Kompendium

DIGITALISIERUNG IN DER ENERGIE-WIRTSCHAFT

Digitalisierung, Daten und Sicherheit: Herausforderungen für Unternehmen in der Energiewirtschaft

Berlin, Mai 2021

Inhaltsverzeichnis

Was Sie inhaltlich erwartet 3
Andreas Corusa (Technische Universität Berlin, Fachgebiet Energiesysteme)

Vorwort 4
Georg Erdmann (Technische Universität Berlin, Fachgebiet Energiesysteme)

BEITRAG 1

Digitalisierung in der Energiewirtschaft: Definition, Datenzugang und Mehrwerte 6
Andreas Corusa (Technische Universität Berlin, Fachgebiet Energiesysteme)
Elena Timofeeva (Technische Universität Berlin, Fachgebiet Energiesysteme)
Johannes Predel (Technische Universität Berlin, Fachgebiet Energiesysteme / nymoen Strategieberatung)

BEITRAG 2

Zukunftsorientiertes IT-Management in Energieversorgungsunternehmen 48
Falk Ritschel (Conomic GmbH)
Christian Sprengel (Conomic GmbH)
Anne Walther (Conomic GmbH)

BEITRAG 3

IT-Sicherheit für KRITIS-Unternehmen in der digitalen Energiewirtschaft 84
Daniel Kaufmann (BBH Consulting AG)
Stefan Brühl (BBH Consulting AG)
Victor Stocker (BBH Consulting AG)

BEITRAG 4

Studie zum exemplarischen Anwenden von Gefährdungsszenarien in der Energiedomäne 110
Christine Rosinger (OFFIS e.V., FuE Bereich Energie)
Mathias Uslar (OFFIS e.V., FuE Bereich Energie)

Zusammenfassung und Schlusswort 146
Simon Schäfer-Stradowsky
(Institut für Klimaschutz, Energie und Mobilität e.V. (IKEM))

Kurzbiographien der Autoren 150

Anhang für Beitrag 4 153

Impressum 223

://

Was Sie inhaltlich erwartet

Dieses Kompendium wendet sich an Leserinnen und Leser, die neben energiewirtschaftlichem Grundwissen vor allem Interesse an Digitalisierungsthemen mitbringen. Wir unternehmen mit diesem Werk den Versuch einen Teil der Komplexität des Themas anhand des Knowhows der beitragenden Autoren aus verschiedenen Disziplinen zu vereinen, um nicht nur Neugier des Lesenden zu wecken, sondern auch und um über das Thema Digitalisierung aufzuklären. Dabei besteht das Kompendium aus vier Teilen, die verschiedene Herausforderungen der Digitalisierung beleuchten und systematische Einschätzungen sowie mögliche Lösungskonzepte präsentieren, die es aus Unternehmensperspektive zu beachten gibt. Das gesamte Werk stellt nur einen kleinen Teil dieser Herausforderungen dar, thematisiert – unserer Meinung nach – aber besonders relevante:

BEITRAG 1

Im ersten Beitrag besprechen wir die allgemeinen als auch die energiewirtschaftlich geprägten Definitionen von Digitalisierung und beschäftigen uns überdies mit energierelevanten Daten, deren Beschaffung und Zugang sowie möglichen datenbasierten Mehrwerten.

BEITRAG 2

Im zweiten Beitrag wurde der Fokus auf IT-Management in Energieversorgungsunternehmen gelegt. Es geht um die strukturierte Vorgehensweise digitaler Transformationsprozesse, um einerseits das bestehende Geschäft adäquat mit IT zu unterstützen und andererseits durch IT gebotene Möglichkeiten Potenziale für neue Geschäftsmodelle zu identifizieren und auszuschöpfen.

BEITRAG 3

Der dritte Beitrag gibt einen Überblick über die rechtlichen Rahmenbedingungen von Betreibern kritischer Infrastrukturen (KRITIS) und deren Auswirkungen auf die IT-Sicherheit am Beispiel der Energiewirtschaft. Zum einen wird die derzeitige Sicherheitslage bewertet und zum anderen wird abschätzt, wie durchgängig das Sicherheitsniveau, im Rahmen der steigenden dezentralen Energieerzeugung und zunehmenden Digitalisierung mit intelligenten Technologien, ist.

BEITRAG 4

Der vierte Beitrag zeigt die praktische Anwendung von Gefährdungsszenarien in der Systementwicklung. Dafür wurde der Anwendungsfall virtuelles Kraftwerke im Rahmen einer Überlastsituation identifiziert und standardisiert erfasst. Auf dieser Basis wurden drei verschiedene Gefährdungsszenarien erfasst und analysiert, so dass systematisch verletzte Schutzziele und Sicherheitsanforderungen identifiziert werden konnten, die dann in einem zu implementierenden System als konkrete Sicherheitsmaßnahmen umgesetzt werden sollten.

Ich hoffe, dass der kurze Einblick in die einzelnen Beiträge Interesse geweckt hat und wünsche Ihnen viel Spaß beim Lesen unseres Kompendiums.

Andreas Corusa

://

VORWORT

Digitalisierung, ein Megatrend dieses Jahrhunderts! Vor 50 Jahren war es noch keineswegs absehbar. Als wir in den 1970er Jahren erstmals mit Computern konfrontiert wurden, mussten diese noch mit Lochkarten gefüttert werden. Trotz der Bezeichnung „Großrechner“ dauerte es oftmals ganze Nächte, bis das Programm seine Ergebnisse auf Endlospaper ausgedruckt hatte, oftmals in Form von Zahlenkolonnen, die in mühsamer Handarbeit ausgewertet werden mussten. So sah die digitale Steinzeit aus. Der erste, noch kleine Schritt in die digitale Moderne waren Terminals für den Dialog mit dem Computer. Der Funktion nach waren diese aber eigentlich nur bessere Schreibmaschinen. Wirklich interessant wurde es erst mit dem Aufkommen von preiswerten „Personal-Computern“ und Workstations in den 1980er Jahren. Plötzlich konnte jeder Arbeitsplatz mit eigenen Rechnerkapazitäten ausgestattet werden, was das Berufsleben in Büros, Labors und Forschungseinrichtungen grundlegend veränderte und erstmals die disruptive Wirkung der neu aufgekommenen Technologie erahnen ließ. Die größte Beschleunigung der Digitalisierung ergab sich durch den großflächigen Ausbau des Internets in den 1990er Jahren sowie dem Aufkommen intelligenter Mobilgeräte seit der Jahrtausendwende. Nichts hat die Gesellschaft seither so radikal verändert wie die fortschreitende Digitalisierung.

Digitalisierung hat inzwischen praktisch alle Lebensbereiche durchdrungen. Dank Digitalisierung wurden viele Tätigkeiten erleichtert und vereinfacht, manche Dinge wie etwa datengetriebene Entscheidungsprozesse wurden überhaupt erst möglich. Die kontinuierliche Beschaffung, Evaluation und Verarbeitung von Daten haben einen zentralen Stellenwert bekommen und dazu beigetragen, dass mit der Digitalisierung per Saldo neue Arbeitsplätze geschaffen wurden, anders als ursprünglich befürchtet.

Demgegenüber hat die Digitalisierung eine höhere hardware- und softwareseitige und für wenige Personen überschaubare Komplexität der Lösungsansätze zur Folge. Damit sind ernst zu nehmende Herausforderungen entstanden, erkennbar etwa in den notorischen Kosten- und Zeitüberschreitungen von Digitalisierungsprojekten sowie die kaum bestreitbare Tatsache, dass es so gut wie keine fehlerfreien Softwarepakete gibt. Regelmäßige Updates helfen dabei nur wenig, weil sie neben der Beseitigung von Bugs und der Berücksichtigung neuer Funktionen immer wieder neue Fehlerquellen schaffen. Vor allem aber ist Deutschland bei der Digitalisierung international ins Hintertreffen geraten, was sich unter anderem während der Corona-Pandemie schmerzhaft bemerkbar gemacht hat.

Die Energiewirtschaft ist dem Digitalisierungstrend in besonderer Weise ausgesetzt. Mit der Strommarktliberalisierung, dem Umstieg von Großkraftwerken auf dezentrale Erzeugung, der damit deutlich anspruchsvolleren Aufgabe, kontinuierlich das Gleichgewicht im Elektrizitätsnetz sicherzustellen, dem notwendigen Aufbau intelligenter Energiespeicher, steuerbarer Verbraucher und Ladeinfrastrukturen für die

Elektromobilität ist sie sogar in besonderer Weise auf die Digitalisierung ihrer Prozesse angewiesen. War es früher vor allem die günstige Beschaffung fossiler Energieträger, so werden künftig die Kapazitäten und Fähigkeiten beim Einsatz dieser Technologie für die Branche zum wesentlichen Erfolgstreiber gehören. Doch gerade in dieser teilweise immer noch traditionell denkenden Branche wird der Veränderungszwang noch relativ zaghaft angegangen. Es erscheint an der Zeit, hier für mehr Dynamik zu sorgen, trotz der damit verbundenen besonderen Herausforderungen.

Die Entwicklung hin zu einer digitalisierten Energiewirtschaft befindet sich noch im Anfangsstadium. Zu den Gründen gehören das Fehlen von Fachleuten und Erfahrungen, ein mit Digitalisierungsprojekten überfordertes Projektmanagement und vieles mehr. Insbesondere fehlt es aber an der Einbettung der Digitalisierungsthematik in den gesellschaftlichen Diskurs. Öffentliche Debatten sind dringend notwendig, und zwar nicht nur unter den einschlägigen Fachleuten. Um die Digitalisierung zum Erfolg zu führen, muss – ähnlich wie die Energiewende – dies als eine gesamtgesellschaftliche Aufgabe angesehen werden. Sie geht alle an, alle werden in der einen oder anderen Form involviert sein, alle müssen mit den IT-Instrumenten umgehen können und alle sollten deshalb die Gelegenheit haben, sich in die Diskussionen einzubringen. In den öffentlichen Debatten sollte es vor allem um die Architektur von Digitalisierungslösungen inkl. Datenschutz und IT-Sicherheit gehen, und zwar unter dem Aspekt qualitativ hochstehender, nützlicher und anwendungsfreundlicher IT-Hilfsmittel und Lösungen. Um die öffentliche Debatte zu fördern, sind die Kapitel dieses Kompendiums in einer (hoffentlich) allgemeinverständlichen Sprache geschrieben. Das Werk hätte aus unserer Sicht seine Ziele erreicht, wenn es den gesellschaftlichen Diskurs befeuert und damit zu einer humaneren IT-Welt beitragen kann.

Prof. a. D. Dr. Georg Erdmann

:// DIGITALISIERUNG IN DER ENERGIE-WIRTSCHAFT:

[DEFINITION, DATENZUGANG UND MEHRWERTE]

ABSTRACT

Dieser Beitrag erörtert systematisch den Digitalisierungsbegriff und stellt den Bezug zu den energiepolitischen Zielen her. Hieraus ergibt sich, dass Sicherheitsanforderungen ein wichtiger Aspekt der Digitalisierung sind: die Cybersicherheit als eine Voraussetzung für einen zuverlässigen Stromnetzbetrieb als auch der potenzielle Beitrag digitaler Technologien zur Systembilanzierung. Wir identifizieren vier Kernfelder der Digitalisierung: Vernetzung, Sicherheit, Daten und Mehrwert.

Eine wichtige Voraussetzung für digitale Innovationen im Energiebereich ist der Zugang zu Daten. Die betrachteten energierelevanten Daten gehen über die Messdaten und Energiesystemdaten hinaus und beziehen ein breites Spektrum weiterer, nicht energiespezifischer Daten mit ein. Über öffentlich zugängliche Energiedaten hinaus sind hoch aufgelöste Messdaten sowie (weitere) personenbezogene Daten für viele innovative Produkte unerlässlich. Für diese Datenkategorien spielt Einwilligung der Kunden bzw. der Einzelpersonen eine tragende Rolle, da diese von jeder Einzelperson separat eingeholt werden muss. Dadurch rückt die (digitale) Kundenkommunikation in den Fokus. Für die Konzeptionierung von den in der Digitalisierungsdiskussion oft erwähnten, datenbasierten Mehrwerten bzw. Mehrwertdiensten, sollten aus unternehmerischer Perspektive nicht nur der durch den Dateneinsatz generierte Mehrwert, sondern gleichermaßen der Datenzugang (hier die Einwilligung der Datenweitergabe) und damit die Kundenschnittstelle betrachtet werden. Die hier zusammengefassten vorhandenen empirischen Untersuchungen zeigen, dass Menschen sehr wohl wissen, dass Unternehmen ihre Daten auswerten und weiterverwenden, und durchaus bereit sind ihre Daten Dritten zur Verfügung zu stellen. Dabei stehen vor allem Transparenz, Datenhoheit und Mehrwerte im Vordergrund. Im Hinblick auf die einzelnen Einflussfaktoren der Datenweitergabe wird ein weiterer Untersuchungsbedarf skizziert.

Unternehmensseitig zeigt sich die Kommunikation und die Weitergabe der Mehrwerte als große Herausforderung. Dabei ist es aufgrund der möglichen Diskrepanz zwischen dem Betroffenenkreis für die Datenbeschaffung und dem Kundenkreis, der von der entwickelten datenbasierten Lösung profitiert, sinnvoll beide externe Schnittstellen separat zu betrachten und dabei nach möglichen Synergien zu suchen. Eine weitere Herausforderung ist der Zeitpunkt der Datenerhebung bzw. -beschaffung. Erzielbare Mehrwerte sind aufgrund mehrfacher möglicher Verwendung der Datensätze für verschiedene Zwecke schwer vorhersehbar; der Mehrwert selbst steigt allerdings bei der Zusammenführung verschiedener Datenquellen.

AUTOREN

Andreas Corusa
Technische Universität Berlin, Fachgebiet Energiesysteme

Elena Timofeeva
Technische Universität Berlin, Fachgebiet Energiesysteme

Johannes Predel
Technische Universität Berlin, Fachgebiet Energiesysteme / nymoen Strategieberatung

Abkürzungsverzeichnis	
BDEW	Bundesverband der Energie- und Wasserwirtschaft
BDSG	Bundesdatenschutzgesetz
BMBF	Bundesministerium für Bildung und Forschung
BMWi	Bundesministerium für Wirtschaft und Energie
BNetzA	Bundesnetzagentur
DSGVO	Datenschutz-Grundverordnung
EE	Erneuerbare Energien
ENTSO-E	European Network of Transmission System Operators for Electricity
EnWG	Energiewirtschaftsgesetz, Gesetz über die Elektrizitäts- und Gasversorgung
EOSC	European Open Science Cloud
EU-ElтRL	EU- Elektrizitätsbinnenmarktrichtlinie
EVU	Energieversorgungsunternehmen
FLM	Freileitungsmonitoring
GIS	Geographisches Informationssystem
IEA	Internationale Energieagentur
IRENA	International Renewable Energy Agency
IT	Informationstechnik
MsbG	Messstellenbetriebsgesetz
NFCI	Nationale Forschungsdateninfrastruktur
SMARD	Strommarktdaten
TSE	Temperature-Stress-Exhaustion
VGI	Volunteered Geographical Information

EINLEITUNG 10
- **1.1 Aktuelle Digitalisierungstrends in der Energiewirtschaft** 10
- **1.2 Aufbau und Methodik** 12

DIGITALISIERUNG UND DEFINITION 13
- **2.1. Vorhandene Digitalisierungsstudien** 13
- **2.2 Englische Definitionen** 14
  - 2.2.1 Digitization 14
  - 2.2.2 Digitalization 15
  - 2.2.3 Digital Transformation 16
- **2.3 Deutsche Definitionen** 17
  - 2.3.1 Digitalisierung 17
  - 2.3.2 Digitale Transformation 18
- **2.4 Anwendung auf den Begriff der Digitalisierung in der Energiewirtschaft** 21

DATEN 25
- **3.1 Definition energierelevanter Daten** 25
- **3.2 Öffentlich verfügbare Daten** 26
- **3.3 Typologie energierelevanter Daten** 28
  - 3.3.1 Energiesystemdaten und Kunden- bzw. Erzeugerdaten 29
  - 3.3.2 Erhebungstechnologien 29
  - 3.3.3 Personenbezogene und nicht personenbezogene Daten 31
  - 3.3.4 Vorgaben für einzelne Datenkategorien 31
  - 3.3.4.1 Vorgaben zum Datenschutz 31
  - 3.3.4.2 Daten aus Messeinrichtungen 33
  - 3.3.4.3 Entflechtungsvorgaben für Daten aus dem Netzbetrieb 34

DATENBASIERTE MEHRWERTE 35
- **4.1 Datenbeschaffung aus Kunden- und Unternehmensperspektive** 35
- **4.2 Vergütungsformen für die Daten** 36
- **4.3 Einflussfaktoren für die Bereitschaft zur Datenweitergabe** 38
- **4.4 Datenbasierte Mehrwerte aus Unternehmensperspektive** 41

FAZIT UND DISKUSSION 43

Literaturverzeichnis 44

:// 1. EINLEITUNG

1.1 Aktuelle Digitalisierungstrends in der Energiewirtschaft

Die Digitalisierung findet heute in nahezu allen Bereichen des Alltags statt und ist ein sehr umfängliches und sehr abstraktes Thema. Von der Art und Weise, wie wir arbeiten, bis hin zur alltäglichen Kommunikation und unserem Konsumverhalten, überall finden wir Ansätze dieser Entwicklung. Dementsprechend definiert die Bundesregierung in ihrem Legislaturbericht "Digitale Agenda" eine Vielzahl an Themen, wie beispielsweise die digitale Ökonomie oder die digitale Gesellschaft, als Pfeiler der gesamtheitlichen digitalen Transformation (Bundesregierung 2017).

Die globalen Trends der letzten Jahre sind klar erkennbar: Digitale Unternehmen sind in vielen Bereichen heute schon Marktführer und bauen ihren Einfluss weiter aus. Sieben (!) der zehn wertvollsten börsennotierten Unternehmen der Welt kommen inzwischen aus der digitalen Wirtschaft: Microsoft, Apple, Amazon, Alphabet (Google), Facebook, Alibaba und Tencent (Forbes 2020). Diese Art von digitalen Unternehmen baut ihre Geschäftsmodelle vor allem auf plattformökonomischen Grundsätzen auf, die stark durch die Erhebung, Auswertung und den Vertrieb von Daten geprägt sind. Auch in der Energiewirtschaft hat man erkannt, dass Digitalisierung ein wichtiges Thema ist, das Unternehmen in ihre Unternehmensstrategie und –kultur einbringen müssen. Denn genauso wie das Energiesystem durch den steilen Ausbau der Erneuerbaren Energien einer ständigen Veränderung ausgesetzt ist, so verändern sich auch Unternehmen in der Energiewirtschaft. Giehl et al. 2020 zeigen, dass es allein in der deutschen Energiewirtschaft mehr als 600 identifizierte Geschäftsmodelle gibt und dass digitale Anforderungen auch Geschäftsprozesse traditioneller Energieversorgungsunternehmen, wie zum Beispiel Stadtwerke, durchdringen.[1] Dabei verändert sich der Energiesektor von einer linear darstellbaren, energiewirtschaftlichen Wertschöpfungskette (Exploration, Erzeugung, Handel, Verteilung und Vertrieb) zu einem energiewirtschaftlichen Wertschöpfungsnetzwerk, in dem die Interaktionen von Dienstleistungen, Daten, Produkten und Energie oft miteinander in multidirektionaler Verbindung stehen (ebd.).

Für wertschöpfungskettenübergreifende Kommunikation und Datenaustausch in der Energiewirtschaft spielt ein breiter Einsatz intelligenter Messsysteme eine besonders wichtige Rolle. Für den geplanten Smart-Meter-Rollout rücken aktuell bei der Zertifizierung der ersten Anbieter von Smart-Meter-Gateway neben der Sicherheitsperspektive auch Anforderungen an die Interoperabilität in den Vordergrund.[2] Mit dem weitflächigen Einbau intelligenter Mess- und Steuerungseinrichtungen wird es erstmals möglich sein, die verbrauchsseitigen Lasten granular abzubilden und dadurch besser zu verstehen, wo weitere Optimierungs-, Flexibilisierungs- und Einsparpotenziale liegen könnten. Zugleich erleichtern Smart Meter die System- und Marktintegration dezentraler Erzeugungsanlagen aus Erneuerbaren Energien. Mehr als 1,6 Millionen (BNetzA 2021), meist sehr kleine Erzeugungsanlagen, sind heute bereits an das deutsche

1 Siehe *→ zweiter Teil* dieses Kompendiums zur Digitalisierung interner Geschäftsprozesse bei EVU.

2 Oberverwaltungsgericht stoppt vorläufig Einbauverpflichtung für intelligente Messsysteme (Stromzähler), Pressemitteilung vom 05.03.2021, abrufbar unter: https://www.ovg.nrw.de/behoerde/presse/pressemitteilungen/18_210305/index.php

Stromnetz angeschlossen. Zur Veranschaulichung: Dividiert man diese Anzahl durch die Gesamtfläche der Bunderepublik, so erhält man vier bis fünf Anlagen pro Quadratkilometer.

Dabei führt die Digitalisierung, vor allem durch Verschaltung und Vernetzung von Erzeugungs- und Verbraucheranlagen, zu einer immer größer werdenden Komplexität. Durch die Verschaltung dieser wird auch die Koordinierung und Orchestrierung des Energiesystems, durch zum Beispiel erhöhte Vernetzungs- und Kommunikationsbedarfe zwischen einer stetig wachsenden Anzahl an installierten Hard- und Software, immer schwieriger. Der vielfältige Einsatz dieser Technologien wird dabei als einer der großen Treiber des Digitalisierungsprozesses angesehen und durch die Bezeichnung „Ermöglicher“ (engl. Enabler) zum Ausdruck gebracht (Schreckling und Steiger 2017).

Die Digitalisierung basiert dabei nicht nur auf Kommunikations-, sondern auch auf Informationstechnologien (IT). Dies rückt (maschinenlesbare) Daten und die daraus zu generierenden Mehrwerte in den Fokus. Der Mathematiker und Datenexperte Clive Robert Humby hat bereits im Jahr 2006 den berühmten Satz “Daten sind das neue Öl” geprägt (Arthur 2013); allerdings sind die Daten nur dann wirklich wertvoll, wenn sie wie Öl raffiniert werden, um eine wertvollere Einheit zu schaffen. Daten müssen also richtig aufgeschlüsselt und analysiert werden, damit sie einen Wert haben (Palmer 2006). Heute sammeln viele Marktakteure riesige Datenmengen, die in technischen Anlagen in Form von Sensorik sowie beim täglichen unternehmensübergreifenden Datenaustausch. Folgendes Beispiel veranschaulicht dies: Ein mittelgroßes deutsches Energieversorgungsunternehmen erzeugte bereits im Jahr 2015 ca. 1,6 Terabyte Datenvolumen pro Tag. Ein handelsüblicher Stromzähler alleine generiert dabei jährlich ca. 1,75 Milliarden Datenpunkte (Bitcom 2013). Dass Mehrwerte durch Daten geschaffen werden können, veranschaulicht das Beispiel eines virtuellen Kraftwerks (Giehl et al. 2020; Lehmbruck et al. 2020). Diese relativ neue Herangehensweise zeigt, dass nicht nur die Verschaltung neuer Technologien und Infrastrukturen zur Verarbeitung von Daten erforderlich sind, sondern auch die Art und Weise, wie große Datenmengen verwaltet und daraus Werte generiert werden können. Konkret werden hier viele oft verschiedenartige Erzeugungsanlagen mit entsprechender Hard- und Software ausgestattet und „intelligent“ gesteuert. Durch die Steuerung bzw. preisorientierte Fahrweise werden nicht nur die Dauer des Anlagenbetriebs erhöht, sondern auch höhere Erlöse durch optimierte Direktvermarktung des erzeugten Stroms erzielt. Eine Win-Win-Situation, sowohl für den Anlagenbesitzer als auch für den virtuellen Betreiber. Bei derartigem weitreichendem Einsatz von Daten spricht man entweder von der Anwendung einer Datenwertschöpfungskette (Data Value Chain) bzw., beim Einsatz von sehr großen Datenmengen, von dem Big Data Wertschöpfungskette (Big Data Value Chain) (Faroukhi et al. 2020). Dabei wird die Verarbeitung und Bereitstellung sehr großer Datensätze mit der weiteren Verschaltung von Maschinen, zum Beispiel mit der Einführung von intelligenten Messsystemen oder Internet-of-Things-Geräten, künftig zu weitaus größeren Herausforderungen führen (BDEW 2015). Vor diesem Hintergrund hat die von der Bundesregierung aktuell ausgearbeitete Datenstrategie das Ziel die Datenbereitstellung und den Datenzugang auf infrastruktureller Ebene zu verbessern und eine sichere, vertrauenswürdige und nachhaltige Dateninfrastruktur als Grundlage für Innovation und Wertschöpfung aufzubauen (Bundesregierung 2021).

Mit der stetigen Weiterentwicklung der IT-Strukturen, dem damit verbundenen erhöhten Kommunikationsbedarf sowie einer immer größer werdenden Datengenerierung kann davon ausgegangen werden, dass es fortwährend wichtiger werden wird, wie Daten verwaltet werden, wer Zugang dazu bekommt, zu welchem Zweck diese eingesetzt werden und welche Mehrwerte daraus entstehen. Die Digitalisierung und somit auch die Diskussion um Daten rückt spürbar in den Vordergrund.

1.2 Aufbau und Methodik

Um die Rahmenbedingungen für digitale Innovationen in der Energiewirtschaft abzustecken und Fokusthemen für deren Förderung aufzuzeigen, bietet der erste Abschnitt dieses Beitrags einen Überblick über den Begriff der Digitalisierung. Die bestehenden Digitalisierungsstudien, die einleitend vorgestellt werden, vermitteln den Eindruck einer ausgeprägten Diversität bei der Auslegung des Digitalisierungsbegriffs. Vor diesem Hintergrund untersuchen wir die Begrifflichkeit im ersten Schritt allgemein und branchenunabhängig, um im zweiten Schritt eine auf die Energiewirtschaft zugeschnittene Definition abzuleiten.

In der entwickelten Digitalisierungsdefinition in → *Kapitel 2.4* „Anwendung auf den Begriff der Digitalisierung in der Energiewirtschaft“ werden vier Kernaspekte identifiziert: Vernetzung, Sicherheit, Daten und Mehrwerte. In diesem Beitrag behandeln wir anschließend zwei dieser Kernaspekte: Daten und Mehrwerte.

