetrations- und Systemtests führen und in welchem Umfang diese stattfinden sollten.

8. Maßnahmen-Cluster: Physische Sicherheitsmaßnahmen:
Neben inhärenten IKT-Sicherheitsmaßnahmen sind auch zusätzliche physische Sicherheitsmaßnahmen erforderlich. Eine lückenlose Videoüberwachung der Lager, in denen beispielsweise Smart Meter vor Auslieferung aufbewahrt werden, kann Manipulationen oder Diebstähle aufzeigen bzw. Täter bereits im Vorfeld abschrecken. Diese Maßnahme könnte gegebenenfalls auch auf alle Smart-Grid-Komponenten ausgeweitet werden, um zu vermeiden, dass Komponenten entwendet, manipuliert und wieder eingeschleust werden. Auch IKT-unabhängige Sicherheitssysteme (z. B. Zutrittssysteme) sollten durch anerkannte Stellen zertifiziert sein und nach Herstelleranleitung aufgebaut werden.

9. Maßnahmen-Cluster: Incident Management:
Bzgl. der Behandlung von Sicherheitsvorfällen ist es wichtig zu unterscheiden, ob die betroffenen Geräte bzw. Netzsegmente tatsächlich abgeschaltet werden oder lediglich eine Alarm- bzw. Fehlermeldung an das Kontrollzentrum abgesetzt wird; Fehlermeldungen dürfen jedenfalls nicht die Aufgabe eines Schutzgerätes übernehmen. Sofern es zu einer Abschaltung kommt, müssen besondere Sicherheitsvorkehrungen beim Wiedereinschalten beachtet werden, insbesondere bei einer – künftig evt. technisch realisierbaren – automatischen Wiedereinschaltung.

10. Maßnahmen-Cluster: Mehrstufiges Sicherheitskonzept:
Sicherheitsvorkehrungen sollten (vor allem bei kritischen Smart-Grid-Komponenten) idealerweise über mehrere Schichten implementiert sein; so sind neben der technischen Sicherheit auch organisatorische Maßnahmen als Teil eines Gesamtkonzeptes erforderlich. Neben kaufmännischen und

technischen Aspekten sollten auch die gesetzlichen Vorgaben beachtet werden, speziell bei personenbezogenen Daten, da der Gesetzgeber nicht zwischen IKT und Fernwirktechnik unterscheidet. Generell ist in diesem Bereich eine langfristige Entwicklung erforderlich, da viele Geräte bzw. Protokolle die entsprechende Funktionalität derzeit nicht anbieten und ein Austausch zu teuer wäre (man beachte, dass die Produktlebenszyklen in der Schalt- und Fernwirktechnik häufig 20 Jahre und mehr betragen). Neue Systeme bzw. Systemkomponenten sollten in der Lage sein, parallel zu bestehenden Komponenten zu arbeiten und trotzdem inkrementell neue Features zulassen.

3. Fazit und Ausblick zum Maßnahmenkatalog

Die Auswertungen haben gezeigt, dass die wichtigsten Sicherheitsmaßnahmen darin bestehen,

1. die **Authentizität und Integrität der Kommunikation** sicherzustellen,
2. **Sicherheitsevaluierung & Funktions-, Interoperabilitäts- und Penetrations-Tests** durchzuführen und
3. ein **effektives Change, Patch und Configuration Management** zu gewährleisten.

Vor allem die Sicherstellung der Authentizität und Integrität ist von zentraler Bedeutung. Die Identität und Berechtigung des Absenders einer Nachricht sollte zweifelsfrei feststellbar sein, um Betrug z. B. durch Spoofing zu verhindern und in weiterer Folge beispielsweise die Umsetzung unberechtigter Steuerbefehle zu unterbinden. Ebenso ist die Unversehrtheit der Nachricht sicherzustellen, d.h. unberechtigte Änderungen müssen erkannt und entsprechend behandelt werden. Für beide Ziele, d.h. Authentizität und Integrität, existieren etablierte Methoden und Werkzeuge aus der Welt der IKT; die große Herausforderung liegt darin, diese auch in industriellen Steuerungssystemen wie z. B. Smart Grids einzusetzen, wo traditionell noch viele Geräte und Systeme aus dem Altbestand vorhanden sind, die ggf. die erforderlichen Methoden nicht unterstützen oder gar durch diese in ihrer Funktionsweise eingeschränkt oder gestört werden können. Die Evaluierung der Sicherheitsmaßnahmen (siehe Teil VI) hat gezeigt, dass viele

der vorgeschlagenen Maßnahmen – trotz ihrer scheinbaren Selbstverständlichkeit – in heutigen Energieinfrastrukturen nicht implementiert sind.

Die Resultate aus der Definition und Priorisierung der Maßnahmen sind konsistent mit den Ergebnissen der praktischen Sicherheitsanalyse aus Teil IV; auch dort hat sich gezeigt, dass insbesondere ein Mangel an geeigneten Authentizitäts- und Integritätsmaßnahmen zu zahlreichen Verwundbarkeiten und Angriffsmöglichkeiten führt. Neben zeitgemäßem, sicherem Design und einer korrekten Implementierung ist umfassendes Testen von kritischen Smart-Grid-Komponenten ein wichtiger Aspekt, um die Sicherheit und Resilienz derselben zu verifizieren.

4. Tool-Implementierung des Maßnahmenkatalogs

4.1. Vorteile einer Tool-Implementierung

Der im $(SG)^2$-Projekt entwickelte Maßnahmenkatalog sollte auch als Tool implementiert werden, um dessen Anwendbarkeit für Netzbetreiber und andere interessierte Stakeholder zu vereinfachen und ihnen die Möglichkeit zu geben, den Implementierungsstatus der einzelnen Sicherheitsmaßnahmen innerhalb ihrer Organisation zu protokollieren.

Der grundlegende Vorteil einer Tool-Implementierung, gegenüber der herkömmlichen Methode der Verwendung von Tabellenkalkulationsapplikationen (z. B. Microsoft Excel), basiert auf der einfacheren, effektiveren und effizienteren Durchführung eines Risikomanagement-Prozesses. Dies hängt mit zahlreichen Auswertungs- und Kontrollmöglichkeiten eines Tools zusammen, welche zur vollständigen und transparenten Durchführung aller relevanten Schritte des Risikomanagements beitragen. Darüber hinaus ist jegliche Berechnungslogik, welche beispielsweise für die Durchführung einer Risikoanalyse notwendig ist, in einem Tool bereits implementiert. Es ergeben sich folgende weiteren Vorteile:

- Möglichkeit der Hinterlegung der jeweiligen Organisationsstruktur (dies kann auch eine technische Systemlandschaft sein)
- Transparente Zuordnung von Risiken, Schwachstellen, Bedrohun-

gen und Assets (in weiterer Folge auch Maßnahmen) zu den passenden Organisationseinheiten
- Möglichkeit der Hinterlegung von Verantwortlichkeiten in Bezug auf die „Pflege" der jeweiligen Risiken
- Generierung verschiedener Reports, basierend auf unterschiedlichen Aspekten des Risikomanagements
- Unterschiedliche Risikobewertungsmethoden stehen zur Auswahl;
- Möglichkeit der Implementierung verschiedener Kataloge für Bedrohungen, Maßnahmen, Schwachstellen, etc. (auch basierend auf einschlägigen Normen/Standards, wie z. B. ISO/IEC 27002)
- Monitoring-Möglichkeiten im Zuge der Risikosteuerung (z. B. Grad der Umsetzung von Maßnahmen)
- Erhöhte Benutzerfreundlichkeit im Allgemeinen

4.2. Auswahl des Tools

Generell existieren zahlreiche Applikationen im Umfeld der Thematik „Risikomanagement", die hier nicht alle näher beleuchtet werden. Im Wesentlichen wird auch hier zwischen kommerziell erhältlichen und frei verfügbaren Programmen unterschieden. Im Folgenden wird jeweils ein Beispiel für beide Kategorien kurz beschrieben.

4.2.1. CRISAM

Bei CRISAM®[241] handelt es sich um ein österreichisches Produkt, welches vom Team der österreichischen Firma Calpana Business Consulting GmbH als Risikomanagement-Methode entwickelt wurde. Es handelt sich dabei um keine Open-Source-Applikation. Seit dem Jahr 2004 wird diese Methode vielfach erweitert und verbessert und hat sich im Unternehmensbereich weitgehend als Industriestandard durchgesetzt (im Umfeld von Österreich und Deutschland). Konkret folgt CRISAM als Risikomanagement-Methode einem sechsstufigen Vorgehensmodell entsprechend der ISO/IEC 31000. Es wird das Ziel der einfacheren Handhabung des Themas „Risikomanagement" verfolgt. Dies bedeutet eine Ermöglichung der präzisen Bewertung, Chancen und Risiken im Unternehmen ganzheitlich und wertorientiert darzustellen, und daraus resultierende Konsequenzen nachvollziehbar

[241] Corporate Risk Application Method

zu machen. Mittels einer Vielzahl an Content Libraries und Bewertungs- und Aggregationsmethoden werden unterschiedliche Anwendungsgebiete des Risikomanagements unterstützt, wie beispielsweise Enterprise Risk Management, Information Risk Management, oder Project Risk Management.

4.2.2. verinice

Bei verinice handelt es sich um ein reines ISMS-Tool (d.h. ein Werkzeug zur Unterstützung eines Informationssicherheitsmanagementsystems), des deutschen Unternehmens SerNet Service Network GmbH. Mit diesem Tool kann die Informationssicherheit definiert, gesteuert, kontrolliert, aufrechterhalten und verbessert werden. Es handelt sich dabei um eine Open Source Software und ist daher frei und kostenlos verfügbar. Basierend auf dem frei zugänglichen Programmcode, kann verinice auf die Anforderungen unterschiedlicher Anwendungsbereiche individuell angepasst werden. Dieses ISMS-Tool ist das einzige, welches sich auf der Referenzliste des BSI befindet und stützt sich daher in erster Linie auf den IT-Grundschutz des BSI (Grundschutzhandbuch ist bereits in das Tool integriert), mit allen verfügbaren Bausteinen, Maßnahmen und Gefährdungen. Darüber hinaus ist die Verwendung weiterer Kataloge, wie beispielsweise die ISO/IEC 27001/2, möglich und durchführbar. Neben dem frei verfügbaren Tool, sind auch kostenpflichtige Dienstleistungen (Consulting, Audit-Dienstleistungen) von SerNet beziehbar.

Die Wahl fiel auf das Tool verinice, da es dem $(SG)^2$-Projektkonsortium wichtig war, die Tool-Implementierung in Form einer offenen Schnittstelle zu vollziehen, die allen interessierten Stakeholdern kostenfrei zur Verfügung gestellt werden kann. Darüber hinaus besteht dadurch die Möglichkeit, eine frei verfügbare sogenannte „Ready-to-Use"-Anwendung im Kontext einer möglichen Risikobewertung einzusetzen.

5. Vorgehensweise bei der Tool-Implementierung

Im Zuge der Tool-Implementierung wurden bereits vorliegende Ergebnisse innerhalb des Projektes (IKT-Architekturmodell, Bedrohungskatalog, Risikomatrix und Maßnahmenkatalog) verwendet und es wurde auf Erfahrun-

gen aus Vorprojekten aufgebaut.

Der Ablauf der Implementierung gliederte sich wie folgt in:

1. Erstellung eines neuen „Information Security Model“, folgend als „Smart Grid Architecture“ bezeichnet
2. Erstellen der Assetstruktur basierend auf der IKT-Architektur
3. Schutzbedarfsfestlegung bei den einzelnen Assets, basierend auf der Business-Impact-Analyse
4. Einfügen der einzelnen Bedrohungen aus dem Maßnahmenkatalog als „Bedrohungen“
5. Einfügen der einzelnen Maßnahmen aus dem Maßnahmenkatalog als „Controls“
6. Anpassung der Darstellung der Bedrohungshäufigkeitswerte in verinice in Bezug auf die, im Zuge der Erstellung des Maßnahmenkatalogs, gewählten Eintrittswahrscheinlichkeiten

In den folgenden Abschnitten erfolgt eine detailliertere Betrachtung des Implementierungsablaufs.

5.1. Abbildung der Komponenten des IKT-Architekturmodells und des Maßnahmenkatalogs

Die folgenden Erläuterungen betreffen den schrittweisen Implementierungsvorgang innerhalb des Tools „verinice“. Initial wurde ein neues „Information Security Model“ mit der Bezeichnung „Smart Grid Architecture“ (siehe auch Abbildung 14) erstellt. Dies stellt einen umfangreichen Konfigurationsbereich zur Verfügung, welcher die Bereiche von „Anforderungen“ bis „Szenarien“ beinhaltet. Im Zuge der Implementierung wurden ausschließlich die Bereiche „Assets“, „Bedrohungen“ und „Controls“ in Betracht gezogen.

5.1.1. Abbildung der IKT-Architektur

Zur übersichtlichen Gestaltung der IKT-Architekturkomponenten wurden im ersten Schritt die Komponenten-Cluster (z. B. „Haushalt“) in Form von „Assetgruppen“ im Bereich „Assets“ eingefügt. Darauf folgend wurden die einzelnen Architekturkomponenten in dem jeweils zutreffenden Kompo-

nenten-Cluster angelegt (z. B. „Smart Meter“ in „Haushalt“). Abbildung 14 zeigt die Assetstruktur mit dem aufgeklappten Komponenten-Cluster „Haushalt“.

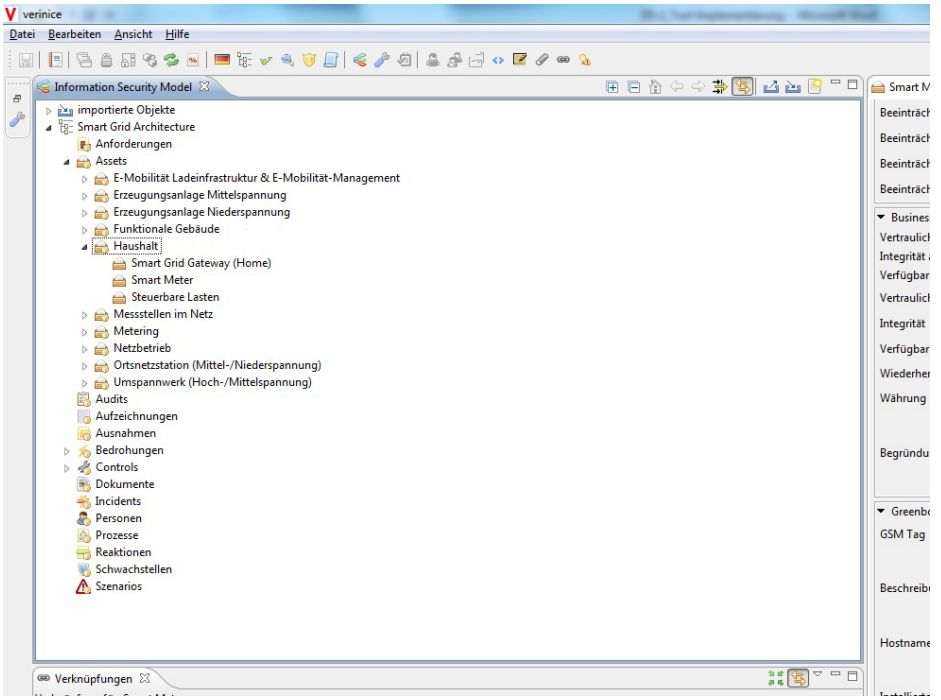


Abbildung 14: Darstellung der IKT-Architektur als Asset-Struktur

5.1.2. Festlegen der Organisationseigenschaften

In Bezug auf die betrachtete Organisation bzw. Organisationseinheit, welche den Geltungsbereich der Risikoanalyse festlegt, können verschiedene Informationen definiert werden. Darunter fallen allgemeine Beschreibungen (Bezeichnung der Organisation, Standort, Adresse, etc.) und Details zur Risikoanalyse. Diesbezüglich sind die Risikoakzeptanzschwellen für die C-, I- und A-Werte[242] festzulegen. Diese entscheiden später über die Kritikalität von bewerteten Risiken. Darüber hinaus können die vorgegebenen Definitionen für die Business-Impact-Klassifizierung, Bedrohungshäufig-

[242] Confidentiality (Vertraulichkeit), Integrity (Integrität), Availability (Verfügbarkeit)

keiten und Schwachstellengrade angepasst werden. Im Zuge der Implementierung des Maßnahmenkatalogs wurde hier die Definition der Bedrohungshäufigkeiten, entsprechend der Vorgaben aus dem Maßnahmenkatalog, angepasst.

5.2. Schutzbedarfsfeststellung der Assets

Nach der Finalisierung der Assetstruktur, erfolgte die Implementierung der Business-Impact-Analyse. Dafür wurde bereits im Vorfeld die von verinice vorgegebene Struktur der Bewertung der C/I/A-Werte berücksichtigt. Tabelle 19 beschreibt die Schutzbedarfsstruktur.

Tabelle 19: Darstellung der Schutzbedarfsstruktur

Vertraulichkeit (C)	0	Öffentlich
	1	Externer Gebrauch
	2	Interner Gebrauch
	3	Vertraulich
Integrität (I)	0	Keine
	1	Normal
	2	Hoch
Verfügbarkeit (A)	0	Basis
	1	Normal
	2	Hoch
	3	Sehr hoch
	4	Außergewöhnlich

Diese durch verinice vorgegebenen Skalen wurden für die Business-Impact-Analyse verwendet. Dazu wurde für jede einzelne Komponente des IKT-Architekturmodells eine Einschätzung vorgenommen, wie sich die Kompromittierung dieser Komponente im Hinblick auf Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) auswirkt. Auf diese Weise konnte der Schutzbedarf der einzelnen Komponenten im Rahmen der in Tabelle 19 aufgeführten Skalen bestimmt werden. Die Business-Impact-Analyse fand zunächst in einer Expertengruppe innerhalb des Projektkonsortiums statt und wurde anschließend dem gesamten Projektkonsortium präsentiert, und das Feedback desselben wurde in die Analyse einbezogen. Abbildung 15 zeigt das Ergebnis im Überblick.