In → *Kapitel 3* „Daten“ geht es vor allem um die Abgrenzung energierelevanter Daten und deren technisch und regulatorisch bedingte Heterogenität. Dabei arbeiten wir vor allem die Herausforderungen für den Zugang zu Daten heraus.

In → *Kapitel 4* „Datenbasierte Mehrwerte“ fokussieren wir uns auf eine wichtige Voraussetzung für digitale Innovationen, die aus der vorgehenden Besprechung in Kapitel 3 folgt: Aufgrund der dargestellten rechtlichen Rahmenbedingungen spielt die Bereitschaft von Kunden ihre Daten weiterzugegeben eine zentrale Rolle für den Zugang zu relevanten Daten. Gleichzeitig sollte die Rentabilität des aus den Daten abgeleiteten Handlungsvorgehens berücksichtigt werden. Angesichts dargestellter Herausforderungen, denen energiewirtschaftliche Unternehmen auf dem Weg der datenbasierten Mehrwertentwicklung begegnen, wird weiterer Forschungsbedarf aufgezeigt.

Methodisch stützt sich dieser Beitrag auf eine integrative Literaturübersicht (Snyder 2019). Es wurden Erkenntnisse aus verschiedenen Fachgebieten explorativ recherchiert und mit Blick auf Zusammenhänge zwischen den jeweiligen Aspekten bzw. Teilgebieten untersucht. Analysiert wurde insbesondere die Literatur zum allgemeinen Digitalisierungsbegriff, Ansätze aus der Datenwissenschaft zum Konzept von Big Data und zur branchenspezifischen Verwendung bestimmter Datentypen in der Datenanalyse, zu rechtlichen Vorgaben zum Datenschutz, Regelungen zum Datenmanagement in der Energiewirtschaft, Studien zu Kundeneinstellungen gegenüber Datenweitergabe sowie vorhandene Ausarbeitungen zur Wertschöpfung aus Daten. Die zusammengefassten und synthetisierten Ergebnisse wurden konzeptualisiert. Dabei wurden neue Forschungsbedarfe aufgezeigt.

:// 2. DIGITALISIERUNG UND DEFINITION

2.1. Vorhandene Digitalisierungsstudien

Die Digitalisierung führt durch riesige Datenmengen und zunehmende Vernetzung zu einer gesteigerten Komplexität in der Energiewirtschaft. Aus der vorhandenen Literatur ist erkennbar, dass Digitalisierungsprozesse in der Branche auf unterschiedlichen Ebenen und nach verschiedenen Ansätzen betrachtet werden. Dies wird insbesondere anhand bisheriger Studien deutlich, die sich mit einer Bestandsaufnahme und Bewertung des Entwicklungsstandes der Digitalisierung in der Energiewirtschaft beschäftigen. Nachfolgend werden einige dieser Studien beispielhaft vorgestellt mit Blick auf deren thematischen Rahmen und deren Verständnis des Begriffs “Digitalisierung”.

Das jährlich im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) durch Ernst & Young erstellte Digitalisierungsbarometer fokussiert sich auf intelligente Messeinrichtungen für Elektrizität. Schlüsselfaktoren und dazugehörige Indikatoren zur Bewertung des Digitalisierungsgrades der Energiewende bilden den Technikstand (Technologieangebot, Gerätezertifizierung, Verfügbarkeit von Geräten, Standardisierung usw.), den Rollout-Fortschritt und die kundenseitige Akzeptanz intelligenter Messeinrichtungen ab. Abgedeckt sind ebenfalls die Smart-Meter-Gateways und einschlägige Telekommunikationstechnologien und -infrastrukturen (EY 2019).

Die gemeinsame Studie von A.T. Kearney und IMP3rove Academy im Auftrag des Bundesverbandes der Energie- und Wasserwirtschaft (BDEW) ermittelt durch eine Umfrage den aktuellen Stand zu Digitalisierungsstrategien bei Energieversorgungsunternehmen (EVU) und untersucht den Inhalt solcher Strategien. Beleuchtet werden beispielsweise die angebotenen digitalen Produkte, Schwerpunktthemen durchgeführter Datenanalysen sowie die Vorgehensweise bei dem notwendigen Unternehmenskulturwandel im Sinne einer digitalen Transformation. Anschließend wird der Einsatz unterschiedlicher Instrumente der Digitalisierung wie digitale Kundenschnittstellen und Prozessdigitalisierung eingegangen (A.T.Kearney, BDEW, IMP3rove 2019).

Mehrere Studien zum Digitalisierungsstand finden ihren Ausgangspunkt in der Vorstellung relevanter Technologien. Die durch die International Renewable Energy Agency (IRENA) erarbeitete Innovationslandkarte für eine EE[3]-basierte Zukunft (IRENA 2019) identifiziert und untersucht Lösungen für die Systemintegration Erneuerbarer Energien. Digitale Technologien werden im Bericht neben weiteren Technologien besprochen, die eine EE-basierte Zukunft ermöglichen. Diese werden wiederum als Teil des Oberbegriffs Innovationen neben neuen Geschäftsmodellen, einem neuen Marktdesign und neuen Ansätzen für den Systembetrieb betrachtet. Der Bericht beschreibt „digitale Technologien“ durch großflächiges Sammeln und Analyse von digitalen Daten und zwei zentrale Anwendungsziele: die Verbesserung der Steuerbarkeit von Erzeugungsanlagen und Lasten sowie die Verbesserung der Flexibilität auf beiden Seiten. Im Vordergrund

3 Steht für Erneuerbare Energien.

stehen dabei Internet of Things, künstliche Intelligenz, Big Data und Blockchain. Der Bericht bietet einen Überblick, geht jedoch nicht ins Detail.
Der durch die Internationale Energieagentur (IEA) veröffentlichte interaktive Wegweiser zu sauberen Energietechnologien „ETP Clean Energy Technology Guide“ stellt eine Datenbank mit über 400 Technologien dar, die nach dem Sektor (Energieumwandlung, Verkehr, Industrie, Gebäude und CO_2-Infrastruktur) und der Stufe in der Wertschöpfungskette unterschieden und nach weiteren Kriterien sortiert werden können. Unter das Kernthema Digitalisierung fallen im Energieumwandlungs- bzw. Strombereich lediglich zwei Technologien, wobei eine davon – Freileitungen mit Spannung ab 800 kV – in Deutschland nicht relevant ist. Die zweite Technologie, transaktionsbasierte Energieversorgung (‘transactive energy’) ist eine der wichtigsten neuen Technologien. Die vorgenannten Technologien stellen offensichtlich nur ein paar Beispiele von einsatzfähigen digitalen Technologien im Energiebereich dar. In dieser Hinsicht ist der Technologiewegweiser unvollständig.

Eine systematische Zusammenschau digitaler Technologien für die Energiewirtschaft wurde 2019 von Weigel und Fischedick durchgeführt. Relevante Technologien wurden aufgelistet, in Gruppen und Untergruppen aufgeteilt und im Hinblick auf deren Vorteile und dahingehend untersucht, welche Stakeholder davon profitieren. Die sechs Vorteile bzw. Anwendungsziele sind: Systemintegration, Umweltschutz, Energieeinsparung, Umsatzsteigerung, Kostensenkung und Kundenorientierung. Dementsprechend sind digitale Technologien nach drei Verwendungszwecken aufgeteilt: Systembilanzierung, Prozessoptimierung und Kundenorientierung. (Weigel und Fischedick 2019).

Bereits aus dieser beispielhaften Übersicht wird die Vielfältigkeit der Diskurse deutlich. Als Grundlage für die weitere Besprechung in diesem und nachfolgenden Teilen dieses Kompendiums untersuchen wir daher zunächst, wie der Begriff "Digitalisierung” in der Literatur verstanden wird. Auf Basis der Sekundärrecherche schlagen wir eine Definition bzw. eine Definitionserweiterung von Digitalisierung in der Energiewirtschaft vor.

Ob es um die Nutzung digitaler Technologien, die Digitalisierung eines Prozesses oder um die digitale Transformation im Allgemeinen geht – letztendlich bleibt bei vielen Diskussionen immer noch die Frage: Was genau ist Digitalisierung? Wo fängt Digitalisierung an und wo hört sie auf?

Zu Beginn dieses Kapitels wird daher eine Definition der Digitalisierung in Bezug auf die Energiewirtschaft aufgebaut, um einen einheitlichen Begriff für den weiteren Verlauf des Beitrags festzulegen. Hierzu werden unterschiedliche Definitionen miteinander verglichen und sprachliche Unterschiede hervorgehoben, da sich zwischen dem englischen und deutschen Sprachgebrauch ein grundlegender Unterschied eingestellt hat. Auch wenn für die Lesenden der gleiche Wortlaut nur in einer anderen Sprache verwendet wird, so bestehen doch entscheidende Unterschiede in den zugrunde liegenden Definitionen.

2.2 Englische Definitionen

2.2.1 Digitization

Die Umstellung von analog auf digital begann mit dem von Gottfried Wilhelm Leibniz im 17. Jahrhundert entwickelten System, in dem er die Darstellung von Informationen mittels zweier Zustände beschrieb. Das binäre System war geboren. Ein binäres System muss nicht zwingendermaßen auf Ziffern beruhen, da jeder binäre Zustand als binäres System gewertet werden kann, wie beispielsweise Licht an/aus oder Ton/kein Ton (Vogelsang 2010).

Die Weitergabe von Informationen mittels binären Systems bildete auch die Grundlage des Morse Alphabets. Hierbei wird ein binäres Signal zusätzlich mit einer Zeitkomponente verbunden, sodass Buchstaben, Ziffern und andere Zeichen übertragen werden können.

Hieraus entwickelte sich später das Telegraphennetz, welches zu Beginn des 20. Jahrhunderts die gesamte Welt umspannte und somit zum ersten Mal einen weltweiten Informationsaustausch ermöglichte.

Der erste elektrische Computer entstand bereits 1946 und basierte auch auf dem System von Leibnitz, doch erst die Fortschritte auf dem Gebiet der Mikroprozessortechnik brachten die Verbreitung von Computern, da nun statt Vakuumröhren Mikroprozessoren, gelötet auf Platinen, binäre Signale ermöglichten (Vogelsang 2010).

Im Englischen wird die Umstellung von Informationen von analog zu digital als Digitization bezeichnet (Brennen und Kreiss 2016). Diese Bezeichnung ist auch auf das binäre System zurückzuführen. Digit ist die lateinische Bedeutung von Ziffer und damit eine Anspielung auf die Darstellung des binären Systems mittels der Ziffern 0 und 1.

Laut Gartner (o. J.b) bezieht sich dies nicht nur auf die Informationen, sondern auch auf den Prozess zu Gewinnung der Informationen, ohne dass hierfür der eigentliche Prozess geändert wird. Beispielhaft kann hier das Schreiben auf einem Computer im Vergleich zu einer Schreibmaschine gesehen werden.
Der Prozess des eigentlichen Tippens verändert sich hierdurch nicht, jedoch liegen die Informationen in digitaler statt analoger Form vor. Der Prozess wurde also „digitized“.

Mit diesen Anpassungen und vor allem mit der Entwicklung des Computers ging auch die Entwicklung des Begriffs Digitalization einher.

2.2.2 Digitalization

Erstmals benutzt wurde der Begriff Digitalization von Wachal (1971) im Jahre 1971 . In seinem Essay "Humanities and Computers: A personal view" beschreibt Wachal, wie Computer gestützte Forschung aussehen könnte. Hier sind bereits erste Abgrenzungen vom Begriff Digitization zu erkennen. Stand vorher eine rein technische Betrachtung im Vordergrund, beschäftigt sich Digitalization in dem Aufsatz von Wachal zum ersten Mal mit der tatsächlichen Anwendung von digitaler Technologie, d.h. mit der Nutzung von computerbasierter Forschung. Auch wenn ein Anwendungsfall im Vordergrund seines Essays steht, so leitet er doch den Begriff mit den Worten "the digitalization of society" (ebd.), S. 30 ein, wodurch die hohe Bedeutung von digitaler Technologie für die Gesellschaft sehr klar hervorgehoben wird.

Brennen und Kreiss (2016) schließen daher in ihren Betrachtungsrahmen die gesamte Gesellschaft für eine Definition von Digitalization ein. In ihrer Metastudie attestieren sie, dass der Begriff häufig mit den Auswirkungen auf das soziale Leben und die Gesellschaft definiert wird. Sie stellen dar, dass Digitalization vor allem die Zusammenführung (convergence) zuvor unterschiedlicher Bereiche unterstützt, sodass dadurch das gesellschaftliche Leben verändert wird.

Auch Vogelsang nutzt den Ansatz der Verbreitung bzw. Vernetzung im gesellschaftlichen Leben und zwischen der Gesellschaft und digitalen Technologien und kombiniert ihn mit der zugrundeliegenden Infrastruktur, indem er schreibt (Vogelsang 2010):

> :// **Digitalization refers to the spread of digital goods and IT services over networks.** //

Weiterhin stellt Vogelsang unterschiedliche Konzepte vor, mit denen diese Verbreitung gemessen werden kann, beispielsweise durch den Digital Opportunity Index (DOI)[4] oder dem Digital Access Index (DAI)[5].

4 Der DOI basiert auf insgesamt 11 Indikatoren, eingeteilt in die Cluster Infrastruktur, Möglichkeit (opportunity) und Anwendung (utilization). Mithilfe des Indikators soll der Zugang zu digitaler Technologie eines Landes bewertet werden (ITU 2010).

5 Der DAI misst, inwiefern Individuen eines bestimmten Landes Zugang zu digitalen Technologien haben.

Gleichzeitig stellt Vogelsang jedoch dar, dass die digitale Technologie, bzw. Informationstechnologie (information technology), heutzutage als

> :// general purpose technology //

angesehen werden kann (Vogelsang 2010, S. 9). Dies stellt eine eher wirtschaftliche Betrachtung in den Vordergrund, der eine weitreichende Verbreitung zugrunde liegt. Es bedeutet unter anderem, dass digitale Technologien genutzt werden können, um neue Produkte und Dienstleistungen anzubieten, die zur Steigerung der Produktivität und zu positiven Übertragungseffekten (spillover effects) führen, zum Beispiel durch den beschleunigten Austausch von Informationen.

Aus (ebd.) (2010) und Brennen und Kreiss (2016) leiten wir ab, dass es grundsätzlich zwei Ansatzpunkte für eine Definition der Digitalisierung gibt. Bei einem stehen die Anwendungen der digitalen Technologie im Vordergrund, bei dem anderen die tatsächliche Ausbreitung oder Verteilungsdichte, auf denen der Begriff Digitalization beruht.

Vogelsang folgend kann jedoch argumentiert werden, dass der Ansatz der Verbreitung für die Definition von Digitalization in den Hintergrund rückt, sobald eine ausreichende Verbreitung vorliegt und ein Fokus auf den Anwendungscharakter gelegt werden sollte. Vielmehr steht nun die Anwendung im Vordergrund. Dies wird zusätzlich häufig in der Literatur mit positiven (wirtschaftlichen) Auswirkungen kombiniert. Gemäß der Definition nach Gartner (o. J.a) bedeutet Digitalization der

> :// use of digital technologies to change a business model and provide new revenue and value-producing opportunities [; it is the process of moving to a digital business]. //

Wie auch bei Vogelsangs Darstellung als "general purpose technology" scheint sich die Digitalization nur mit positiven wirtschaftlichen Auswirkungen bei der Nutzung erklären zu lassen, was bei der ersten Definition von Wachal noch nicht im Vordergrund stand. Überhaupt ist es schwierig, die Vorteile einer Computer-gestützten Wissenschaft bei Wachal herauszulesen. Möglich wäre hier eine etwaige Zeitersparnis, die durchaus auch wirtschaftlich definiert werden könnte.

Der Definition von Gartner (siehe → *Tabelle 1*) folgend, können weitere Ansätze gefunden werden, welche im Kern jedoch die gleiche Richtung einschlagen und der Anwendung von digitaler Technologie folgen.

Da Digitalization vor allem mit positiven wirtschaftlichen Effekten definiert wird, sollte neben der wissenschaftlichen Betrachtung auch eine Perspektive aus der Wirtschaft miteingeschlossen werden.

I-Scoop (o. J.) etwa definiert Digitalization als

> :// use of digital technologies and of data (digitized and natively digital) in order to create revenue, improve business, replace/transform business processes (not simply digitizing them) and create an environment for digital business, whereby digital information is at the core. //

Wie bei Gartner wird auch bei I-Scoop schon angedeutet, dass Digitalisierung ein Fortschreiten des Geschäftsmodells bedeutet, hin zum Ziel eines digitalen Geschäfts (Gartner o. J.a) bzw. der Schaffung der dafür notwendigen Umgebung.

2.2.3 Digital Transformation

Das Ziel eines „digitalen Geschäfts“ und die Schaffung einer dafür notwendigen Umgebung als der

Weg dahin werden von manchen Autoren auch als digitale Transformation definiert. Bei I-Scoop bleibend sind hierbei nicht nur einzelne Prozesse gemeint, sondern die Gesamtheit aller Prozesse in einem Unternehmen, und zwar unabhängig davon, ob sie dem eigentlichen digitalen Geschäft angeschlossen sind (I-Scoop o. J.). Ob dieser Wandel in der Realität stattfindet oder ob eine Schwelle existiert, ab der man von einer abgeschlossenen Digital Transformation sprechen kann, ist in der Literatur nicht geklärt.

Vielmehr wird der Wandel als bewusste und fortschreitende digitale Evolution (deliberate and ongoing digital evolution (Mazzone 2014)) dargestellt. Diese ist bei der Definition von Mazzone nicht nur auf bestimmte Prozesse reduziert, sondern ändert das grundlegende Handeln und Denken innerhalb eines Unternehmens. Somit kann ein tiefgreifender Eingriff in die Arbeitswelt durch die Digital Transformation beschrieben werden, die ihren Ursprung nicht unbedingt in einer ursprünglich digitalen Geschäftsidee hat.

Eine exakte Abgrenzung zwischen digital transformiert und nicht-transformiert erscheint kaum möglich. Auch wenn Digitalization dazu dient, diese Veränderung (transformation) einzuleiten, ist nicht definiert, ob dies das eigentliche Ziel der Digitalization sein sollte.

Insgesamt kann festgehalten werden, dass mit der Entwicklung von digitalen Technologien und ihrer immer größeren Verbreitung, auch eine Entwicklung der Definition zu erkennen ist. Gleichzeitig ist die Annahme einer historischen Abfolge von Digitization, Digitalization und Digital Transformation falsch. Zwar haben sich die Begriffe im Laufe der Zeit den neuen Möglichkeiten, die durch den Einsatz digitaler Technologien eröffnet werden, angepasst, doch wäre es nicht richtig zu behaupten, dass beispielsweise der Begriff Digitization in der heutigen Zeit seine Berechtigung verloren hat. Vielmehr kann argumentiert werden, dass der Weg zu einer Digital Transformation immer mit einer Digitization beginnt. Ebenso verkehrt wäre es, von einer Digitalization zu sprechen, um damit nur auf den Beginn der Nutzung von digitalen Technologien zu verweisen. Es handelt sich nämlich um einen sich wiederholenden Prozess, der bisher noch kein festes Ziel hat.

2.3 Deutsche Definitionen

Die entsprechenden Begrifflichkeiten in der deutschen Sprache weichen von dem englischen Sprachgebrauch grundlegend ab, denn eine eigenständige Übersetzung des Begriffs Digitization ist nicht vorhanden, sondern wird dem Begriff Digitalisierung gleichgesetzt. Auch dieser Sachverhalt ist gemeint, wenn Mertens schreibt:

> **:// Der äußerst unscharf benutzte Begriff Digitalisierung ist u.E. keine glückliche Episode in der Geschichte der deutschen Sprache. //**

2.3.1 Digitalisierung

Eine scharfe Trennung des Begriffs der Digitalisierung, wie in der englischen Sprache, ist im Deutschen schwierig. Dies zeigt sich auch an den deutschen Definitionsversuchen, die aufgrund dieser sprachlichen Trennung eine größere Bandbreite an Definitionsebenen abbilden. Im eigentlichen Sinne, also aus technischer Perspektive, stellt die Digitalisierung nach Wolf und Strohschen (2018) eine Umstellung der Leistungserbringung von einem analogen, hin zu einem digitalen, maschinenlesbaren Modell dar. Sie argumentieren, dass der Begriff aus der Elektro- und Informationstechnik kommt und diesem Bereich auch die Begriffsdefinition zuzuordnen ist. Dieser Definition entspricht der englische Begriff Digitization *(→ vgl 2.2.1 Digitization)*.

Auch Mertens et al. (2017) nutzen die Herkunft des Begriffs für dessen Definition, bringen jedoch die zugrundeliegende Infrastruktur und

Datenaustausch in die Diskussion mit ein, sodass die Digitalisierung

> :// die Überführung von analogen in digitale Größen zwecks Übertragung in Netzen und Verarbeitung auf Digitalrechnern //

sei. Hier lassen sich Parallelen zu der von Brennen und Kreiss beobachteten Konvergenz erkennen.

Digitalisierung ist daher in der Lage mittels Infrastruktur und einer digitalen Speicherung von Informationen (Daten), Bereiche der Gesellschaft näher zusammen zu rücken. Vogelsang erwähnt auch, dass bei den beiden vorgestellten Definitionsversuchen die Verfolgung von wirtschaftlichen Zielen – wie es an einigen Stellen in den englischen Definitionen zu finden war – sowie der Verbreitungsgrad der digitalen Technologie kaum Verwendung findet.

Neben der rein technischen Betrachtung wurde der Begriff Digitalisierung auch aus Perspektive der Politik und Wirtschaft aufgegriffen, um dem Anwendungscharakter gerechter zu werden, sodass der die Definition näher an die anglo-amerikanische Betrachtung heranrückt.

Die wahrscheinlich zutreffendste Definition ist die vom BMWi. Hier heißt es zu Digitalisierung (BMWi 2015):

> :// Die Digitalisierung steht für die umfassende Vernetzung aller Bereiche von Wirtschaft und Gesellschaft sowie die Fähigkeit, relevante Informationen zu sammeln, zu analysieren und in Handlungen umzusetzen. //

Hier werden nicht nur Parallelen zu den englischen Definitionen deutlich, die Definition schließt sogar eine Lücke, die im Englischen existiert. So würdigt das BMWi zum einen die Vernetzung sowohl in Wirtschaft als auch Gesellschaft, was dem Verbreitungsansatz nach Brennen, Kreiss und Vogelsang entspricht. Gleichzeitig geht das BMWi jedoch auch auf den Umgang mit Daten ein, dessen Ziel neue Handlungen sein sollten. Dieser Aspekt fehlt in den englischen Definitionen.

Was in der Definition des BMWi keine Rolle spielt, sind der Bezug zu wirtschaftlichem Erfolg sowie zu einem gänzlich digital organisierten Unternehmen.

2.3.2 Digitale Transformation

Dieses Bild ändert sich, wenn die digitale Transformation analysiert wird. Der von Bouee und Schaible (2015) geprägte Ansatz der digitalen Transformation ähnelt der Definition der Digitalisierung vom BMWi sehr, wird jedoch ergänzt durch die

> :// Gegebenheiten der digitalen Ökonomie. //

Des Weiteren wird der Zielhorizont der Informationsverarbeitung (sammeln, analysieren, umsetzen) ergänzt durch

> :// Berechnungen und Bewertungen von Optionen, sowie Initiierung von Handlungsempfehlungen und Einleitung von Konsequenzen // (ebd.), S. 6.

Die Erweiterung des Begriffs Digitalisierung im Hinblick auf wirtschaftliche Interessen werden mit der digitalen Transformation im Deutschen in Verbindung gebracht, was der wirtschaftlichen Sphäre von Digitalization entspräche. Noch allgemeiner ausgedrückt, stellt im Deutschen die digitale Transformation den

> :// grundlegenden Wandel in der gesamten Unternehmenswelt //

(PWC 2013) durch die Anwendung digitaler Technologien dar. Vor allem der Bezug auf die gesamte Unternehmenswelt ist bereits aus dem englischen Begriff geläufig. Auch hier sind Veränderungen im gesamten Unternehmen zu erkennen, die sich weder auf einen bestimmten Prozess beziehen, noch einen bestimmten Anwendungsfall definieren. Vielmehr ist von einem „grundlegenden Wandel“ die Rede, der bisherige Methoden und Herangehensweisen in Frage stellt. Anders als in englischen Definitionen beschränken sich die Auswirkungen bei den deutschen Definitionen nicht nur auf Unternehmen – oder allgemeiner der Wirtschaft –, sondern auf die gesamte Gesellschaft. Allerdings räumte auch Wachal den digitalen Technologien schon diesen Einfluss ein, als er seine Auffassung über den Einsatz von Computern in der Wissenschaft mit den Worten

:// the digitalization of society //

(Wachal 1971) einleitete.

Abbildung 1 stellt zum Ende des Kapitels die deutschen Definitionen (rechts) den englischen (links) gegenüber und vergleicht sie anhand der wesentlichen Kriterien. Dadurch werden die unterschiedlichen Aspekte der Digitalisierung, auf die sich die einzelnen Definitionen fokussieren, noch einmal deutlich.

Abschließend sind in Tabelle 1 die Definitionen zusammengefasst, die in diesem Kapitel aufgegriffen wurden. Sie machen deutlich, wie inkonsistent die Begriffe in den unterschiedlichen Sprachen angewendet werden.

Abbildung 1: Gegenüberstellung der Definitionen englischer und deutscher Sprache
Quelle: eigene Darstellung

	Englische Definitionen			Deutsche Definitionen	
	Digitization	Digitalization	Digital Transformation	Digitalisierung	Digitale Transformation
Technische Umstellung von analog zu digital	✓			✓	
Anwendung digitaler Technologien		✓		✓	
Vernetzung aller Breiche		✓		✓	
Mehrwertgenerierung/ Ableitung von Handlungsempfehlungen		✓			✓
Verbesserung von Prozessen		✓			✓
Grundlegender Wandel in der (Arbeits-)welt			✓		✓
Andauernde Evolution			✓		

Tabelle 1: Gegenüberstellung von Definitionsansätzen im Deutschen und Englischen

Digitization	Brennen und Kreiss 2016	„Transfer of information into a digital form“
	Gartner o. J.b	“Process of changing from analog to digital form, also known as digital enablement. Said another way, digitization takes an analog process and changes it to a digital form without any different-in-kind changes to the process itself.”
		Begriff in der deutschen Sprache nicht vorhanden.
Digitalization/ Digitalisierung	Gartner o. J.a	“the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business.”
	I-Scoop o. J.	“Digitalization means the use of digital technologies and of data (digitized and natively digital) in order to create revenue, improve business, replace/transform business processes (not simply digitizing them) and create an environment for digital business, whereby digital information is at the core.“
	Mertens et al. 2017	„Der Begriff Digitalisierung stammt aus den Fachgebieten Elektronik, Informatik, Nachrichtentechnik einschließlich Signaltechnik und bedeutet dort die Überführung von analogen in digitale Größen zwecks Übertragung in Netzen und Verarbeitung auf Digitalrechnern.“
	BMWi 2015	„Die Digitalisierung steht für die umfassende Vernetzung aller Bereiche von Wirtschaft und Gesellschaft sowie die Fähigkeit, relevante Informationen zu sammeln, zu analysieren und in Handlungen umzusetzen.“
	Wolf und Strohschen 2018	„Wir sprechen von Digitalisierung, wenn analoge Leistungserbringung durch Leistungserbringung in einem digitalen, computerhandhabbaren Modell ganz oder teilweise ersetzt wird.“
Digital Transformation/ digitale Transformation	Mazzone 2014	“Digital transformation is the deliberate and ongoing digital evolution of a company, business model, idea process, or methodology, both strategically and tactically”
	I-Scoop o. J.	“Digital transformation encompasses all aspects of business, regardless of whether it concerns a digital business or not”
	Bouee und Schaible 2015	„Digitale Transformation verstehen wir als durchgängige Vernetzung aller Wirtschaftsbereiche und als Anpassung der Akteure an die neuen Gegebenheiten der digitalen Ökonomie. Entscheidung in vernetzen Systemen umfassen Datenaustausch und –analyse, Berechnungen und Bewertung von Optionen, sowie Initiierung von Handlungsempfehlungen und Einleitung von Konsequenzen“
	PWC 2013	„Die digitale Transformation beschreibt den grundlegenden Wandel der gesamten Unternehmenswelt durch die Etablierung neuer Technologien auf Basis des Internets mit fundamentalen Auswirkungen auf die auf die gesamte Gesellschaft“

In Bezug auf die anfangs gestellte Frage nach dem Beginn und Ende der Digitalisierung wird deutlich, dass je nach Definitionsansatz zwar ein Anfang erkennbar ist, das Ende aus heutiger Sicht jedoch noch nicht quantifiziert wurde. Es ist daher gut möglich, dass die digitale Transformation im Deutschen bzw. die Digital Transformation im Englischen, nicht die letzte Ausprägung dieser Sprachentwicklung darstellen, sondern vielmehr als eine Zwischenstation fungieren. Es bleibt dabei zu hoffen, dass dies dann eine, in Anlehnung an Mertens, glücklichere Episode in der deutschen Sprache darstellt und die für mehr Klarheit sorgt.

2.4 Anwendung auf den Begriff der Digitalisierung in der Energiewirtschaft

Auch in Bezug auf die Energiewirtschaft können unterschiedliche Definitionsansätze zur Digitalisierung in der Literatur gefunden werden. → *Tabelle 2* stellt einen kurzen Auszug aus der Literatur dar. Dabei ist zu erkennen, dass sich die genutzten Definitionsansätze an den Schwerpunkt der jeweiligen Studie anpassen, inhaltlich jeweils unterschiedlichen Ebenen (Digitization, Digitalization und Digital Transformation) entsprechen und dabei immer noch generisch formuliert sind.

Gleichzeitig kann auch eine engere Verwendung des Digitalisierungsbegriffs im Kontext der deutschen Energiewirtschaft beobachtet werden, beispielsweise in dem oben besprochenen Digitalisierungsbarometer von EY im Auftrag des BMWi (EY 2019). Dieses engere Verständnis wurde gewissermaßen durch das Mantelgesetz zur Digitalisierung der Energiewende vom 29. August 2016 geprägt. Das Gesetz konzentriert sich, in dem dadurch eingeführten Messstellenbetriebsgesetz (MsbG), im Wesentlichen auf den Einbau von Smart Metern, einschließlich technischer Anforderungen und der damit einhergehenden Datenkommunikation und -verarbeitung. Obwohl die Bedeutung intelligenter Messsysteme für die Vernetzung von Akteuren und Geräten in der Stromwirtschaft und auch darüber hinaus mit anderen Wirtschaftssektoren einleuchtet, kann die Digitalisierung in der Energiewirtschaft nicht darauf reduziert werden. Es bleibt daher auch im Energiesektor die Aussage bestehen, dass der Begriff Digitalisierung

:// seltsam unbestimmt //

bleibt (Krickel, 2015).

Die Energiewirtschaft verfügt dabei über Alleinstellungsmerkmale, die auch den Digitalisierungsprozess in der Branche prägen. Diese kommen in dem wirtschaftspolitisch und gesetzlich verankerten energiepolitischen Zieldreieck zum Ausdruck. Während das Ziel der Wirtschaftlichkeit sektorübergreifend und durch die allgemeinen marktwirtschaftlichen Grundsätze bzw. das Stichwort Mehrwert abgedeckt ist, haben die zwei anderen Ziele – Versorgungssicherheit und Umweltverträglichkeit – eine besondere Stellung in der Energiewirtschaft. Beide Ziele werden durch die Digitalisierung tangiert und beeinflussen daher den sektorspezifischen Digitalisierungsbegriff.

Im Vergleich zu anderen Sektoren kommt der Energiewirtschaft eine Schlüsselposition in der Gesellschaft und Ökonomie zu. Ohne eine sichere Energieversorgung sind Störungen des öffentlichen Lebens, des Staates und der Wirtschaft vorprogrammiert.
Es besteht daher eine wechselseitige Abhängigkeit zwischen der Energiewirtschaft und dem Sektor der Informations- und Kommunikationstechnologien (IKT) (Bartsch und Frey 2017; BNetzA 2018). Dies begründet das Verständnis der Energieversorgung als eine Aufgabe der öffentlichen Daseinsvorsorge und das energiepolitische Ziel der Versorgungssicherheit. Eine naheliegende Auswirkung der Digitalisierung in diesem Bereich ist die zunehmende Bedeutung der IT-Sicherheit. Das schadhafte Ausnutzen einer Sicherheitslücke im Energiesektor könnte zu einer "Kettenreaktion" führen (Fassing 2020). Angreifer könnten daher einen hohen Grad der Digitalisierung ausnutzen, um einen großen Schaden anzurichten.[6]

6 Eine Einordnung von Angriffsarten kann im → vierten Teil des Kompendiums nachgelesen werden.

Tabelle 2: Definitionsansätze Digitalisierung aus energiewirtschaftlicher Perspektive

Autor/ Quelle	Definition
BDEW 2015, 2016	Basierend auf den Triebfedern definiert sich die Digitalisierung der Energiewirtschaft als die „Vernetzung von Anwendungen, Geschäftsprozessen sowie von Geräten auf Basis von Internettechnologien unter Verwendung von Sensoren und selbststeuernden Geräten“
bbh 2017	Unser Versuch der Digitalisierung ist, dass diese Entwicklung vermutlich am ehesten mit der „Definition von Standards, einer darauf aufbauenden Automatisierung von Prozessen, und der Nutzung von Plattformen und Kooperationen als Basis für den Informationsaustausch und die Mehrwertgewinnung durch die Nutzung von Skaleneffekten zu beschreiben ist“
IRENA 2019	“Digitalisation can be defined as converting data into value for the power sector”
Krickel 2015	„Einsatz von Technik, um die Performance oder die Reichweite von Unternehmen drastisch zu erhöhen – statt neue Technologien nur zu implementieren, geht es hierbei um Transformierung und Weiterentwicklung der Betriebsprozesse, des Kundenerlebnisses und der Geschäftsmodelle“

Viele Bereiche der Energiewirtschaft, insbesondere jener der Erzeugung und Übertragung von Elektrizität, gelten unter anderem deshalb als kritische Infrastruktur, da hier der Sicherheitsgedanke eine hervorgehobene Stellung einnimmt. Neben der Stromversorgung gehören beispielsweise Teile der Gesundheitsversorgung sowie die Wasserversorgung auch zur kritischen Infrastruktur (BSI o. J.).

Dass die IT-Sicherheit einen wichtigen Aspekt eines sicheren Stromnetzbetriebes darstellt, ist gesetzlich festgehalten (§11 Abs. 1a EnWG).[7]

Dabei ist es bemerkenswert, dass das jährliche Monitoring der Versorgungssicherheit durch das BMWi auf

> // **der vorhandenen Stromerzeugung, den Möglichkeiten zum Stromtransport und der Verfügbarkeit von Energieträgern für die Stromerzeugung** //

fokussiert ist, ohne Aspekte der IT-Sicherheit zu beleuchten (BMWi 2019). Auf der Webseite der BNetzA fungiert die IT-Sicherheit als einer von mehreren Bausteinen der Versorgungssicherheit – neben der Transportfähigkeit des Netzes, ausreichenden Erzeugungskapazitäten und belastbaren Regelungsmechanismen.[8] Vor diesem Hintergrund ist zu erwarten, dass auch der Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme in den ab 2021 vorgesehenen jährlichen Monitoringberichten der BNetzA bewertet wird.

Gleichzeitig wird eine digitale Infrastruktur benötigt, um Lösungen für die Herausforderungen vor dem Hintergrund der Energiewende zu finden. Eine große Anzahl von fluktuierenden erneuerbaren Stromerzeugern wird kontinuierlich in das bestehende Stromnetz integriert. Dabei müssen Angebot und Nachfrage zu jedem Zeitpunkt ausbalanciert und genügend Flexibilität unter

7 Nachzulesen im → dritten Teil des Kompendiums

8 https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/versorgungssicherheit-node.html

Berücksichtigung physikalischer Eigenschaften im Stromsystem vorgehalten werden (Gerrits 2019), um eine unterbrechungsfreie Stromversorgung sicherzustellen. Die IKT-basierte Vernetzung von Verbrauchern, Erzeugern und Netzinfrastruktur kann u. A. eine effizientere Bilanzierung von Stromerzeugung und -nachfrage ermöglichen und somit die Versorgungssicherheit verbessern (Lange und Santarius 2018). Da die Systembilanzierung in einem zunehmend von den Erneuerbaren geprägten System immer stärker von der Systemintegration volatiler Erneuerbarer Energien getrieben wird, kann der geschilderte Beitrag der Digitalisierung gleichzeitig bei dem energiepolitischen Ziel der Umweltverträglichkeit eingeordnet werden. Die Bemühungen streben am Ende insbesondere das Erreichen einer nachhaltigen Zukunft an, in welcher es zu einer drastischen Reduzierung der Emissionen kommen muss. Borghesi und Glachant bezeichnen die Digitalisierung in der Energiewirtschaft daher als ein „Fragment“, mit welchem die Dekarbonisierung verfolgt werden kann (Borghesi und Glachant 2019). In der Datenstrategie der Bundesregierung wird die Bedeutung von Energiedaten (die im Zuge der Digitalisierung entstehen) für den Übergang zu einer klimaneutralen Energieinfrastruktur unterstrichen, insbesondere im Hinblick auf Erneuerbare Energien und Energieeinsparmaßnahmen. (Bundesregierung 2021).

Wird das generelle, branchenübergreifende Verständnis von Digitalisierung mit der besonderen Bedeutung der Energieversorgung für die Wirtschaft und Gesellschaft kombiniert, so liegt der Schluss nahe, dass der Aspekt der Sicherheit einen wesentlichen Bestandteil der Digitalisierung darstellen sollte. Dieses Bewusstsein beschreibt die dena in ihrer Publikation zum Thema Datenschutz und Datensicherheit als

:// Säule der Systemstabilität //

(dena 2018).

Der Aussage soll daher auch in einer Definition der Digitalisierung im Kontext der Energiewirtschaft Rechnung getragen werden, indem der Sicherheitsgedanke bereits auf der Definitionsebene verankert wird.

Basierend auf den Schwerpunkten aus vorangegangenen Studien zum Thema Digitalisierung und unter Berücksichtigung der vorangegangenen Überlegungen zu Definitionsansätzen sollte eine Definition von Digitalisierung im Kontext der Energiewirtschaft nach Auffassung der Autoren folgende Punkte einschließen:

- ↳ *Darstellung der technischen Ebene (vgl. engl. Digitization)*
- ↳ *Berücksichtigung einer wirtschaftlichen/ gesellschaftlichen Vorteilhaftigkeit bzw. eines Mehrwertes (vgl. engl. Digitalization)*
- ↳ *Berücksichtigung der sektorspezifischen Besonderheiten der Energiewirtschaft*

Auf Grundlage der Formulierung des BMWi und der Ausführungen aus diesem Kapitel, leiten wir daher folgende Definition ab:

:// Die Digitalisierung steht für die umfassende Vernetzung von Systemen, für die Erhebung und Übertragung von Informationen in digitaler Form (Daten) sowie die Fähigkeit, relevante Informationen zu sammeln, zu analysieren und in Handlungen umzusetzen mit dem Ziel der Schaffung eines Mehrwerts für Wirtschaft und/oder Gesellschaft, unter Berücksichtigung vorhandener Sicherheitsanforderungen. //

Durch diese Definition wird zum einen sichergestellt, dass die Erkenntnisse der Definitionsanalyse in die Energiewirtschaft überführt werden, und zum anderen, dass die sektorenspezifischen Besonderheiten

der Energiewirtschaft Berücksichtigung finden. Aus der Definition lassen sich somit vier Kernbereiche der Digitalisierung in der Energiewirtschaft identifizieren:

1. Vernetzung: Hiermit ist vor allem die physische und/oder virtuelle Verknüpfung sowie der Austausch von Informationen unter allen relevanten Akteuren (Mensch, Maschine und Markt) gemeint.

2. Sicherheit: Mit Sicherheit werden sowohl Aspekte der Energieversorgungssicherheit als auch die Cybersicherheit (privat, innerhalb und außerhalb des Unternehmens) gemeint und alle damit einhergehenden rechtlichen und technischen Anforderungen.

3. Daten: Alle Daten, die gesammelt, gespeichert, analysiert, ausgewertet und für weitere Zwecke verwendet werden können.

4. Mehrwert: Hiermit wird die Schaffung eines wirtschaftlichen oder gesellschaftlichen Vorteils gemeint. Dies schließt direkte und indirekte Mehrwerte ein.

Abbildung 2: Das energiepolitische Zieldreieck vor dem Hintergrund des gewählten Definitionsansatzes
Quelle: eigene Darstellung

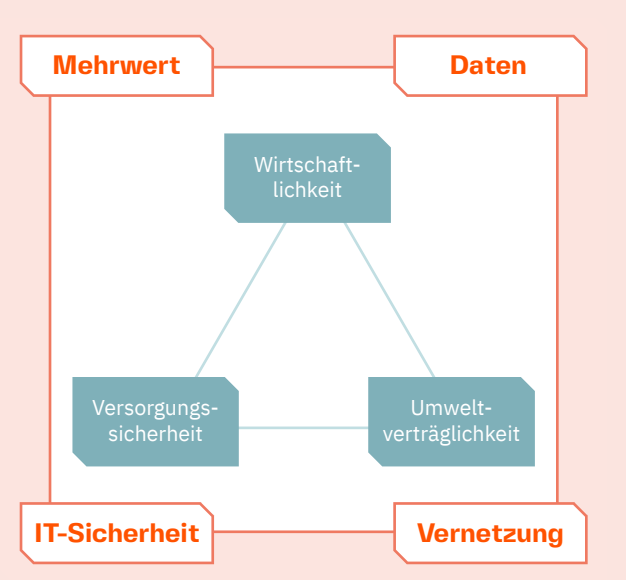


Abbildung 2 verdeutlicht diesen Zusammenhang visuell. Das energiepolitische Zieldreieck wird hierbei vor dem Hintergrund der Digitalisierung gesehen, der durch die benannten Eckpunkte des Definitionsansatzes aufgespannt wird. Es soll damit eine ganzheitliche Betrachtung verdeutlicht werden.

Auf Vernetzungstechnologien, wie beispielsweise das Cloud Computing, intelligente Geräte oder IKT, gehen wir in diesem Kompendium nicht weiter ein. Die Cybersicherheit wird in den Teilen drei und vier aus regulatorischer und technischer Sicht beleuchtet. Wir widmen den weiteren inhaltlichen Verlauf den beiden letztgenannten Kernbereichen: den Daten und den daraus resultierenden Mehrwerten.

://3. DATEN

3.1 Definition energierelevanter Daten

Daten sind ein zentrales Element und wichtiger Treiber der Digitalisierung. Im energiewirtschaftlichen Kontext wird der erschwerte Zugang zu Daten sowohl in wissenschaftlichen Abhandlungen als auch in der politischen Diskussion als ein Hemmnis für digitale Innovationen gesehen. (Catapult Energy Systems 2018). Neben allgemeinen Problemen mit der Datenqualität und dem Datenschutz im Bereich Big Data, trägt die Komplexität des branchenspezifischen Regulierungsrahmens erschwerend dazu bei.

Der Begriff von Energiedaten (im Sinne von energiewirtschaftlich relevanten Daten) ist nicht eindeutig festgelegt und wird in der Literatur – je nach Hintergrund der Untersuchung – unterschiedlich definiert. Eine Übersicht verwendeter Definitionen von verschiedenen Autoren findet sich beispielsweise bei (Rigoll 2017). Neben dem Verständnis als statistische bzw. volkswirtschaftliche Informationen (insbesondere in der Sammlung von Energiedaten des BMWi) werden mehrere Definitionen vorgestellt, die sich auf Mess- bzw. Verbrauchsdaten beziehen. In seiner Dissertation zu einem nutzerorientierten Datenmanagement definiert Rigoll Energiedaten für seine Zwecke als Daten zum Energieverbrauch sowie zum Netzzustand und Zustand einzelner Netzkomponenten in Form von Zeitreihen. (ebd.)

In der neuen EU-Strombinnenmarktrichtlinie[9] (EU-EltRL) werden Daten als

> :// **Mess- und Verbrauchsdaten sowie die für den Kunden für einen Versorgerwechsel, die Laststeuerung und andere Dienstleistungen erforderlichen Daten** //

verstanden. Diese Definition ist breiter als das oben vorgestellte Verständnis von Energiedaten als Messdaten. Die „erforderlichen Daten“ für „andere Dienstleistungen“ sind in der Richtlinie nicht näher definiert. (Ducuing 2019) Bei der Ausgestaltung nationaler Regelungen könnte die Definition durch beispielhafte Benennung relevanter Datenkategorien präzisiert werden, zugleich soll durch die offene (nicht abschließende) Definition ein diskriminierungsfreier Zugang zu allen relevanten Daten sichergestellt werden.

Ferner ist die Datendefinition in der Studie zur Datenlandschaft in der deutschen Energiewirtschaft von Seim et al. zu erwähnen, die im weiteren Verlauf dieses Beitrags einbezogen und weiterentwickelt wird. Die Studie setzt den Fokus auf den Datenzugang für Energiesystemmodellierung. Dementsprechend betrachten die Autoren alle Daten, die sich auf die analysierten Energieträger Strom, Gas und Wärme, beziehen und klammern Kontextdaten wie soziodemografische und geografische Informationen aus (Seim et al. 2019).

In diesem Beitrag untersuchen wir die Rahmenbedingungen und Hemmnisse für datengetriebene Innovationen in der Energiewirtschaft mit dem Fokus auf den Datenzugang. Dementsprechend umfassen die relevanten energiewirtschaftlichen Daten für unsere Zwecke alle Daten, die für die Entwicklung neuer digitaler Produkte oder Prozesse

9 Richtlinie (EU) 2019/944 vom 05.06.2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU.

verwendet werden können. Hierzu zählen – neben den Messdaten zum Stromverbrauch und zur Stromerzeugung sowie Informationen zum Netzzustand und zum technischen Zustand von Netz-, Erzeugungs-, Speicher- und Verbraucheranlagen – auch kundenbezogene Daten. Neben den üblichen Stammdaten, die von der normativen Definition von Daten umfasst sind (etwa im Messstellenbetriebsgesetz), werden Informationen zu Kundenpräferenzen und Nutzerverhalten, beispielsweise aus sozialen Medien und Anwendungen, berücksichtigt. Dazu kommen diverse Kontextdaten wie raumbezogene Informationen, Wetterdaten, Daten aus angrenzenden Sektoren wie Verkehrs-, Gas- und Wasserverbrauchs-Daten sowie aus energiefremden Branchen. Gleichzeitig werden auch Wetterdaten als energiebranchenfremde Daten eingeordnet. Trotz deren großer Bedeutung für die Vorhersage von Erzeugung und Verbrauch werden sie gleichwohl für andere Zwecke vielfältig genutzt (Akhavan-Hejazi und Mohsenian-Rad 2018). Gleichwohl haben Energiedaten in Verbindung mit anderen Daten durchaus das Potential auch außerhalb der Energiewirtschaft Anwendung zu finden. Der Fokus liegt bei unserer Untersuchung auf den Daten aus der Stromwirtschaft. Andere Energieträger werden nicht explizit betrachtet. Dieses weite Verständnis von Daten spiegelt eines der Merkmale von Big Data – der sog. Vs[10] – wider: die Vielfalt von Daten. Die vielfältigen Daten kommen aus unterschiedlichen internen wie externen Quellen und in unterschiedlichen Formaten (Elia et al. 2020).

3.2 Öffentlich verfügbare Daten

Bestimmte Kategorien von energierelevanten Daten sind öffentlich bzw. für alle Interessierten zugänglich. Es handelt sich um zusammengeführte Energiestatistiken, Marktdaten des Großhandels sowie vielfältige Informationen, die von Marktakteuren gemeldet werden, um gesetzlich verankerten Melde- und Veröffentlichungspflichten nachzukommen.

Um einen Überblick über die Relevanz und Verfügbarkeit von typischen energiewirtschaftlichen öffentlich zugänglichen Daten zu bekommen, wurde von Seim et. al. eine Analyse von Datensätzen auf deutschen und europäischen Datenplattformen (beispielsweise AG Energiebilanzen, Energiedaten des BMWi, SMARD[11] und ENTSO-E[12]) anhand folgender Kriterien unternommen und ausgewertet (Seim et al. 2019):

- *Häufigkeit*
- *Räumliche Auflösung*
- *Zeitliche Auflösung*
- *Datenbereitsteller*
- *Verfügbarkeit*
- *Zugang*

Die Studie kommt zum Ergebnis, dass es in Deutschland aktuell eine große Anzahl an Datenplattformen (mehr als 20) gibt. Sie weisen ein hohes Maß an Heterogenität auf und stellen Daten, je nach Energieträger und Wertschöpfungsstufe, entweder automatisiert über eine Schnittstelle oder individuell zur Verfügung.

Der überwiegende Anteil der Datenquellen hat einen deutschlandweiten Fokus, Bundesland- und Regionalebene sind nur in geringerem Umfang vertreten. Lediglich im Netzbereich ist die Aufteilung zwischen deutschlandweiten, Landes- und Regionalebene nahezu gleichmäßig verteilt, was in den vielen Veröffentlichungspflichten im Netzsektor zu begründet liegt. Ausschlaggebend dafür ist, dass in Netzen viele Informationen erfasst werden, die überdies

10 Die Anzahl der Merkmale von Big Data, die im Englischen mit dem Buchstaben „V“ anfangen, variiert in der Literatur von drei bis zehn.

11 SMARD ist eine Informationsplattform der Bundesnetzagentur über den deutschen Strommarkt (www.smard.de).

12 ENTSO-E (European Network of Transmission System Operators for Electricity) ist das europäische Netzwerk der Übertragungsnetzbetreiber und vertritt 42 Stromübertragungsnetzbetreiber (TSOs) aus 35 Ländern in ganz Europa.

für die Gewährleistung eines stabilen Netzbetriebs benötigt werden. Weiterhin will der Gesetzgeber, aufgrund der Eigenschaft von Netzen als natürliche Monopole, eine hohe Transparenz schaffen, um die staatliche Regulierung zu ermöglichen und um das Informationsinteresse der Öffentlichkeit sowie der Marktakteure zu befriedigen.

Bei der zeitlichen Auflösung der erfassten Datenquellen dominiert die jährliche Auflösung, was insbesondere auf statistisch erfasste Daten der staatlichen Einrichtungen und Verbände sowie jährliche Veröffentlichungspflichten zurückzuführen ist. Viele der untersuchten Datenquellen haben allerdings eine nicht definierte zeitliche Auslösung, was auf einen wiederkehrenden oder unbekannten Aktualisierungsturnus eines Datensatzes hindeutet. Historische Werte einiger Datenquellen, die keine zeitliche Auflösung haben, werden aller Wahrscheinlichkeit nach durch die jeweiligen Datenbereitsteller aufgezeichnet, aber nicht öffentlich zur Verfügung gestellt. Datenquellen höherer zeitlicher Auflösung sind dagegen nur vereinzelt vorhanden, obwohl vor allem für Modellierungsansätze insbesondere zeitlich hochaufgelösten Daten eine entscheidende Rolle zukommen kann. Die für das Stromsystem üblichen viertelstündlichen Werte für einzelne Erzeuger und Verbraucher – obwohl technisch durch das Messstellenbetriebsgesetz als Stand der Technik definiert – sind vor dem Hintergrund ihrer energiewirtschaftlichen Relevanz deutlich unterrepräsentiert.

Der Anteil der Bereitstellungsgruppen, also diejenigen, die die Daten möglichen Nutzern bereitstellen, verteilen sich nahezu gleich zwischen Netzbetreibern, privatwirtschaftlichen Unternehmen, Forschungsinstituten und Verbänden. Der größte Anteil der Datenquellen wird allerdings durch staatliche Einrichtungen (beispielsweise BNetzA und BMWi) veröffentlicht. Neben der Bundesnetzagentur und anderen Behörden sind hier insbesondere die statistischen Bundes- und Landesämter zu nennen.

Statistisch erfasste Daten in jährlicher Zeitauflösung werden in Zeiträumen größer als neun Jahren abgebildet und vor allem von staatlichen Einrichtungen zur Verfügung gestellt. Auch für kürzere Zeiträume von einigen Jahren gibt es Beispiele für Datenquellen, der Großteil der Daten (ca. ein Drittel) wird jedoch für einen Zeitraum von maximal einem Jahr veröffentlicht. In den wenigsten Fällen sind keine historischen Daten, sondern nur aktuelle Werte vorhanden.