Asset Cluster	Asset	C+I+A	Vertraulichkeit - C	Integrität - I	Verfügbarkeit - A
Funktionale Gebäude	Smart Grid Gateway (Building)	4	1	1	2
Funktionale Gebäude	Gebäudeleittechnik	3	1	1	1
Funktionale Gebäude	Gebäudeautomation	3	1	1	1
Funktionale Gebäude	HVAC	2	1	0	1
E-Mobilität	E-Mobility Management System	7	3	2	2
E-Mobilität	Ladestation	6	2	2	2
E-Mobilität	E-Fahrzeug	3	1	0	2
Haushalt	Smart Grid Gateway (Home)	3	1	1	1
Haushalt	Smart Meter	5	3	2	0
Haushalt	Steuerbare Lasten	2	1	0	1
Erzeugungsanlage LV	Smart Grid Gateway (DER LV)	5	2	1	2
Erzeugungsanlage LV	Erzeugungsanlage (LV)	3	1	0	2
Erzeugungsanlage MV	Automation Frontend	5	0	2	3
Erzeugungsanlage MV	Smart Grid Gateway (DER MV)	5	0	2	3
Erzeugungsanlage MV	Erzeugungsanlage (MV)	4	0	1	3
Messstellen im Netz	Automation Frontend	2	0	1	1
Messstellen im Netz	Messstellen MV	2	0	1	1
Umspannwerk (HV / MV)	Automation Frontend	4	0	2	2
Umspannwerk (HV / MV)	Primary Substation Node	4	0	2	2
Umspannwerk (HV / MV)	Local I/O	4	0	2	2
Ortsnetzstation (MV / LV)	Datenkonzentrator	5	3	1	1
Ortsnetzstation (MV / LV)	Secondary Substation Node	2	0	1	1
Ortsnetzstation (MV / LV)	Local I/O	2	0	1	1
Netzbetrieb	SCADA	8	2	2	4
Netzbetrieb	Distribution Management System	7	2	2	3
Netzbetrieb	Automation Headend	6	1	2	3
Metering	Meter Data Management	7	3	2	2
Metering	AMI Headend	6	3	2	1

Abbildung 15: Ergebnisse der Business-Impact-Analyse im Überblick

Die Konfiguration der Schutzbedarfswerte eines jeden Assets erfolgt in verinice direkt über das Registerblatt des jeweiligen Assets im dafür vorgesehenen Bereich „Business Impact“. In diesem Bereich befinden sich u.a. die Optionsfelder für die C/I/A-Werte und ein Textfeld „Begründung“,

welches zur Erklärung der gewählten Schutzbedarfswerte herangezogen wurde. Abbildung 16 zeigt beispielhaft die Schutzbedarfskonfiguration für das Asset „Smart Meter“.

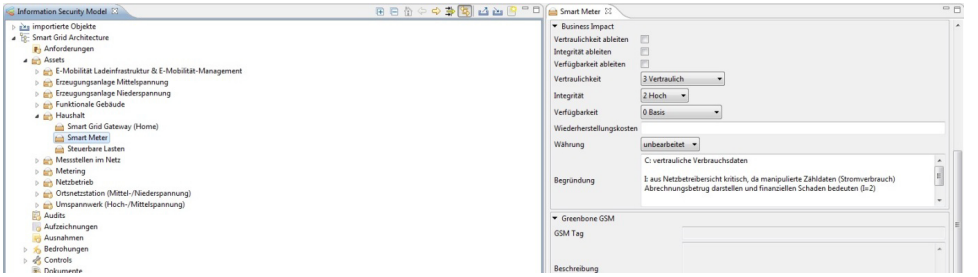


Abbildung 16: Schutzbedarfskonfiguration für das Asset „Smart Meter“

5.3. Abbildung des Maßnahmenkatalogs

Die Bedrohungen wurden in verinice innerhalb der Smart Grid Architecture in dem passenden Komponenten-Cluster „Bedrohungen“ eingefügt. Zusätzlich wurde auch die inhaltliche Beschreibung der einzelnen Bedrohungen aus dem Bedrohungskatalog übernommen und in das dafür vorgesehene Feld „Beschreibung“ im Registerblatt jeder Bedrohung eingefügt. Eine Bewertung der „Bedrohungshäufigkeit“ wurde berücksichtigt und basiert auf die Anwendung des Maximalprinzips alle Einzelbewertungen einer Bedrohung in der Bedrohungsmatrix. Abbildung 17 zeigt die soeben genannten Konfigurationsschritte beispielhaft anhand der Bedrohung „Ausfall oder Störung von IT-Systemen“.

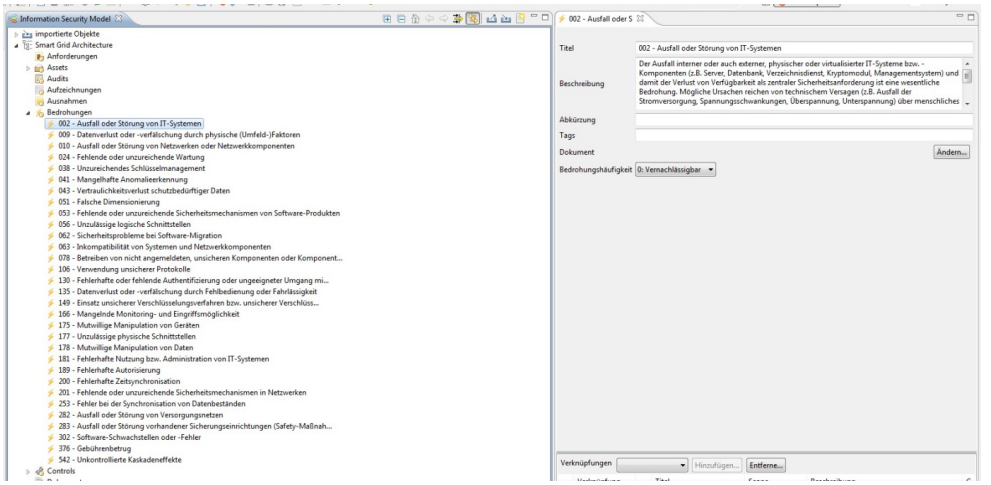


Abbildung 17: Darstellung der Bedrohungen

Die Maßnahmen wurden dem Maßnahmenkatalog entnommen und im Feld „Titel“ im Control-Registerblatt beschrieben. Die idealen Umsetzungsszenarien (siehe Abschnitt 2.5) wurden in das Feld „Zielsetzung“ übernommen, die konkreten Umsetzungsbeispiele in das Feld „Erklärung“ (siehe Abschnitt 2.6). Beide Textfelder befinden sich ebenfalls im Control-Registerblatt, allerdings in der Rubrik „Implementation“. Eine Bewertung der „Control-Level“ (gleichnamige Rubrik im Control-Registerblatt) hinsichtlich der Auswirkungen dieser Maßnahme, wurde nicht durchgeführt und obliegt der zukünftigen Einschätzung der Anwender dieses Maßnahmenkatalogs. Darunter fällt auch die fortlaufende Dokumentation der Implementierung („Implementieren“ in der Rubrik „Implementation“) und des Reifegrads (gleichnamige Rubrik). Abbildung 18 zeigt die soeben beschrieben Konfiguration beispielhaft für die Maßnahme „Change, Patch & Configuration Management“.

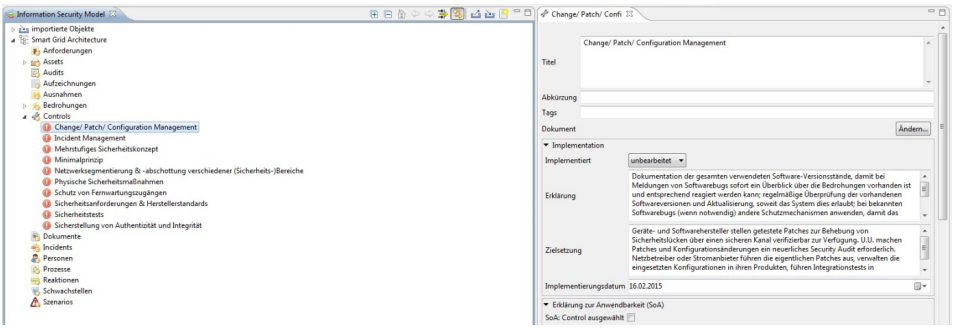


Abbildung 18: Darstellung der Controls

6. Evaluierung der Tool-Implementierung

In diesem Abschnitt wird die Nutzwertanalyse beschrieben, die im Rahmen des $(SG)^2$-Projektes für verinice durchgeführt wurde. Im Zuge dieser Analyse wurde das Tool anhand relevanter Software-spezifischer Kriterien bewertet. Die Bewertung basiert auf einem Fünf-Punkte-Schema, welches den durch verinice möglichen Erfüllungsgrad des jeweiligen Kriteriums widerspiegelt. Die Bewertung reicht von 1 (Anforderung nicht erfüllt) bis 5 Punkte (Anforderung erfüllt). Die einzelnen Kriterien werden für die Berechnung des Gesamtwertes gewichtet. Tabelle 20 zeigt die Ergebnisse der Nutzwertanalyse.

Tabelle 20: Nutzwertanalyse des Tools „verinice“

Ziele / Kriterien	**Gewichtung**	**Bewertung**	**Wert**	**Anmerkungen**
ISMS/Risikomanagement				
Modellieren der Risikoobjekte	1	5	5	Gegeben
Darstellung Abhängigkeiten zwischen den Risikoobjekten	1	5	5	Klar ersichtlich, entsprechende Visualisierung
Festlegen von Risikoakzeptanzschwellen	1	5	5	Im Zuge der Festlegung der Organisationseigenschaften
Festlegen der Bedrohungsklassen	1		0	

Ziele / Kriterien	Gewichtung	Bewertung	Wert	Anmerkungen
Schutzbedarfsanalyse je Asset	1	5	5	Gegeben
Festlegen der Kriterien für die Risikobewertung (Basis für die Bewertung festlegen)	1		0	
Abbildung von Bedrohungen & Häufigkeit	1	5	5	Gegeben
Business Impact Analyse	1	2	2	Textuell möglich
Bewertung der IST-Qualität	1	5	5	Gegeben, eingeschränkte Detailierungsstufe
Maßnahmen identifizieren und verfolgen	1	5	5	Gegeben
Kosten-Nutzen-Analyse	1	0	0	Nicht möglich
Asset Register gem. ISO 27001 (Inventory of Assets)	1	5	5	Expliziter Export eines Asset-Registers
Verfügbare Kataloge	1	5	5	Kataloge im Internet als Download frei verfügbar
Compliance mit Normen und Standards	1	4	4	IT-Grundschutz, ISO 27001, VDA Anforderungen
Self Assessment	1	5	5	möglich
Fehlerbaumanalyse	1	1	1	
BCM-Unterstützung	1	1	1	BS 25999
Klares Vorgehensmodell zur Risikoanalyse	1	1	1	Kein klares Vorgehensmodell, auf BSI-Vorgehensmodell ausgerichtet
RM Spezifische Technische Anforderungen				
Funktionsumfang des Systems	1	4	4	Mehrere Perspektiven (Audits, BSI GS, Datenschutz, ISM, Security Assessment), kein klares Vorgehensmodell
Reporting Funktion	1	5	5	BIRT Reporting, individuell anpassbare Reports

Ziele / Kriterien	Gewichtung	Bewertung	Wert	Anmerkungen
				über integrierten Designer
Verfügbare Report-Formate	1	5	5	Ausgabeformate: pdf, doc, html, xls, ods, odt
Import eigener Kataloge, Bausteine, etc.	1	5	5	Eigene Kataloge möglich, .csv-Format, einfache Importmöglichkeit
BSI Kataloge	1	5	5	BSI GS-Katalog
GS-Tool-Import	1	5	5	Import möglich
Benutzeroberfläche				
Selbstbeschreibungsfähigkeit	1		0	
Aufgabenangemessenheit	1		0	
Erwartungskonformität	1		0	
Fehlertoleranz	1		0	
Individualisierbarkeit/ Anpassbarkeit	1		0	
Bedienbarkeit	1	4	4	Komplexere GUI, kein intuitives Design
Mobile Version	1	2	2	Keine Mobile Version vorhanden, kann unternehmensspezifisch programmiert werden
Mehrsprachigkeit	1	5	5	Deutsch, Englisch
Handbücher und weitere Dokumentationen	1	3	3	Tutorials im Tool (Deutsch/Englisch), kostenpflichtiges Benutzerhandbuch (49,98) für PRO-Variante
Schulungsmöglichkeiten	1	5	5	Schulungen und Workshops durch SerNet
Workflow Funktionalitäten				
Workflow Engine	1	5	5	Möglich, in kostenpflichtiger PRO-Version
Zentrale Dokumentenablage	1	5	5	Möglich
Mailbenachrichtigungen	1	5	5	Möglich, in kostenpflichtiger PRO-Version

Ziele / Kriterien	Gewichtung	Bewertung	Wert	Anmerkungen
Audit Management	1	5	5	Möglich, in kostenpflichtiger PRO-Version
Web Frontend	1	5	5	Möglich, in kostenpflichtiger PRO-Version
Task Management	1	5	5	Möglich, in kostenpflichtiger PRO-Version
Technische Anforderungen				
Multi-Platform (Unix, Windows, Mac)	1	5	5	Unix, Windows, Mac (Plattformunabhängigkeit)
Mandantenfähigkeit / Multiuser-Fähigkeit	1	5	5	Gegeben
Rollenkonzept	1	5	5	Gegeben
Lizenzmodell	1	5	5	Keine Lizenz- oder Bezugskosten
Softwarekosten	1	5	5	Kostenlose Basisversion, Upgrade auf kostenpflichtige PRO Version möglich
Software Customizing	1	4	4	Interne Software-Anpassungen (Open Source) oder mit Unterstützung von SerNet (zusätzliche Kosten) möglich
Herstellerabhängigkeit	1	5	5	Open Source, hausinterne Weiterentwicklung möglich
Verteilung der Software	1	5	5	Exe-File, kein Setup notwendig
Erweiterbarkeit/Updates	1	5	5	Kostenlose Updates möglich, Umsetzung eigener Anforderungskataloge, PRO-Variante
Upgradefähigkeit	1	5	5	Im Tool möglich
Offline-Fähigkeit	1	5	5	Gegeben
Erforderliche Software (Zusätzlich benötigte Programme)	1	5	5	JRE (RCP), Oracle, PostgreSQL, Apache, keine Unterstützung von Microsoft SQL Server
LDAP / AD / Direc-	1	5	5	Möglich mit PRO-

Ziele / Kriterien	Gewichtung	Bewertung	Wert	Anmerkungen
tory Integration				Variante
Access Controls	1	5	5	Möglich mit PRO-Variante
Encryption / Secure Access	1	5	5	Sichere Verbindung (SSL) umgesetzt, Secure Access mit PRO-Variante möglich
Browser-Abhängigkeit	1	5	5	Nein
Ergebnis			**216**	

7. Ausblick zur Tool-Implementierung

Angesichts der bereits erwähnten breiten Verwendung des Tools CRISAM bei verschiedenen Energielieferanten und Netzbetreibern in Österreich wird eine Integration des entwickelten Maßnahmenkatalogs in CRISAM angestrebt. Dies soll zu einer breiten praktischen Anwendung der wissenschaftlich fundierten Ergebnisse der Entwicklung des Maßnahmenkatalogs führen. In Folge dessen erscheint auch eine kontinuierliche Anpassung des erarbeiteten Maßnahmenkatalogs möglich und sinnvoll.

Die Tool-Implementierung des $(SG)^2$-Maßnahmenkatalogs inkl. Installationsanleitung ist auf Anfrage erhältlich über Herrn Thomas Hecht (thomas.hecht@ait.ac.at).

Teil VI: Evaluierung der Sicherheitsmaßnahmen bei der Energie AG

1. Zielsetzung und Vorgehensweise

Ziel dieses Teiles der Projektarbeiten war die Darstellung der Anwendbarkeit des in Teil V definierten Maßnahmenkataloges in bestehenden Systemen. Einige Maßnahmen wurden in dem Testlabor beim Projektpartner Energie AG umgesetzt und einer Maßnahmenprüfung unterzogen. Maßnahmen auf Managementebene wurden in der Ausprägung der derzeit verwendeten Richtlinien und Anforderungen des in den Unternehmen verwendeten Informationssicherheitsmanagementsystems dargestellt (die Energie AG ist seit 2008 gemäß ISO 27001 zertifiziert; die IKT-Systeme liegen im Fokus dieser Zertifizierung).

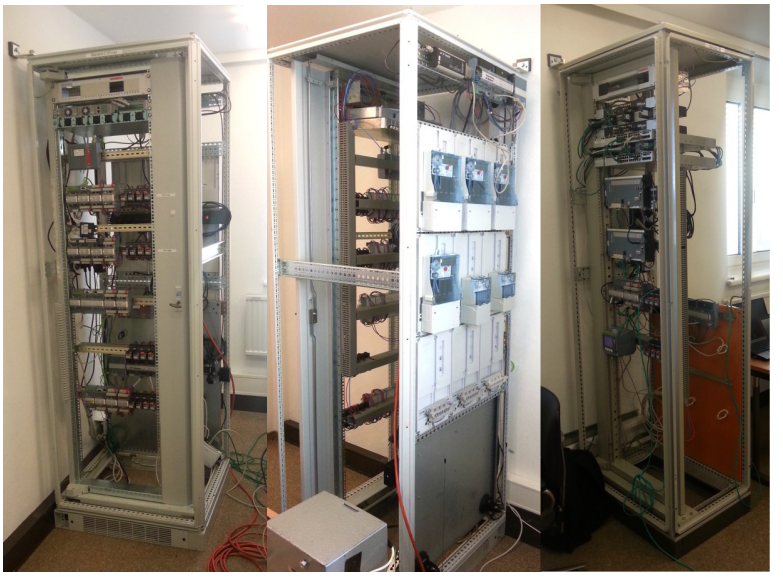
Die Energie AG hat das in der Nähe des Netzführungszentrums bestehende Testsystem gemäß einigen Anforderungen aus dem Maßnahmenkatalog adaptiert. Dies diente in erster Linie dazu festzustellen, ob die festgelegten Maßnahmen in der Praxis auch anwendbar sind. Vor allem stellte sich die Frage, inwieweit die Sicherheitsanforderungen auch Systeme, die seit mehr als 20 Jahre bestehen, miteinbeziehen bzw. deren Sicherheit erhöhen können. Das von der Energie AG aufgestellte Testsystem entspricht der Realität des Netzes im verkleinerten Maßstab. Es wurden alle Szenarien der IKT-Anbindungen der Fernwirkstationen abgebildet. Diese IKT-Anbindungen sind in mehrfacher Ausführung im Feld gleich implementiert. Zudem konnte ein zweiter Systemanbieter gewonnen werden, der eines seiner Systeme für die Einbindung in den Testaufbau zur Verfügung gestellt hat.