Gut zwei Drittel der identifizierten Daten haben keine eindeutige Lizenzbestimmung und können oft kostenfrei von Unternehmen, Verbänden, Forschungsinstituten und staatlichen Einrichtungen bezogen werden. Der Zugang zu den restlichen Daten erfordert eine gebührenpflichtige Lizenz. Nur in den wenigsten Fällen waren die Daten öffentlich nicht einsehbar und verfügbar. Dabei handelt es sich höchstwahrscheinlich um Betriebsgeheimnisse oder anderweitig stark restriktive und schützenswerte Informationen.

Insgesamt ist zu beobachten, dass eine Vielzahl an Datenquellen über mehrere Energieträger und Wertschöpfungsstufen vorhanden und dadurch viele Daten öffentlich verfügbar sind; eine ganzheitliche Einordnung der Daten ist somit sehr schwierig. Die Daten sind oft heterogen verteilt bzw. liegen in nicht-maschinenlesbarer Form vor. Ein verstärkter Bedarf nach zeitlich und räumlich höher aufgelösten Erzeugungs- und Verbrauchsdaten für den Stromsektor konnte identifiziert werden, da für das Gelingen der Energiewende eine Vielzahl an hoch aufgelösten Daten aus verschiedenen Wertschöpfungsstufen benötigt wird, um den Um- und Ausbau des Energiesystems simulieren und somit die Entscheidungsfindungen datenbasiert unterstützend vorantreiben zu können. Die vom Bundesministerium für Bildung und Forschung (BMBF) ins Leben gerufene Nationale Forschungsdateninfrastruktur (NFDI) spiegelt die Notwendigkeit eines übergreifenden Forschungsdatenmanagements wieder, welche Standards bei der nachhaltigen Nutzung und Verwendung von Daten setzen soll (Bundesregierung 2021).

Auch das Thema der unzureichenden Lizensierung stellt ein Problem dar und führt dazu, dass Daten entweder nicht verwendet werden dürfen oder dass eine Nutzung nur in einer Grauzone stattfinden kann (Hirth 2020).

Daher kann es sinnvoll sein, in Zukunft Daten in einer festgelegten Art und Weise zu erheben, um Konsistenz in Form und Qualität der Daten zu gewährleisten und im Sinne eines Open-Data-Ansatzes zu veröffentlichen. Die Veröffentlichungspflichten sollten anhand von Bedingungen der Maschinenlesbarkeit, wie zum Beispiel bei der Initiative Green Button des Weißen Hauses aus dem Jahr 2012 (Office of Science and Technology Policy 2012) umgesetzt werden. Green Button ist eine Initiative, die den Kunden von Versorgungsunternehmen einen Zugang zu ihren Energieverbrauchsdaten in einem verbraucher- und computerfreundlichen Format bietet. Kunden können ihren eigenen detaillierten Energieverbrauch mit einem einfachen Klick von den Websites der Stromversorger verwalten. Die freiwillige Annahme eines Konsens-Branchenstandards durch Energieversorger und Unternehmen schafft dabei Anreize für die Entwicklung innovativer Anwendungen, Produkte und Dienstleistungen.

Ein weiteres Beispiel einer öffentlich geförderter Dateninitiative ist das Smart Energy Research Lab. Es handelt sich dabei um ein Pilotprojekt, das feingranulare und hochqualitative Energiedaten für wissenschaftliche Forschungszwecke verfügbar machen soll. Über die von der britischen Regierung geförderte Plattform sollen halbstündliche Strom- und Gasverbrauchsdaten von ursprünglich 8.000-10.000 Haushalten zusammen mit Kontextdaten (soziodemografische Merkmale, Informationen zum Gebäude, Standort, Wetterdaten usw.) gesammelt und akkreditierten Forschern aus Großbritannien zur Verfügung gestellt werden (Webborn und Elam 2019).

Ähnliche Ansätze finden sich auch in der Datenstrategie der Bundesregierung mit der Vernetzung und dem Ausbau von Dateninfrastrukturen wieder. Ein prominentes Beispiel ist die European Open Science Cloud (EOSC), deren Ziel es ist eine europaweite vertrauenswürdige Verbundumgebung zu schaffen, in der forschungsrelevante Daten und Informationen aller Art gespeichert und geteilt werden können. Hierzu setzt EOSC auf die Zusammenarbeit europäischer Initiativen, in Deutschland insbesondere durch die nationale Forschungsdateninfrastruktur (Bundesregierung 2021).

Wie oben angemerkt, wurden relevante Kontextdaten aus anderen, nicht notwendigerweise energiebezogenen Bereichen von Seim et al. nicht betrachtet. Vollständigkeitshalber sind hier offene Quellen auch solcher relevanten Informationen für die datengetriebene Produktentwicklung zu erwähnen. Von besonderer Bedeutung sind die Wetterdaten, die insbesondere für die Vorhersage von Stromerzeugung und -verbrauch unabdingbar sind, und raumbezogene (GIS[13]) Daten (Zhou et al. 2016). In der Literatur wird beispielsweise auf das Verwendungspotenzial von sog. freiwillig erhobenen geographischen Informationen (‘volunteered geographical information’, VGI) beim Datamining für die Energiewirtschaft hingewiesen, insbesondere für eine präzisere Klassifizierung von Haushalten für Vertriebszwecke. (Hopf 2018) Unter VGI verstehen sich gemeinschaftlich von Freiwilligen gesammelte, öffentlich verfügbare raumbezogene Informationen, u.a. in Form von Karten (z. B. OpenStreetMap).

3.3 Typologie energierelevanter Daten

Vorgehend wurden Energiedaten besprochen, die hauptsächlich aufgrund gesetzlicher Melde- und Veröffentlichungspflichten, für statistische Zwecke sowie als Voraussetzung für das Funktionieren von Energiemärkten erhoben werden und – ob entgeltlich oder unentgeltlich – öffentlich verfügbar sind. Beschränkte Verfügbarkeit von Daten, deren differenzierte bzw. unzureichende Qualität und ggf. niedrige zeitliche Auflösung führen dazu, dass Unternehmen Daten selbst erheben oder

13 Geographisches Informationssystem

anderweitig beschaffen müssen, um neue digitale Produkte und Prozesse zu entwickeln. Auch in diesem Bereich der Energiedatenlandschaft wird der Zugang zu Daten insbesondere aufgrund von Datenschutz als ein wesentliches Hemmnis für digitale Innovationen thematisiert (Rhodes 2020).

Um die Barrieren für den Zugang zu Energiedaten besser zu verstehen und Ansätze aufzuzeigen, wie sie überwunden werden können, werden nachfolgend relevante Daten nach verschiedenen Kriterien kategorisiert und die regulatorischen Vorgaben zu deren Erhebung und Weitergabe differenziert betrachtet.

3.3.1 Energiesystemdaten und Kunden- bzw. Erzeugerdaten

Auf einer systemübergreifenden Ebene lassen sich alle im Energiebereich erhobenen Daten in zwei große Kategorien aufteilen: Systemdaten und Daten, die sich auf einzelne Erzeuger oder Endkunden bzw. Anschlussnutzer beziehen. Zur ersten Kategorie gehören beispielsweise Netzflussdaten, Wetterprognosedaten, allgemeine Marktdaten, aggregierte Stromerzeugungsmengen sowie der Standort wichtiger Anlagen in einem Stromversorgungssystem. Die zweite Kategorie beinhaltet insbesondere Informationen zum Stromverbrauch einzelner Endkunden sowie Eigenerzeugungsmengen dezentraler Erzeugungsanlagen, Kunden- und Anlagenstammdaten, Abrechnungsdaten und Abrufdaten für steuerbare Verbrauchseinrichtungen (ebd.).

Bei Erzeuger- und Kundendaten liegt es nahe, dass sie sich auf einzelne Erzeuger bzw. Kunden beziehen und bei diesen erhoben werden. Systemdaten entstehen entweder an zentralen Stellen wie beispielsweise bei Netzbetreibern und Strombörsen oder werden durch Übermittlung dezentral erhobener Daten aggregiert, u.a. im Rahmen von Meldepflichten für das Marktstammdatenregister, Datenmeldung zu dezentraler Erzeugung gegenüber der BNetzA, im Rahmen der Transparenzplattform von ENTSO-E nach der EU-Verordnung Nr. 543/2013. Zum Teil werden diese Daten in aggregierter Form auf vorher erwähnten Plattformen (beispielsweise SMARD) oder als Statistiken (beispielsweise Energiebilanzen) veröffentlicht. Darüber hinaus sind sie größtenteils nicht öffentlich zugänglich. Aus unserer Sicht ergeben sich jeweils Überschneidungen zwischen den skizzierten Kategorien System-, Erzeuger- und Endkundendaten. Die grundsätzlich als Systemdaten einzuordnenden Netzzustandsdaten beinhalten u. A. Werte, die bei Erneuerbaren Erzeugungsanlagen sowie bei steuerbaren Verbrauchseinrichtungen und größeren Stromkunden gemessen werden. Überschneidungen von Endkunden- und Erzeugungsdaten ergeben sich dabei im Fall von Prosumern.

3.3.2 Erhebungstechnologien

Im Hinblick auf die Erhebungsmethode energiewirtschaftlich relevanter Daten kann zwischen Stromzählern, (anderen) Sensoren, Mobiltelefonen bzw. PCs und sonstigen Datenquellen unterschieden werden.

Daten aus Messeinrichtungen stehen im Vordergrund. Der Einsatz unterschiedlicher Zählertypen – herkömmlicher Ferraris-Zähler, digitaler Zähler ohne Kommunikationseinheit (moderne Messeinrichtungen) und mit Kommunikationseinheit (intelligente Messsysteme) – führt zu Unterschieden bei der zeitlichen Auflösung der Daten sowie deren Übertragungsfähigkeit. Auch Smart Meter unterscheiden sich technisch untereinander. Das Smart Meter Gateway als zentrale Kommunikationseinheit wird dabei einer fortwährenden Weiterentwicklung unterworfen sein, um mit der dynamischen IT-Entwicklung in Form neuer Funktionalitäten Schritt halten zu können (BSI 2020).

Die technische Heterogenität spiegelt sich einerseits in unterschiedlicher Wertigkeit der Daten wider (dena 2018). Andererseits spielt der Datenschutz, je größer der Bezug zum Endkunden, einzelnen Verbrauchseinrichtungen und je höher die zeitliche Datenauflösung, eine immer wichtigere Rolle (Zwanziger 2019). Der Datenschutz und die Datensicherheit werden durch Zertifizierung von Messsystemen und Smart Meter Gateway sowie durch

entsprechende gesetzliche Vorgaben an alle zur Datenverarbeitung berechtigte Stellen gewährleistet. Die technischen Vorgaben beziehen sich auf Produktkomponenten, den IT-Betrieb und die Kommunikationsinfrastruktur (BSI 2020). Auf die Behandlung von Messdaten wird im Laufe des Beitrags noch ausführlicher eingegangen.

Entsprechend dem oben beschriebenen breiten Verständnis energierelevanter Daten werden hier neben den Messdaten auch Daten aus anderen Quellen berücksichtigt. Insbesondere kommen mit Sensoren gesammelte Daten in Betracht. Diese können vielfältig sowohl auf der Netz- bzw. Systemebene als auch bei Erzeugern und Stromverbrauchern eingesetzt werden. Im Netzbereich kann beispielsweise ein Freileitungsmonitoring (FLM) – eine zeitdynamische Auslastung von Stromleitungen je nach Wetterbedingungen – eine höhere Ausnutzung vorhandener Stromnetzkapazitäten ermöglichen und so den Netzausbaubedarf verringern (Agora Energiewende 2019). Im Rahmen des FLM nutzt beispielsweise TenneT neben den Wetterdaten von Verteilnetzbetreibern und allgemeinen Wetterprognosen auch Daten wie Umgebungstemperatur, Windgeschwindigkeit und Sonneneinstrahlung, die in eigenen Wetterstationen entlang den Stromleitungen gesammelt werden (TenneT). Überwachung von Stromleitungen mit Sensoren kann nicht nur einem optimierten Netzbetrieb dienen, sondern auch wertvolle Daten für Marktanalysen liefern. Dies zeigt beispielsweise die PowerRT-Plattform von Genscape mit fundamentalen Strommarktdaten für Energiehändler, Marktanalysten und Portfoliomanager. Das Alleinstellungsmerkmal der Plattform sind Echtzeitdaten zu Lastflüssen in den Stromnetzen aus eigenen Sensoren, die neben üblichen Informationsquellen verwendet werden.[14]

Ein Beispiel zum Einsatz von Sensoren in Stromerzeugungsanlagen ist TSE[15] – eine von TÜV SÜD in Zusammenarbeit mit Stadtwerken München entwickelte Lösung zur Überwachung thermischer Ermüdung in Kraftwerkskomponenten. Die Analyse gewinnt an Bedeutung und wird zugleich erschwert durch eine unregelmäßigere Fahrweise konventioneller Kraftwerke mit dem zunehmenden Anteil volatiler Erneuerbarer Erzeugung. Die TSE besteht aus Sensoren zur Erhebung und Echtzeitübermittlung von Betriebswerten kritischer Komponenten und einer Software zur Auswertung dieser Daten (TÜV SÜD 2019). Zum Einsatz von Sensoren im Endkundenbereich bietet sich ein Beispiel aus dem Verbundprojekt WindNODE[16] an. Durch den Einbau von Temperaturfühlern, elektrischen Thermostatventilen, Bewegungsmeldern und die Steuerungsdisplays in traditionellen Wohnhäusern wurde eine hochmoderne Smart-Building-Technik eingesetzt. Damit wurde insgesamt 24 Prozent Heizenergie eingespart, zusätzlich zu den getätigten Sanierungsmaßnahmen. Als selbstlernendes System legt ein Wohnungsmanager autonom fest, wie viel Zeit für das Aufwärmen der Wohnungen tatsächlich benötigt wird.

Ein breites Spektrum potenziell relevanter Daten wird durch Mobiltelefone bzw. PCs, insbesondere über Apps und soziale Netzwerke gesammelt (Moreno-Munoz et al. 2016). Dazu gehören beispielsweise raumbezogene Daten, Bild- und Videoinhalte, Mobilitätsprofile (etwa durch Tracking per Smartphone) (Grünewald und Reisch 2020), Nutzer- bzw. Verhaltensprofile. Solche Informationen können sowohl durch Energie-Apps als auch außerhalb des Energiekontextes erhoben werden. Ein bekanntes Beispiel ist Facebook. Die Plattform sammelt Interaktionen der Nutzer und erstellt aus diesen Daten unikale personenbezogene Profile. Dies ermöglicht es wiederum anderen Unternehmen ihre Reichweite zu verbessern, indem sie ihre Produkte mit personalisierter Werbung an genau definierte Zielgruppen (zum Beispiel nach Alter, geografisches Einzugsgebiet, Interessen etc. geclustert) auf Facebook

14 Vgl. https://www.woodmac.com/research/products/power-and-renewables/powerrt-europe/

15 Steht für Temperature-Stress-Exhaustion

16 Teilprojekt Quartier „Hosemannstraße“ in Berlin-Prenzlauer Berg. Weitere Infos unter https://www.windnode.de/ergebnisse/windnode-konkret/smart-building/

bewerben. Auch Energieunternehmen könnten solche Kanäle zur Datenakquise nutzen. Im Hinblick auf den betroffenen Personenkreis handelt es sich bei Daten aus Apps und sozialen Medien hauptsächlich um natürliche Personen.

3.3.3 Personenbezogene und nicht personenbezogene Daten

Von essenzieller Bedeutung für den Zugang zu energierelevanten Daten im Hinblick auf Datenschutz ist deren Einordnung als personenbezogene oder nicht personenbezogene Daten. Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, gelten als personenbezogene Daten (Art. 4 Nr. 1 DSGVO) und unterliegen den allgemeinen Vorgaben zum Datenschutz nach der EU-Datenschutz-Grundverordnung (DSGVO)[17], ergänzt und konkretisiert durch das Bundesdatenschutzgesetz (BDSG). Der Bezug zu einer natürlichen Person kann auch durch Kombination mit anderen Daten hergestellt werden, solange dies mit einem vertretbaren Aufwand verbunden ist (Purtova 2018).

Nur ein Teil des oben skizzierten Kreises energierelevanter Daten fällt unter personenbezogene Daten bzw. unterliegt dem Datenschutz. Bei jeder Erhebungsart (Stromzähler einschließlich Smart Meter, Sensoren, Mobiltelefone und PCs etc.) werden – je nach Einordnung nach der Definition in der EU-DSGVO – sowohl personenbezogene als auch nicht personenbezogene Daten gesammelt. Im Hinblick auf die Klassifizierung nach Energiesystem- und Kunden- bzw. Erzeugerdaten lässt es sich ebenfalls feststellen, dass in den beiden Kategorien sowohl personenbezogene als auch nicht personenbezogene Daten vorzufinden sind. Ohne die allerdings notwendige Einzelfallprüfung vorwegzunehmen, lässt es sich pauschal festhalten, dass Kundendaten tendenziell am meisten und die Systemdaten am wenigsten durch den Datenschutz geprägt sind. Aus der Perspektive eines Energieversorgungsunternehmens kann es sich bei personenbezogenen Daten vor allem um natürliche Personen handeln, die entweder seine Kunden, potenzielle Kunden oder andere Dritte sind. In einzelnen Fällen ist es jedoch denkbar, dass auch Messdaten von Gewerbe-, Handels- oder Industriekunden unter die DSGVO fallen. Dies wäre beispielsweise dann der Fall, wenn ein Zählpunkt sich auf eine Anlage oder ein Gebäude bezieht, die nur durch einen Mitarbeiter des Kunden gleichzeitig genutzt werden (bzw. bei mehreren, wenigen Mitarbeitern, wenn sich aus Stromverbrauchsdaten Informationen über einzelne Personen ableiten lassen). Im Bereich der Erzeugerdaten kommen insbesondere Daten zu dezentralen, von privaten Haushalten betriebenen Stromerzeugungsanlagen als personenbezogene Daten in Betracht. Soweit Daten von Verbrauchseinrichtungen bei Haushaltskunden zur Laststeuerung verwendet werden, ist deren Einordnung als systemrelevante personenbezogene Daten vertretbar.

Die beschriebenen Verhältnisse zwischen verschiedenen Kategorien energierelevanter Daten sind in → *Abbildung 3* schematisch dargestellt.

3.3.4 Vorgaben für einzelne Datenkategorien

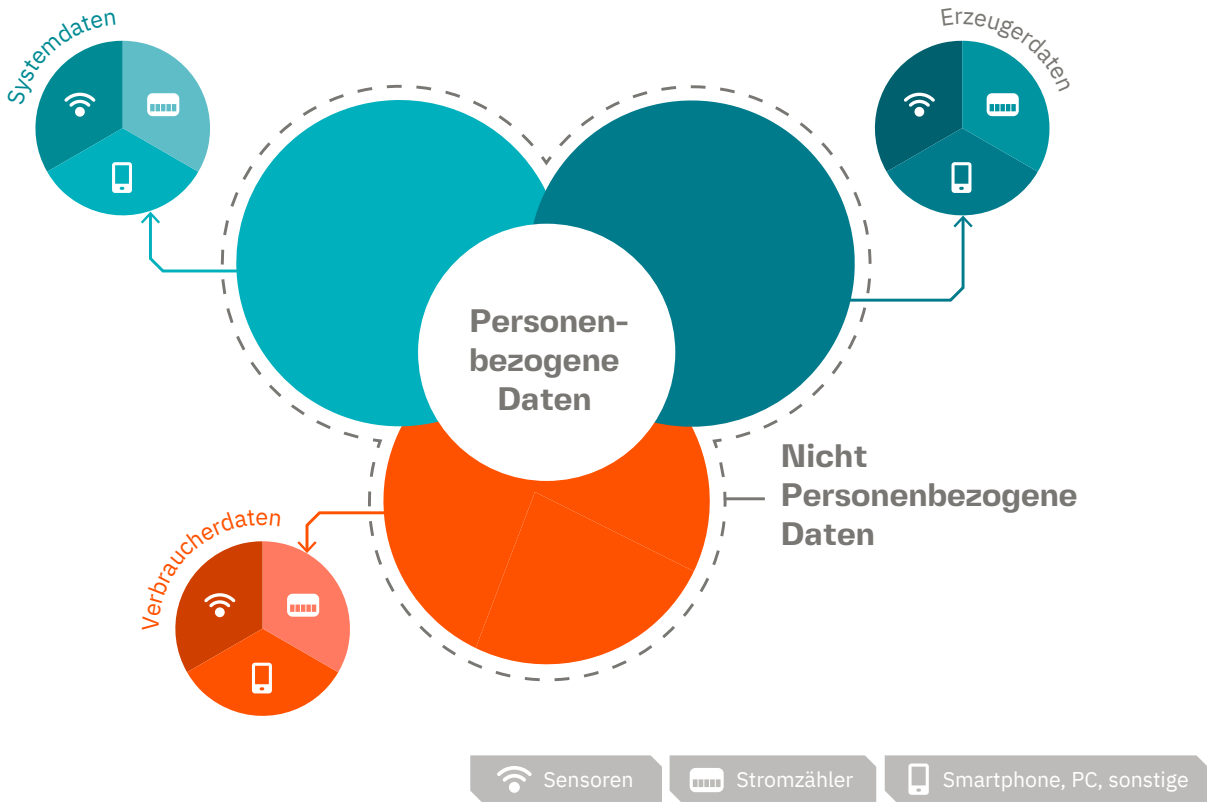
3.3.4.1 Vorgaben zum Datenschutz

Das komplexe Datenschutzregime für personenbezogene Daten nach der DSGVO[18] richtet sich nach den Grundsätzen der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, der Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie der Rechenschaftspflicht des Verantwortlichen bezüglich der Einhaltung der Datenschutzvorgaben

17 Verordnung (EU) 2016/679 vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Verkehr und zur Aufhebung der Richtlinie 95/46/EG.

18 Siehe eine Zusammenfassung von Datenschutzvorgaben beispielsweise in: dena 2018 und bei Spiecker genannt Döhmer, I. in: Doleski 2017.

Abbildung 3: Typologische Zusammenhänge energierelevanter Daten
Quelle: eigene Darstellung



bei der Datenverarbeitung (Art. 5 DSGVO). Während alle anderen Grundsätze sich auf die Art und Weise der Verarbeitung bereits erworbener Daten beziehen, sind vor allem die Rechtmäßigkeit und die Zweckbindung für den Zugang zu Daten relevant. Nach dem Rechtmäßigkeitsgrundsatz ist die Verarbeitung personenbezogener Daten, unter welcher jede Handlung von Erhebung bis zur Löschung verstanden wird, nur bei Vorliegen einer von mehreren eng vordefinierten Bedingungen möglich. Die Einwilligung der betroffenen Person ist unter diesen Bedingungen von primärer praktischer Relevanz, weswegen unsere nachfolgende Untersuchung sich auf diesen Fall fokussiert. Die Einwilligung unterliegt einer Reihe von Anforderungen wie Freiwilligkeit, Informiertheit, Bestimmtheit und Zweckbindung, Unmissverständlichkeit und Höchstpersönlichkeit (Lüdemann und Pokrant 2019). Die DSGVO gibt eine strenge Zweckbindung bei Erhebung und Verarbeitung personenbezogener Daten vor. Die informierte Einwilligung der Betroffenen muss sich bereits bei der Datenerhebung auf klar definierte Zwecke beziehen, welche bei späterer Nutzung der Daten einzuhalten sind (ebd.). Verwendung der Daten zu anderen, als bei der

Erhebung erklärten Zwecken ist in anonymisierter Form möglich.[19] Allerdings könnte sich dabei das Problem von fehlenden notwendigen Kontextdaten stellen (Webborn und Elam 2019). Gleichzeitig wird in der Literatur auf potenzielle Möglichkeiten hingewiesen, anonymisierte oder pseudonymisierte Daten zu personalisieren, beispielsweise durch Analyse in Kombination mit lokalen Wetterdaten mit der Anwendung Weatherman (Chen und Irwin 2017). Abweichend von dem allgemeinen Grundsatz der strengen Zweckbindung bei der Erhebung personenbezogener Daten ist deren spätere Nutzung u.a. für wissenschaftliche Forschungszwecke und statistische Zwecke zulässig. Im Hinblick auf den Zugang zu Energiedaten für die Entwicklung innovativer datenbasierter Produkte kann diese Berechtigungsgrundlage den Weg über wissenschaftliche Auseinandersetzung und erste Plausibilisierung neuer Geschäftsideen öffnen. In Abhängigkeit von dem Ergebnis der Hypothesenüberprüfung mit bereits verfügbaren Daten würden Investitionen in die Datenbeschaffung bzw. -erhebung dann erst im nächsten Schritt anfallen.

3.3.4.2 Daten aus Messeinrichtungen

Daten aus Stromzählern werden weitgehend als personenbezogene Daten eingestuft (Lüdemann und Pokrant 2019), obwohl dies nicht zwingend der Fall ist (Zwanziger 2019). So greifen die Datenschutzvorgaben i. d. R. nicht für große, von Unternehmen betriebene Stromerzeugungsanlagen und Stromkunden aus dem Industrie-, Gewerbe- und Handelsbereich mit Ausnahme solcher Messdaten, die Rückschlüsse auf einzelne natürliche Personen erlauben (s. o.).

Der eingesetzte Zählertyp hat hingegen keine Auswirkung für die datenschutzrechtliche Relevanz. Stromverbrauchswerte, die auf natürliche Personen zurückzuführen sind, werden schon dann als personenbezogene Daten eingestuft, wenn sie mit einem Standardlastprofil-Zähler (SLP) gemessen wurden.

Bereits der aggregierte monatliche Stromverbrauch eines Haushalts (Arbeitswert ohne den zeitlichen Lastverlauf) lässt sich beispielsweise auf seine Einkommenssituation schließen (Fratini und Pizza 2018).

Doch unabhängig von der Einordnung als personenbezogene Daten[20] (Lüdemann und Pokrant 2019) unterliegen Daten aus Stromzählern Einschränkungen, die den Datenschutzvorgaben ähnlich sind: mit Ausnahme einer abschließenden[21] Liste, gesetzlich vorgesehener Verarbeitungszwecke ist die Weitergabe an Dritte nur mit Einwilligung des Anschlussnutzers möglich.