Im Zuge dieser Tests (topologische Analysen, Netzwerkscans, Port-Scans, Analysen der Systemkonfigurationen, praktische Tests von konfigurierten Sicherheitsmaßnahmen, Network Sniffing, Protokollanalyse, etc.) wurde die Teststellung bei der Energie AG den $(SG)^2$-Sicherheitsmaßnahmen gegenübergestellt und praktisch evaluiert. Der vorliegende Bericht beschreibt einen Teil der erzielten Ergebnisse. Kritische Informationen, durch welche Detailergebnisse der Sicherheitstests oder Schlussfolgerungen auf das be-

stehende Kommunikationsnetz möglich wären, wurden für die Publikation entfernt. Neben der hier beschriebenen Evaluierung wurden weitere Systemteile wie z. B. die Switches auf Leittechnik-Ebene und Außenanlagen-Übergaben evaluiert; die Ergebnisse dieser Prüfungen sind aus Platzgründen nicht in dieser Publikation enthalten.

2. Teststellung bei der Energie AG

Abbildung 19 gibt einen Überblick über den Aufbau der Testschränke. Die aufgebaute Versuchsanordnung entspricht der Struktur des Energie AG IKT-Netzes und der vorhandenen Fernwirksysteme in den Außenanlagen einschließlich des SCADA-Systems. Die Netzstruktur wurde soweit vereinfacht, als dass jeweils eine vor Ort eingesetzte Technik aufgebaut wurde und nicht wie in der Realität diese dann mehrfach. Auf die Funktionsfähigkeit und Leistungsfähigkeit des Systems und der in dem System erfolgten Prüfungen hat dies jedoch keine Auswirkungen. Die Bandbreiten zwischen den einzelnen Systemen sind durch das konzerninterne Glasfasernetz sicher als ausreichend anzulegen. Die Schnittstellen zu externen schmalbandigen Übertragungssystemen sind nur vereinzelt vorhanden. Größtenteils wird die Übertragung mit eigener Infrastruktur gewährleistet.



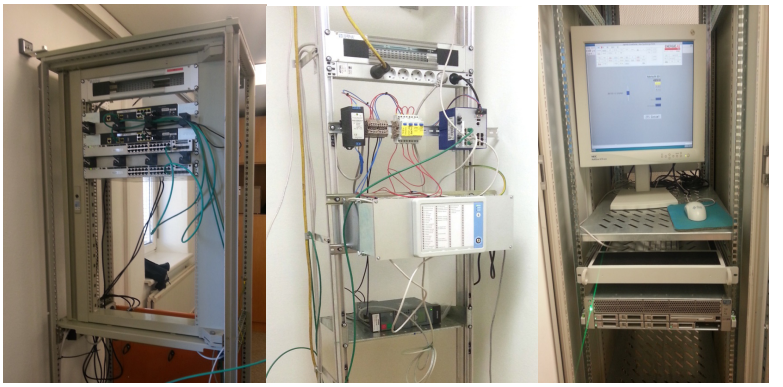


Abbildung 19: Teststellung bei der Energie AG

Die wichtigsten Knotenpunkte besitzen eine physische Überwachung mit Zutrittskontrolle und Videosystemen, wobei ausgehend von den Anregungen der Systeme Meldungen in der zentralen Leitwarte erfolgen, aufgrund welcher das vorhandene Bedienpersonal Maßnahmen zu setzen hat. Diese Maßnahmen wurden aufgrund der Einfachheit und des Zeitaufwandes nicht überprüft. Eine Gewährleistung dieser Maßnahmen wird durch das jährliche ISO 27001 Audit extern und intern unangekündigt kontrolliert. Ein Nichteinhalten von Maßnahmen führt dazu, dass ein Risikobericht erfasst wird und entsprechende mit der Geschäftsführung und dem Kunden abgestimmte Verbesserungen durchgeführt werden. Diese Verbesserungen werden einem Systemaudit unterzogen; der daraus gewonnene Informationsgehalt wird dokumentiert, in den ISMS-Überprüfungszyklus aufgenommen und im System abgelegt.

2.1. Beschreibung der Komponente zentraler Netzrechner

Als zentraler Netzrechner (ZNR) kommt eine Siemens SPECTRUM Software für die Netzleittechnik und eine Visualisierung mit kundenspezifischen Erweiterungen zum Einsatz. Über die Software lassen sich die einzelnen in der Teststellung verbauten Smart-Grid-Komponenten steuern bzw. deren Messwerte auslesen. Die eigens für die Teststellung eingerichtete ZNR-Instanz war im Rahmen der Evaluierung nur für die Energie AG zugänglich und somit nur begrenzt in den durchgeführten Tests inkludiert. Ein Zugriff auf das zentrale System ist nur unter erzwungenem Zutritt zu dem Netzführungszentrum möglich und wurde aus diesem Grund als

schwer durchführbar eingestuft. Durch die auf diesem System vorhandenen Informationen ist die gesamte IKT-Systemlandschaft der zentralen Steuerung des Energienetzes darstellbar. Für die notwendigen Tests der externen Systeme war dies nicht notwendig Für die Tests war der ZNR insbesondere für das Mitschneiden der Kommunikationsvorgänge mit den Smart-Grid-Komponenten und für das Generieren von Test-Stimuli notwendig. Der ZNR befindet sich in einem gesondert ausgewiesenen Bereich und kann nur von für den Zugang autorisierten Personen betreten werden. Der Zutritt erfolgt über eine zwei Faktoren Authentifizierung an zwei Standorten der Netz Oberösterreich GmbH, welche durchgehend mit mindestens zwei Mitarbeitern besetzt sind. Die Netzwerksegmentierung und die Firewall-Übergänge des aktiven Netzes wurden in dem Testlabor nicht ausgeführt. Systemtests (Penetrationstests) über die Wirksamkeit der Segmentierung und Firewall-Implementierung werden von unabhängigen Security-Unternehmen in regelmäßigen Abständen getestet. Eine zusätzliche Anforderung an Tests kommt auch zustande, wenn neue Systemkomponenten implementiert werden.

2.2.1. Kommunikationsverbindungen der Komponente

Der zentrale Netzleitrechner (ZNR) ist über den Backbone Switch direkt an den Backbone des Netzwerks angebunden, wodurch die Kommunikation mit sämtlichen Smart-Grid-Komponenten ermöglicht wird. Die Backbone Switches des Netzwerks sind physisch redundant (LWL, Hard- und Software) ausgeführt (jeweils zwei Geräte pro Standort). Die in den großen Verteilzentren (Umspannwerken) befindlichen Security Router dienen als Firewall zwischen Backbone-Netzwerk und den Komponenten der Umspannwerke und sind ebenfalls redundant ausgeführt. An den Backbone Switches war zum Zeitpunkt der Tests jeweils nur eine Verbindung zwischen den Komponenten angeschlossen (keine Redundanz), was jedoch die Tests nicht beeinträchtigt hat, da von der korrekten Redundanzumsetzung ausgegangen werden kann.

Die Backbone Switches und die Router waren jeweils hintereinandergeschaltet, um den Netzwerkverkehr entsprechend filtern zu können. Seitens des simulierten Umspannwerks waren die Smart-Grid-Komponenten entweder direkt, über Funkverbindungen (Richtfunk bzw. GSM-Datenfunk) oder über einen Switch angebunden. Im Umspannwerk werden Endgeräte

und Router mit Switches verbunden. Die Switches besitzen teils erhebliche Intelligenz sowie Management- und Security-Funktionen.

In der Teststellung kam jeweils ein Außenanlagen-Switch wie auch ein Leittechnik-Switch zur Anwendung. Der Außenanlagen-Switch war über den Backbone Switch am Standort A an das Netz angebunden (Uplink). An den Switch waren die Smart-Grid-Komponenten CMIC, TM 1703, ZFS, eine SAT230 Console sowie ein AMIS Datenkonzentrator angebunden. Der Leittechnik-Switch ermöglicht eine redundante Anbindung an den Backbone Switch am Standort B (daher über zwei Leitungen), in der Teststellung war diese jedoch nicht umgesetzt.

2.2.2. Endpunkte an den Umspannwerken

Die Endpunkte in den Umspannwerken werden durch Switches über Security Router an den Backbone angehängt und durch den ZNR gesteuert und überwacht. In der Teststellung wurden folgende Endgeräte verbaut: Schutzschalter, Siemens TM 1703, Siemens CMIC Modul, Siemens MIC Modul, AMIS Datenkonzentrator. Die einzelnen Komponenten haben jeweils Schalt- bzw. Messaufgaben (z. B. Schutzschalter, CMIC, MIC). Die TM 1703 diente in der vorliegenden Konfiguration als Medienkonverter, um von einer Ethernet-Verbindung auf eine serielle Verbindung zu übersetzen, welche für die Anbindung über die GSM-Modemstrecke benötigt wird. Die Komponenten CMIC, TM 1703, ZFS, die SAT230 Console/Visualisierung und der AMIS Datenkonzentrator waren über einen Switch angebunden. Zwei MIC-Module waren über Funkstrecken (Datenfunk bzw. GSM-Funkstrecke) angebunden. Das Modem war an einen Switch angebunden, das GSM-Modem hingegen über eine TM 1703, um von einer seriellen Verbindung auf Ethernet zu gelangen.

2.2. Beschreibung und Funktion der Komponentengruppe AMIS Metering

Im Testlabor waren AMIS Smart Meters (TD-3511) und AMIS Datenkonzentratoren verfügbar. Diese wurden durch einen Uplink mit TM 1703 ACP und Transaktionsserver verbunden. Beide Komponenten waren nicht Teil des Testlabors und konnten aus diesem Grund bei der Evaluierung nicht berücksichtigt werden. Die Smart Meter waren mittels PLC-

Kommunikation (Siemens CX1-Protokoll) an die Datenkonzentratoren angebunden. Alle anderen Komponenten verfügen über eine LAN-Schnittstelle und kommunizieren über TCP/IP.

3. Festlegung der Anwendungsszenarien für die Evaluierung

Die folgenden Ausführungen beziehen sich auf die im $(SG)^2$-Maßnahmenkatalog definierten Sicherheitsmaßnahmen, siehe Abschnitte 2.5 und 2.6 in Teil V. Die innerhalb der Teststellung bei der Energie AG angewendete Evaluierungsmethodik wird beschrieben. Bei der Überprüfung wird jeweils zwischen den im Rahmen der Verifikation feststellbaren und evaluierbaren Sicherheitsmaßnahmen und denjenigen Maßnahmen unterschieden, die sich nur durch einen tiefergreifenderen und umfangreichen Security Audit der jeweiligen Komponenten überprüfen lassen. Diese Trennung ist notwendig, da sich insbesondere (Software- und Hardware-) Implementierungsdetails sowie die Details von proprietären Protokollen der zahlreichen in der Teststellung verbauten Komponenten nur in einer Tiefenanalyse („Security Audit“) mit entsprechendem Zusatz-Aufwand überprüfen lassen.

Sicherheitsmaßnahmen auf (IT-Security-) Management-Seite wurden durch Mitarbeiter der Energie AG evaluiert. Die Betreuung der technischen IKT und der Netzwerktechnik erfolgt durch die Energie AG Oberösterreich Data GmbH (Energie AG). Die Energie AG ist seit 2008 ISO 27001 zertifiziert, ebenso einige weitere Energieversorgungsunternehmen (EVU) in Österreich. Im Folgenden wird ausschließlich der Standpunkt der Energie AG wiedergegeben.

3.1. Maßnahmen-Cluster 1: Authentizität und Integrität

3.1.1. Durchführbare Tests innerhalb der Teststellung bei der Energie AG

Die Sicherstellung von Authentizität und Integrität ist im Zuge der Verifikation innerhalb der Teststellung anhand der analysierten Kommunikations- und Steuerdaten sowie dem Systemverhalten und der Systemkonfigu-

ration überprüfbar (sofern verfügbar). Auf Kommunikationsseite werden dazu folgende Analysemethoden angewendet:

- Netzwerk- und Portscans: Über die Scans lassen sich in einem ersten Schritt Kommunikationsschnittstellen zwischen den Geräten identifizieren.
- Netzwerk-Sniffing: Zwischen Komponenten werden absichtlich durch Stimuli Kommunikationsvorgänge verursacht (z. B. mittels der SCADA Software oder durch Änderung von Inputs an Sensoren). Der Kommunikationsvorgang wird folglich auf der Leitung mitgeschnitten und zur weiteren Analyse gespeichert.
- Protokoll-Analyse: Mitgeschnittene Kommunikationsvorgänge werden in einer Software zur Protokollanalyse (Wireshark) analysiert. Bei bekannten Protokollen können hier verwendete Sicherheitsfeatures erkannt und oberflächlich analysiert werden. Auch der Einsatz von Verschlüsselungstechnologien und Zertifikaten sowie deren Konfiguration ist hier ersichtlich, sofern es sich nicht um ein proprietäres Protokoll handelt.
- Extraktion der Konfigurationsdaten: Die Konfigurationsdaten sind üblicherweise im Gerät gesichert und nicht für die Verifikation verfügbar. Können sie dennoch ausgelesen werden, so können die Konfigurationseinstellungen hinsichtlich Authentizität und Integrität überprüft werden.
- Test des Systemverhaltens: Durch (absichtliches) Fehlverhalten können Sicherheits-Einstellungen des Systems praktisch überprüft werden (beispielsweise die Sperre eines Netzwerkports beim Anschluss eines fremden Kommunikationspartners).

3.1.2. Vorgeschlagene Tests für einen Security Audit

- Sämtliche proprietären Protokolle können nur durch einen Security Audit hinsichtlich Authentizität und Integrität überprüft werden, da bei einem proprietären Protokoll keine Details über dessen Implementierung oder dessen genaue Funktionalität vorliegen. Diese Informationen müssen somit erst beispielsweise durch eine Software-Analyse (Disassemblierung, Debugging) in Verbindung mit Protokollanalysen gewonnen werden.
- Sämtliche softwaretechnischen Maßnahmen (Code-Signing, Über-

prüfung von Code-Signing, Hardware UUIDs, etc.) können nur durch eine detaillierte Software-Analyse im Rahmen eines Security Audits überprüft werden.
- Software-Implementierung von Authentizitäts- und Integritätsüberprüfungen (z. B. Überprüfung von Checksummen, etc.) in den jeweiligen Produkten.

3.1.3. Maßnahmenevaluierung auf Management-Seite

Sämtliche Management-Aufgaben von der sicheren Installation von Geräten und Software über deren Wartung bis hin zur Schulung des Personals sind vom Kunden entsprechend sicher zu gestalten. Dies ist im Zuge von Interviews bzw. durch den Kunden selbst mit den $(SG)^2$-Maßnahmen abzugleichen und zu verifizieren. Eine Zertifizierung des Unternehmens nach ISO 27001 würde die sichere Durchführung der Maßnahmen gewährleisten und für das Management die Sicherheit einer kontinuierlichen Verbesserung mit entsprechenden Anforderungen an Security Tests und Schulungen für das Personal sicherstellen. Mittels durchgeführter Risikoanalysen nach den Anforderungen aus dem BDEW Whitepaper für Fernwirksysteme von Österreichs Energie[243] und der ISO/IEC Norm 27019 können die Risiken in den Fernwirksystemen ermittelt und aus den ermittelten Risiken eine Abwägung von zu treffenden Maßnahmen getroffen werden. Die Energie AG erfüllt in diesem Bereich diese Vorgaben seit 2008. Entsprechende Anforderungen wie Umgang mit IT-Komponenten oder Bestellanforderungen für technische IT sind bereits umgesetzt. Andere ISMS-Anforderungen wie sichere Systementwicklung, Dokumentenklassifizierung usw. sind derzeit in der Umsetzung.

[243] Österreichs Energie: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme. Ausführungshinweise zur Anwendung des BDEW Whitepaper. Version 1.0, 2012.

3.2. Maßnahmen-Cluster 2: Sicherheitsevaluierung & Funktions-, Interoperabilitäts- und Penetrations-Tests

3.2.1. Durchführbare Tests innerhalb der Teststellung bei der Energie AG

Die Durchführung von regelmäßigen Security Audits lässt sich nicht mit technischen Mitteln anhand der Teststellung evaluieren. Durch regelmäßige interne Security Audits, vor allem nach Änderungen im System (neuer Software, Tausch von Geräten, usw.) und externe Security Audits kann eine kontinuierliche Verbesserung des Systems gewährleistet werden. Vor allem reduziert sich durch eine regelmäßige Überprüfung des Systems die Gefahr, Schwachstellen nicht ausreichend betrachtet zu haben. Mit der Implementierung eines funktionierenden ISMS gewährleistet das Unternehmen ein Mindestmaß an Sicherheit zum Betrieb der kritischen Infrastruktur.

3.2.2. Vorgeschlagene Tests für einen Security Audit

Die Durchführung von Security Audits lässt sich nicht mittels technischer Security Audits verifizieren. Stattdessen könnten hier entsprechende Management-Audits zur Anwendung kommen, die die kundeninternen Management-Prozesse z. B. in Hinblick auf ISO 27001 verifizieren.

3.2.3. Maßnahmenevaluierung auf Management-Seite

Sämtliche Management-Aufgaben, die regelmäßige Security Audits und Sicherheitsüberprüfungen betreffen, sind im Zuge von Interviews bzw. durch den Kunden selbst mit den $(SG)^2$-Maßnahmen und den aus den vorangegangenen Audits gewonnen Informationen abzugleichen und zu verifizieren. Erkannte Schwachstellen sind entsprechend der daraus gewonnenen Erkenntnisse und Maßnahmen in das vorhandene ISMS zu übernehmen und den Mitarbeitern bekannt zu geben. Bei erkannten personenbezogenen Schwachstellen sind von den ISMS-Verantwortlichen entsprechende Schulungs- und Informationsmaßnahmen zu treffen. Durch die entsprechenden Sicherheitsleitlinien wie die Vorgaben der Leitung zur Informationssicherheit nach Normenpunkt 5 und der entsprechenden Organisation der Informationssicherheit nach Normenpunkt 6, des jährlichen externen Audits, der erforderlichen internen Audits und des mit der Lei-

tung jährlich abgestimmten Auditplanes werden die Umsetzung der erforderlichen Normenpunkte aus dem ISMS sichergestellt.

3.3. Maßnahmen-Cluster 3: Minimalprinzip

3.3.1. Durchführbare Tests innerhalb der Teststellung bei der Energie AG

- Netzwerk- und Portscans: Über die Scans lassen sich in einem ersten Schritt Kommunikationsschnittstellen zwischen den Geräten identifizieren. Dadurch lassen sich zusätzlich zu den benötigten Schnittstellen auch Schnittstellen (Ports) identifizieren, die zwar offen, jedoch für den Einsatz nicht benötigt werden (Minimalprinzip). Zudem ist bei der Verwendung der Schnittstellen zu hinterfragen, d.h. ob diese für den produktiven Betrieb überhaupt notwendig sind. Eine zusätzliche Maßnahme wäre eine anforderungs- und anlassbezogene Freischaltung von für Mess- und Kontrollzwecken erforderlichen Ports, welche nur zu bestimmten Zeiten erforderlich sind. Erforderlicher Zugang für Wartungs- und Implementierungsarbeiten sollte nur explizit auf Zeit freigeben werden und der Datenaustausch mitüberwacht werden. Fremddienstleister erhalten nur einen zeitlich begrenzten Zugang zu den Systemen nach Freigabe des für das System verantwortlichen Mitarbeiters über eine gesicherte Verbindung. Die Kommunikation auf dem Management der Netzwerkkomponenten sollte mittels SNMPv3 gesichert sein. Ist dies nicht möglich, sind entsprechende Maßnahmen zur Sicherheit des Managementports an den Übertragungstechnikkomponenten zu treffen.
- Netzwerk-Sniffing: Zwischen Komponenten werden absichtlich durch Stimuli Kommunikationsvorgänge verursacht (z. B. mittels der SCADA Software oder durch Änderung von Inputs an Sensoren). Der Kommunikationsvorgang wird folglich auf der Leitung mitgeschnitten und zur weiteren Analyse gespeichert.
- Protokoll-Analyse: Mitgeschnittene Kommunikationsvorgänge werden in einer Software zur Protokollanalyse (Wireshark) analysiert. Auf diese Weise kann der Einsatz von Kommunikationsprotokollen, die ggf. nicht für den Betrieb notwendig sind, ermittelt werden.

- Extraktion der Konfigurationsdaten: Die Konfigurationsdaten sind üblicherweise im Gerät gesichert und nicht für die Verifikation verfügbar. Können sie dennoch ausgelesen werden, so können die Konfigurationseinstellungen hinsichtlich des Minimalprinzips überprüft werden (d.h. sämtliche nicht für den produktiven Betrieb benötigten Funktionen sind deaktiviert zu konfigurieren).

3.3.2. Vorgeschlagene Tests für einen Security Audit

Für Software- und Hardware-Produkte ist das Minimalprinzip mittels regelmäßiger Security Audits zu überprüfen. Sie sollen zeigen, ob auch in den jeweiligen Implementierungen der Geräte ungenutzte Funktionen deaktiviert (bzw. deaktivierbar) sind. Zudem lassen sich Debug-Funktionalitäten, ungenutzte Code-Teile und entsprechende Sicherheitslücken aufspüren.

3.3.3. Maßnahmenevaluierung auf Management-Seite

Die Anforderungen sind in einem für die Systementwicklung festgelegten Prozessdokument festzuhalten und werden bei der Vergabe neuer Komponenten von den Anbietern mit den oben genannten Anforderungen verbindlich gefordert. Erfüllen Anbieter diese Anforderungen nicht, so scheiden sie im Ausschreibungs- bzw. Bestellprozess aus. Wenn dies nicht möglich ist, so sind entsprechende technische und organisatorische Maßnahmen auf Netzwerk-, Firewall- oder Komponentenebene (z. B. Frontend, Firewall) zu setzen. Derzeitige Ausschreibungsanforderungen der Energie AG beinhalten diese Minimalanforderung an die Systeme. In der ISMS-Verfahrensanweisung 209 Planung und Beschaffung wird auf diese Anforderung und die erforderlichen Maßnahmen für eine Umsetzung speziell eingegangen.

3.4. Maßnahmen-Cluster 4: Netzwerksegmentierung & Abschottung verschiedener (Sicherheits-) Bereiche

3.4.1. Durchführbare Tests innerhalb der Teststellung bei der Energie AG

Die Sicherstellung der Netzabschottung und Segmentierung ist im Zuge der Verifikation innerhalb der Teststellung anhand der analysierten Kom-

munikations- und Steuerdaten sowie dem Systemverhalten und der Systemkonfiguration überprüfbar (sofern verfügbar). Auf Kommunikationsseite werden dazu folgende Analysemethoden angewendet:

- Netzwerk- und Portscans: Über die Scans lassen sich in einem ersten Schritt Kommunikationsschnittstellen zwischen den Geräten identifizieren. Dadurch lassen sich Netzsegmente sowie die Abschottung (etwa durch Firewalls) evaluieren. Vor allem könnten Kommunikationswege nach außen (z. B. ins Internet), welche bei der Inbetriebnahme eingebaut wurden, festgestellt und behoben werden, da sie eine kritische Sicherheitslücke darstellen.
- Netzwerk-Sniffing: Zwischen den Komponenten werden absichtlich durch Stimuli Kommunikationsvorgänge verursacht (z. B. mittels der SCADA Software oder durch Änderung von Inputs an Sensoren). Der Kommunikationsvorgang wird folglich auf der Leitung mitgeschnitten und zur weiteren Analyse gespeichert. Über diesen Weg lassen sich übliche Kommunikationsvorgänge identifizieren, die durch die umgesetzte Netzabschottung hindurchgehen (dürfen).
- Extraktion der Konfigurationsdaten: Die Konfigurationsdaten sind üblicherweise im Gerät gesichert und nicht für die Verifikation verfügbar. Können sie dennoch ausgelesen werden, so können die Konfigurationseinstellungen hinsichtlich der Netzabschottung, Netzsegmentierung und den Firewall-Regeln überprüft werden.
- Test des Systemverhaltens: Durch Senden von entsprechenden Testpakten lässt sich überprüfen, ob die Netzabschottung, Netzsegmentierung und die Firewall-Regeln richtig umgesetzt sind. Im Speziellen kann versucht werden, innerhalb der Testumgebung über die Netzsegmentierungen hinweg mit Smart-Grid-Komponenten zu kommunizieren. Ist dies möglich, jedoch nicht für den Betrieb notwendig, so liegt keine geeignete Abschottung vor.

3.4.2. Vorgeschlagene Tests für einen Security Audit

In der Teststellung bei der Energie AG konnten keine IDS- oder IPS-Systeme analysiert werden. Im Rahmen eines entsprechenden Security Audits wäre zu klären, inwieweit die IDS-/IPS-Systeme auf Angriffe innerhalb der Teststellung reagieren bzw. überhaupt reagieren können. Zudem sollte

auf Komponentenebene analysiert werden, ob innerhalb der Software-Implementierung entsprechende Härtungs-Maßnahmen (Sandboxing, Virtualisierung, etc.) überhaupt bzw. auch korrekt umgesetzt sind. Aus Kosten- und Sicherheitsgründen wurde im Testsystem kein IPS/IDS implementiert (eigene Firewall). In der Firewall für den Zugang ins World Wide Web (www) ist ein IPS-/IDS-System implementiert und aktiviert. Derzeit wird ein IDS-/IPS-System im Bereich Smart Metering in der Kommunikation zwischen Transaktionsserver und Datenkonzentrator implementiert. Dabei dient dieses System in erster Linie der Überwachung von Abschaltbefehlen aus dem SAP und in zweiter Linie der Protokollüberwachung, welche vom Smart Meter in Richtung Transaktionsserver läuft. Zwischen den einzelnen DMZ Zonen und ins www ist ein IDS/IPS System implementiert. Das Netzwerk des Testlabors ist aus Sicherheitsgründen von allen Bereichen abgeschottet. Vor allem aus Gründen der Systemverfügbarkeit und des Risikos der Firewall-Integrität wird dies auch nicht in Betracht gezogen. Der Zugriff ins www ist im Testlabor nur über Kundenzugang (WLAN) möglich. Die allgemeine Netzwerksicherheit (Datennetz Office) wird durch ein NAC-System sichergestellt. Der Rollout ist noch nicht an allen Standorten durchgeführt.

3.4.3. Maßnahmenevaluierung auf Management-Seite

In den vorhandenen ISMS-Richtlinien sind die notwendigen Anforderungen zur Einhaltung der Sicherheit verankert. Durch eine technische Trennung der Netzwerke zwischen technischer IT und Büro-IT mittels durch Firewalls abgesicherter Übergänge ist eine zusätzliche Sicherheit der Netzwerke vorhanden. Die Verfügbarkeit des Betriebsnetzwerkes wird durch redundante Glasfaser- und IKT-Systeme gewährleistet. Die Systemverfügbarkeit der verwendeten Komponenten ist durch eine ausreichend dimensionierte USV (mind. 24 bzw. 48 Stunden) gewährleistet. Die ISMS-Richtlinien 301, 303 und 306 regeln klar den Zugriff von Fremdsystemen oder Fremddienstleistern auf die Systeme der Energie AG. Eine Überprüfung und die Effektivität dieser ISMS-Anforderungen erfolgt durch den Nachweis der Erfüllung der Normenpunkte 9.4 und 15.2 bei den jährlichen Audits. Zudem wird täglich ein Reporting über Fernzugriffe (SSL VPN), welche von der Firewall geloggt werden, von den Verantwortlichen überprüft.

3.5. Maßnahmen-Cluster 5: Schutz von (Fern-) Wartungszugängen & verpflichtende Transparenz seitens der Hersteller

3.5.1. Durchführbare Tests innerhalb der Teststellung bei der Energie AG

- Netzwerk- und Portscans: Über die Scans lassen sich in einem ersten Schritt Kommunikationsschnittstellen zwischen den Geräten identifizieren. Dadurch lassen sich zusätzlich zu den benötigten Schnittstellen auch Schnittstellen (Ports) identifizieren, die für Fernwartungszugänge verwendet werden können (z. B. Toolbox, SSH, VPN).
- Netzwerk-Sniffing: Zwischen den Komponenten werden absichtlich durch Stimuli Kommunikationsvorgänge verursacht (z. B. mittels der Fernwartungssoftware). Der Kommunikationsvorgang wird folglich auf der Leitung mitgeschnitten und zur weiteren Analyse gespeichert.
- Protokoll-Analyse: Mitgeschnittene Kommunikationsvorgänge werden in einer Software zur Protokollanalyse (Wireshark) analysiert. Auf diese Weise kann der Einsatz von Fernwartungsprotokollen ermittelt werden. Zudem kann festgestellt werden, ob es sich bei diesen Protokollen um offene Protokolle handelt, oder ob proprietäre Protokolle ohne Herstellertransparenz zum Einsatz kommen.
- Extraktion der Konfigurationsdaten: Die Konfigurationsdaten sind üblicherweise im Gerät gesichert und nicht für die Verifikation verfügbar. Können sie dennoch ausgelesen werden, so können die Konfigurationseinstellungen hinsichtlich Fernwartungszugängen überprüft werden.

3.5.2. Vorgeschlagene Tests für einen Security Audit

Es wird dringend empfohlen, zumindest jene Fernwartungszugänge in einem Security Audit zu analysieren, die auf proprietäre Protokolle setzen (z. B. Toolbox). Über Fernwartungszugänge lassen sich typischerweise sämtliche Einstellungen inkl. der Software auf den Geräten verändern. Ist das Fernwartungsprotokoll nicht entsprechend abgesichert, so stehen diese Möglichkeiten ggf. auch einem Angreifer zu. Derzeit sind einige Fernwar-

tungszugänge zu Außenstellen von Tochtergesellschaften mit Teamviewer realisiert. Alle anderen Fernwartungszugänge wurden die letzten Jahre umgestellt auf SSL VPN; der Zugang erfolgt mit Token-Freigabe anlassbezogen explizit durch den Administrator. Eine externe Analyse durch die FH Hagenberg hat ein Bedrohungsrisiko des Teamviewers festgestellt. Auf Grund dieser Analyse wurden die restlichen Teamviewer-Fernwartungszugänge bis Ende 2015 auf eine sichere Lösung umgestellt. Für kritische Bereiche wurden eigene Netzwerksegmente eingerichtet und die Übergänge mittels Firewall zusätzlich eingeschränkt.

3.5.3. Maßnahmenevaluierung auf Management-Seite

Die Zugriffsfreigabe ist durch ISMS-Richtlinien für die Administratoren geregelt. Fremdwartungspersonal erhält einen Remote Access Zugang über den Token des Administrators. Die für den Fernwartungszugriff erforderlichen Unternehmen und deren Mitarbeiter verpflichten sich im Vorfeld durch Vertraulichkeits- und Verpflichtungserklärungen dazu, die Sicherheitsmaßnahmen der Energie AG zu beachten und einzuhalten. Zudem haben die verantwortlichen Mitarbeiter des Fremdwartungsunternehmens entsprechende Remote-Access-Richtlinien zu unterzeichnen. Die Bekanntgabe der notwendigen Dokumente erfolgt durch die Energie AG an die Fernwartungsunternehmen. Fernwartungszugänge sind nach den ISMS-Richtlinien nur für eine bestimmte maximale Zeit freigeschaltet. Ein Fernwartungszugang ohne Überwachung der Energie AG sollte dabei ausgeschlossen sein. Die Mitarbeiter werden in den jährlichen Informationssicherheitsveranstaltungen auf Schwachstellen und Risiken hingewiesen und entsprechend geschult. Festgestellte nicht genehmigte Zugänge oder nicht erklärbare Datenkommunikationen werden analysiert und im Anschluss daran entsprechende Sicherheitsmaßnahmen getroffen, welche diese Zugänge verhindern. Werden aus den Erfahrungen im Betrieb Erkenntnisse gezogen, welche die Sicherheit für andere Bereiche erhöhen, so wird eine konzernweite Umsetzung geprüft. Festgestellte Schwachstellen in den einzelnen Bereichen werden diskutiert und weitere Analysen von möglichen betroffenen Bereichen eingeleitet. Sind Unternehmen nicht bereit, sich dieser Anforderung zu unterziehen, so scheiden diese bei zukünftigen Ausschreibungen frühzeitig aus. Die einzelnen Systeme werden in mindestens dreijährigen Abständen einer Sicherheitsüberprüfung durch Externe im Hinblick auf die Fernzugriffsmöglichkeiten unterzogen. Eine interne Über-

prüfung erfolgt nach jeder Änderung oder Erweiterung im System entsprechend dem Normenpunkt 15.2.

3.6. Maßnahmen-Cluster 6: Sicherheitsanforderungen für Hersteller

3.6.1. Durchführbare Tests innerhalb der Teststellung bei der Energie AG

Die Energie AG führt den Bestellvorgang unter Einhaltung verschiedener Anforderungen, welche in den ISMS-Dokumenten und teilweise in den Einkaufbedingungen des Konzerns und der einzelnen Gesellschaften verankert sind, durch. In den Anforderungsdokumenten Planung und Beschaffung und IKT-Systementwicklung, IT Software und Produktentwicklung sind die Anforderungen explizit festgelegt. In diesen Dokumenten werden jeweils zu Beginn eines Abschnitts sogenannte Controls des internationalen Standards ISO/IEC 27002:2013 „Information technology – security techniques – Code of practice for Information Security Management" referenziert. Diese Referenzen dienen lediglich als Hinweis auf die im Standard aufgeführte „Implementation Guidance", die bei der Umsetzung der Forderungen zu Rate gezogen werden kann. Verbindlich umzusetzen sind jedoch immer nur die in dieser Richtlinie explizit aufgeführten Forderungen. Zu beachten ist ebenfalls, dass sich die Systematik dieser Richtlinie von der des Standards ISO/IEC 27002 unterscheidet. Zudem wird auf die in dem Dokument IKT-Vertragsbedingungen für Leistungen auf dem Gebiet der Informations- und Kommunikationstechnologie (IKT) der Energie AG Oberösterreich und Ihrer Konzerngesellschaften vom 1.1.2014 angeführten gesetzlichen Regelungen sowie Normen und Standards verwiesen, sowie auf Dokumente, welche den gängigen Stand der Technik verifizieren wie z. B. das BDEW Whitepaper für Fernwirksysteme, entsprechende Wartungsverträge, usw. Eine Überprüfung, inwieweit die einzelnen Komponenten den Anforderungen entsprechen, wird derzeit nicht durchgeführt. Hier verlässt man sich auf die vertragliche Regelung und die darin zugesicherten Erfüllungsgrade.

3.6.2. Vorgeschlagene Tests für einen Security Audit

Die Einhaltung von Sicherheitsanforderungen für Hersteller lässt sich nicht mittels technischer Security Audits verifizieren. Stattdessen könnten hier

entsprechende Management-Audits zur Anwendung kommen, die die kundeninternen Management-Prozesse z. B. in Hinblick auf ISO 27001 verifizieren. Diesen Anforderungen wird in dem seit 2008 bestehenden ISMS der Energie AG Rechnung getragen.

3.6.3. Maßnahmenevaluierung auf Management-Seite

Derzeit erfolgt durch den Arbeitskreis Sicherheit von Österreichs Energie eine Prüfung möglicher europäischer Dienstleister im Hinblick auf die Entwicklung von Prüfroutinen und -protokollen und die Erstellung unabhängiger Prüfzertifikate für Smart-Grid- bzw. Smart-Meter-Komponenten. Der Fokus liegt dabei auf der Prüfung einzelner Komponenten und einzelner Software. Eine Überprüfung des Verhaltens eines gesamten Systems ist nicht vorgesehen. Bei den einzelnen EVU sind unterschiedliche Systeme in den differenziertesten Ausprägungen und mit den unterschiedlichsten Softwareständen in Verwendung. Eine Prüfung in einer annähernd gleichen Testumgebung gibt keine Gewähr auf die durchgängige Funktionalität und Sicherheit des Systems. Werden neue Komponenten in das bestehende Fernwirknetz eingebunden, so erfolgt immer eine entsprechende Prüfung des gesamten Systems zuerst im Testlabor, dann in den Stand-By-Systemen und anschließend im aktiven System. Die Anforderungen des Normenpunktes 14 werden durch die verschiedenen ISMS-Verfahrensanweisungen der Energie AG, welche bei der Ausschreibung und Bestellung fixer Bestandteil sind, gewährleistet. Derzeit findet auf Ebene Österreichs Energie und E-Control Austria eine Erhebung möglicher Dienstleister für ein Prüfzertifikat von IKT-Systemkomponenten statt. Durch die unterschiedlichen IKT-Systeme und -Netze müssen die einzelnen Komponenten explizit nochmals im Verbund mit den im System vorhandenen Komponenten überprüft werden.

3.7. Maßnahmen-Cluster 7: Change Management, Patch Management, Configuration Management

3.7.1. Durchführbare Tests innerhalb der Teststellung bei der Energie AG

Die Anwendung von Maßnahmen im Bereich Change, Patch und Configuration Management lässt sich nicht mit technischen Mitteln anhand der

Teststellung evaluieren, da es sich um Maßnahmen auf Management-Ebene handelt. Im Zuge des externen ISMS-Audits werden diese Anforderungen überprüft und eine Konsistenz in der Umsetzung nachgewiesen.

3.7.2. Vorgeschlagene Tests für einen Security Audit

Die Anwendung dieser Maßnahmen lässt sich nicht mittels technischer Security Audits verifizieren. Stattdessen könnten hier entsprechende Management-Audits zur Anwendung kommen, die die kundeninternen Management-Prozesse z. B. in Hinblick auf ISO 27001 verifizieren.