Die gesetzlichen Fälle einwilligungsfreier Verarbeitung von Zählerdaten sind im deutschen Messstellenbetriebsgesetz festgehalten und umfassen vertragliche, vorvertragliche und gesetzliche Belange. Hierzu gehören insbesondere Strombelieferung einschl. Abrechnung, Stromeinspeisung einschl. Abrechnung, die Netzentgeltabrechnung, die Bilanzkreisbewirtschaftung, Bilanzierung und Bilanzkreisabrechnung, die Steuerung unterbrechbarer Verbrauchseinrichtungen in der Niederspannung nach §14a EnWG u. a. Für die nachfolgende Besprechung ist

> **// die Durchführung eines Mehrwertdienstes oder eines anderen Vertragsverhältnisses auf Veranlassung des Anschlussnutzers //**

als einen der gesetzlich begründeten Fälle der Datenverarbeitung gesondert zu erwähnen. Aus technischer Sicht werden die streng zweckgebundenen Berechtigungen zur Datenverarbeitung durch sternförmige Datenkommunikation für Messdaten aus Smart Metern sichergestellt (Privacy by Design) (BDEW 2019). Somit wird das Vertrauen durch verbindliche technische Vorgaben an die Produktkomponenten, den IT-Betrieb und die Kommunikationsinfrastruktur hergestellt (BSI 2020).

19 Siehe einen praktischen Leitfaden zu technischen Werkzeugen für Datenanonymisierung: Bitcom 2020.

20 Deutscher Bundestag, Drucksache 18/7555, S. 105.

21 Ebenda.

3.3.4.3 Entflechtungsvorgaben für Daten aus dem Netzbetrieb

Einem uneingeschränkten Zugriff auf energierelevante Daten stehen nicht nur der Schutz der Privatsphäre von Einzelnen, sondern auch die Sicherstellung operationeller Unabhängigkeit von Netzbetreibern als Voraussetzung für Wettbewerb in Stromerzeugung und -vertrieb entgegen. Nach Vorgaben der informatorischen Entflechtung hat die Weitergabe von Daten aus dem Netzbereich diskriminierungsfrei zu erfolgen. Wirtschaftlich sensible Informationen Dritter, von denen der Netzbetreiber durch die Wahrnehmung seiner Aufgaben Kenntnis erlangt, sollen vertraulich behandelt werden.

Da die Entflechtungsvorschriften mit der Sicherstellung eines unabhängigen, erzeugungs- und vertriebsneutralen Netzbetriebs begründet sind, wird die Identifizierung relevanter sensibler Informationen an die Ermittlung von kritischen Geschäftsprozessen angelehnt, in dessen Rahmen die Informationsflüsse analysiert werden. Die Bundesnetzagentur sieht folgende Bereiche als mit besonderem Diskriminierungspotenzial behaftet: Lieferantenwechsel, Netzanschluss, Netznutzung, Bearbeitung von Kundenanfragen und Kapazitätsprognosen (BNetzA 2007). Kapazitätsprognosen erfassen den Bedarf an Durchleitungskapazität unter Berücksichtigung von neu zugebauten Erzeugungskapazitäten und Änderungen der Last und dienen als Grundlage für die Netzausbauplanung. Diese Informationen sind beispielsweise für den Anschluss neuer Anlagen von Bedeutung. So ist auf der Webseite von Amprion ein Lastflussmodell auf Anfrage, unter Darlegung eines berechtigten Interesses verfügbar.[22]

Sobald Informationen aus dem Bereich des Netzbetriebs an einen Dritten weitergegeben werden, sind sie gegenüber allen potenziellen Interessenten offen zu legen, um eine diskriminierungsfreie Behandlung von mit dem Netzbetreiber assoziierten und allen anderen Marktakteuren sicherzustellen. Wie oben erwähnt, entstehen durch die diskriminierungsfreie Veröffentlichungspflicht allgemein zugängliche energierelevante Daten. Zugleich führt die informatorische Entflechtung dazu, dass einige Daten, auch wenn sie bei dem Netzbetreiber vorhanden und wirtschaftlich wertvoll sind – auch für die Entwicklung neuer Produkte – vertraulich bleiben und nicht an assoziierte Vertriebseinheiten weitergegeben werden dürfen. Diese regulatorische Schranke dient der Gleichbehandlung aller Marktakteure. Dementsprechend muss ein Stromanbieter beispielsweise Informationen zum Wechselverhalten fremdversorgter Kunden durch eigene Bemühungen (etwa Umfragen) sammeln, obwohl sie der konzernzugehörigen Netzgesellschaft vorliegen.

Aus der obigen Darstellung wird ersichtlich, dass der Zugang zu einem großen Teil energiewirtschaftlicher Daten nur mit Einwilligung der Betroffenen bzw. Anschlussnutzer möglich ist. Dies betrifft in erster Linie alle Daten aus Stromzählern unabhängig von deren datenschutzrechtlichen Einordnung. Aber auch für die Datenerhebung durch Sensoren, Apps und auf anderen Wegen ist die Einwilligung notwendig, soweit es sich um personenbezogene Daten handelt. Für ein Unternehmen, das auf diese Daten für Entwicklung digitaler Produkte oder Prozessoptimierung angewiesen ist, bedeutet die Einwilligungspflicht, dass sie mit den Kunden in Kontakt treten müssen, um deren Einwilligung für die Datenverwendung zu sichern.

22 https://www.amprion.net/Strommarkt/Netzkunde/Netzanschlussregeln/Kraftwerke.html

:// 4. DATENBASIERTE MEHRWERTE

4.1 Datenbeschaffung aus Kunden- und Unternehmensperspektive

Bei der Entwicklung neuer digitaler Lösungen lassen sich im Hinblick auf die Daten zwei Handlungsfelder identifizieren. Einerseits stellen Daten einen essenziellen Input für die Produkt- bzw. Prozessentwicklung dar. Für die Verarbeitung von Messdaten und (nicht verlässlich anonymisierten) personenbezogenen Daten[23] ist eine Einwilligung der betroffenen Person bzw. des Anschlussnutzers notwendig. Aus ökonomischer Sicht stellt dies die Entwickler vor die Notwendigkeit, der Einhaltung von Datenschutzvorgaben, den Betroffenen eine Gegenleistung in einer adäquaten Form und Höhe anzubieten. Insofern handelt es sich dabei um Kosten, die mit den zu erwerbenden Daten der Datensubjekte[24] verbunden sind. Hinzu kommen der Kommunikationsaufwand, um die Einwilligung einzuholen, plus ggf. die Kosten der DSGVO-Compliance.

Auf der Profit-Seite stellt sich die Herausforderung, dass die entwickelte datenbasierte Lösung einen Mehrwert generieren muss. Diese Fragestellung ist unabhängig von dem Aufwand der Datenbeschaffung zu betrachten. Denn auch um aus bereits im Unternehmen vorhandenen Daten einen Mehrwert zu generieren, fallen Kosten bei der Datenverarbeitung an (dies entspricht Speicherung, Datenanalyse und Umsetzung von abgeleiteten Handlungsoptionen) (Oswald und Kleinemeier 2017; Moro Visconti et al. 2017).

Je nach konkretem Geschäftsfall kann der Personenkreis von Anschlussnutzern, Kunden und anderen Betroffenen, zu deren Daten nicht nur ein Zugang benötigt wird, sondern denen ein datengestütztes Produkt angeboten werden soll, zusammen- oder auseinanderfallen. Ein Geschäftsmodelltyp, bei dem solche Personenkreise zusammenfallen, sind sog. Mehrwertdienste. Beispielsweise werden im Rahmen eines Vertragsverhältnisses mit dem Kunden (etwa Strombelieferung) Daten erhoben, mit deren Hilfe das Unternehmen sein Angebot an diesen Kunden verbessern oder erweitern kann. Die Datensubjekte sind somit gleichzeitig auch die Zielgruppe für die neuen Mehrwertdienste.

Hingegen sind Energieplattformen ein Beispiel dafür, wie Personen, deren Daten erhoben werden, und potenzielle Kunden, denen ein daraus abgeleitetes Wertversprechen angeboten wird, auseinanderfallen können. Beispielsweise ermöglicht die Lösung powerfox durch den Einbau eines Hardware-Moduls bei Stromverbrauchern, Messwerte in Echtzeit abzulesen und zu übermitteln. Im Gegenzug profitieren die Stromverbraucher von der Visualisierung ihrer Energiedaten in der powerfox-App. Die erhobenen Daten werden (mit Einwilligung der jeweiligen Stromverbraucher bzw. Anschlussnutzer) über eine Plattform Dritten zur Verfügung gestellt. Alternativ nutzt der Plattformbetreiber die Energiedaten selbst für die Entwicklung innovativer

23 Wie oben im Kapitel dargestellt, überschneiden sich diese Datentypen teilweise.

24 Bei Datensubjekten handelt es sich um betroffene Personen im datenschutzrechtlichen Sinne und Anschlussnutzer in Bezug auf Messdaten. Für unsere Zwecke wird dies gemeinsam betrachtet, da in beiden Fällen eine Einwilligung zur Datenweitergabe erforderlich ist.

Kundenlösungen.[25] Die Datensubjekte sind in diesem Fall daher meist nicht die Zielgruppe von Mehrwertdiensten oder anderen Produkten, da der Datenverwalter, hier die Plattform, als ergebnisoffener Ort fungiert und jeder Interessierte die Möglichkeit hat auf die Daten, je nach Lizenzierungsart, zuzugreifen.

Ein weiteres Beispiel zeigt mögliche Kombinationen aus beiden Geschäftsmodelltypen. Der kommerzielle Messstellenbetreiber Solandeo verwendet Messdaten aus den von der Firma betriebenen Messsystemen bei EE-Stromerzeugern zur Erstellung von Erzeugungsprognosen. Als Gegenleistung für die Einwilligung der Verwendung von Messdaten erhalten die EE-Anlagenbetreiber Prognosedaten. Daneben bietet Solandeo die erstellten Prognosen auch anderen Marktakteuren an, und nicht nur seinen Kunden im Bereich Messstellenbetrieb.[26]

Die beiden Gesichtspunkte – der Zugang zu Daten einzelner Stromkunden und der mithilfe der Daten generierte Mehrwert – werden nachfolgend separat untersucht und im Anschluss der Zusammenhang aufgezeigt. Die Basis bilden unterschiedliche vorgefundene Kategorisierungen in der Literatur zu datengetriebenen Mehrwerten, die anhand der vorgeschlagenen Unterteilung in die Kunden- und Unternehmensperspektive systematisiert und besprochen wird. Dabei werden sowohl branchenübergreifende Konzepte zu Big Data als auch Abhandlungen mit Bezug auf die Energiewirtschaft und angrenzende Sektoren wie Gebäude und Mobilität einbezogen.

4.2 Vergütungsformen für die Daten

Aus der Kundenperspektive lässt es sich bei den Vergütungsformen für die Datenweitergabe zwischen monetären und nichtmonetären Vorteilen unterscheiden.

Zu monetären Mehrwerten zählen insbesondere: Zahlungen für Daten, Kostenersparnisse durch Energieeinsparung und Kostenersparnisse durch einen reduzierten Preis für ein Produkt.

Bisher sind uns keine existierenden Geschäftsmodelle im Energiebereich bekannt, in denen Kunden für ihre Daten mit Geldbeträgen vergütet worden wären. Ein eher traditionelles, aber dennoch valides Beispiel aus aktuell gängiger Praxis sind bezahlte Online-Umfragen, meist zu Marktforschungszwecken. Parallel zur Entwicklung von Online-Plattformen, die Kunden den Verkauf ihrer Daten ermöglichen, werden auch wissenschaftliche Studien durchgeführt, die die Bereitschaft der Datenweitergabe gegen Geldbeträge von Einzelpersonen untersuchen. Insbesondere wurde angestrebt die Wertigkeit der Daten für die Datensubjekte anhand akzeptabler Geldbeträge empirisch zu eruieren. Einige Ergebnisse dieser Untersuchungen werden im → *Kapitel 4.3* Einflussfaktoren für die Bereitschaft zur Datenweitergabe vorgestellt.

Dass Kostenersparnisse durch Energieeinsparung Ergebnis eines Mehrwertdienstes sein können, zeigt beispielsweise die Visualisierung des Stromverbrauchs. So unterstreicht der wettbewerbliche Messstellenbetreiber Discovergy in seinem Angebot an Stromhaushaltskunden die umfassende Kontrolle über die Stromkosten durch die Visualisierung von Messdaten aus einem Smart Meter in einer App. Neben der reinen Visualisierung auf Anschlussebene macht die App durch maschinelles Lernen die Verbrauchsprofile einzelner Geräte innerhalb eines Haushalts für die Kunden erkennbar.[27]

In der Kosten-Nutzen-Analyse für den Roll-Out intelligenter Messsysteme in Deutschland wird bei

25 Vgl. https://www.powerfox.energy/ueber-powerfox/

26 Vgl. https://www.solandeo.com/produkte/prognosen/ https://www.strommarkttreffen.org/2019-06-07_Rojahn_Schuermann_Portfolio_Bewirtschaftung_mit_Auto-Trading_und_maschinellem_Lernen.pdf

27 Vgl. https://discovergy.com/files/images/Blog/MessstellenbetreiberWechseln/wettbewerblicher-messstellenbetrieb.pdf

möglichen Mehrwerten für Endkunden für die Weitergabe von Messdaten – neben kundenindividuellen Produkten – erwähnt, dass ein Stromlieferant seinen Kunden einen Abschlag auf den Strompreis anbieten kann (Ernst & Young 2013). Wettbewerbliche Messstellenbetreiber bieten u.a. einen kostenfreien Einbau intelligenter Messsysteme und/oder günstigere Entgelte für den Messstellenbetrieb, im Vergleich mit den regulierten Entgelten von Netzbetreibern als grundzuständigen Messstellenbetreibern an.

Unter nichtmonetären Vorteilen, die Kunden im Austausch für ihre Daten angeboten werden können, sind vor allem Mehrwerte in Form von Mehrwertdiensten zu erwähnen. Ein Mehrwertdienst ist ein sehr weit genutzter, aber nicht eindeutig definierter Begriff. Dies stellten beispielsweise Meyer und Blümelhuber (2000) fest. Im Gegensatz zu dem verbreiteten Verständnis eines Mehrwertdienstes als eine Zusatzdienstleistung mit einem ergänzenden Charakter, schlagen die Autoren ihre eigene Definition vor, die auf zwei Kriterien basiert. Erstens ist ein Mehrwertdienst kein Kernprodukt des Unternehmens, sondern hat einen komplementären Charakter. Dabei wird das Zusatzangebot als ergänzende Komponente in Verbindung mit einem Produkt oder Serviceangebot vermarktet. Zweitens zeichnen sich Mehrwertdienste durch ihre Funktion aus, die Gewinnung von Neukunden zu erleichtern und/oder die Loyalität von Bestandskunden zu stärken. Die im Austausch für Daten angebotenen Mehrwertdienste müssen nicht zwingenderweise datengetrieben sein. Bei datenbasierten Mehrwerten nimmt das Smart Meter Gateway als zentrale Kommunikationseinheit in Haushalt in Zukunft eine wichtige Rolle ein und bietet Drittanbietern Anbindungsmöglichkeiten für die Entwicklung von datenbasierten Mehrwertdiensten.

Neben Mehrwertdiensten könnten Kunden im Austausch für ihre Daten von einer verbesserten Nutzererfahrung bei demselben Produkt profitieren (Catapult Energy Systems 2018). Dies ist insbesondere dann der Fall, wenn die Daten genutzt werden, um unternehmensinterne Prozesse zu optimieren.

Eine weitere denkbare Kategorie nichtmonetärer Vorteile, die Kunden aus der Weitergabe ihrer Daten erwachsen könnten, sind ideeller Natur. In einer Umfrage finnischer Stromverbraucher untersuchten (Immonen et al. 2020) u.a. mögliche Beweggründe in den Einbau von Smart Metern und die Anschaffung intelligenter, ferngesteuerter Geräte und Systeme zu investieren. Als einer solcher Beweggründe wurden in einer offenen Frage mit freier Texteingabe u.a. „ökologische Vorteile und Umweltschutz“ angegeben. Da der Betrieb von Smart Home-Lösungen eng mit der Verwendung der erhobenen Daten durch den Anbieter zusammenhängt, ist daher durch weitere Umfragen zu untersuchen, inwiefern ein konkreter Klimaschutzbeitrag der datenbasierten Lösung ein Anreiz für Kunden sein kann, ihre Daten mit dem Produktentwickler zu teilen. Es lässt sich vermuten, dass, wenn ein ideeller Vorteil aus Datenweitergabe an die Kunden vermittelt wird, der Zweck der Datennutzung und die Identität des datenverarbeitenden Unternehmens eine besonders wichtige Rolle spielen. Denkbar ist dies bei der Gewinnung von Teilnehmern für öffentlich geförderte Energiedatenplattformen für Forschungszwecke, wie das vorgehend vorgestellte britische Smart Energy Research Lab.

Welche Art der Vergütung dem Datensubjekt angeboten werden sollte, hängt einerseits von den damit verbundenen Kosten für das Unternehmen und andererseits von der Wahrnehmung und den Präferenzen des Datensubjektes ab. Dementsprechend ist eine Bewertung aus beiden Perspektiven notwendig.

Aus der Sicht eines Unternehmens, das einen Zugang zu energierelevanten Daten benötigt, ist generell davon auszugehen, dass Vergütungsformen mit den niedrigsten Opportunitätskosten vorgezogen werden, um die Kosten der Datenbeschaffung zu minimieren. Besonders attraktiv erscheint dabei ein Geschäftsmodell, bei dem dieselbe datenbasierte Lösung sowohl den Datenlieferanten als auch einem weiteren Kundenkreis angeboten wird, wie beispielsweise im oben beschriebenen Fall von

Solandeo. Das Unternehmen stellt die Erzeugungsprognosen sowohl einzelnen Betreibern von Erneuerbaren Erzeugungsanlagen als seinen Datenlieferanten als auch anderen Marktakteuren zur Verfügung. Vor dem Hintergrund der Einwilligungspflicht für die Datenverarbeitung ist ein direkter individueller Kommunikationskanal zu einzelnen Kunden und wirksame Kommunikation unerlässlich. Unternehmen ohne direkten Kundenkontakt im Rahmen eines Geschäftsverhältnisses bzw. einer Dienstleistung sind darauf angewiesen, solche Kontakte – etwa durch ein Dienstleistungsangebot aufzubauen. Anderenfalls könnten sie Daten ggf. über Datenplattformen beziehen, wobei das Unternehmen in diesem Fall keinen unmittelbaren Einfluss auf das Datenformat und möglicherweise keinen Zugang zu benötigten Kontextdaten hat.

Während bei neuen digitalen Produkten ein Mehrwert an die Kunden kommuniziert bzw. von diesen wahrgenommen wird, bleibt er im Falle von datenbasierten Verbesserungen unternehmensinterner Prozesse (auch wenn diese zu einem verbesserten Kundenerlebnis führen) für die Kunden unsichtbar.

Bei der Kommunikation des angebotenen Mehrwertes an die Kunden empfehlen Morey et al. (2015) mit Datenarten von einem geringen Wert anzufangen und im Gegenzug eine greifbare Verbesserung des Nutzererlebnisses anzubieten, um die Kunden dadurch zu motivieren, weitere Daten zu teilen. Allerdings stellt sich bei dieser Vorgehensweise das Problem mit mehrfachem Kundenkontakt zwecks Einwilligung der Datenverarbeitung, der bereits dann eine Hürde für die geplanten Aktivitäten darstellen dürfte, wenn er nur einmalig stattfindet – sowohl bei Bestands- als auch bei Neukunden.

Soweit es sich um keine Messdaten und keine personenbezogenen handelt, ist die Datenerhebung durch unternehmenseigene Geräte (beispielsweise Temperatursensoren) eine denkbare Alternative zur kundenindividuellen Einholung von Einwilligung für die Datenweitergabe. Anders als bei Stromzählern fallen dabei Einbau-, Betriebs- und Wartungskosten an. Je nach Einbauort und -kontext könnte ein zusätzlicher Abstimmungsaufwand mit den Anlagenbetreibenden anfallen.

4.3 Einflussfaktoren für die Bereitschaft zur Datenweitergabe

Neben den Kostenbetrachtungen und der unternehmensspezifischen Ausrichtung des Unternehmens hinsichtlich der Kundenkommunikation spielt die Kundenperspektive bei der Datenweitergabe eine wichtige Rolle. Während sich monetäre Kundenvorteile im Austausch für Daten direkt quantifizieren lassen, gestaltet es sich bei nichtmonetären Vorteilen deutlich schwieriger. Der wahrgenommene Nutzen ist subjektiv und kundenspezifisch. Auch bei monetären Vorteilen (etwa einer erzielten Energiekosteneinsparung durch Stromeinsparung oder innovative Tarife) kommt es darauf an, ab welcher Betragshöhe die entsprechenden Angebote für die Kunden hinreichend attraktiv sind, um sie zum Teilen von Daten anzureizen.

Soweit aus einer gezielten Literaturrecherche über Google Scholar ersichtlich, gibt es bisher nur wenige empirische Studien, die die Einstellung einzelner Personen zur Datenweitergabe im Hinblick auf die akzeptable Form und Höhe der Vergütung als auch auf Transparenz, Vertrauen und weitere relevante Faktoren untersuchen. Die identifizierte Literatur ist in Tabelle 3 zusammengefasst. Obwohl die empirischen Daten in den Veröffentlichungen geografisch, thematisch (bzgl. untersuchter Produkte bzw. Datenarten) und methodisch heterogen und nur eingeschränkt miteinander vergleichbar sind, bieten sie einen Einstieg in die Fragestellung und lassen gemeinsame Themen erkennen, die weiterführende Forschung motivieren. Vor diesem Hintergrund wurden insbesondere erkennbare Qualitätsunterschiede bei der methodischen Konzeption der Umfragen nicht berücksichtigt.

Tabelle 3: Übersicht empirischer Studien zur Datenweitergabe aus Kundenperspektive

Veröffentlichung	Studienteilnehmer	Produkt(e)	Datenart(en)	Untersuchte Einflussfaktoren
Grünewald und Reisch 2020	701 Einwohner Großbritanniens, über 18 J. alt	Smart Home	Standortdaten	Vertrauen, Datenhoheit
TÜV Rheinland 2020	334-653 Teilnehmer, Deutschland (online)	Smartphones, smarte Lautsprecher, vernetzte Fahrzeuge	Nutzungsverhalten, Fotos und Videos, Passwort- und Logindaten, Fahr- und Geschwindigkeitsprofile, Sensordaten	Datenwissen, Vertrauen, Datenwert bzw. Monetarisierung
Rickert 2016	78 Teilnehmer aus dem Bekanntenkreis der Autorin, über 18 J. alt, international (überwiegend deutsch und niederländisch)	IoT-Geräte	k. A.	Bereitschaft der Datenweitergabe an Dritte, Vertrauen und Transparenz
Morey et al. 2015	Zusammengetragen aus verschiedenen Quellen	intelligente, vernetzte Produkte einschl. Smart Home	diverse Datenkategorien, u. A. Gesundheitsdaten, digitale Kommunikation, Standortdaten, demografische Daten, Energieverbrauch	Datenwissen, Vertrauen, Datenwert bzw. Monetarisierung
Immonen et al. 2020	2110 finnische Stromverbraucher	fernsteuerbare, intelligente Geräte	k. A.	Datenverwertung, Datenhoheit, Fernsteuerbarkeit
Hellmuth und Jakobs 2020	15 deutsche Mieter zwischen 24-40 Jahren mit einem mittleren Einkommen und akademischen Hintergrund	Smart Meter	personenbezogene und nicht personenbezogene Daten aus Smart	Bereitschaft an Datenweitergabe an Metern Dritte

Angesichts der Hinweise in der Literatur auf Zusammenhänge zwischen der Vergütung für Daten und anderen relevanten Faktoren für die Datenweitergabe, werden die beiden Voraussetzungen zusammen besprochen. So stellten Morey et al. (2015) beispielsweise in einer internationalen Umfrage fest, dass eine angebotene monetäre Vergütung die Bereitschaft Daten zu teilen sogar verringern könnte.

Neben der Vergütung für die Weitergabe von Daten – und im Allgemeinen dem Vorteil für die Datensubjekte – wird in der Literatur deren subjektive Einstellung gegenüber der Datenweitergabe thematisiert. Im Vordergrund steht dabei das Vertrauen. Hierzu liegen mehrere empirische Untersuchungen zu möglichen Einflussfaktoren vor, die die Kundenbereitschaft beeinflussen Daten an Gerätehersteller und andere Unternehmen und Organisationen weiterzugeben. Die Studien beschränken sich typischerweise auf einen Produkttyp (Smart Home, vernetzte Fahrzeuge usw.).

Nachfolgend werden die Umfrageergebnisse zu den wichtigsten untersuchten Faktoren für die Bereitschaft Einzelner zur Datenweitergabe zusammengefasst.

1. Datenarten: Morey et al. (2015) kommen zum Ergebnis, dass Kunden eigens angegebenen Daten den geringsten und Profiling-Daten den größten Wert beimessen. In einem Online-Experiment im

Rahmen der TÜV-Studie zu Daten aus vernetzten Fahrzeugen, demonstrierten die Teilnehmer eine höhere Bereitschaft gerätebezogene Daten mit Dritten zu teilen als etwa private Kommunikationsinhalte oder andere Daten, aus denen sich persönliche Informationen ableiten lassen, beispielsweise Mobilitätsprofile (TÜV Rheinland 2020). In der Mieterumfrage von Hellmuth und Jakobs (2020) zu Daten aus intelligenten Messsystemen, wurde ein deutlicher Unterschied zwischen personenbezogenen und nicht personenbezogenen Daten dokumentiert.

2. Identität des Datennutzers: Hellmuth und Jakobs (2020) stellten in einer Mieterumfrage eine höhere Bereitschaft fest, Daten an Wissenschaftler für Forschungszwecke weiterzugeben als an Stromanbieter. In der deutschen Studie für (TÜV Rheinland 2020) wurde das Vertrauen gegenüber Geräteherstellern und unterschiedlichen Datentreuhändertypen – einem deutschen Telekommunikationsunternehmen, dem deutschen Staat, Universitäten und einer unabhängigen Organisation wie TÜV – miteinander verglichen und ein deutlich höheres Vertrauen gegenüber unabhängigen Datentreuhänder sowie universitären Einrichtungen festgestellt.