3.7.3. Maßnahmenevaluierung auf Management-Seite

Die für diese Anforderung vorrangig notwendigen Normenpunkte sind der Normenpunkt 12.5 Kontrolle Software im Betrieb und der Normenpunkt 14.1 Sicherheitsanforderungen für Informationssysteme. Die ISMS-Richtlinie schreibt Vorgehensweisen für die Dokumentation von Geräte- und Systemkonfigurationen vor. Änderungen sind in den entsprechenden Betriebshandbüchern zu vermerken, ein Verweis auf das aktuelle Dokument ist einzufügen. Die Betriebshandbücher werden jährlich bei den Administratorengesprächen geprüft. Eine fehlende oder unzureichende Dokumentation wird vermerkt und als Hinweis mit einer Erfüllungszeit für den Administrator vorgegeben. Verantwortlich für die Dokumentation ist immer der zuständige Systemadministrator. Bei jeder geplanten oder durchzuführenden Änderung im System ist der Systemadministrator miteinzubeziehen. Vor Integration einzelner Systeme (Hard- und Software) wird eine schriftliche Bestätigung des Lieferanten zur Sicherstellung der Systembetriebsfähigkeit gefordert. Nach Lieferung erfolgen Integrationstests im Testsystem und anschließend auf die redundant ausgeführten Betriebssysteme, wobei immer zuerst das Stand-by-System geprüft wird. Im Anschluss erfolgen entsprechende Penetrationstests in den einzelnen Systemkomponenten. Bei größeren Änderungen wird das gesamte System geprüft und die Aktualität der Dokumentation kontrolliert. Die einzelnen Softwarestände werden in einer zentralen Datenbank geführt, damit man auf bekanntwerdende Bedrohungen schneller reagieren kann. Sollten bekannte Softwarebugs nicht gepatcht werden können, sind entsprechende Maßnahmen zu setzen, welche einen annähernd gleichen Sicherheitsstandard gewährleisten (Abschottung des Systems in einer eigenen DMZ, Ex-

plizite Firewall-Einstellungen für diese DMZ und eventuelle physische Sicherungsmaßnahmen). Für neue Systeme wird bei der Ausschreibung ein entsprechender Anforderungskatalog beigelegt. In diesem sind derzeit verfügbare und soweit vorhersehbar mögliche neue Sicherheitsanforderungen explizit vorgesehen. Die Erstellung des Anforderungskataloges erfolgt unter Einbeziehung des Sicherheitsverantwortlichen und bei nicht ausreichendem Wissensstand unter Einbeziehung externer Berater. Die in den Systemen eingesetzte Software ist in einem zentralen Managementsystem gelistet. Bekannt gewordene Schwachstellen oder Sicherheitslücken können dadurch für jedes System schnellst erhoben und entsprechende Maßnahmen bis zu einem Softwareupgrade getroffen werden. Dies ist erforderlich, weil ein Großteil der Systeme nur nach Rücksprache mit dem Hersteller upgegradet werden kann.

3.8. Maßnahmen-Cluster 8: Physische Sicherheitsmaßnahmen

3.8.1. Durchführbare Tests innerhalb der Teststellung bei der Energie AG

Die physischen Sicherheitsmaßnahmen werden nicht innerhalb der Teststellung evaluiert, da sich die technische Evaluierung auf die Komponenten- bzw. Netzwerkebene beschränkt.

3.8.2. Vorgeschlagene Tests für einen Security Audit

Es wird empfohlen, die Komponenten und Systeme für den Zutrittsschutz (z. B. Zutrittssysteme mit drahtlosen Zutrittskarten) einem technischen Security Audit zu unterziehen. Basieren diese Systeme auf unsicheren oder veralteten Technologien (z. B. dem bereits gebrochenen MIFARE RFID System), so besteht die Gefahr, dass sich Angreifer unautorisiert Zutritt zu gesicherten Bereichen verschaffen können.

3.8.3. Maßnahmenevaluierung auf Management-Seite

Physische Sicherheitsmaßnahmen, wie beispielsweise das bestehende Schließsystem und die Zutrittsregelung, werden in den verschiedenen Geschäftsbereichen regelmäßig geprüft. Die Energie AG prüft die einzelnen für die Dienstleistungsbereitstellung notwendigen Räume und legt dazu

entsprechende Sicherheitsstandards fest. Ein funktionierendes ISMS gewährleistet eine kontinuierliche Überprüfung der festgelegten Standards. Für die Anlagen erfolgt eine ISMS-konforme Abstufung nach Kritikalität der Räume von AR1 bis AR3, wobei AR1-Räume systemkritische Anlagen beinhalten, welche redundant vorhanden sind. Die wichtigsten Normenpunkte sind hier der Normenpunkt A7 Sicherheit des Personals, der Normenpunkt A9 Zugriffskontrolle und Benutzerverwaltung sowie der Normenpunkt A11 Schutz vor physischen Zugang und Umwelteinflüssen.

Die Sicherheit der Systeme wird bei der Energie AG in verschiedenen Sicherheitsstufen gewährleistet. Je nach Kritikalität der in den Räumen vorhandenen Komponenten gibt es unterschiedliche Zugangsstufen. Zudem wird die Sicherheit der einzelnen Komponenten auf verschiedenen Ebenen sichergestellt (physische Sicherheit, Zugriffssicherheit an den einzelnen Komponenten, Sicherheit der einzelnen Applikationen). Da die derzeit verwendeten Systeme vor allem im Energielenkungsbereich (Smart Grid) eine Lebensdauer von 20 Jahren und länger haben, ist es oft nicht möglich, alle drei Ebenen zu implementieren.

Die erste Ebene ist die physische Sicherheit. Diese wird je nach Kritikalität der Komponenten in verschiedene Stufen unterteilt. Bei Räumen der Stufe 1 handelt es sich um kritische Systemräume (z. B. Serverräume, Rechenzentrum, zentrale Leitsysteme), die nur mittels Zwei-Faktor-Authentifizierung zu betreten sind. Dazu werden die Eingangstüren mittels Türkontakt und Videokameras innen und außen überwacht. Die Räume sind zusätzlich mit einer Alarmanlage gesichert, in die Brandmelder, Leckage-Wächter, Glasbruchmelder, Türkontakte, usw. eingebunden sind. Zudem sind die Anlagen durch mehrere physische Zonen wie Umzäunung mit Überwachung, Gebäudeüberwachung und der Raumzutrittsüberwachung ausgestattet.

Die zweite Ebene der physischen Sicherheit wird durch Türkontakte auf den verschiedenen Zutrittsebenen erreicht. Derzeit ist ein sicheres Schließsystem mit für den Zugang dokumentierten Mitarbeitern und Fremddienstleistern mit einer Aufzeichnung des Türkontaktes in Verwendung. Die Fremddienstleister sind durch entsprechende Dokumente auf die Anforderungen hingewiesen und verpflichtet worden. Treten bei nichtangekündigten Überprüfungen Ungereimtheiten auf, so wird den Fremddienstleistern

nach einmaliger Verwarnung der Zutritt entzogen. Eine Abänderung auf ein elektronisches Schließsystem mit zusätzlich dokumentierter Zugangsüberwachung des betreffenden Mitarbeiters oder Fremddienstleisters explizit auf einen auf max. 24 Stunden freigeschalteten Bereich ist in der Umsetzung.

Die dritte Ebene der physischen Sicherheit wird durch für Mitarbeiter und Fremddienstleister explizit freigegebene Bereiche festgelegt. Hier erfolgt keine zusätzliche Überwachung der physischen Sicherheit wie derzeit z. B. bei den Trafostationen.

Besteht in Folge von Sicherheitsaudits und Überprüfungen Bedarf an einer zusätzlichen Überwachung, so werden Videokameras mit Bewegungsmelder installiert und in die zentrale Meldestelle geleitet. Vor jeder Installation einer Videokamera wird eine Übereinkunft mit dem Betriebsrat getroffen und das Erfordernis einer Datenschutzmeldung mit der Rechtsabteilung geprüft. Erst nach erfolgter positiver Prüfung dürfen Videokameras installiert werden. Dabei kann es aus Datenschutzgründen zu Einschränkungen kommen, wie z. B. bei Arbeitsplätzen. Hier erfolgt über Bewegungsmelder und Türkontakt eine Überwachung des Bereiches mit Alarmierung in der zentralen Meldestelle. Das vorhandene Videosystem legt die Daten verschlüsselt im System für den genehmigten festgelegten Zeitpunkt ab. Ein Zugriff auf die verschlüsselten Daten ist nur mittels Vier-Augen-Prinzip möglich (Betriebsrat und systemverantwortlicher Mitarbeiter).

Fernzugriffe werden nur nach Anforderung des Systemadministrators für einen definierten Zeitbereich freigegeben und dokumentiert. Der Zeitbereich ist automatisch nochmals auf acht Stunden eingeschränkt.

3.9. Maßnahmen-Cluster 9: Incident Management

3.9.1. Durchführbare Tests innerhalb der Teststellung bei der Energie AG

Im Rahmen der technischen Evaluierung der Komponenten in der Teststellung wird durch gezielte Netzwerk-Stimuli getestet, ob Komponenten mit absichtlich fehlerhaftem oder schädlichem Verhalten erkannt bzw. abgeschaltet werden.

3.9.2. Vorgeschlagene Tests für einen Security Audit

- Es werden allgemeine regelmäßige Security Audits der Smart-Grid- und Netzwerk- Komponenten sowie der ZNR-Systeme empfohlen mit dem spezifischen Ziel zu prüfen, wie sich die Systeme im Vorhandensein von (absichtlich) fehlerhaften oder Schadhaften Komponenten bzw. Kommunikationsverhalten im Netzwerk verhalten. Dabei ist zumindest zu bestimmen, ob das Verhalten in der Umgebung detektiert wird, wie weit die Auswirkungen des Störverhaltens das Gesamtsystem beeinträchtigen und ob die störenden bzw. fehlerhaften Komponenten entsprechend vom Gesamtsystem abgekoppelt werden können.

- Regelwerk-Audit auf Management-Seite: Es wird empfohlen, das Incident-Management Regelwerk regelmäßig mit Hinblick auf aktuelle technische Angriffsszenarien (d.h. Angriffsszenarien, die die aktuelle technische Konfiguration widerspiegeln) zu auditieren. Dabei sollen etwa mögliche technische Auswirkungen auf das Gesamtsystem während eines Störfall bzw. Angriffs gemeinsam mit den Maßnahmen im Incident-Response-Regelwerk auf deren Effektivität hin überprüft werden.

3.9.3. Maßnahmenevaluierung auf Management-Seite

Zur Sicherstellung der Anforderungen ist die Einhaltung der Normenpunkte A.12.6 Management technischer Schwachstellen, A.14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen und A.16 Management von Informationssicherheitsvorfällen und Verbesserungen zu gewährleisten.

Abbildung 20 zeigt Verantwortungen und Abläufe, um eine schnelle und effektive Reaktion auf entdeckte Sicherheitsvorfälle und -schwachstellen zu gewährleisten.

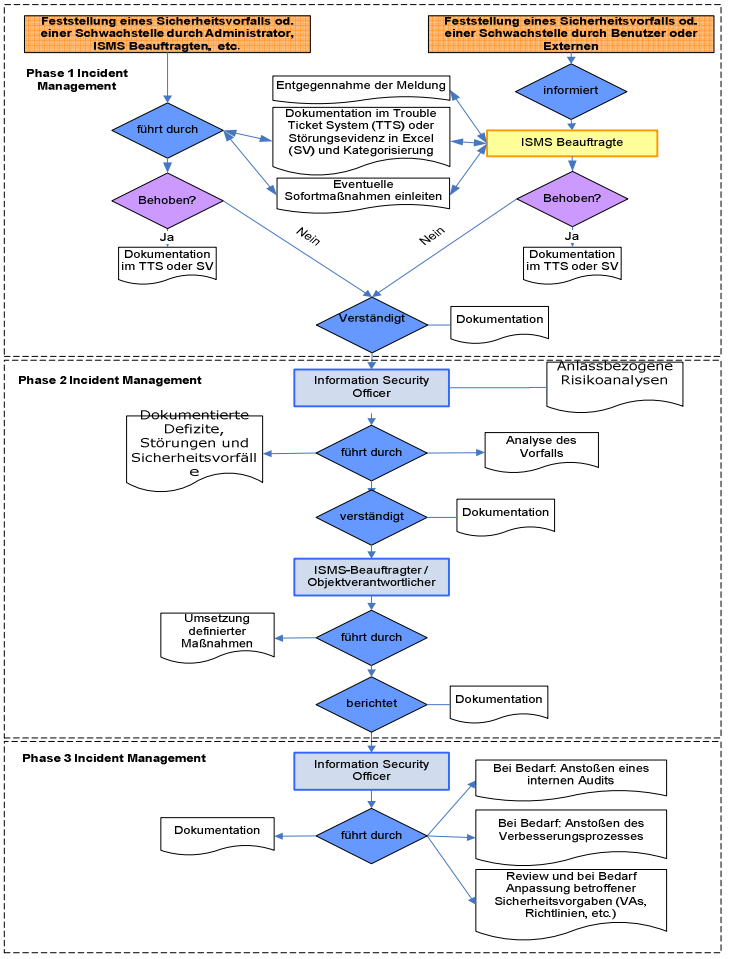


Abbildung 20: Abläufe Incident Management

3.10. Maßnahmen-Cluster 10: Mehrstufiges Sicherheitskonzept

3.10.1. Durchführbare Tests innerhalb der Teststellung bei der Energie AG

- Netzwerk- und Portscans: Über die Scans lassen sich in einem ersten Schritt Kommunikationsschnittstellen zwischen den Geräten identifizieren. Zudem ist es so bereits möglich, einzelne Sicher-

heitsmaßnahmen (z. B. Firewalls, Scan Protections, Logging, IPS, Netzwerksegmentierung, etc.) zu überprüfen.

- Netzwerk-Sniffing: Zwischen Komponenten werden absichtlich durch Stimuli Kommunikationsvorgänge verursacht (z. B. mittels der SCADA Software oder durch Änderung von Inputs an Sensoren). Der Kommunikationsvorgang wird folglich auf der Leitung mitgeschnitten und zur weiteren Analyse gespeichert.

- Protokoll-Analyse: Mitgeschnittene Kommunikationsvorgänge werden in einer Software zur Protokollanalyse (Wireshark) analysiert. Bei bekannten Protokollen können hier verwendete Sicherheitsfeatures erkannt und oberflächlich analysiert werden. Auch der Einsatz von Verschlüsselungstechnologien und Zertifikaten sowie deren Konfiguration ist hier ersichtlich sofern es sich nicht um ein proprietäres Protokoll handelt.

- Extraktion der Konfigurationsdaten: Die Konfigurationsdaten sind üblicherweise im Gerät gesichert und nicht für die Verifikation verfügbar. Können sie dennoch ausgelesen werden, so können die Konfigurationseinstellungen hinsichtlich Authentizität und Integrität überprüft werden.

- Test des Systemverhaltens: Durch (absichtliches) Fehlverhalten können Sicherheits-Einstellungen des Systems praktisch überprüft werden (beispielsweise die Sperre eines Netzwerkports beim Anschluss eines fremden Kommunikationspartners).

Die Kombination und die Ergebnisse der einzelnen Tests ermöglichen somit die Analyse und die Evaluierung einzelner, ineinander verschachtelter Sicherheitsmaßnahmen, die gemeinsam ein mehrstufiges Sicherheitskonzept ergeben.

3.10.2. Vorgeschlagene Tests für einen Security Audit

Es werden regelmäßige Security Audits der Smart-Grid- und Netzwerk-Komponenten sowie der ZNR-Systeme empfohlen. In Hinblick auf ein mehrstufiges Sicherheitskonzept ist dieses zu überprüfen, indem im Rah-

men des Security Audits die einzelnen Sicherheits-Schichten (z. B. Netzwerkkomponenten und -systeme) auditiert werden. Auf Basis der Ergebnisse können Aussagen getroffen werden, wie leicht ein Angreifer eine jeweilige Sicherheitsschicht überwinden kann. Für einen erfolgreichen Angriff müssten viele Sicherheitsschichten durchbrochen werden. Sind diese effektiv, so wird der notwendige Aufwand für einen erfolgreichen Angriff erheblich gesteigert, womit die Eintrittswahrscheinlichkeit sinkt.

3.10.3. Maßnahmenevaluierung auf Management-Seite

Die Umsetzung des ISMS-Normenpunktes 10 Kryptografische Maßnahmen bedingt einen Schutz der im System übertragenen Daten. Derzeit wird auf der Übertragungsebene Mac Sec in der Kommunikation mit Nebenanlagen und IPSec in der Kommunikation des Backbones installiert. Eine Überprüfung der Maßnahmenumsetzung bzgl. des mehrstufigen Sicherheitskonzeptes sowie des Umgangs mit personenbezogenen Daten auf Management-Seite erfolgt in mindestens jährlichen Abständen, wobei durch die Verwendung der verschiedenen Übertragungseinrichtungen (LWL, Funk, GSM, DSL) jeweils gezielt auf eine sichere Kommunikation der entsprechenden Anwendung fokussiert wird.

Die einzelnen Systeme (Fernwirksystem, Smart Metering, Büro-LAN, usw.) befinden sich in unterschiedlichen Firewall-Zonen. Die Sicherheit der Systeme wird bei der Energie AG durch physische Zutrittssicherheit, Portüberwachung, Systemredundanzen, verschlüsselter Übertragung (IPSEC), Schutz des Managementkanals, IPS/IDS Systemüberwachung, entsprechend mit Verschlüsselung geschützten mobilen Komponenten (AES 256) und ab 2015 Verschlüsselung der Daten der Smart-Meter-Systeme gewährleistet.

4. Ergebnisse der Evaluierung des Zentralen Netzrechners

Dieser Abschnitt beschreibt Ergebnisse der Evaluierung für die Komponente Zentraler Netzrechner (ZNR). Zunächst wird je Maßnahmen-Cluster die konkrete Evaluierungsmethodik einschließlich der Ergebnisse dargestellt, anschließend wird die Umsetzung und Effektivität der Maßnahmen lt. $(SG)^2$-Katalog bewertet.

Die Maßnahmen-Cluster 2 (Sicherheitsevaluierung & Funktions-, Interoperabilitäts- und Penetrations-Tests), 6 (Sicherheitsanforderungen für Hersteller) und 7 (Change Management, Patch Management, Configuration Management) konnten im Rahmen einer technischen Überprüfung innerhalb der Teststellung nicht evaluiert werden, da sich diese Maßnahmen wie beschrieben nicht mit technischen Mitteln evaluieren lassen.

4.1. Maßnahmen-Cluster 1: Authentizität und Integrität

4.1.1. Konkrete Evaluierungsmethodik und Ergebnisse

Zunächst wurde die Kommunikation des Servers entlang der verschiedenen Kommunikationswege aufgezeichnet. Die beobachtete Kommunikation erfolgte ausschließlich zwischen ZNR und Endgeräten, wobei die Verbindungen stets durch den ZNR aufgebaut wurden.

Anschließend an die passive Aufzeichnung des normalen Datenverkehrs wurde der ZNR einem aktiven Netzwerkscan von der Position der TM1703 GSM ZFS aus unterzogen.

Beim Sniffing wurde festgestellt, dass die Kommunikation über ein spezifisches Protokoll erfolgt. Dieses Protokoll wurde in der Teststellung nicht durch zusätzliche Maßnahmen geschützt und bietet selbst keine Sicherheitsfeatures wie Authentifizierung oder Verschlüsselung. Daher kann ein Angreifer an einem geeigneten Punkt im Netzwerk die Pakete des ZNR fälschen und dadurch Endgeräte steuern.

Versuche eines Logins mit Standard-Zugangsdaten wie z. B. User root und Passwort root waren nicht erfolgreich.

4.1.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 21: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 1

Maßnahme	**Über-prüfbar**	**Vorhan-den**	**Effektiv**
Sicherstellung von Authentizität und Integrität von Software	N (1)	?	?
Sicherstellung von Authentizität und Integrität von Kommunikations- und Steuerdaten	J (2)	Teilw. (2)	J (2)

Anmerkungen:

(1) Am ZNR selbst (d.h. innerhalb des Betriebssystems) erfolgte auf Wunsch der Energie AG keine Evaluierung. Grund war der Schutz vor einer Offenlegung der Fernwirkstruktur.

(2) Der Remote-Zugang zum ZNR ist ausreichend sowie effektiv mit entsprechendem Schutz bzgl. Authentizität und Integrität abgesichert. Die ausgehenden Verbindungen vom ZNR zu den Smart-Grid-Komponenten setzen jedoch auf bekannte Protokolle.

4.2. Maßnahmen-Cluster 3: Minimalprinzip für sicherheitskritische Schnittstellen

4.2.1. Konkrete Evaluierungsmethodik und Ergebnisse

Der ZNR wurde einem Portscan unterzogen um die resultierende Angriffsfläche zu evaluieren.

Es war nur ein Port erreichbar, dieser war ausreichend abgesichert. Über die Stärke der eingesetzten Passwörter kann keine Aussage getroffen werden.

4.2.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 22: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 3

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Minimalprinzip für sicherheitskritische Schnittstellen (Internetverbindung)	J	J	J
Minimalprinzip für sicherheitskritische Schnittstellen (physischer Zugriff)	N (1)	?	?
Minimalprinzip für sicherheitskritische Schnittstellen (logischer Zugriff)	J	J	J
Minimalprinzip für Sammlung, Speicherung und Übermittlung schutzbedürftiger Daten	J	J	J
Kapselungsprinzip	N (2)	?	?

Anmerkungen:

(1) Maßnahmen zur Unterbindung von physikalischem Zugriff konnten im Rahmen der Teststellung nicht überprüft werden. Der physische Zugriff auf den ZNR ist über zwei Ebenen und Zwei-Faktor-Authentifizierung abgesichert. Zudem werden die Zutrittstüren videoüberwacht. Die Räume befinden sich in geschlossenen Arealen im Keller und sind mittels Alarmanlage gesichert. Der Test-ZNR hat keine Verbindung zu den aktiven und passiven Systemen und kann aus diesem Grund jedem Angriffsszenario unterzogen werden.

(2) Der Zentrale Netzrechner wurde als Black-Box betrachtet, daher kann keine Aussage über die Kapselung getroffen werden.

4.3. Maßnahmen-Cluster 4: Netzwerksegmentierung & Abschottung verschiedener (Sicherheits-) Bereiche

4.3.1. Konkrete Evaluierungsmethodik und Ergebnisse

Die in Abschnitt 4.1.1 beschriebenen Portscans und Kommunikationsmitschnitte wurden an mehreren Stellen im Netzwerk durchgeführt. Der ZNR war in einem eigenen Subnet und direkt mit dem Backbone verbunden. Über den Backbone konnten Portscans auf den ZNR durchgeführt werden; sobald aber ein Router dazwischen war, gelang keinerlei Verbindungsaufbau und dementsprechend auch kein Portscan.

4.3.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 23: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 4

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Netzwerksegmentierung	J	J	J
Abschottung der Sicherheitsbereiche durch Firewalls	J	J	J
Besonderer Schutz kritischer Bereiche (Sandboxing, VLANs, IPS/IDS, etc.)	Teilw.	J	J

4.4 Maßnahmen-Cluster 5: Schutz von (Fern-) Wartungszugängen & verpflichtende Transparenz seitens der Hersteller

4.4.1. Konkrete Evaluierungsmethodik und Ergebnisse

Wie in Abschnitt 4.1.1 beschrieben wurde ein Portscan zur Evaluierung genutzt. Der Portscan des ZNR zeigte, dass der Wartungszugang offen war. Dieser war ausreichend abgesichert.

4.4.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 24: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 5

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Besonderer Schutz von (Fern-) Wartungszugängen durch verschlüsselte Kommunikationstunnel	J	J	J
Verpflichtende Herstellertransparenz zur Offenlegung von möglichen Wartungsschnittstellen	N (1)	?	?
Access Control	J	J	J
Protokollierung von Rollen, Personen, Zeiten und Tätigkeiten	N (1)	?	?
Schulung von Wartungspersonal zur Förderung von Sicherheitsbewusstsein	N (1)	?	?

Anmerkungen:

(1) Konnte im Rahmen der Teststellung nicht überprüft werden. Die Schulung des Personals in Bezug auf das Sicherheitsbewusstsein wird durch das vorhandene ISMS-System gesichert. Bei den jährlichen externen Audits werden die Unterweisungen überprüft und nachgewiesen. Derzeit findet mindestens einmal jährlich eine Sicherheitsunterweisung in den Abteilungsbesprechungen statt. Zudem wird einmal jährlich, in einer Teambesprechung, eine entsprechend auf die Anforderungen des Teams abgestimmte Unterweisung durchgeführt. Bedrohungen, welche über Cert, Heise und andere Security-Communities eintreffen, werden explizit von dem CISO der Energie AG an die betroffenen Systemadministratoren weitergeleitet. Darüber hinaus erfolgt in Abstimmung mit den Systemadministratoren eine Bedrohungs- und Risikoanalyse. Das Ergebnis wird an die verantwortlichen Vorgesetzten weitergeleitet, und es werden geeignete Maßnahmen definiert.

4.5 Maßnahmen-Cluster 8: Physische Sicherheitsmaßnahmen

Dieser Maßnahmen-Cluster konnte im Rahmen der Teststellung nicht überprüft werden. Die physische Sicherheit der kritischen Räume (AR1 Räume) ist durch das bestehende ISMS der Energie AG gewährleistet. Zudem besteht ein Zutrittssystem auf Seiten der Netz OÖ GmbH. Dies ist auf Grund der erforderlichen Maßnahmen für den Schutz elektrischer Anlagen (Mittel- und Hochspannung) erforderlich und wird dadurch auch gewährleistet. Der Zutritt zu den Umspannwerken und Umspannstationen ist durch entsprechende Türkontakte stufenweise geregelt. Hier ist zuerst die Hürde der Umzäunung und anschließend die des Gebäudezutrittes zu überwinden. Meldungen von den Türkontakten werden in der Zentrale erfasst. Bei nicht verifizierbaren Zutritten wird der zuständige Objektverantwortliche alarmiert. Dieser kontrolliert und leitet weitere Schritte ein. Bei unautorisierten oder nicht gemeldeten Fremdzutritten wird der Schlüssel entzogen. Nicht autorisierter Schlüsselbesitz wird zur Anzeige gebracht.

4.6 Maßnahmen-Cluster 9: Incident Management

4.6.1. Konkrete Evaluierungsmethodik und Ergebnisse

Durch Portscans und wiederholte Loginversuche wurde getestet, ob der ZNR letztendlich seinen Port schließt oder die Anmeldung verweigert. Der ZNR ließ im Test beliebig viele Loginversuche zu. Dies ermöglicht ggf. Bruteforce-Angriffe.

4.6.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 25: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 9

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Umsetzung Incident Management	N (1)	?	?
Identifizierung, (Fern-) Abschaltung und Austausch von Komponenten mit fehlerhaftem oder schädlichem Verhalten (HW wie SW)	J	N (2)	J
Notsignalgebung bei (Verdacht auf) Unregelmäßigkeiten	J	N (2)	J
Regelwerkerstellung zu Fehlerbehebungsabläufen	N (3)	?	?

Anmerkungen:

(1) Konnte ohne Hersteller-Dokumentation nicht überprüft werden.
(2) Es wurden keine Hinweise auf entsprechende Maßnahmen gefunden.
(3) Konnte im Rahmen der Teststellung nicht überprüft werden. Wird durch ein ISMS und Qualitätsmanagement gewährleistet.

4.7. Maßnahmen-Cluster 10: Mehrstufiges Sicherheitskonzept

4.7.1. Konkrete Evaluierungsmethodik und Ergebnisse

Es konnte im Rahmen der Teststellung kein mehrstufiges Sicherheitskonzept getestet werden. Wie in Abschnitt 4.3.1 beschrieben, schützten jedoch die Router den ZNR vor effizienten Portscans. Über weitere Sicherheitsfeatures wie z. B. innerhalb des Betriebssystems des ZNR (Solaris) kann keine Aussage getroffen werden.

4.7.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 26: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 10

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Mehrstufiges Sicherheitskonzept	N	?	?
Verschlüsselte Datenkommunikation	J	Teilw.	J
Anonymisierung und Aggregation von personenbezogenen Daten wo möglich	J	J	J

5. Ergebnisse der Evaluierung des zentralen Netzwerkes zwischen den Umspannwerken

5.1. Maßnahmen-Cluster 1: Authentizität und Integrität

5.1.1. Konkrete Evaluierungsmethodik und Ergebnisse

Zur Evaluierung wurden Portscans von Seiten der aktiven Ports durchgeführt sowie Traffic gesnifft.

Im Rahmen des Kommunikationsmitschnitts zeigte sich, dass die Switches regelmäßig typische Announcements wie OSPF, STP und CDP aussenden, die keine Sicherheitsrelevanz haben. Abgesehen von Broadcasts geht von den Routern und Backbones selbst keine Kommunikation aus. Die Kommunikationsmitschnitte waren hilfreich, da anhand der Broadcasts die IP der Switches festgestellt werden konnten.

Anhand der Kommunikationsmitschnitte zeigte sich auch, dass die Backbone-Kommunikation nicht verschlüsselt war, sofern es die benutzten Protokolle nicht inhärent vorsahen. Das IEC 60870-5-104 Protokoll war etwa im Klartext mitzulesen und könnte an dieser Stelle auch dementsprechend

durch einen Angreifer manipuliert werden. Die Kommunikation zwischen den Backbone-Switches ist verschlüsselt. Die Übergabeports sind bei den Fernwirksystemen in den Umspannwerken nicht geschützt. Hier wird durch die zusätzliche physische Hürde in den Umspannwerken ein geringes Risiko gesehen. Zudem sind die Fernwirkendgeräte nicht in eine Netzwerküberwachung zu integrieren.

Switches
Ein Portscan des Switches (einem der Backbone-Switches) zeigte Ergebnisse: Loginversuche mit üblichen Standardpasswörtern waren erfolglos. Auf einem Port wartet ein Server auf Verbindungen. Bei eingehender Verbindung fragt der Server nach Benutzername und Passwort. Diese Logindaten konnten im Rahmen der Tests nicht erraten werden. Hinter dem Port verbarg sich vermutlich die Konfigurationsschnittstelle. Dieser Port konnte aber in der zur Verfügung stehenden Zeit nicht weiter analysiert werden, da keine aktiven Verbindungen zu diesem Port festgestellt werden konnten und das Cisco-Konfigurationstool nicht zur Verfügung stand.

Router
Der Router zeigte selbst keine offenen Ports von außen und filterte TCP-Verbindungen von Seiten der Endgeräte. Durchgelassen wurden Verbindungen des ZNR von Seiten des Backbones. Der Router filtert auf LAN Seite sämtliche Ports, auch langsame Netzwerkscans waren erfolglos.

Auf WAN-Seite ist der SSH-Port geöffnet und stellt SSH-Login mit Passwort zur Verfügung, das Passwort konnte allerdings während der Verifizierung nicht erraten werden. Der Router erkennt scheinbar Portscans und fehlgeschlagene SSH-Loginversuche und lässt danach keine Verbindungen mehr zu.

5.1.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 27: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 1 (Evaluierg. ZNR)

Maßnahme	**Über-prüfbar**	**Vorhan-den**	**Effektiv**
Sicherstellung von Authentizität und Integrität von Software	N	?	?
Sicherstellung von Authentizität und Integrität von Kommunikations- und Steuerdaten	J	J	J

5.2. Maßnahmen-Cluster 3: Minimalprinzip für sicherheitskritische Schnittstellen

5.2.1. Konkrete Evaluierungsmethodik und Ergebnisse

Wie in Abschnitt 5.1.2 beschrieben wurden Portscans durchgeführt und Traffic gesnifft.
Während die Router sehr gut abgeschottet waren und lediglich auf WAN-Seite einen SSH-Port geöffnet hatten, zeigten die Backbone-Switches offene Ports, von denen vermutlich zumindest SSH und HTTPS Zugang zu den Konfigurationseinstellungen ermöglichten. Da die Loggingdaten nicht bekannt waren, kann allerdings keine Aussage darüber getroffen werden, wie wichtig es ist, diese Ports zu öffnen und ob diese mit starken Passwörtern abgesichert sind.

5.2.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 28: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 3 (Evaluierg. ZNR)

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Minimalprinzip für sicherheitskritische Schnittstellen (Internetverbindung)	J	J	J
Minimalprinzip für sicherheitskritische Schnittstellen (physischer Zugriff)	N (1)	?	?
Minimalprinzip für sicherheitskritische Schnittstellen (logischer Zugriff)	N (2)	?	?
Minimalprinzip für Sammlung, Speicherung und Übermittlung schutzbedürftiger Daten	J	J	J
Kapselungsprinzip	N (3)	?	?

Anmerkungen:

(1) Maßnahmen zur Unterbindung von physischem Zugriff konnten im Rahmen der Teststellung nicht überprüft werden.
(2) Wie oben beschrieben, konnte die Notwendigkeit der Öffnung einzelner Ports nicht überprüft werden.
(3) Es konnten keine speziellen Maßnahmen festgestellt werden.

5.3. Maßnahmen-Cluster 4: Netzwerksegmentierung & Abschottung verschiedener (Sicherheits-) Bereiche

5.3.1. Konkrete Evaluierungsmethodik und Ergebnisse

Die durch Router und Backbone verbundenen Netzwerke wurden durch Kommunikationsmitschnitte identifiziert. Das Routing zwischen diesen Netzen wurde mittels manuellen Verbindungsaufbaus getestet.

Während die Backbone-Switches naturgemäß die Verbindung zum Backbone-Netz zur Verfügung stellten, wurden die Router zur Absicherung des WANs gegenüber dem LAN verwendet. Dementsprechend wurden mehrere verschiedene Subnets auf beiden Seiten eingesetzt. Die Router blockten Verbindungen von LAN zu WAN. Verbindungen des ZNR von WAN zu LAN wurden (zweckgemäß) durchgelassen.

5.3.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 29: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 4 (Evaluierg. ZNR)

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Netzwerksegmentierung	J	J	J
Abschottung der Sicherheitsbereiche durch Firewalls	J	J	J
Besonderer Schutz kritischer Bereiche (Sandboxing, VLANs, IPS/IDS, etc.)	J	J	J

5.4. Maßnahmen-Cluster 5: Schutz von (Fern-) Wartungszugängen & verpflichtende Transparenz seitens der Hersteller

5.4.1. Konkrete Evaluierungsmethodik und Ergebnisse

Es wurden Portscans genutzt, um Fernwartungszugänge zu identifizieren. Die Portscans zeigten, dass die Router lediglich gut gesicherte SSH-Verbindungen am Port entgegennehmen. Auf den Switches konnten Ports festgestellt werden, die Verbindungen entgegennahmen.

5.4.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 30: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 5 (Evaluierg. ZNR)

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Besonderer Schutz von (Fern-) Wartungszugängen durch verschlüsselte Kommunikationstunnel	J	J	J
Verpflichtende Herstellertransparenz zur Offenlegung von möglichen Wartungsschnittstellen	N (1)	?	?
Access Control	J	J	J
Protokollierung von Rollen, Personen, Zeiten und Tätigkeiten	N (1)	?	?
Schulung von Wartungspersonal zur Förderung von Sicherheitsbewusstsein	N (1)	?	?

Anmerkungen:

(1) Konnte im Rahmen der Teststellung nicht überprüft werden. Schulung des Wartungspersonals erfolgt im Zuge des vorhandenen ISMS der Energie AG. Fernwartungszugänge sind nur explizit über Freigabe des Systemadministrators möglich. Es erfolgt eine Überwachung und Protokollierung der zeitlich begrenzten Fernwartung.

5.5. Maßnahmen-Cluster 8: Physische Sicherheitsmaßnahmen

Dieser Maßnahmen-Cluster konnte im Rahmen einer technischen Überprüfung innerhalb der Teststellung nicht evaluiert werden. Die geforderten Maßnahmen sind eine Anforderung aus der Risikoanalyse in der E-Wirtschaft und werden je nach Kritikalität der Anlagen abgestuft durchgeführt. Die Netzgesellschaften haben zusätzliche eigene physische Anforderungen an Anlagen und Gebäudeschutz aufgrund der Gefährdung durch fremde, nicht fachkundige Personen in den Anlageräumen von Mittel- und Hochspannungsanlagen. Die physischen Anforderungen der IKT knüpfen

nahtlos an diese an.

5.6. Maßnahmen-Cluster 9: Incident Management

5.6.1. Konkrete Evaluierungsmethodik und Ergebnisse

Im Rahmen der Tests wurde die Reaktion auf Stimuli wie Portscans und mehrfache Verbindungen und Loginversuche getestet.

Der Router verhielt sich vorbildlich. Er erkannte Portscans und blockierte sie umgehend. Gescheiterte Loginversuche führten schnell dazu, dass der Router vorübergehend keine Verbindungen mehr auf den Port entgegennahm.