3. Vergütungshöhe/Gegenwert: Erste Untersuchungen wie Morey et al. (2015) und TÜV Rheinland (2020) zeigen, dass bei Einzelpersonen grundsätzlich die Bereitschaft zum Datenteilen existiert. Je privater die Datenart war, desto höher wurde der Verkaufspreis von den Befragten angegeben. Die Vergütungsspanne reichte dabei von einigen wenigen Euro im einstelligen Bereich für umgebungs- und gerätebezogene Daten von intelligenten Geräten, bis hin zu vierstelligen Beträgen für Mediendaten und Passwörter bzw. Login-Daten. Morey et al. zeigen weiterhin, dass, wenn Daten verwendet werden, um ein Produkt oder eine Dienstleistung zu verbessern, die Verbraucher im Allgemeinen die Verbesserung selbst als einen fairen Austausch (fair trade) für ihre Daten empfinden. Der Wert, den die Verbraucher ihren Daten beimessen, steigt mit der vorher erwähnten Personenbezogenheit, die das Unternehmen durch Analysen ableiten kann, und nimmt dabei weiter in dem Maße zu, in dem ihre Verwendung nicht mehr in erster Linie dem Verbraucher (in Form von Produktverbesserungen), sondern vor allem dem Unternehmen (in Form von Einnahmen aus dem Datenverkauf) zugutekommt (Morey et al. 2015). Die erwarteten Gegenwerte von ferngesteuerten, intelligenten Haushaltsgeräten sind in den meisten Fällen (mehr als 90%) die Senkung der Stromrechnung, gefolgt von der Unterstützung von Emissionsreduktionen (ca. 50%) (Immonen et al. 2020).

4. Transparenz/Datenhoheit: Grünewald und Reisch (2020) zeigen in ihrer Umfrage, dass ein der Großteil der Befragten Schwierigkeiten hat den Unterscheid zwischen der Datennutzung selbst und den Organisationen, die letztendlich Zugriff auf die Daten haben, zu verstehen. Bei dem Beispiel der Standortdaten wird dies sehr deutlich, da die meisten Menschen bereits von „Unbehaglichkeit“ sprechen, wenn es um die Kontrolle bzw. die Datenhoheit dieser Daten geht. Die Datensammlung Dritter sei nicht mehr unter ihrer Kontrolle, heißt es dort. Weiter beschreibt Rickert (2016), dass bei der Existenz von Transparenz, Menschen bereitwilliger sind ihre Daten zu teilen, als ohne. Weitere Hinweise zur Datenhoheit finden sich bei Immonen et al. (2020). Die mehr als die Hälfte Befragten der hatten prinzipiell kein Problem mit der Fernsteuerung intelligenter Geräte, solange die Nutzung nicht eingeschränkt und weiterhin eine vom Nutzer gesteuert Limitierung der Kontrolle möglich ist.

Aus der Zusammenschau vorhandener Literatur ist Bedarf nach weiteren empirischen Untersuchungen zu den Einflussfaktoren erkennbar, die sich auf die Bereitschaft der Kunden auswirken, ihre energierelevanten Daten mit interessierten Unternehmen und Organisationen zu teilen.

Die besprochenen Studien richten sich an Privatpersonen bzw. Haushalte. Da der Zugang zu Messdaten auch dann einwilligungsbedürftig ist, wenn sie nicht personenbezogen sind, d. h. in der Regel im Falle von Gewerbe-, Handels- und Industriekunden, stellt sich dieselbe Frage auch im B2B-Verhältnis. Auch hier besteht ein weiterer Untersuchungsbedarf.

4.4 Datenbasierte Mehrwerte aus Unternehmensperspektive

Nachdem der Zugang zu Daten im Hinblick auf die Kundeninteraktion beleuchtet wurde, ist ebenfalls zu berücksichtigen, dass der Aufwand der Datenbeschaffung mit dem Mehrwert ins Verhältnis gesetzt werden muss, den das Unternehmen mithilfe der Daten schaffen kann. Nachfolgend wird vorhandene Literatur zum Mehrwert bzw. zur Monetarisierung vorgestellt, und zwar sowohl im Kontext von digitalen Technologien und Daten bzw. Big Data allgemein als auch sektorspezifisch im Kontext der Energiewirtschaft. Die unterschiedlichen vorgefundenen Kategorisierungen werden systematisiert und diskutiert.

Zunächst ist grundlegend zwischen unternehmensinternem und unternehmensexternem Mehrwert zu unterscheiden (Faroukhi et al. 2020). Beispielsweise kann eine datengetriebene Prozessoptimierung zu einer Kostensenkung führen, die für das Unternehmen einen Wettbewerbsvorteil darstellt und nicht zwingend an Kunden weitergegeben werden muss. Andererseits kann sie auch auf ein verbessertes Nutzererlebnis abzielen und hätte in diesem Fall Auswirkungen auf die Kunden.

Elia et al. (2020) beschreiben den Mehrwert, der mithilfe von Big Data geschaffen werden kann, als ein sehr breites Konzept. Es erstreckt sich über die ökonomischen und finanziellen Aspekte hinaus über unterschiedliche strategische Vorteile bis hin zu Vorteilen für die Allgemeinheit im Hinblick auf die soziale Verantwortung eines Unternehmens. In diesem Zusammenhang ist anzumerken, dass nicht alle diese Dimensionen ohne Weiteres quantifizierbar sind (z. B. strategische Vorteile).

Anknüpfend an einen konzeptionellen Rahmen von Wamba et al. (2015), identifizieren die Autoren elf Richtungen von datenbasierter Wertschöpfung:

- *Marktpositionierung*
- *Marktreaktivität*
- *bessere Kundenbindung*
- *neue Fertigkeiten*
- *höhere Erträge*
- *höhere Produktivität*
- *Kostenersparnisse*
- *Unterstützung bei Entscheidungsfindung*
- *neue Erkenntnisse*
- *organisatorische Vorteile*
- *verbesserte IT-Infrastruktur*

Die vorgeschlagenen Richtungen sind in fünf Dimensionen gruppiert: sie beziehen sich auf Informationen, Transaktionen, Transformation, Strategie und Infrastruktur. Die meisten der aufgelisteten Aspekte beziehen sich auf das Unternehmen selbst und beschreiben unterschiedliche Kompetenzen, die sowohl firmenintern als auch -extern eingesetzt werden können.

Die notwendigen Schritte, um aus rohen Daten einen Mehrwert zu generieren, sind in dem Konzept einer Datenwertschöpfungskette abgebildet. Diese beinhaltet die Datenerhebung, -bearbeitung, -analyse und den Datenaustausch (Faroukhi et al. 2020). In Anlehnung an dieses Konzept identifizierten Cavanillas et al. (2016) unterschiedliche Wege, auf

denen ein Mehrwert aus Daten entstehen kann: durch Datenbeschaffung, Kombination von Daten aus verschiedenen Quellen und Sektoren, einen erleichterten Datenzugang, verbesserte Datenqualität, Sicherstellung der Datenintegrität, durch Datenanreicherung, Gewinnung neuer Erkenntnisse sowie durch einen wirksamen Datenschutz. All diese Wege (außer dem Datenschutz) beziehen sich auf den Prozess der Datenverarbeitung selbst, so dass Rückkopplung auf die Stufen von Datenanalyse naheliegt.[28]

Eine erweiterte Sicht bietet die herkömmliche Wertschöpfungskettenanalyse. Im energiewirtschaftlichen Kontext wurde dieser Ansatz beispielsweise in der bereits besprochenen Kosten-Nutzen-Analyse von Ernst & Young zum Einbau intelligenter Messsysteme in Deutschland umgesetzt. In der Studie wurden zunächst drei Bereiche identifiziert, in welchen aus intelligenten Messsystemen ein Nutzen erwachsen kann: Stromkosteneinsparung, vermiedene Investitionen in Netze und Kraftwerkskapazitäten und Optimierung von Prozessen (beispielsweise Abrechnung und Zählerablesung). Im nächsten Schritt wurden unmittelbare Auswirkungen auf verschiedene Marktakteure (Stromlieferant, Netzbetreiber, Endkunde usw.) aufgezeigt. Die sparten- bzw. marktrollenspezifischen Mehrwerte wurden schließlich quantifiziert (Ernst & Young 2013).

Die vorgestellte Betrachtung eignet sich, um zu analysieren, wie der generierte Mehrwert entlang der Wertschöpfungskette weitergegeben wird. Allerdings ist auch die Option zu beachten, rohe Daten und daraus erstellte Analysen an andere Marktakteure zu verkaufen – sowohl innerhalb als auch außerhalb der Energiebranche. In diesem Sinne unterscheiden Morey et al. (2015) drei allgemeine Nutzungsarten von bzw. Mehrwerte aus Daten: verbesserte Angebote (Waren und Dienstleistungen), verbesserte Marketing bzw. Werbung und Veräußerung von Daten an Dritte. Im Energiekontext findet sich eine eng daran angelehnte Kategorisierung der Bereiche für datenbasierte Mehrwerte bei Catapult Energy Systems (2018): Beziehungen zu Kunden, optimierter Systembetrieb für einen besseren Ausgleich von Stromerzeugung und -verbrauch und Datenverwendung außerhalb der Energiebranche.

An dieser Stelle liegt der Fokus auf dem tatsächlich generierten Wert aus Daten. In diesem Zusammenhang stellt sich die mehrfach in der Literatur thematisierte Herausforderung, dass zum Zeitpunkt der Datenerhebung bzw. -beschaffung der erzielbare Mehrwert i. d. R. nicht vorhersehbar ist, insbesondere aufgrund mehrfacher möglicher Verwendung der Datensätze für verschiedene Zwecke (Ducuing 2019). Gleichzeitig steigt der aus Daten zu generierende Mehrwert exponentiell, wenn Daten aus verschiedenen Quellen zusammengeführt werden (Moro Visconti et al. 2017). Der Datenwert für das Unternehmen und die Kundenbereitschaft zur Weitergabe sollten aufeinander abgestimmt sein.

28 Eine genauere Analyse der Datenwertschöpfungskette könnte es ermöglichen den Datenverarbeitungsprozess zu optimieren. → Teil 2 dieses Kompendiums bietet weiterführende Einblicke in eine systematische Bestandsaufnahme von vorhandenen IT-Systemen (Hardware, Software und Datenbanken) zum Beispiel mittels Erstellung von IT-Landkarten.

:// 5.
FAZIT UND DISKUSSION

Diese Untersuchung leitet die nachfolgende Besprechung einzelner Digitalisierungsthemen in der Energiewirtschaft mit einer systematischen Erörterung des Digitalisierungsbegriffs ein. Um den besonderen Merkmalen der Stromversorgung Rechnung zu tragen, haben wir – zusätzlich zum allgemeinen Digitalisierungsdiskurs – den Bezug von Digitalisierungsprozessen zu den energiepolitischen Zielen herausgestellt. Daraus ergeben sich Sicherheitsanforderungen als ein wichtiger Aspekt der Digitalisierung. Dies beinhaltet sowohl die Cybersicherheit als eine Voraussetzung für einen zuverlässigen Stromnetzbetrieb als auch den potenziellen Beitrag digitaler Technologien zur Systembilanzierung. Dementsprechend wurden bei der Digitalisierung im energiewirtschaftlichen Kontext vier Felder identifiziert: Vernetzung, Sicherheit, Daten und Mehrwert.

Für die Auseinandersetzung mit dem Zugang zu Daten als eine essenzielle Voraussetzung für digitale Innovationen im Energiebereich sind wir von einem weiten Verständnis energierelevanter Daten ausgegangen. Der verwendete Begriff geht über die Messdaten und Energiesystemdaten hinaus und bezieht ein breites Spektrum weiterer, nicht nur energiespezifischen Daten mit ein, die in datenbasierte Innovationen für die Energiewirtschaft einfließen. Wir konnten beobachten, dass öffentlich zugängliche Energiedaten weiterhin größere Zugangs- und Qualitätseinschränkungen aufweisen. Daher wird es in Zukunft unabdingbar sein, Daten in definierter Konsistenz und Qualität zu erheben und den Open-Data-Veröffentlichungsansatz zu stärken. Projekte wie die Green Button Initiative oder die European Open Science Cloud (EOSC) können dabei als geeignete Vorbilder fungieren. Es empfiehlt sich weiterhin den tatsächlichen Datenbedarf (Datenarten, -qualität, zeitliche und anlagenspezifische Auflösung, Aggregationsgrad usw.) bei verschiedenen Marktakteuren etwa durch gezielte Umfragen genauer zu analysieren. Die Erkenntnisse sollten in die Findung geeigneter Maßnahmen zur Förderung solcher „digitalen“ Innovationen in Form von digitalen Produkten oder Prozessoptimierungen einfließen.

Mindestens steht fest, dass hoch aufgelöste Messdaten sowie weitere personenbezogene Daten für viele innovative Produkte unerlässlich sind. Für diese Datenkategorien spielt Einwilligung der Kunden bzw. der Einzelpersonen eine tragende Rolle, da diese mit jeder Einzelperson separate vereinbart werden muss. Dadurch rückt die (digitale) Kundenschnittstelle bzw. Kundenkommunikation in den Fokus. Für die Konzeptionierung von den in der Digitalisierungsdiskussion oft erwähnten, datenbasierten Mehrwerten bzw. Mehrwertdiensten, sollten aus unternehmerischer Perspektive nicht nur der durch den Dateneinsatz generierten Mehrwert, sondern vor allem der Datenzugang (hier die Einwilligung der Datenweitergabe) und damit die Schnittstelle zum Menschen betrachtet werden. Empirische Studien belegen nicht nur, dass Menschen sehr wohl wissen, dass Unternehmen ihre Daten auswerten und weiterverwenden, sondern zeigen auch, dass Menschen durchaus bereit sind ihre Daten Dritten zur Verfügung zu stellen. Dabei stehen vor allem Transparenz, Datenhoheit und Mehrwerte (zum Beispiel in Form von monetärer Kompensation) im Vordergrund. Das Vertrauen für die

Datenweitergabe genießen dabei seriöse und unabhängige Datentreuhänder sowie wissenschaftliche Einrichtungen. Allerdings besteht weiterer Forschungsbedarf bei der Einstellung von Kunden gegenüber Datenweitergabe, insbesondere bei den Arten von Mehrwertdiensten, die als Gegenleistung für einwilligungspflichtige Daten angeboten werden, und bei unterschiedlichen Einflussfaktoren im Hinblick auf das Vertrauen. Eine große Hürde für Unternehmen zeichnet sich bei der Kommunikation und der Weitergabe der Mehrwerte ab. Dabei stimmen die Betroffenen, deren Daten für datenbasierte Innovationen notwendig sind, mit den Kunden des Unternehmens nicht immer überein. Aufgrund der möglichen Diskrepanz zwischen dem Betroffenenkreis für die Datenbeschaffung und dem Kundenkreis, der von der entwickelten datenbasierten Lösung profitiert, ist es sinnvoll beide externe Schnittstellen separat zu betrachten.

Eine weitere, oft in der Literatur thematisierte, Herausforderung für Unternehmen ist der Zeitpunkt der Datenerhebung bzw. -beschaffung. Erzielbare Mehrwerte sind aufgrund mehrfacher möglicher Verwendung der Datensätze für verschiedene Zwecke schwer vorhersehbar; der Mehrwert selbst steigt allerdings bei der Zusammenführung aus verschiedenen Datenquellen gleichzeitig.

Speziell im „Datenraum Energie“ sollen Energiedaten von Erzeugern (insbesondere von EE) wie auch Verbrauchern aller Art (beispielsweise Energieverbräuche von Industrieanlagen, Haushalten etc.) einen flexiblen, optimal ausgestalteten und kosteneffizienten Übergang in eine klimaneutrale Energieinfrastruktur ermöglichen. Diese Daten sollen maßgeblich bei der Ableitung konkreter Maßnahmen zu einem gezielten und passgenauen Ausbau der Energieinfrastruktur beitragen (Bundesregierung 2021). Eine unserer Meinung nach richtige und wichtige Positionierung, die die zukünftigen nationalen Digital kompetenzen im Energiesektor weiter stärkt.

Auch der datengetriebene Wertschöpfungsprozess bei Unternehmen bedarf einer näheren Untersuchung. Neben dem Zugang zu Daten kommen dabei auch andere Aspekte zum Tragen, wie beispielsweise Fähigkeiten der Mitarbeiter im Bereich der Datenanalyse (A.T.Kearney, BDEW, IMP3rove 2019). Der anschließende → *Teil 2* dieses Kompendiums skizziert ein ganzheitliches Bild von dem IT-Management in Energieversorgungsunternehmen und bietet somit eine Grundlage für die Betrachtung einzelner Stufen in der Datenwertschöpfungskette.

Literaturverzeichnis

A.T.Kearney, BDEW, IMP3rove (2019): Digital@EVU 2019. Wo steht die deutsche Energiewirtschaft?

Agora Energiewende (2019): Toolbox für die Netze. Für die künftige Integration von Erneuerbaren Energien und für das Engpassmanagement.

Akhavan-Hejazi, Hossein; Mohsenian-Rad, Hamed (2018): Power systems big data analytics: An assessment of paradigm shift barriers and prospects. In: Energy Reports (4), S. 91–100.

Arthur, Charles (2013): Tech giants may be huge, but nothing matches big data. When Nasdaq stopped trading this week, it again showed how global firms are at the mercy of a power that created them. In: The Guardian 2013, 23.08.2013. Online verfügbar unter https://www.theguardian.com/technology/2013/aug/23/tech-giants-data, zuletzt geprüft am 19.01.2021.

Bartsch, Michael; Frey, Stefanie (2017): Digitalisierung der Börsen: Energiewirtschaft als Cyberopfer. In: Oliver D. Doleski (Hg.): Herausforderung Utility 4.0. Wie sich die Energiewirtschaft im Zeitalter der Digitalisierung verändert. Wiesbaden: Springer Fachmedien Wiesbaden; Imprint; Springer Vieweg, S. 301–308.

BDEW (2015): Digitalisierung in der Energiewirtschaft. Bedeutung, Treiber und Handlungsempfehlungen für die IT-Architektur in den Unternehmen. Online verfügbar unter https://www.bdew.de/media/documents/Awh_20150609_Digitalisierung_in_der_Energiewirtschaft.pdf, zuletzt geprüft am 27.01.2021.

BDEW (2016): Die Digitalisierung der Energiewirtschaft. Agenda für Unternehmen und Politik. Online verfügbar unter https://www.bdew.de/service/publikationen/die-digitale-energiewirtschaft/, zuletzt geprüft am 01.12.20.

BDEW (2019): Das Messstellenbetriebsgesetz 2016. Anwendungshilfe. 5. Aufl.

Bitcom (2013): Management von Big-Data-Projekten. Leitfaden. Hg. v. BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Online verfügbar unter https://www.bitkom.org/sites/default/files/file/import/130618-Management-von-Big-Data-Projekten.pdf, zuletzt geprüft am 27.01.2021.

Bitcom (2020): Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens. Eine Handreichung für Unternehmen.

BMWi (2015): Industrie 4.0 und Digitale Wirtschaft. Impulse für Wachstum, Beschäftigung und Innovation. Online verfügbar unter https://www.bmwi.de/Redaktion/DE/Publikationen/Industrie/industrie-4-0-und-digitale-wirtschaft.pdf, zuletzt geprüft am 28.01.2021.

BMWi (2019): Monitoringbericht nach § 63 i. V. m. § 51 EnWG zur Versorgungssicherheit im Bereich der leitungsgebundenen Versorgung mit Elektrizität.

BNetzA (2007): Gemeinsame Richtlinie der Regulierungsbehörden des Bundes und der Länder zur Umsetzung der informatorischen Entflechtung nach §9 EnWG.

BNetzA (2018): IT-Sicherheitskatalog gemäß §11 Absatz 1b Energiewirtschaftsgesetz. Online verfügbar unter https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_2018.pdf?__blob=publicationFile&v=4, zuletzt geprüft am 31.01.2021.

BNetzA (2021): Auszug aus Marktstammdatenregister. Registrierte Anlagenbetreiber. Online verfügbar unter https://www.marktstammdatenregister.de/MaStR/Akteur/Marktakteur/IndexOeffentlich, zuletzt geprüft am 23.02.2021.

Bouee, Charles-Eduard; Schaible, Stefan (2015): Die Digitale Transformation der Industrie. Online verfügbar unter https://bdi.eu/media/presse/publikationen/information-und-telekommunikation/Digitale_Transformation.pdf, zuletzt geprüft am 28.01.2021.

Brennen, J. Scott; Kreiss, Daniel (2016): Digitalization. In: Klaus Bruhn Jensen, Eric W. Rothenbuhler, Jefferson D. Pooley und Robert T. Craig (Hg.): The International Encyclopedia of Communication Theory and Philosophy: Wiley, S. 1–11.

BSI (o. J.): Kritische Infrastrukturen. Online verfügbar unter https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html, zuletzt geprüft am 31.01.2021.

BSI (2020): Marktanalyse zur Feststellung der technischen Möglichkeit zum Einbau intelligenter Messsysteme nach §30 MsbG. Version 1.1.1.

Bundesregierung (2017): Legislaturbericht Digitale Agenda 2014–2017. Frankfurt am Main: Verlagshaus Zarbock GmbH & Co. KG. Online verfügbar unter https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda-legislaturbericht.pdf?__blob=publicationFile&v=20, zuletzt geprüft am 19.01.2021.

Bundesregierung (2021): Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum. Berlin. Online verfügbar unter https://www.bundesregierung.de/breg-de/suche/datenstrategie-der-bundesregierung-1845632, zuletzt geprüft am 28.01.2021.

Catapult Energy Systems (2018): Energy data review. Summary report. Unter Mitarbeit von Richard Dobson.

Cavanillas, Jose Maria; Curry, Edward; Wahlster, Wolfgang (Hg.) (2016): New horizons for a data-driven economy. A roadmap for usage and exploitation of big data in Europe: Springer Open. Online verfügbar unter https://www.springer.com/de/book/9783319215686, zuletzt geprüft am 19.08.2020.

Chen, D.; Irwin, D. E. (2017): Weatherman: Exposing weather-based privacy threats in big energy data.

dena (2018): Datenschutz und Datensicherheit. Status quo, Herausforderungen und Handlungsbedarf im Rahmen der Digitalisierung der Energiewirtschaft.

Doleski, Oliver D. (Hg.) (2017): Herausforderung Utility 4.0. Wie sich die Energiewirtschaft im Zeitalter der Digitalisierung verändert. Wiesbaden: Springer Fachmedien Wiesbaden; Imprint; Springer Vieweg.

Ducuing, Charlotte (2019): Data as infrastructure? A study on data sharing legal regimes. In: Competition and Regulation in Network Industries, S. 1–19.

Elia, Gianluca; Polimeno, Gloria; Solazzo, Gianluca; Passiante, Giuseppina (2020): A multi-dimension framework for value creation through Big Data. In: Industrial Marketing Management.

Ernst & Young (2013): Kosten-Nutzen-Analyse für einen flächendeckenden Einsatz intelligenter Zähler.

EY (2019): Barometer Digitalisierung der Energiewende. Wichtige Voraussetzungen für die Digitalisierung wurden geschaffen. Berichtsjahr 2019.

Faroukhi, Abou Zakaria; El Alaoui, Imane; Gahi, Youssef; Amine, Aouatif (2020): Big data monetization throughout Big Data Value Chain: a comprehensive review. In: Journal of Big Data (7:3).

Fassing, Philip (2020): Digitalisierung bis zum Blackout? Online verfügbar unter https://www.it-zoom.de/it-director/e/digitalisierung-bis-zum-blackout-26876/, zuletzt geprüft am 31.01.2021.

Fratini, Alessandra; Pizza, Giulia (2018): Data protection and smart meters: the GDPR and the 'winter package' of EU clean energy law. Online verfügbar unter http://eulawanalysis.blogspot.com/2018/03/data-protection-and-smart-meters-gdpr.html.

Gartner (o. J.a): Digitalization. Online verfügbar unter https://www.gartner.com/en/information-technology/glossary/digitalization, zuletzt geprüft am 28.01.2021.

Gartner (o. J.b): Digitization. Online verfügbar unter https://www.gartner.com/en/information-technology/glossary/digitization, zuletzt geprüft am 28.01.2020.

Gerrits, Lucas (2019): Digitale Energiewende und ständiger Cyberkrieg? Was wir für mehr Sicherheit im vernetzten Zeitalter tun können. Stiftung Energie & Klimaschutz. Online verfügbar unter https://www.energie-klimaschutz.de/digitale-energiewende-cyberkrieg-was-wir-fuer-sicherheit-im-vernetzten-zeitalter/, zuletzt geprüft am 31.01.2021.

Giehl, Johannes; Göcke, Hayri; Grosse, Benjamin; Kochems, Johannes; Müller-Kirchenbauer, Joachim (2020): Survey and Classification of Business Models for the Energy Transformation. In: Energies 13 (11), S. 2981. DOI: 10.3390/en13112981.

Grünewald, Phil; Reisch, Theresa (2020): The trust gap: Social perceptions of privacy data for energy services in the United Kingdom. In: Energy Research & Social Science (68).

Hellmuth, Nils; Jakobs, Eva-Maria (2020): Informiertheit und Datenschutz beim Smart Metering. In: Zeitschrift für Energiewirtschaft 44, S. 15–29.

Hirth, Lion (2020): Open data for electricity modeling: legal aspects. In: Energy Strategy Reviews (27), S. 100433.

Hopf, Konstantin (2018): Mining volunteered geographic information for predictive energy data analytics. In: Energy Informatics (1:4), S. 1–21.

Immonen, Anne; Kiljander, Jussi; Aro, Matti (2020): Consumer viewpoint on a new kind of energy market. In: Energy Power Systems Research.

IRENA (2019): Innovation landscape for a renewable-powered future: Solutions to integrate variable renewables. Online verfügbar unter https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Feb/IRENA_Innovation_Landscape_2019_report.pdf, zuletzt geprüft am 28.08.2020.

I-Scoop (o. J.): Digitization, digitalization and digital transformation: the differences. Online verfügbar unter https://www.i-scoop.eu/digital-transformation/digitization-digitalization-digital-transformation-disruption/.

ITU (2010): DOI and DAI. Online verfügbar unter https://www.itu.int/en/pages/default.aspx, zuletzt geprüft am 25.01.2021.

Krickel, Frank (2015): Digitalisierung in der Energiewirtschaft. In: Werner Hecker, Carsten Lau und Arno Müller (Hg.): Zukunftsorientierte Unternehmenssteuerung in der Energiewirtschaft. Wiesbaden: Springer Fachmedien Wiesbaden, S. 41–73.

Lange, Steffen; Santarius, Tilman (2018): Smarte grüne Welt? Digitalisierung zwischen Überwachung, Konsum und Nachhaltigkeit. München: oekom verlag.

Lehmbruck, Lotte; Kretz, Julian; Aengenvoort, Jan; Sioshansi, Fereidoon (2020): Aggregation of front-and behind-the-meter: the evolving VPP business model. In: Behind and Beyond the Meter: Elsevier, S. 211–232.