Der Backbone zeigte keinerlei derartige Schutzmechanismen und ließ im Test beliebig viele Loginversuche und Verbindungen zu. Die Implementierung dieser Schutzmaßnahme ist in Umsetzung. Alle offenen Ports sind gesperrt, die zur Verfügung stehenden Ports sind mittels NAC gesichert. Das Risiko eines unberechtigten Zugriffs auf die Zentralkomponenten wird als gering eingestuft, da verschiedene Maßnahmen im Bereich der Zugangssicherung getroffen wurden.

5.6.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 31: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 9 (Evaluierg. ZNR)

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Umsetzung Incident Management	N (1)	?	?
Identifizierung, (Fern-) Abschaltung und Austausch von Komponenten mit fehlerhaftem oder schädlichem Verhalten (HW wie SW)	J	Teilw. (2)	J
Notsignalgebung bei (Verdacht auf) Unregelmäßigkeiten	J	N (2)	J
Regelwerkerstellung zur Fehlerbehebungsabläufen	N (3)	?	?

Anmerkungen:

(1) Konnte ohne Hersteller-Dokumentation nicht überprüft werden.
(2) Der Router verhinderte Portscans auf die eigenen Ports, erkannte aber keine Angriffe auf andere Komponenten.
(3) Konnte im Rahmen der Teststellung nicht überprüft werden.

Punkt (3) wird durch ISMS-Anforderungen wie z. B. Sicherheitsvorfälle, Verbesserungsmaßnahmen und die Dokumentation in einem Troubleticketsystem zur Erhebung von Häufigkeiten bei geringer Fehlerauswirkung (z. B. Lebensdauer von Systemen) gewährleistet.

5.7. Maßnahmen-Cluster 10: Mehrstufiges Sicherheitskonzept

5.7.1. Konkrete Evaluierungsmethodik und Ergebnisse

Aus den Tests, die im Rahmen der anderen Maßnahmen-Cluster durchgeführt wurden, zeigte sich, dass die Router Bestandteil eines mehrstufigen Sicherheitskonzeptes sind, welches das Backbone-Netzwerk vor Angriffen über das lokale Netz im Umspannwerk absichern soll.

5.7.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 32: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 10 (Evaluierg. ZNR)

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Mehrstufiges Sicherheitskonzept	J	N (1)	J
Verschlüsselte Datenkommunikation	J	N (2)	J
Anonymisierung und Aggregation von personenbezogenen Daten wo möglich	J	J	J

6. Ergebnisse der Evaluierung der Metering-Umgebung

6.1. Maßnahmen-Cluster 1: Authentizität und Integrität

6.1.1. Konkrete Evaluierungsmethodik und Ergebnisse

Zunächst wurde die Kommunikation zwischen Datenkonzentratoren und Uplink aufgezeichnet. Dadurch konnten sowohl Steuerbefehle vom Transaktionsserver, als auch Nachrichten der Smart Meter aufgezeichnet werden. Anschließend fand ein aktiver Portscan in dem Netzwerksegment statt. Der ausgewählte Angriffspunkt stellt aufgrund der Exponiertheit der Datenkonzentratoren (Trafohäuschen) den Punkt mit dem höchsten Risiko dar.

Beim Sniffing wurde festgestellt, dass die Kommunikation über das IEC 60870-5-104 Protokoll erfolgt. Dieses Protokoll wurde in der Teststellung nicht durch zusätzliche Maßnahmen geschützt und bietet selbst keine Sicherheitsfeatures wie Authentifizierung oder Verschlüsselung. Daher kann ein Angreifer an einem geeigneten Punkt im Netzwerk die Steuerbefehle des Transaktionsservers bzw. die Nachrichten der Smart Meter fälschen und dadurch Endgeräte steuern und falsche Informationen an den Trans-

aktionsserver senden.

Des Weiteren wird das Network Time Protocol (NTP) in seiner unsichersten Form (ohne Authentifizierung) verwendet. Dadurch kann ein Angreifer die Pakete manipulieren und die Zeit der Datenkonzentratoren und der Smart Meter auf beliebige Werte setzen. Das führt dazu, dass der Angreifer Ereignisse auslösen oder blockieren kann.

6.1.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 33: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 1 (Evaluierg. Metering)

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Sicherstellung von Authentizität und Integrität von Software	N	?	?
Sicherstellung von Authentizität und Integrität von Kommunikations- und Steuerdaten	J	N (1)	?

Anmerkungen:

(1) Die Endpunkte setzen auf Protokolle auf, die keinerlei entsprechende Schutzmaßnahmen beinhalten (z. B. IEC 60870-5-104).

Derzeit wird auf Netzwerksicherheit gesetzt. In der Zeit der Tests war diese jedoch nicht aktiviert. Dies betrifft die Punkte Port Link down, MACSec, Authentifizierung, NAC am Office Port.

6.2. Maßnahmen-Cluster 3: Minimalprinzip für sicherheitskritische Schnittstellen

6.2.1. Konkrete Evaluierungsmethodik und Ergebnisse

Von dem in Abschnitt 6.1 beschriebenen Angriffspunkt wurde ein Netzwerkscan inklusive Portscan durchgeführt.

Transaktionsserver:
Die von dem beschriebenen Angriffspunkt aus erreichbaren Ports des Transaktionsservers werden an dieser Stelle nicht genannt, da es sich um eine sicherheitskritische Information handelt.

Im Testlabor befindet sich keine Firewall-Implementierung. Am aktiven System und am Redundanzsystem ist jedoch eine Firewall vorhanden.

Datenkonzentratoren / TM 1703 ACP
Neben der notwendigen IEC 60870-5-104 Server boten die Geräte auch Webserver an. Über die Notwendigkeit der Webserver kann keine Aussage getroffen werden, es konnte jedoch festgestellt werden, dass während des Normalbetriebs keine HTTP-Verbindungen aufgebaut wurden.

6.2.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 34: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 3 (Evaluierg. Metering)

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Minimalprinzip für sicherheitskritische Schnittstellen (Internetverbindung)	J	J	J
Minimalprinzip für sicherheitskritische Schnittstellen (physischer Zugriff)	N (1)	?	?
Minimalprinzip für sicherheitskritische Schnittstellen (logischer Zugriff)	J	N (2)	?
Minimalprinzip für Sammlung, Speicherung und Übermittlung schutzbedürftiger Daten	J	J	J
Kapselungsprinzip	N	N (2)	?

Anmerkungen:

(1) Maßnahmen zur Unterbindung von physikalischem Zugriff konnten im Rahmen der Teststellung nicht überprüft werden. Der Datenkonzentrator befindet sich im Feld. Der Transaktionsserver befindet sich in einem geschützten Bereich (physischer und optischer Schutz).

(2) Es konnten keine speziellen Maßnahmen festgestellt werden.

6.3. Maßnahmen-Cluster 4: Netzwerksegmentierung & Abschottung verschiedener (Sicherheits-) Bereiche

6.3.1. Konkrete Evaluierungsmethodik und Ergebnisse

Der Netzwerkaufbau wurde durch Kommunikationsmitschnitte und manuelle Verbindungsversuche evaluiert.

Alle TCP/IP-fähigen Komponenten (auch die mittels Uplink angebundenen) befanden sich im selben Subnetz, ebenso der Transaktionsserver, welcher als besonders kritische Komponente angesehen wird. In dem Segment wurde keine Firewall eingesetzt.

Anmerkungen:
Im aktiven System ist eine Netzwerksegmentierung und eine Firewall vorhanden. Bei dem Testsystem wurde dies leider übersehen. Im aktiven System befindet sich ein IPS/IDS-System. Der Smart Meter ist durch VLANs von den SCADA-Systemen getrennt. Der Übergang erfolgt über eine spezielle Firewall.

6.4. Maßnahmen-Cluster 5: Schutz von (Fern-) Wartungszugängen & verpflichtende Transparenz seitens der Hersteller

6.4.1. Konkrete Evaluierungsmethodik und Ergebnisse

Fernwartungsservices wurden mittels Portscans ermittelt.

Sowohl die Datenkonzentratoren als auch die Komponente TM 1703 ACP boten Webserver mit passwortgeschütztem Login. Die Übertragung (HTTP) war komplett ungeschützt. Es sollte abgewogen werden, ob diese Zugänge notwendig sind und gegebenenfalls besser abgesichert (HTTPS) oder deaktiviert werden sollten.

Die Komponente TM 1703 ACP stellte den Fernwartungszugang für die Siemens Toolbox II zur Verfügung. Das verwendete Protokoll bietet keine Authentifizierung oder Verschlüsselung. Da dies nur von Seiten des Herstellers geändert werden kann, sind die Risiken sorgfältig abzuwägen und der Zugang nach Möglichkeit zu schließen.

6.4.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 35: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 5 (Evaluierg. Metering)

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Besonderer Schutz von (Fern-) Wartungszugängen durch verschlüsselte Kommunikationstunnel	J	J	?
Verpflichtende Herstellertransparenz zur Offenlegung von möglichen Wartungsschnittstellen	N (1)	?	?
Access Control	J	J	?
Protokollierung von Rollen, Personen, Zeiten und Tätigkeiten	N (1)	?	?
Schulung von Wartungspersonal zur Förderung von Sicherheitsbewusstsein	N (1)	?	?

Anmerkungen:

(1) Konnte im Rahmen der Teststellung nicht überprüft werden.

6.5. Maßnahmen-Cluster 8: Physische Sicherheitsmaßnahmen

Physische Sicherheit, Zutrittskontrolle samt Änderungsprotokollierung, Token und Alarmanlagen sind in den ISMS-Dokumenten geregelt und werden entsprechend diesen Anforderungen umgesetzt.

6.6. Maßnahmen-Cluster 9: Incident Management

6.6.1. Konkrete Evaluierungsmethodik und Ergebnisse

Die Reaktion auf Stimuli wurde mittels Portscans und manueller Verbindungsversuche getestet.

Weder die Datenkonzentratoren noch die Komponente TM 1703 ACP konnten erkennen, ob sie mit dem Transaktionsserver oder jemand Drittem kommunizieren. Solange die Geräte erreichbar sind, lassen sich beliebige Steuerbefehle generieren und senden.

6.6.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 36: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 9 (Evaluierg. Metering)

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Umsetzung Incident Management	N (1)	?	?
Identifizierung, (Fern-) Abschaltung und Austausch von Komponenten mit fehlerhaftem oder schädlichem Verhalten (HW wie SW)	J	J	?
Notsignalgebung bei (Verdacht auf) Unregelmäßigkeiten	J	J	?
Regelwerkerstellung zu Fehlerbehebungsabläufen	N (2)	?	?

Anmerkungen:

(1) Konnte ohne Hersteller-Dokumentation nicht überprüft werden.
(2) Konnte im Rahmen der Teststellung nicht überprüft werden.

Incident Management inkl. eines Regelwerkes für Fehlerbehebungsabläufe ist in den ISMS-Dokumenten geregelt und wird bei den jährlichen Audits überprüft. Die Befehlsfolge über den Transaktionsserver wird überwacht, bei Überschreiten oder Systemunregelmäßigkeiten wird eine Alarmierung ausgelöst

6.7. Maßnahmen-Cluster 10: Mehrstufiges Sicherheitskonzept

6.7.1. Konkrete Evaluierungsmethodik und Ergebnisse

Im Rahmen der Teststellung konnte kein mehrstufiges Sicherheitskonzept getestet werden.

Die Übertragung zwischen Transaktionsserver und den Endpunkten erfolgt ungeschützt, es waren keine zusätzlichen Maßnahmen zur Absicherung ersichtlich.

6.7.2. Umsetzung und Effektivität der (SG)²-Maßnahmen

Tabelle 37: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 10 (Evaluierg. Metering)

Maßnahme	**Überprüfbar**	**Vorhanden**	**Effektiv**
Mehrstufiges Sicherheitskonzept	J	N (1)	?
Verschlüsselte Datenkommunikation	J	N (2)	?
Anonymisierung und Aggregation von personenbezogenen Daten wo möglich	J	J	J

Anmerkungen:
(1) Es konnte kein mehrstufiges Sicherheitskonzept festgestellt werden.
(2) Die verwendeten Protokolle unterstützen keinerlei Verschlüsselung.

Ende-zu-Ende-Verschlüsselung ist im System implementiert. Die Kommunikation über die Infrarotschnittstelle und die Auftragsübermittlung erfolgt verschlüsselt. Ein mehrstufiges Sicherheitskonzept befindet sich derzeit im Aufbau.

7. Anwendung des Maßnahmenkataloges

Die in dem Maßnahmenkatalog vorgeschlagenen Maßnahmen sind zu einem Teil bereits in dem System der Energie AG umgesetzt. Alle österreichischen Energieversorger sind derzeit mit der Umsetzung einiger dieser Maßnahmen betraut. Die Evaluierung der bei der Energie AG im Testlabor bereits umgesetzten Maßnahmen zeigt die Effizienz dieser Maßnahmen auf, vor allem auch im Hinblick auf die Techniklebensdauer der in der Energieversorgung eingesetzten Leitsysteme. Ein Austausch der Leitsysteme ist finanziell nur über einen längeren Zeitraum möglich. Die jetzt geforderten Sicherheitsmaßnahmen wie Verschlüsselung auf Applikationsebene, Signatur, usw. muss über einen Lebenszyklus von 20 Jahren gewährleistet sein. Dabei ist zu betrachten, dass neue Systeme flexibel auf neue, zukünftige Anforderungen (Änderungen des Verschlüsselungssystems usw.) reagieren können.

Der Aufbau einer sicheren Kommunikation und der Schutz der Schnittstellen ist auf den für die Steuerung erforderlichen Übertragungseinrichtungen leichter und schneller realisierbar. Bei diesen Systemen geht man von einem Produktlebenszyklus von sechs Jahren aus.

Zusätzliche Schutzmechanismen wie

- physischer Schutz durch Überwachung der Gebäude, Räume, Geräteschränke und Systemkomponenten,
- Verfügbarkeit der Systeme wie der Übertragungstechnik, der erforderlichen Bandbreiten, der USV-Anlagen mit Überbrückungszeiten > 48 Stunden,
- Redundanzen für Virtualisierung der Außenanlagen,
- Notkommunikationssysteme für Sprache, Datenaustausch, Systemspeichereinheiten,
- Berücksichtigung von Cyber-Warneinrichtungen wie Cert,
- Kommunikation mit Ende-zu-Ende-Verschlüsselung oder
- Zugriffschutz (verschlüsselte Datenhaltung, starke Passwörter) und Skalierung der Benutzer

sind derzeit die am schnellsten realisierbaren Sicherheitsmechanismen, welche in relativ kurzer Zeit (einige Jahre) implementiert werden können.

Die im Rahmen der erfolgten Überprüfung gefundenen Schwachstellen wurden in Abstimmung mit den Systemlieferanten, soweit es Adaptierungen zulassen, einem Sicherheitsupdate unterzogen und nochmals von der Energie AG einem Penetrationstest unterzogen. Sofern sich diese Sicherheitsupdates als erfolgreich erweisen, werden die Ergebnisse in den Arbeitsgruppen von Österreichs Energie den anderen EVUs mitgeteilt und, soweit es mit den großen Netzbetreibern vereinbar ist, in den Anforderungsdokumenten von Österreichs Energie für sichere Fernwirksysteme und sichere Smart-Meter-Systeme aufgenommen.

8. Evaluierung der Methodik

Die Eignung der im $(SG)^2$-Projekt angewandten Methodik, Maßnahmen zu definieren, welche die Sicherheit der Energiesysteme nach den heute zur Verfügung stehenden Mitteln gewährleisten und zugleich auch in die (nähere) Zukunft blicken, wurde durch die Evaluierung ausreichend bewiesen. Für die Sicherheitsanforderungen der Zukunft ist es erforderlich, die vorhandenen Schwachstellen zu erkennen, zu analysieren und Maßnahmen gegen die Ausnutzung dieser Schwachstellen zu treffen.

Aus technischer Sicht ist klar festzustellen, dass Schwachstellen in den grundlegenden Systemen (Fernwirkanlagen, Schutztechnik, usw.) nicht kurzfristig lösbar sind. Hier ist die einzig praktikable Lösung, die Sicherheitsrisiken mit den bestehenden, am Markt erhältlichen Systemen zu reduzieren und die Anforderungen an die Lieferanten in die Lebenszyklusplanung einzubinden sowie die neuen Systeme über softwaretechnische Lösungen entsprechend zu schützen. Die neuen Systeme sollten nach den derzeitigen technischen Sicherheitsanforderungen („Best Practice") konzipiert werden. Flexible Zukunftslösungen sind gegenüber starren Systemen zu bevorzugen.

Der größte Schwachpunkt liegt in der für den technischen Betrieb von kritischen Infrastrukturen mangelnden Zertifizierung (als Nachweis einer umfassenden Geräte- und Systemprüfung). Hierbei sollte sich in Europa in den nächsten Jahren eine Prüfnorm einschließlich entsprechender Prüfstellen mit Zertifikat (wie z. B. VDE-/ÖVE-Prüfzeichen) entwickeln. Damit wären die einzelnen Systemlieferanten aufgefordert, nur mehr sicherheitsgeprüfte Endgeräte und Systemkomponenten zur Verfügung zu stellen. Vor allem würden sich dadurch auch die Kosten für die Systemüberprüfung und -härtung aufseiten der Betreiber kritischer Infrastrukturen reduzieren. Derzeit prüft jedes einzelne Unternehmen mit entsprechendem Aufwand die zur Verfügung gestellten Komponenten auf sicherheitskritische Schwachstellen und ist meist aus Zeit- und Ressourcengründen nicht in der Lage, Prüfungen auf Bedienerebene oder Gesamtsystemebene im erforderlichen Ausmaß durchzuführen.

Die Tests zur Evaluierung wurden unter der Prämisse durchgeführt, dass unter Umgehung des physischen Zutrittsschutzes ein direkter Zugang zu den Systemen möglich ist. Gleichfalls war es im Rahmen der technischen Tests nicht möglich, Managementanforderungen zu evaluieren. Diese sollten durch eine gültige ISMS-Zertifizierung gewährleistet sein, wobei in diesem Falle der Scope des Systems zu berücksichtigen ist.