Lüdemann, Volker; Pokrant, Patrick (2019): Die Einwilligung beim Smart Metering. Anforderungen nach dem Messstellenbetriebsgesetz und der EU-Datenschutz-Grundverordnung. In: Datenschutz und Datensicherheit (6), S. 365–370.

Mazzone, Dominic (2014): Digital or death. digital transformation - the only choice for business to survive, smash or conquer: Smashbox Consulting.

Mertens, Peter; Barbian, Dina; Baier, Stephan (2017): Digitalisierung und Industrie 4.0 – eine Relativierung. Wiesbaden: Springer Fachmedien Wiesbaden.

Meyer, Anton; Blümelhuber, Christian (2000): Relationship Marketing Success Through Investments in Services. In: Thorsten Hennig-Thurau und Ursula Hansen (Hg.): Relationship Marketing. Gaining Competitive Advantage Through Customer Satisfaction and Customer Retention. Berlin, Heidelberg: Springer.

Moreno-Munoz, A.; Bellido-Outeirino, F. J.; Siano, P.; Gomez-Nieto (2016): Mobile social media for smart grids customer engagement: Emerging trends and challenges. In: Renewable and Sustainable Energy Reviews, S. 1611–1616.

Morey, Timothy; Forbath, Theodore "Theo"; Schoop, Alison (2015): Customer data: designing for transparency and trust. In: Harvard Business Review (May), S. 5–11.

Moro Visconti, Roberto; Larocca, Alberto; Marconi, Michele (2017): Big data-driven value chains and digital platforms: from value co-creation to monetization. Online verfügbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903799.

Office of Science and Technology Policy (2012): Administration Announces New Tools to Help Consumers Manage Electricity Use and Shrink Bills. Online verfügbar unter https://obamawhitehouse.archives.gov/administration/eop/ostp/pressroom/01182012, zuletzt geprüft am 01.12.2020.

Oswald, Gerhard; Kleinemeier, Michael (Hg.) (2017): Shaping the Digital Enterprise. Cham: Springer International Publishing.

Palmer, Michael (2006): Data is the New Oil. Online verfügbar unter https://ana.blogs.com/maestros/2006/11/data_is_the_new.html, zuletzt geprüft am 26.01.2021.

Purtova, Nadezhda (2018): The law of everything. Broad concept of personal data and futuer of EU data protection law. In: Law, Innovation and Technology (10:1), S. 40–81. Online verfügbar unter https://www.tandfonline.com/doi/pdf/10.1080/17579961.2018.1452176?needAccess=true, zuletzt geprüft am 25.11.2020.

PWC (2013): Digitale Transformation. Der größte Wandel seit der industriellen Revolution.

Rhodes, Aidan (2020): Digitalisation of energy. An Energy Futures Lab briefing paper. Online verfügbar unter https://spiral.imperial.ac.uk/handle/10044/1/78885, zuletzt geprüft am 22.10.2020.

Rickert, Jana Marina (2016): The relationship between transparency, consumer trust and willingness to share data – a Vignette survey. In: IBA Bachelor Thesis Conference, July 1st 2016. Enschede. The Netherlands.

Rigoll, Fabian (2017): Nutzerorientiertes Energiedatenmanagement. Dissertation.

Schreckling, Edward; Steiger, Christoph (2017): Digitalize or Drown. In: Gerhard Oswald und Michael Kleinemeier (Hg.): Shaping the Digital Enterprise. Cham: Springer International Publishing, S. 3–27.

Seim, Stephan; Verwiebe, Paul; Blech, Katharina; Gerwin, Christoph; Müller-Kirchenbauer, Joachim (2019): Die Datenlandschaft der deutschen Energiewirtschaft. Working Paper Energie und Ressourcen, 28.11.2019. Online verfügbar unter https://www.er.tu-berlin.de/fileadmin/a38331300/Dateien/Seim__Verwiebe__Blech__Gerwin__M%C3%BCller-Kirchenbauer__2019__-_Die_Datenlandschaft_der_dt_Energiewirtschaft__FG_E_R__TU_Berlin.pdf, zuletzt geprüft am 15.10.2020.

Snyder, Hannah (2019): Literature review as a research methodology: An overview and guidelines. In: Journal of Business Research, S. 333–339.

TenneT (Hg.): Freileitungsmonitoring. Witterungsabhängiger Freileitungsbetrieb.

TÜV Rheinland (2020): "Kundenvertrauen bei disruptiven Technologien": Methodik und Studienergebnisse.

TÜV SÜD (2019): Proactively assessing fatigue in power plant infrastructure and components. Unter Mitarbeit von Franz Binder.

Vogelsang, Michael (2010): Digitalization in Open Economies. Heidelberg: Physica-Verlag HD.

Wachal, Robert (1971): Humanities and Computers: A Personal View. In: The North American Review 1971 (256), S. 30–33. Online verfügbar unter https://www.jstor.org/stable/25117163, zuletzt geprüft am 28.01.2021.

Wamba, Samuel Fosso; Akter, Shahriar; Edwards, Andrew; Chopin, Geoffrey (2015): How 'big data' can make big impact: Findings from a systematic review and alongitudinal case study. In: Int. J. Production Economics (165), S. 234–246.

Webborn, Ellen; Elam, Simon (2019): Utilising smart meter data for innovation and research in the UK (ECEEE Summer Study Proceedings).

Wolf, Thomas; Strohschen, Jacqueline-Helena (2018): Digitalisierung: Definition und Reife.
In: Informatik Spektrum 41 (1), S. 56–64.
DOI: 10.1007/s00287-017-1084-8.

Zhou, Kaile; Fu, Chao; Yang, Shanlin (2016): Big data driven smart energy management: From big data to big insights. In: Renewable and Sustainable Energy Reviews (56).

Zwanziger, Xenia (2019): Die Digitalisierung des Messwesens als Voraussetzung zur Integration der erneuerbaren Energien in das Energieversorgungssystem. 1. Auflage. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG (Kartell- und Regulierungsrecht, 29).

ZUKUNFTS-ORIENTIERTES IT-MANAGEMENT IN ENERGIE-VERSORGUNGS-UNTERNEHMEN

Erarbeitung und Reflektion eines Vorgehens für das IT-Management zur digitalen Transformation in Energie-versorgungsunternehmen

ABSTRACT

Die vielfältigen Herausforderungen, die sich aus der Energiewende und der zunehmenden Digitalisierung der Arbeitswelt ergeben, üben einen enormen Anpassungsdruck auf Energieversorger aus. Diese sind gezwungen, sich strategisch mit dem IT-Einsatz in ihren Unternehmen zu beschäftigen, um erfolgreich am Markt bestehen zu können, indem sie einerseits ihr bestehendes Geschäft adäquat mit IT unterstützen und andererseits die durch IT gebotenen Möglichkeiten gezielt ausschöpfen, um neue Geschäftsmodelle zu implementieren.

Dem Management der IT kommt in diesem Spannungsfeld eine ganz erhebliche Schlüsselfunktion und Verantwortung zuteil. Dabei unterliegt es selbst derselben dynamischen Entwicklung wie andere Unternehmensbereiche und muss sich fortlaufend Veränderungsprozessen stellen und weiterentwickeln.

Zur Unterstützung eignet sich ein Vorgehensmodell, welches ausgehend von einer Betrachtung des Umfeldes und des eigenen Unternehmens den Reifegrad der Digitalisierung ermittelt, die Geschäfts- und Anwendungsarchitektur (Ist und Ziel) erfasst und eine Digitalstrategie ausgehend von der Unternehmensstrategie formulieren lässt. Erst die genaue Kenntnis der vielfältigen Geschäftsprozesse und der derzeitigen IT-Bebauung ermöglicht die gezielte Ableitung geeigneter Maßnahmen.

Darauf aufbauend erfolgt die unternehmensspezifische Definition der IT-Organisation und IT-Governance mit dem Ziel einer optimalen Unterstützung der digitalen Transformationsprozesse. Dabei wandelt sich tendenziell die früher vorherrschende Rolle der IT vom reinen Unterstützer betrieblicher Prozesse im Sinne eines Arbeitsmittels zu einem stark gestaltenden Element mit hohem Wertschöpfungspotential.

Die Umsetzung der abgeleiteten Maßnahmen sollte im Rahmen eines Change-Management-Prozesses erfolgen, da es sich in der Regel um hochkomplexe Veränderungsprozesse im Unternehmen handelt. Die Zielerreichung kann durch geeignete Instrumente des strategischen IT-Controllings gemessen werden.

AUTOREN

Falk Ritschel
Conomic

Christian Sprengel
Conomic

Anne Walther
Conomic

Abkürzungsverzeichnis	
BPMN	Business Process Model and Notation
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technology
CRM	Customer-Relationship-Management
EDM	Evaluate, direct and monitor, hier: Evaluieren, Vorgeben und Überwachen
ERP	Enterprise-Resource-Planning
EVU	Energieversorgungsunternehmen
GIS	Geografische Informationssysteme
IoT	Internet of Things
ISMS	Information Security Management Systems
MES	Manufacturing-Execution-Systeme
PMS	Portfoliomanagementsysteme
PPS	Produktionsplanungs- und Steuerungssysteme
SWOT	Strengths-Weaknesses-Opportunities-Threats

EINFÜHRUNG 52

1.1 Energieversorger im Strudel der Energiewende und digitalen Transformation 52
1.2 Neue Anforderungen an alle Unternehmensbereiche / Das IT-Management 54
1.3 Methodik 55

BESCHREIBUNG DES STATUS QUO DES IT-MANAGEMENTS DEUTSCHER EVU 56

2.1 Digitalisierung im IT-Management betrifft vor allem Daten und Prozesse 56
2.2 Auslöser und Treiber für die Digitalisierung des IT-Managements 57
2.3 Erfolgsfaktoren für die Digitalisierung des IT-Managements 57
2.4 Hemmnisse und Rückschläge bei der Digitalisierung des IT-Managements 58
2.5 Die Größe des Energieversorgers ist auf Ebene der Prozessdigitalisierung nicht relevant 59
2.6 Kooperationen mit anderen Akteuren 60
2.7 Fazit 61

VORGEHENSMODELL ZUM AUFBAU EINES ZUKUNFTSORIENTIERTEN IT-MANAGEMENTS BEI EVU 62

3.1 Stufe 1: Die Analyse 63
3.1.1 Die Unternehmensstrategie als Grundlage für die Digitalisierungsstrategie 63
3.1.2 Geschäfts- und Anwendungsarchitektur für Prozessklarheit und -transparenz 64
3.1.3 Reifegradbestimmung 66
3.2 Stufe 2: Die Definitionsphase 68
3.2.1 IT-Organisation 68
3.3 Stufe 3: Die Umsetzung 72
3.3.1 Change-Management 72
3.3.2 Strategisches IT-Controlling und Datensicherheit 74

ABLEITUNG WICHTIGER BESTANDTEILE DES IT-MANAGEMENTS 76

4.1 Flexible Geschäftsprozesse 76
4.2 IT-Governance – agile Frameworks für mehr Innovationsraum 77
4.3 Darstellung und Kontrolle agiler IT-Landschaften durch IT-Landkarten 78

ZUSAMMENFASSUNG 80

Literaturverzeichnis 82

:// 1. EINFÜHRUNG

1.1 Energieversorger im Strudel der Energiewende und digitalen Transformation

System-, Branchen- sowie Unternehmenstransformationen halten Einzug in Energieversorgungsunternehmen (EVU)[1], die Jahrzehnte lang ohne Komplikationen einen unveränderten Kurs fahren konnten. Mit der Liberalisierung der Strommärkte in den 1990ern (dena 2021) und nun durch die Digitalisierung wird die Entwicklung von EVU und deren Wirken und Handeln wesentlich beeinflusst. Dabei entscheidet die jeweilige, individuelle Reaktion von kleinen und großen Versorgern auf diese neuen Herausforderungen bzw. Chancen über deren zukünftige Marktposition. Denn dass Energieversorger reagieren müssen, steht außer Frage. Wer sich nicht verhältnismäßig schnell und dazu noch möglichst gewinnbringend den neuen Spielregeln anpasst, wird früher oder später Marktanteile verlieren und hinter den Wettbewerbern zurückbleiben.

Vor der Energiewende sorgte ein natürliches Monopol durch Stromnetze und die Aufteilung der Versorgungsgebiete für einen wettbewerbsfreien Raum, in welchem Energieversorger bedenkenlos agieren konnten. Kunden waren fest an den Dienstleister gebunden, Kundenmanagement eher auf den unwichtigeren Handlungsebenen verortet. Seit den neunziger Jahren wendet sich die Situation: die Strommärkte wurden liberalisiert, gefolgt von Gas, und Wettbewerb im Vertrieb wurde erstmals sichtbar. Preise können nun frei gestaltet werden, was auch eine neue Herangehensweise zur Erreichung und Bindung von Kunden erfordert. Alte Strukturen wie die Dominanz von Stadtwerken und Regionalversorgern, die den Paradigmenwechsel in den 1990ern überstanden haben, verlieren wirtschaftlich an Boden. Die umfassende Einführung von Wettbewerb auf Erzeugungs- und Verbrauchsseite für die Schaffung transparenter Preise oder die Zugangserleichterung von Drittanbietern am Markt rückt gerade jetzt durch die zunehmende Relevanz von erneuerbaren Energien mehr und mehr in den Mittelpunkt (Grashof 2014).

Konventionelle Erzeugung aus Kohle und Gas wird durch den Atomausstieg etc. in Zukunft vermehrt der Energie aus erneuerbaren Energieträgern weichen. Das Zukunftsbild des Energiemarktes zeichnet sich durch eine (intelligente) Kopplung und Kommunikation der Sektoren aus, Energie wird dezentral und Stromflüsse werden zunehmend flexibel gesteuert (Grashof 2015). Die Digitalisierung ist durchgehend im Rahmen der Verknüpfung von Energie, Telekommunikation und Automatisierung präsent. Der notwendige Aus- und Umbau der Strominfrastruktur für eine erfolgreiche und nachhaltige Umstellung auf Energiegewinnung aus Wind, Sonne und Biomasse verleiht ihr zwangsläufig eine zentrale Rolle, wenn in Zukunft auf ein nachhaltiges dezentrales Energiesystem im Sinne der Sektorenkopplung und Smart-Grid-Vernetzung gesetzt werden soll. Anwendungen aus den Bereichen IoT und Big Data sind maßgebliche Treiber für die Integration und den Ausbau

1 Das EnWG definiert Energieversorgungsunternehmen als „natürliche oder juristische Personen, die Energie an andere liefern, ein Energieversorgungsnetz betreiben oder an einem Energieversorgungsnetz als Eigentümer Verfügungsbefugnis besitzen […]“. Dies umschließt alle Elektrizitäts- und Gasversorgungsunternehmen, die Übertragungs-, Elektrizitätsverteilernetze oder geschlossene Verteilernetze betreiben. Energieversorgungsunternehmen (EVU) umfasst in diesem Kapitel alle Unternehmen, die in der Energieversorgung (Strom und Gas) tätig sind. Dies umfasst sowohl überregionale Energieversorger als auch Regionalversorger wie Stadtwerke oder Tochterunternehmen der Großversorger.

dezentraler Anlagen wie z.B. digital gesteuerter PV- oder Windkraftanlagen, um bedarfsgerecht und flexibel auf gewonnene Energien zugreifen zu können. Dabei müssen die einhergehenden Prozesse bei Handel, Beschaffung, Abrechnung und anderen Services mindestens genauso stark in den Fokus rücken, um zukünftig organisatorisch dieselbe Flexibilität wie der Anlagen- und Netzbetrieb zu gewährleisten.

Neben regulatorischen Vorgaben und zahlreichen Maßnahmen zur Verbrauchssenkung wird bei der Transformation ein deutlicher Kostensenkungsdruck geschaffen. Kundenbedürfnisse ändern sich und passen sich dem ökologischen und ökonomischen Wandel an – zunehmender Wettbewerb durch künftig neue Akteure und damit sinkende Loyalität zum ”Energieversorger des Vertrauens” erfordern ein zielgerichtetes Handeln von Seiten der EVU. Ein Großteil der Verbraucher (BDEW 2017) beginnt verstärkt, die Versorgungskette zu hinterfragen und verlangt Transparenz und angepassten Service. Bonusprogramme für den Einbau von erneuerbaren Energieanlagen wie Photovoltaik mit zugehörigem Speicher, mehr Transparenz durch Energiemanagementsysteme für Daten- sowie Analyseabruf in Echtzeit via App oder die Förderung einer gemeinschaftlich autarken Lebensweise als sogenannte Energiegemeinschaft stellen die Zukunft der Energiewirtschaft auf Kundenseite dar (ebd.).

Auch Marktteilnehmer aus anderen Branchen weiten ihr Leistungsspektrum auf den Energiemarkt aus. So beispielsweise der Einzelhändler ALDI oder das Internetunternehmen GMX, die neuerdings auch Strom- und Gasprodukte anbieten. Anbieter neuer Technologien der künstlichen Intelligenz oder Blockchain treiben die Digitalisierung und Datensammlung auf dem Energiemarkt voran. Hersteller von modernen Stromspeichern wie Batterien von beispielsweise Tesla beginnen auch für private Haushalte zunehmend interessant und erschwinglich zu werden. In der Mobilitäts- und Logistikbranche fördert der Trend zu Elektrofahrzeugen Innovationen im Bereich alternative Antriebe sowie Smart Mobility, auf dem Wohnungsmarkt versuchen sich Anwendungen für Smart Meter und Smart Home/ Smart Building zu etablieren.

Die fünf absatzstärksten Anbieter an den deutschen konventionellen Erzeugungskapazitäten beherrschten 2019 rund 61% des Stromerstabsatzmarkts, Tendenz fallend (BNA und BKA 2020). Die kleineren Wettbewerber müssen sich im Angesicht des Wegfallens weiterer konventioneller Kapazitäten und der steigenden Erzeugung durch Erneuerbare Energien ebenfalls ihren Platz im Markt sichern. Die Energiewende findet dabei vor allem in den Verteilnetzen statt, an welche 97% der erneuerbaren Stromerzeuger angeschlossen sind. 45% der Netze bewirtschaften dabei kommunale Unternehmen (Doleski 2017).

Neben den größeren und ganz großen der Energiebranche müssen also auch die etwa 900 Stadtwerke (VKU 2019) mit ihren unterschiedlichen Geschäftsfeldern, die nicht nur die Energie, sondern oftmals auch Wasser, Breitband, Abfallwirtschaft, Bäder etc. betreffen, spätestens jetzt Handlungsbedarf erkennen und ihr Portfolio entsprechend der digitalen Transformation sinnvoll anpassen sowie intelligente und klare Lösungen für die neuen, komplexen Fragestellungen finden. Tun sie dies nicht, riskieren sie nachhaltige Marktanteilsverluste und Gewinnrückgänge, nicht rechtzeitig genutzte Chancen werden dann von neuen Wettbewerbern wahrgenommen. Um die Potenziale zu heben, ist es zwingend notwendig, nicht nur Geschäftsmodelle, sondern auch die Unternehmens-IT neu zu denken und damit eine Grundlage für ein neues, effizientes System bzw. eine nachhaltige Digitalisierungsstrategie zu legen. Diesen Sachverhalt kann man aus zwei Perspektiven betrachten, die zum Schluss zum gleichen Ergebnis führen. Denn ob nun die Digitalisierung die Energiewirtschaft oder die Energiewirtschaft die Digitalisierung beeinflusst, ist schlussendlich egal – wichtig ist, dass stattfindende Veränderungen bei EVU eine entsprechende Reaktion hervorrufen.

1.2 Neue Anforderungen an alle Unternehmensbereiche / Das IT-Management

Die Digitalisierung sorgt für das Aufbrechen der einst festen System- und Prozessgrenzen der bisherigen Wertschöpfungsstufen wie Netze, Vertrieb, konventionelle und nun verstärkt auch regenerative Erzeugung sowie Handel und Beschaffung. Das Auflösen der Grenzen zwischen den Wertschöpfungsstufen, die Schaffung neuer Geschäftsmodelle und Wettbewerber sowie die Relevanz individueller Kundenwünsche werden durch die Digitalisierung laut BDEW durch neue Faktoren beeinflusst und verändert. Dazu zählen neue Technologien wie Big Data Analytics oder Cloud und Mobile Computing, neue Geschäftsprozesse und -modelle weg vom assetbasierten Geschäftsmodell, energiewirtschaftliche Treiber wie die Flexibilisierungsnotwendigkeit oder das IT-Sicherheitsgesetz und Kundennachfrage und Anbieterdruck wie die Reaktion auf Wünsche der digitalen Kunden (BDEW 2016). Dynamische Wertschöpfungsnetzwerke aus der Energiewirtschaft und anderen Branchen werden befördert und so Kompetenzen zusammengeführt und neue Geschäftsmodelle wie die Erzeugung in virtuellen Kraftwerken, Smart Home und „Real Time Pricing“ oder Smart City generiert.

Dieser Wandel sollte sich auch an einer neuen Kundenzentrierung orientieren. Es findet ein Wechsel vom reinen Konsumenten zum aktiven Marktakteur statt. Das neue Marktumfeld, geprägt durch technische und digitale Neuerungen, zieht die Notwendigkeit nach sich, Kundenbedürfnisse neu aufzuschlüsseln und Produkte, Dienstleistungen und Geschäftsmodelle an diesen auszurichten (A.T. Kearney, BDEW, IMP³rove 2019).

Neben dem Wandel nach außen Richtung Markt und Kunden beeinflusst die Digitalisierung auch EVU bei internen Prozessen und Vorgängen. Es kommen zahlreiche Geschäftsprozesse zu bestehenden hinzu, es werden noch mehr Daten gesammelt, die verarbeitet und analysiert werden müssen. Die IT muss während der digitalen Transformation neue Schwerpunkte bilden und ihr Handlungsspektrum erweitern, um die Unternehmensdigitalisierung erfolgreich zu unterstützen. IT ist damit nicht länger eine einzelne Abteilung oder eine outgesourcte Fachkraft, welche Softwareentscheidungen trifft oder bei Problemen auftaucht. Vielmehr erstreckt sich die IT nun in jeden Unternehmensbereich, bestenfalls sogar in jeden einzelnen Prozess. Das betrifft die Veränderung der Unternehmenskultur, der Führung, der Organisation, der digitalen Kompetenzen und der Innovationsfähigkeit.

Die Sicherstellung einer positiven Einstellung von betroffenen Akteuren - einschließlich der Mitarbeitenden eines EVU - zur Gewährleistung der Umsetzung einer digitalen Transformation sei dabei schon an dieser Stelle als wichtiger Faktor genannt. Gerade weil die IT im Idealfall ein alles durchdringendes Netz im gesamten EVU formt und jeder Akteur an informationstechnischen Prozessen beteiligt ist, sollte die umfassende Implementierung eines sinnvollen IT- Managements vollzogen werden. Die IT hat das Potenzial, zum strategischen Erfolgsfaktor zu werden. Prozesse müssen weiterentwickelt und umgestaltet werden. Eine detailreiche Analyse sowie transparente Aufarbeitung sind dafür essenziell. Dadurch kann das Unternehmen Kernprozesse identifizieren, Synergien und Abhängigkeiten erkennen und schlussendlich wichtige Optimierungspotenziale ableiten.

Nach Krcmar kann das IT-Management als Teilbereich der Unternehmensführung betrachtet werden, welcher den bestmöglichen Einsatz der Ressource Informatik gewährleisten soll. Zu den Aufgaben zählen dabei das Management der Informationswirtschaft, der Informationssysteme sowie der Informations- und Kommunikationstechnik eines Unternehmens sowie generelle Führungs- und Gestaltungsaufgaben (Mangiapane und Büchler 2015). Durch den Paradigmenwechsel erhält das IT-Management zunehmend Form und Funktion und wird nach dem Modell von Resch zwischen der IT

und dem IT-Kunden sowie der Gesamtorganisation eingeordnet. Das IT-Management übernimmt dabei eine wichtige Koordinationsfunktion und muss alle Bereiche aufeinander abstimmen und aktiv managen (Mangiapane und Büchler 2015).

Weiterhin wird zwischen dem strategischen und dem operativen IT-Management unterschieden. Das strategische IT-Management stellt die Synchronisierung der Unternehmensziele mit der IT-Strategie sicher. Die Initiierung und Planung von IT-Vorhaben und deren Priorisierung für die Verbesserung der strategischen Position des Unternehmens durch die implementierten Informationssysteme sind zentral und stets auf eine kontinuierliche Anpassung und Verbesserung bedacht. Im operativen IT-Management steht die wirtschaftliche Nutzung der IT-Ressourcen im Vordergrund und konzentriert sich auf die effektive Entwicklung von IT-Lösungen, einen reibungslosen IT-Betrieb und die Weiterentwicklung und Wartung von Informationssystemen.
Der strategische und der operative Aspekt sollten gleichermaßen beim IT-Management im Fokus stehen, um kurzfristige Erfolge und den langfristigen Erhalt des Unternehmens zu sichern (Tiemeyer 2017). Bei alldem darf das IT-Management seine eigene Digitalisierung nicht vergessen.

1.3 Methodik

Ziel des Kapitels zur Etablierung eines zukunftsfähigen IT-Managements für EVU ist die Entwicklung und Beschreibung eines entsprechenden Vorgehensmodells, auf Basis dessen Energieversorger eine sinnvolle und nachhaltige Strategie für eine zielgerichtete Digitalisierung und schlagkräftiges IT-Management aufsetzen können.

Zu Beginn der Erarbeitung wurden im Rahmen von Workshops mit auf die Energiewirtschaft spezialisierten IT-Experten die relevanten Bestandteile eines Vorgehensmodells ermittelt, analysiert und zueinander ins Verhältnis gesetzt. Aufbauend auf dieser Grundstruktur folgten tiefgreifende Sekundärrecherchen zu den einzelnen Phasen, ihren Elementen und jeweiligen Einflussfaktoren. Aktuelle Marktentwicklungen und Best-Practices sorgen für eine möglichst branchenspezifische Ausrichtung des Vorgehensmodells.

Um einen Überblick über den Status quo des IT-Managements in EVU zu bekommen, wurden im Rahmen von leitfadengestützten qualitativen Experteninterviews IT-Verantwortliche zu Treibern, Erfolgsfaktoren und Hindernissen der eigenen Digitalisierung befragt. Zudem standen Kooperationen mit anderen Akteuren sowie die Relevanz der Größe eines EVU für die Prozessdigitalisierung im Mittelpunkt. Die Interviews fanden telefonisch zwischen Januar und März 2020 statt, befragt wurden 12 IT-Verantwortliche der Branche. Die Ergebnisse der Befragung werden in Punkt 2 anonymisiert zusammengefasst dargestellt.