Abkürzungsverzeichnis

A	Availability (Verfügbarkeit)
ADSL	Asymmetric Digital Subscriber Line
AMIS	Produktname für ein Smart Metering System von Siemens
BBPLC	BroadBand Powerline Communication
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSS	Business Support System
C	Confidentiality (Vertraulichkeit)
CVCU	Central Voltage Control Unit
DER	Distributed Energy Resources
DG	Distributed Generation
DLMS	Device Language Message Specification
DMZ	Demilitarized Zone
EGT	Ergebnis der gewöhnlichen Geschäftstätigkeit
EM	Energiemanagement
EVU	Energieversorgungsunternehmen
GPRS	General Packet Radio Service
HBAM	Home And Building Automation
HV	High Voltage (Hochspannung)
I	Integrity (Integrität)
IDS	Intrusion Detection System
IEM	Intelligent Energy Management
IKT	Informations- und Kommunikationstechnologien
IPS	Intrusion Prevention System
IR	Infrarot
ISMS	Informationssicherheitsmanagementsystem
LON	Local Operating Network
LV	Low Voltage (Niederspannung)
LWL	Lichtwellenleiter
MBUS	Metering Bus
MDM(S)	Meter Data Management (System)
MEP	Multipurpose Expansion Port
MODBUS	Protokoll für Master-Slave-Kommunikation
MV	Medium Voltage (Mittelspannung)
NBPLC	Narrowband Powerline Communication
NES	Networked Energy Services

OPC	Object Linking and Embedding for Process Control
OS	Operating System
OSS	Operation Support System
PLC	Power Line Communication
PQ	Power Quality
QM	Qualitätsmanagement
SCADA	Supervisory Control and Data Acquisition
SICAM	Produktname für ein Leitsystem von Siemens
THD	Total Harmonic Distortion
USV	Unterbrechungsfreie Stromversorgung
VDSL	Very High Speed Digital Subscriber Line
VPN	Virtual Private Network
WAN	Wide Area Network
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WWW	World Wide Web
XML	Extensible Markup Language
ZNR	Zentraler Netzrechner
ZUQDE	Zentrale Spannungs- (U) und Blindleistungsregelung (Q) mit dezentralen Einspeisungen

Literaturverzeichnis

Beer, Johannes: Die Convention on Cybercrime und österreichisches Strafrecht, Dissertation, Linz 2005.

Bertel, Christian / Schwaighofer, Klaus: Österreichisches Strafrecht Besonderer Teil I, 12. Auflage, Wien 2012.

Birklbauer, Alois / Hilf, Marianne Johanna / Tipold, Alexander: Strafrecht Besonderer Teil I, Wien 2011.

BSI: Protection Profile for the Gateway of a Smart Metering System (BSI-CC-PP-0073), 2013.

BSI: Protection Profile for the Security Module of a Smart Metering System (Security Module PP, BSI-CC-PP-0077), 2013

Bundesverband der Energie- und Wasserwirtschaft (BDEW): Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme, Version 1.0, Juni 2008.

Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kataloge, siehe http://www.bsi.bund.de/gshb.

Buschmann, Moritz / Motyka, Simone: Energieeffizienz als Schlüssel zur Klima- und Ressourcenschonung? – am Beispiel des Smart Metering, wbl 2011, S. 11-17.

Cyber Security Austria: Smart Metering Chancen und Risiken, abrufbar unter:
http://www.cybersecurityaustria.at/images/pdf/csa_smart_metering_-_chancen_und_risiken.pdf

European Union Agency for Network and Information Security (ENISA): Appropriate security measures for smart grids. Dezember 2012

Dohr, Walter / Pollirer, Hans-Jürgen / Weiss, Ernst / Knyrim, Rainer (Hrsg.): DSG online – Kommentar zum Datenschutzgesetz, 17. Auflage, Wien 2014.

Fischer, Thomas: Strafgesetzbuch und Nebengesetze, Kurzkommentar, 60. Auflage, München 2013.

Fritz, Gernot / Burtscher, Bertram: Data Breach Notification Duty für Betreiber öffentlicher Telekommunikationsdienste, ZIR 2015, S. 5-10.

Fuchs, Helmut: Österreichisches Strafrecht Allgemeiner Teil I, 7. Auflage, Wien 2008.

Gantner, Felix: Computerviren Technik und Recht, Wien 1995.

Gercke, Marco / Brunst, Phillip W.: Praxishandbuch Internetstrafrecht, Stuttgart 2009.

Hayek, F.: The use of knowledge in society. The American Economic Review 35 (4), 1945, S. 519-530.

Hilgendorf, Eric / Valerius, Brian: Computer- und Internetstrafrecht, Ein Grundriss, 2. Auflage, Berlin 2012.

Hinterhofer, Hubert / Rosbaud, Christian: Strafrecht Besonderer Teil II, 5. Auflage, Wien 2012.

Hoffer, Martin: Der Kilometerzähler: Messgerät – Beweismittel – Daten – oder doch „gar nichts"?, JBl 2011, S. 542-543.

Jahnel, Dietmar: Datenschutzrecht, Wien 2010.

Joecks, Wolfgang: Studienkommentar StGB, 10. Auflage, München 2012.

Judmann, Kurt P.: Zum „Stand der Technik" in der Informationstechnik, in: Gerhard Saria (Hrsg.), Der „Stand der Technik", Wien/Graz 2007, S. 87-98.

Kienapfel, Diethelm / Höpfel, Frank / Kert, Robert: Grundriss des Strafrechts Allgemeiner Teil, Wien 2012.

Kletečka, Andreas / Schauer, Martin: ABGB-ON - Kommentar zum Allgemeinen bürgerlichen Gesetzbuch, Wien 2013.

Knyrim, Rainer: Die Datenschutz-Grundverordnung: Entwicklung und Anwendungsbereich, Dako 2012/21, S. 32-35.

Knyrim, Rainer: Entwurf der neuen EU-Datenschutz-Grundverordnung, in: Matthias Scholz / Axel Funk, DGRI Jahrbuch 2012, Köln 2012, S. 25-38.

Kudlich, Hans / Oglakcioglu, Mustafa Temmuz: Strom-„Diebstahl" durch die Manipulation von Stromzählern, in: Schulz, Lorenz / Reinhart, Michael / Sahan, Oliver, Festschrift für Imme Roxin, Heidelberg 2012, S. 265-278.

Lackner, Karl / Kühl, Kristian: Kommentar StGB, 27. Auflage, München 2011.

Leissler, Günther: Hackattacken: Verletzter Datenschutz, in: Dietmar Jahnel (Hrsg.), Datenschutzrecht und E-Government, Jahrbuch 2012, Wien 2012, S. 167-175.

Markl, Beatrice: Smart Metering und Datenschutz, in: Horst Steinmüller / Andreas Hauer / Friedrich Schneider (Hrsg.), Energiewirtschaft, Jahrbuch 2011, Wien/Graz 2011, S. 35-52.

Münchner Kommentar zum Bürgerlichen Gesetzbuch, 6. Auflage, München 2013.

Nomos Kommentar, Strafgesetzbuch Band 2, Kindhäuser, Urs / Neumann, Ulfried / Paeffgen, Hans-Ullrich (Hrsg.), 4. Auflage, Baden-Baden 2013.

Oesterreichs Energie: ElWOG Kommentar, 2. Auflage, Wien 2013.

Österreichs Energie: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme. Ausführungshinweise zur Anwendung des BDEW Whitepaper. Version 1.0, 2012

Palandt, Otto: Bürgerliches Gesetzbuch Kommentar, 72. Auflage, München 2013.

Reichl, Johannes / Schmidthaler, Michael / Schneider, Friedrich: The value of supply security: The costs of power outages to Austrian households, firms and the public sector, Energy Economics, Volume 36, 2013, S. 256-261.

Reindl-Krauskopf, Susanne: Computerstrafrecht im Überblick, 2. Auflage, Wien 2009.

Rengier, Rudolf: Strafrecht Besonderer Teil I, 15. Auflage, München 2013.

Rengier, Rudolf: Strafrecht Besonderer Teil II, 13. Auflage, München 2012.

Rummel, Peter: ABGB online – Kommentar zum Allgemeinen bürgerlichen Gesetzbuch, Wien.

Salimi, Farsam: Zahnloses Cyberstrafrecht? Eine Analyse der gerichtlichen Straftatbestände zum Daten- und Geheimnisschutz, ÖJZ 2012/115, S. 998-1003.

Salzburger Kommentar zum Strafgesetzbuch, Triffterer, Otto / Rosbaud, Christian / Hinterhofer, Hubert (Hrsg.), Wien 2013.

Santer, Stefan / Spiel, Silke: Der Weg ins digitale Energiezeitalter – Eine Abhandlung technischer und rechtlicher Fragen im Zusammenhang mit der Einführung von intelligenten Messgeräten, ZTR 2012, S. 93-102.

Saria, Gerhard: Grundsätzliches zum „Stand der Technik" aus rechtswissenschaftlicher Sicht, in: Gerhard Saria (Hrsg.), Der „Stand der Technik, Wien/Graz 2007, S. 25-75.

Saria, Gerhard: Technikklauseln und technische Normen – Neuere Entwicklungen im Recht der Technikklauseln, ZTR 2011, S. 24-31.

Schoeman, F. D.: Privacy and social freedom. Cambridge university press, 1992.

Schönke, Adolf / Schröder, Horst: Kommentar zum Strafgesetzbuch, 29. Auflage, München 2014.

Schmid, Barbara: Produkthaftungsgesetz Kurzkommentar, Wien 2011.

Schrott, Alexandra: Einführung intelligenter Messgeräte („Smart Meter") im Zusammenhang mit Datenschutz und Datensicherheit, in: Dietmar Jahnel (Hrsg.), Datenschutzrecht, Jahrbuch 2014, Wien 2014, S. 163-190.

Schuh, Daniel: Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz, Dissertation, Berlin 2012.

Seiler, Stefan: Strafrecht Allgemeiner Teil, Band 1, Wien 2007.

Smart Metering Projects Map, https://www.google.com/maps/d/viewer?mid=zReklSu043lk.kZ_YiimMzyXc&ie=UTF8&oe=UTF8&msa=0

Solove, D. J.: A taxonomy of privacy. University of Pennsylvania Law Review 154 (3), 477, 2006.

Sonntag, Michael: Einführung in das Internetrecht, Wien 2010.

Steininger, Einhard: Strafrecht Allgemeiner Teil, Band 2, Wien 2012.

Steininger, Einhard: Verbandsverantwortlichkeitsgesetz, Wien 2006.

Stigler, G. J.: The economics of information. The Journal of Political Economy 69 (3), 1961, S. 213-225.

Warren, S. und L. Brandeis: The right to privacy. Harvard Law Review 4 (5), 1890, S. 193-203.

Westin, A.: Privacy and Freedom. New York: Atheneum Publishers, 1967.

Wegscheider, Herbert: Strafrecht Besonderer Teil, 4. Auflage, Wien 2012.

Welser, Rudolf / Rabl, Christian: Produkthaftungsgesetz Kommentar, 2. Auflage, Wien 2004.

Wessels, Johannes / Hillenkamp, Thomas: Strafrecht Besonderer Teil 2, 35. Auflage, Heidelberg 2012.

Wiener Kommentar zum StGB, Höpfel, Frank / Ratz, Eckart (Hrsg.), 2. Auflage, Wien 2008.

Abbildungsverzeichnis

Abbildung 1: Smart Grid Architecture Model (SGAM) gemäß CEN-CENELEC-ETSI (2012) 21
Abbildung 2: IKT-Architekturmodell aus dem Projekt $(SG)^2$ 24
Abbildung 3: Komponenten-Cluster im IKT-Architekturmodell 25
Abbildung 4: Mapping der Teststellungen auf das IKT-Architekturmodell: „Secure Substation Automation“ (rot) und „Smart Metering“ (grün) 137
Abbildung 5: „Secure Substation Automation“-Teststellung (SCADA System nicht abgebildet) 141
Abbildung 6: Topologieübersicht „Secure Substation Automation“-Teststellung 143
Abbildung 7: Testkoffer für die Analyse von Smart-Metering-Systemen 144
Abbildung 8: Topologie der Teststellung „Smart Metering“ 145
Abbildung 9: Typischer Aufbau eines Smart-Metering-Systems 145
Abbildung 10: Erstellung einer Whitelist auf einem System 146
Abbildung 11: Programmausführung wird verhindern, da das Programm nicht in der Whitelist enthalten ist 147
Abbildung 12: Skriptausführung wird verhindert, da das Skript nicht in der Whitelist enthalten ist 147
Abbildung 13: Beispiele für den Verallgemeinerungsschritt bei der Definition des Maßnahmenkatalogs 157
Abbildung 14: Darstellung der IKT-Architektur als Asset-Struktur 177
Abbildung 15: Ergebnisse der Business-Impact-Analyse im Überblick 179
Abbildung 16: Schutzbedarfskonfiguration für das Asset „Smart Meter“ 180
Abbildung 17: Darstellung der Bedrohungen 181
Abbildung 18: Darstellung der Controls 182
Abbildung 19: Teststellung bei der Energie AG 189
Abbildung 20: Abläufe Incident Management 209

Tabellenverzeichnis

Tabelle 1: Ausgewählte österreichische Smart-Grid-Projekte 20
Tabelle 2: Komponenten-Cluster "funktionale Gebäude" 26
Tabelle 3: Konponenten-Cluster "E-Mobilität" 27
Tabelle 4: Komponenten-Cluster "Haushalt" 27
Tabelle 5: Komponenten-Cluster "Erzeugungsanlage LV" 28
Tabelle 6: Komponenten-Cluster "Erzeugungsanlage MV" 28
Tabelle 7: Komponenten-Cluster "Messstellen im Netz" 29
Tabelle 8: Komponenten-Cluster "Umspannwerk (HV/MV)" 29
Tabelle 9: Komponenten-Cluster "Ortsnetzstation (MV/LV)" 30
Tabelle 10: Komponenten-Cluster "Netzbetrieb" 30
Tabelle 11: Komponenten-Cluster "Metering" 31
Tabelle 12: Skala für die Bewertung der Eintrittswahrscheinlichkeit 40
Tabelle 13: Skala für die Bewertung der Auswirkungen 40
Tabelle 14: Einstufung Risikopotential 41
Tabelle 15: Einfluss von Wahrscheinlichkeit und Schwere der Auswirkungen auf den Risk-Score 140
Tabelle 16: Kategorien Risk-Score 141
Tabelle 17: Häufigkeit der übergeordneten Maßnahmen über den gesamten Maßnahmenkatalog hinweg 160
Tabelle 18: Gewichtete Häufigkeit der übergeordneten Maßnahmen über den gesamten Maßnahmenkatalog hinweg 161
Tabelle 19: Darstellung der Schutzbedarfsstruktur 178
Tabelle 20: Nutzwertanalyse des Tools „verinice“ 182
Tabelle 21: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 1 213
Tabelle 22: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 3 214
Tabelle 23: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 4 215
Tabelle 24: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 5 216
Tabelle 25: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 9 218
Tabelle 26: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 10 219

Tabelle 27: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 1 (Evaluierg. ZNR) 221
Tabelle 28: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 3 (Evaluierg. ZNR) 222
Tabelle 29: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 4 (Evaluierg. ZNR) 223
Tabelle 30: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 5 (Evaluierg. ZNR) 224
Tabelle 31: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 9 (Evaluierg. ZNR) 226
Tabelle 32: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 10 (Evaluierg. ZNR) 227
Tabelle 33: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 1 (Evaluierg. Metering) 228
Tabelle 34: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 3 (Evaluierg. Metering) 230
Tabelle 35: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 5 (Evaluierg. Metering) 232
Tabelle 36: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 9 (Evaluierg. Metering) 233
Tabelle 37: Bewertung der (SG)²-Maßnahmen im Maßnahmen-Cluster 10 (Evaluierg. Metering) 234

Herausgeber und Autoren

Herausgeber

Johannes Göllner
Landesverteidungsakademie Wien
johannes.goellner@bmlvs.gv.at

Lucie Langer
AIT Austrian Institute of Technology GmbH
lucie.langer@ait.ac.at

Matthias Tischlinger
Energie AG Oberösterreich Data GmbH
matthias.tischlinger@energieag.at

Autoren (alphabetisch)

Kathrin de Bruyn
Energieinstitut an der Johannes Kepler Universität Linz
deBruyn@energieinstitut-linz.at

René Freingruber
SEC Consult Unternehmensberatung GmbH
r.freingruber@sec-consult.com

Johannes Göllner
Landesverteidungsakademie Wien
johannes.goellner@bmlvs.gv.at

Robert Gottwald
Bundesministerium für Inneres
robert.gottwald@bmi.gv.at

Berthold Haberler
LINZ AG TELEKOM
b.haberler@linzag.at

Thomas Hecht
AIT Austrian Institute of Technology GmbH
thomas.hecht@ait.ac.at

Markus Kammerstetter
Technische Universität Wien, Automation Systems Group
mkammerstetter@auto.tuwien.ac.at

Georg Kienesberger
Technische Universität Wien, Institut für Computertechnik
georg.kienesberger@tuwien.ac.at

Christian Kudera
SEC Consult Unternehmensberatung GmbH
c.kudera@sec-consult.com

Friederich Kupzog
AIT Austrian Institute of Technology GmbH
friederich.kupzog@ait.ac.at

Lucie Langer
AIT Austrian Institute of Technology GmbH
lucie.langer@ait.ac.at

Andreas Mattern
Bundesministerium für Inneres
andreas.mattern@bmi.gv.at

Marcus Meisel
Technische Universität Wien, Institut für Computertechnik
marcus.meisel@tuwien.ac.at

Christian Meurers
Landesverteidungsakademie Wien
christian.meurers@bmlvs.gv.at

Sasa Milojkovic
Omnetric GmbH
sasa.milojkovic@omnetric.com

Raffaele Montagna
Innsbrucker Kommunalbetriebe AG
raffaele.montagna@ikb.at

Andreas Peer
Landesverteidungsakademie Wien
andreas.peer@bmlvs.gv.at

Johannes Reichl
Energieinstitut an der Johannes Kepler Universität Linz
reichl@energieinstitut-linz.at

Alexander Sadofsky
Siemens AG Österreich
alexander.sadofsky@siemens.com

Florian Skopik
AIT Austrian Institute of Technology GmbH
florian.skopik@ait.ac.at

Thomas Stotter
Innsbrucker Kommunalbetriebe AG
thomas.stotter@ikb.at

Matthias Tischlinger
Energie AG Oberösterreich Data GmbH
matthias.tischlinger@energieag.at

Band 15 / 2016

Die Stromversorgung der Zukunft wird weit mehr auf Informations- und Kommunikationstechnologien (IKT) setzen als bisher. Damit werden Cybersecurity-Risiken auch zu einer Gefahr für die Energieversorgung. Viele Sicherheitsfragen in diesen zukünftigen Netzen sind noch ungeklärt, denn die speziellen Umgebungen erfordern neuartige Sicherheitsmechanismen und Prozesse. Im Projekt Smart Grid Security Guidance $(SG)^2$ wurden daher aktuelle Smart-Grid-Technologien in Bezug auf IKT-Sicherheitsaspekte evaluiert und effektive Schutzmaßnahmen vor Cyber-Attacken definiert.

ISBN: 978-3-902944-98-6