Auf Basis der Sekundärrecherche, der Experteninterviews sowie der Workshops werden in Punkt 3 im Rahmen der drei Phasen „Analyse, Definition und Umsetzung“ eines möglichen IT-Managements relevante Bestandteile aufgezeigt und detailliert erläutert.

In weiteren Workshops wurden schließlich einzelne Elemente der Phasen identifiziert, die sich durch ein besonderes Maß an Flexibilität auszeichnen (sollten) und so für das Vorgehensmodell und dessen Erfolg eine hohe Bedeutung aufweisen. Zu diesen zählen flexible Geschäftsprozesse, agile Frameworks der IT-Governance sowie agile IT-Landkarten. Diese werden in Punkt 4 genauer dargestellt.

:// 2.
BESCHREIBUNG DES STATUS QUO DES IT-MANAGEMENTS DEUTSCHER EVU

Die Digitalisierung etabliert sich zunehmend fest in den Strukturen deutscher EVU. Rund 82% aller EVU sehen die Entwicklung von digitalen Technologien als zentralen Treiber für interne Veränderungsprozesse unabhängig von der eigenen Unternehmensgröße (BBH 2017). Bei der Prozessanalyse hinsichtlich Digitalisierungspotentialen scheinen große EVU weiter fortgeschritten als kleine und mittlere Vertreter der Branche, vor allem mittlere EVU haben an dieser Stelle noch nicht angegriffen. Sogenannte „gelebte“ Prozesse dominieren, der Einsatz von unterstützenden Softwarewerkzeugen zum Modellieren, Umsetzen und Überwachen von Prozessen wird vorrangig bei großen EVU geprüft (ebd.). Dabei bestehen zwischen den Best-In-Class EVU, sprich den Branchenführern in Bezug auf Effizienz und den Durchschnitts-EVU große Lücken. Best-In-Class EVU setzten bei der Digitalisierung auf einen kompletten Kulturwandel im Unternehmen, haben ein klares Bild der zukünftigen digitalen Fähigkeiten, die sie nachhaltig etablieren wollen und wenden im Alltag bereits erfolgreich und situationsbezogen agile Methoden an (A.T. Kearney, BDEW, IMP³rove 2019).

Um herauszufinden, wie EVU die Digitalisierung ihres IT-Managements angehen, wurden 12 ausgewählte IT-Verantwortliche aus EVU im Rahmen qualitativer Experteninterviews befragt. Treiber und Auslöser für die Digitalisierung im Unternehmen, individuelle Erfolgsfaktoren sowie Hemmnisse aber auch Kooperationen und die Einschätzung der Relevanz der Unternehmensgröße bei der Prozessdigitalisierung standen dabei im Mittelpunkt. Im Folgenden werden die Meinungen und Ansichten der IT-Verantwortlichen unkommentiert wiedergegeben.

2.1 Digitalisierung im IT-Management betrifft vor allem Daten und Prozesse

Aufstrebende digitale Technologien wie Smart Meter und Smart Grid und die Konfrontation mit hohen Datenmengen und deren Verarbeitung fordern auch entsprechende Maßnahmen zur Neuausrichtung des IT-Managements. IT-Verantwortliche erkennen einen deutlich stärkeren serviceorientierten Ansatz der Unternehmens-IT. Diese Services betreffen vor allem die Vorverarbeitung von Daten, die Verknüpfung und Voranalyse von Informationen und Services für Front-End-Prozesse sowie die Entwicklung und Planung der Netzwerkinfrastruktur.

IT-Verantwortliche sehen die Ziele der Digitalisierung vor allem im thematischen, technologischen und kulturellen Bereich u.a. bei der Automatisierung von Geschäftsprozessen, dem Beseitigen von Medienbrüchen, der Vernetzung von Wertschöpfungsketten sowie der Agilität und Flexibilität in der Arbeitsweise.

Entsprechende IT-Strategien existieren größtenteils und werden vor allem mit dem Vertrieb und zugehörigen Einheiten abgestimmt. Die Digitalisierungsstrategie wird weniger IT-, sondern mehr geschäftsseitig betrachtet.

Laut der befragten IT-Verantwortlichen existiert die IT dabei u.a. als Stabsstelle der Geschäftsführung und ist direkt am Vorstand verankert, wo auf Augenhöhe mit Bereichsleitern agiert werden kann.

Bei großen Konzernen ist ebenso das Modell einer verteilten, dezentralen IT mit zentraler Koordinierung vorzufinden, da die Trennung von Vertrieb und Netz die dezentrale Aufteilung der IT fordert. Zentralisiert hingegen ist die IT-Governance, wo die entsprechende Architektur etc. verortet wird. Neue Anwendungen werden top-down eingeführt, d.h., je nach Vorgaben bzw. Vorschlägen des Mutterkonzerns wird in Zusammenarbeit der Verantwortlichen über führende Systeme entschieden, welche Maßnahmen Vorteile wie beispielsweise die Einsparung von Kosten mit sich bringen.

2.2 Auslöser und Treiber für die Digitalisierung des IT-Managements

Starker Wettbewerb, Kostenreduzierung, neue Kundenanforderungen, dynamische Workflows und beschleunigte Veränderungsprozesse treiben die Digitalisierung des IT-Managements voran.

Als Auslöser für die Digitalisierung des IT-Managements geben die Befragten u.a. die Wahrnehmung des Managements hinsichtlich einer mangelhaften digitalen Aufstellung an, aus welcher die Aufgabe für sie resultiert, entsprechende Digitalisierungsmaßnahmen nach innen und außen voranzutreiben. Einen weiteren Auslöser stellt die Kostenreduzierung durch die effizientere digitale Prozessgestaltung dar. Vor allem hinsichtlich erfolgreicher, digitaler Wettbewerber sehen EVU die Notwendigkeit mitzuhalten und sich ebenfalls besser digital aufzustellen.

Abbildung 1: Auslöser für die Digitalisierung in EVU
Quelle: Eigene Darstellung

Auch die neuen Anforderungen der Kunden treiben die Digitalisierung von Vertriebskanälen und die Ausgestaltung des Kundenerlebnisses voran, was auch Auswirkungen auf das IT-Management und dessen zukünftige Gestaltung hat.

Die Implementierung spezifischer Tools wie Cloud-Lösungen, Kollaborationstools und Tools zur Prozessvisualisierung wird zunehmend vorangetrieben. Immer dynamischere Geschäftsprozesse erfordern Anpassungen der Anwendungslandschaft in EVU und eine adäquate Weiterentwicklung des IT-Managements.

Durch Digitalisierung beschleunigte Veränderungsprozesse laufen nicht linear, sondern dynamisch ab. Vorhersagen für Geschäftsfelder und 5-Jahres-Pläne sind schwer zu erstellen, iteratives Handeln ist gefragt.

2.3 Erfolgsfaktoren für die Digitalisierung des IT-Managements

Transparente Kommunikation im Rahmen eines umfassenden Kulturwandels, Kooperationen, eine modulare und flexible Architektur, der Fokus auf einen entsprechenden Datenumgang sowie die Etablierung einer Fehlerkultur sind wichtige Erfolgsfaktoren.

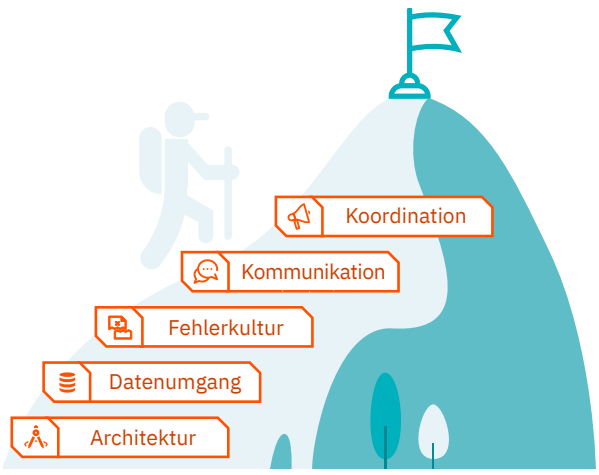
Ein reger und offener Austausch und interne sowie externe Netzwerke machen einen wichtigen Erfolgsfaktor auf dem Weg in ein neues IT-Management aus. Es muss in diesem Rahmen eine Organisation der digitalen Transformation über Verantwortlichkeiten geschaffen werden. In jedem Segment existiert im Idealfall ein Digital-Verantwortlicher. Auf zwischenmenschlicher Ebene ist zudem eine transparente Kommunikation der bevorstehenden bzw. sich vollziehenden Änderungen überaus wichtig, um Missverständnisse auszuschließen.

Wichtig ist zudem eine übergeordnete Koordination, die Netzwerke in anderen Gesellschaften bedient. Dort werden Informationen und Best Practices geteilt, was vor allem bei einer iterativen Arbeitsweise als sinnvoll erachtet wird.

Ein weiterer Erfolgsfaktor liegt laut der befragten IT-Verantwortlichen im Aufbau einer modularen und flexiblen Architektur, z. B. mit sogenannten Microservices. Dadurch wird die Entkopplung vom System erreicht und einzelne Bausteine können besser ausgewechselt werden.

Weiterhin kann die Art der Datennutzung erfolgsentscheidend sein. Daten müssen identifiziert, erschließbar gemacht und schließlich veredelt werden, um einen Mehrwert für das Unternehmen zu generieren. Gerade durch das Aufkommen von Technologien der Künstlichen Intelligenz, Advanced Analytics, Big Data und Business Intelligence müssen Daten kombiniert und Prozesse automatisiert werden.

Abbildung 2: Erfolgsfaktoren für die Digitalisierung des IT-Managements
Quelle: Eigene Darstellung



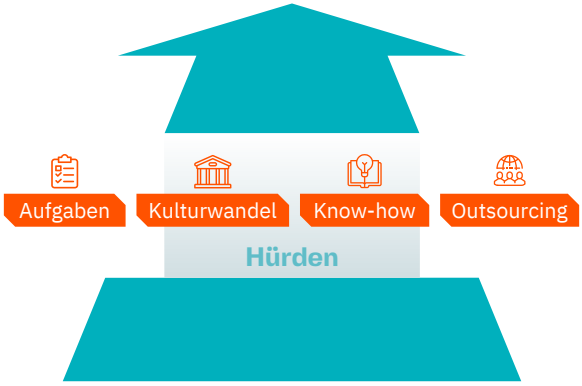
Ein weiterer wichtiger Aspekt für das Gelingen der Digitalisierung des IT-Managements ist die Etablierung einer Fehlerkultur. Fehler und deren Bearbeitung sind vor allem bei innovativen Themen relevant. Innovationen können nur entstehen, wenn gewisse Freiheiten und Tests zugelassen und Fehler als Grundlage für das Einschlagen eines anderen, besseren Weges nicht nur in Kauf genommen, sondern auch toleriert werden. In diesem Sinne ist auch die Etablierung einer Innovationskultur nennenswert. Beispielsweise werden im Rahmen einer Digitalagenda Mitarbeiter dazu aufgefordert, Ideen zu entwickeln, um einen Innovationspush zu befördern.

2.4 Hemmnisse und Rückschläge bei der Digitalisierung des IT-Managements

Hürden auf dem Weg zum zukunftsgerichteten IT-Management liegen vor allem beim Unterschätzen der Relevanz des Change-Managements und des Kulturwandels, beim Behandeln von Rückschlägen und dem Umgang mit Know-how.

Das Unterschätzen der Relevanz der Unternehmenskultur bzw. des Change-Managements macht eine große Hürde bei der Implementierung digitaler Strategien und eines digitalen IT-Managements aus. Ein zu forsches Herangehen und ein zu schneller Umbruch stoßen dabei schnell auf Widerstände unter Mitarbeitern. Die Angst vor dem „Ersetzt werden“ durch Technik und Software ist eine ernstzunehmende Sorge unter Angestellten, welche es zu beseitigen gilt.

Abbildung 3: Hürden auf dem Weg zur Digitalisierung des IT-Managements
Quelle: Eigene Darstellung



Die Effizienzsteigerung im IT-Management durch digitale Prozesse bringt zwar viele Vorteile mit sich, doch geschaffene Freiräume im Arbeitsalltag müssen perspektivisch mit neuen Aufgaben gefüllt werden. In diesem Sinne erklären die Befragten, dass es an Aufgaben zwar nicht mangele, aber die Dynamik und der Veränderungswille nicht bei jedem Mitarbeiter gleichermaßen gegeben sind, sich neuen Herausforderungen zu stellen.

Eine weitere Hürde auf dem Weg zum digitalisierten IT- Management kann der Umgang mit externen Softwaredienstleistern darstellen. Es besteht die Gefahr, durch unzureichende und intransparente Kommunikation in einem Unternehmen ähnliche Inhalte entwickeln zu lassen, wobei unnötig Ressourcen beansprucht werden und Mehrwerte für das Unternehmen durch mangelnde interne Abstimmung nicht erzielt sind.

Ein weiteres Hemmnis sind personelle Ressourcen wie Mitarbeiter und Know-how, welche gehalten beziehungsweise verankert werden müssen, damit Fortschritte oder Erfolge des Unternehmens auf dem Weg zum zukunftsfähigen IT-Management nicht bei Verlassen eines wichtigen Verantwortlichen wegbrechen.

2.5 Die Größe des Energieversorgers ist auf Ebene der Prozessdigitalisierung nicht relevant

Die befragten IT-Verantwortlichen sehen Regionalversorger grundsätzlich mit weniger Ressourcen als große EVU ausgerüstet. Beim Aufkommen neuer Trends und Technologien können kleine Versorgungsunternehmen erst später einsteigen, große EVU hingegen besitzen nötige finanzielle und personelle Mittel, innovative und entsprechend risikoreichere Projekte oder Investitionen anzugehen. Netzwerkeffekte werden von den großen Playern eher als bei Regionalversorgern gesehen, da mehr Initiativen entwickelt werden können.

Hinsichtlich der IT-Strategie werden Regionalversorger als „eleganter“ und schneller als die großen EVU eingeschätzt. Teilweise wird sogar die Möglichkeit einer schnelleren und schlagartigen Digitalisierung in kleinen EVU gesehen. Grundlage für diese Einschätzung liefern Erfahrungswerte aus der kürzlichen Corona-Pandemie und der Notwendigkeit einer schnellen Umstellung und Digitalisierung von Prozessen.

Grund für eine langsamere Digitalisierung sehen kleine Versorger in der zähen Organisation der großen EVU, der Vielzahl an Meinungen und Wegen sowie dem oftmals starren hierarchischen System. Vertreter großer EVU sehen diesen Trend ähnlich.

Abbildung 4: Vor- & Nachteile großer & kleiner EVU
Quelle: Eigene Darstellung

Bei der Prozessdigitalisierung wird bei großen EVU kein Vorteil gegenüber kleinen gesehen. Entsprechende Angebote sind für alle gleichermaßen zugänglich, bei einer Automatisierung erfolgen Einsparungen in jedem Maßstab, weswegen Geld für eine Refinanzierung auch für kleine Versorger zur Verfügung steht.

2.6 Kooperationen mit anderen Akteuren

Große und kleine Energieversorger ziehen aus einer facettenreichen Vernetzung mit Startups, Wettbewerbern und Forschungseinrichtungen viele Vorteile für die eigene Weiterentwicklung und Sicherung der Marktposition.

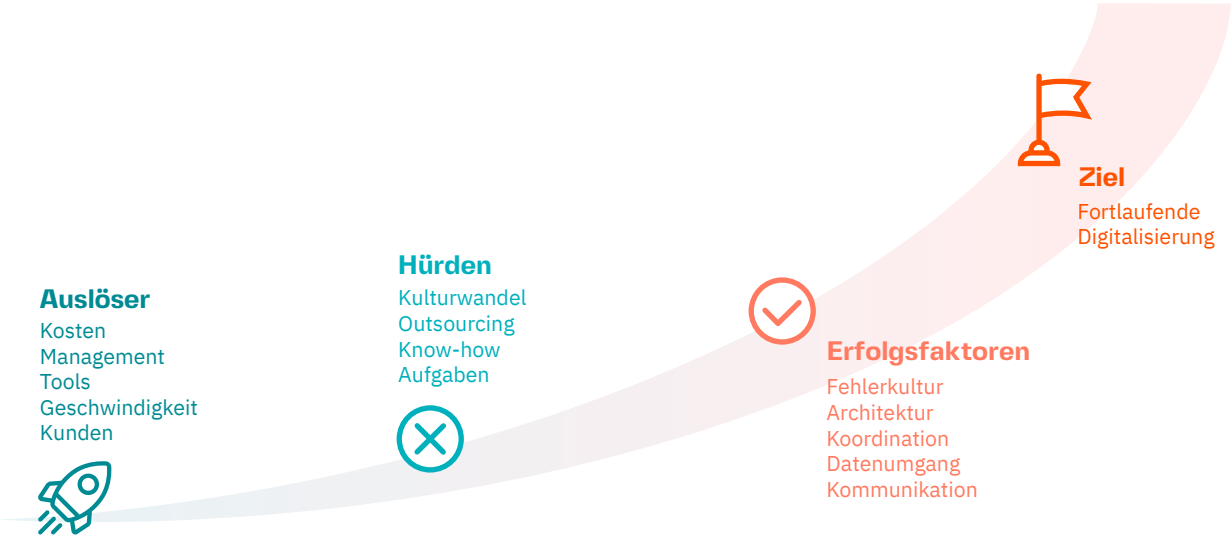
IT-Verantwortliche kleiner Energieversorger gaben im Rahmen der Befragung an, Strategien aufgrund der Unternehmenskenntnis lieber selbst, anstatt durch externe Berater etc. zu entwickeln, wobei vor allem der Austausch mit anderen Energieversorgern hilft. Dabei werden Best Practices aus dem unmittelbaren Umkreis als sehr wichtig angesehen. Lernen aus den Fehlern der anderen stellt für Energieversorger ein wichtiges Mittel für die eigene Weiterentwicklung dar.

Bei großen Konzernen findet vor allem reger Austausch über Schwesterunternehmen und Netzgesellschaften statt, da diese ähnlich arbeiten und teilweise Vorlagen bieten, die übernommen werden können.

Die Zusammenarbeit mit Hochschulen und Forschungsinstituten im regionalen Umkreis und Kontakte zu Startups und Gründungszentren sind für IT-Verantwortliche ebenso wichtig, um neue Trends zu erkennen und Kooperationen zu befördern. Businesskooperationen für Verbundprojekte wie WindNODE oder ARGEnergie spielen ebenfalls eine Rolle.

Das Internet als Plattform und Informationsträger bringt zwar eine Vielzahl an Informationen mit sich, doch persönliche Kontakte und Treffen wie beispielsweise bei Messen oder Branchenkongressen besitzen weiterhin hohe Relevanz.

Abbildung 5: Der Weg der Digitalisierung
Quelle: Eigene Darstellung



2.7 Fazit

Die Befragung der IT-Verantwortlichen zeigt, dass die Digitalisierung des IT-Managements ein Prozess ist, der zum einen auf eine gute Vorbereitung und Planung und zum anderen eine konsequente Durchführung und stetige Kontrolle sowie Anpassung angewiesen ist. Der oder die Auslöser für die Digitalisierung in einem EVU können dabei vollkommen unterschiedlicher Natur und Intensität sein. So individuell wie diese Auslöser sind auch die Hürden, die sich auf dem Weg der Digitalisierung in den Weg stellen und welche durch die erfolgreiche Entwicklung und Anwendung von Erfolgsfaktoren überwunden werden können. Maßgeblich für die Herausbildung all dieser Elemente ist die Größe aber auch Ausrichtung und „Stil“ des EVU. Vor allem die unterschiedliche Ausprägung bzw. Ausgestaltung der Organisation, der Veränderungsgeschwindigkeit, der bestehenden Ressourcen oder der Zusammenarbeit mit Kooperationspartnern beeinflussen den Weg der digitalen Transformation bei großen und kleinen EVU sehr individuell. Gemeinsam jedoch haben alle EVU unabhängig von ihrer Größe, dass sie langfristige Erfolge nur durch die Unterstützung der Führungsebene sowie den nötigen Umsetzungswillen bei Mitarbeitenden erzielen können. Denn die Chancen zur Digitalisierung von Prozessen sind bei jedem EVU gleichermaßen vorhanden, sie müssen nur genutzt werden.

Wichtig ist vor allem, dass wie die Unternehmensdigitalisierung selbst auch die Digitalisierung des IT-Managements nicht als einzelnes Projekt, sondern als ein fortlaufender Teil der Unternehmensentwicklung betrachtet wird und nicht nach der Durchführung einzelner Maßnahmen stoppt.

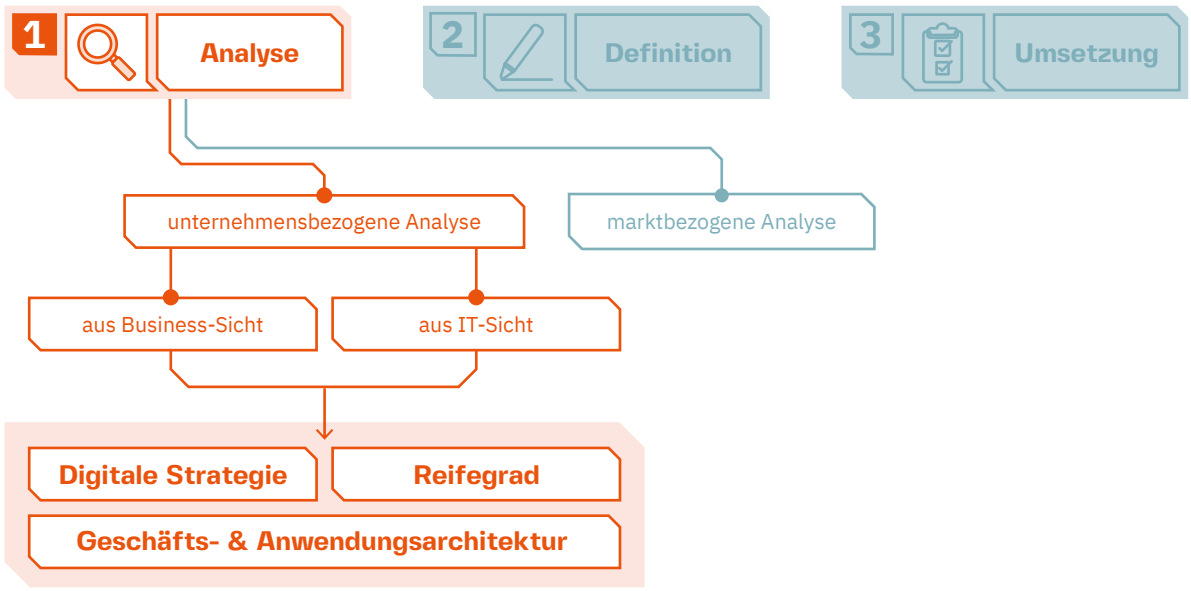
:// 3.
VORGEHENSMODELL ZUM AUFBAU EINES ZUKUNFTSORIENTIERTEN IT- MANAGEMENTS BEI EVU

Vorgehensmodelle oder sogenannte Roadmaps zur digitalen Transformation für Energieversorger existieren in zahlreichen Varianten (ifaa 2019) und geben in verschiedenen Phasen Aufschluss zur Strategie, Taktik und jeweiligen Umsetzung. Betroffen sind dabei die Wertschöpfung und das Geschäftsmodell, die Organisation sowie Prozesse und die IT. Wie bereits eingangs erklärt, bezieht sich das IT-Management auf all diese Kernbereiche und sollte sie im Idealfall auch aktiv managen. Die Digitalisierung des IT-Managements selbst spielt demnach eine mindestens ebenso wichtige Rolle.

Für die Implementierung eines zukunftsfähigen IT-Managements wird im Folgenden ein dreiphasiges Vorgehensmodell beschrieben, welches begonnen bei der Analysephase über die Strategiedefinition bis hin zur Strategieumsetzung speziell Energieversorgern einen Leitfaden aufzeigen soll, wie der Transformation des IT-Managements auf strategischer Ebene begegnet werden kann. Nur wenn diese Schritte ausreichend bearbeitet werden, kann in den anschließenden Phasen auf operativer Ebene nachhaltig gehandelt werden. Wichtig dabei ist – und das macht dieses Vorgehensmodell so essenziell – dass die ersten drei Phasen für jedes EVU individuell erschlossen werden müssen. Erfolgreiche Vorgehensweisen der Wettbewerber können in anderen EVU zum Scheitern führen. Aus diesem Grund sollte jeder Phase ausreichend Beachtung geschenkt werden.

Abbildung 6: Phasen des Vorgehensmodells
Quelle: Eigene Darstellung

Abbildung 7: Phase 1 – Analyse
Quelle: Eigene Darstellung



3.1 Stufe 1: Die Analyse

Die unternehmensbezogene Analyse aus Business- und IT-Sicht bildet zusammen mit der marktbezogenen Analyse die Grundlage für die zielgerichtete Definition eines Vorgehensmodells zur Transformation des IT-Managements. Im Rahmen der marktbezogenen Analyse werden durch eine ausführliche Branchenstrukturanalyse das marktseitige Bedrohungspotenzial und Chancen im Umfeld des Unternehmens identifiziert und bewertet. Dabei steht der Grund der Veränderung branchenüblicher Geschäftsmodelle durch die Digitalisierung im Mittelpunkt. Genauer wird die Bedrohung durch neue Anbieter und Ersatzprodukte, die Verhandlungsstärke von Abnehmern und Lieferanten sowie die Rivalität unter bestehenden Wettbewerbern betrachtet. Die marktbezogene Analyse ist für ein vollständiges Bild der Unternehmenssituation wichtig, eine detaillierte Beschreibung würde an dieser Stelle aber den Rahmen sprengen. Deswegen steht in diesem Kapitel die unternehmensbezogene Analyse im Mittelpunkt.

Bei der Analyse aus Business- sowie aus IT-Sicht spielen die Geschäftsarchitektur und die digitale Strategie eine Rolle. Stärken und Schwächen verschiedener relevanter Dimensionen des IT-Managements können zuverlässig über eine Reifegradermittlung erhoben werden.

3.1.1 Die Unternehmensstrategie als Grundlage für die Digitalisierungsstrategie

Die Analyse der Unternehmensstrategie bildet den ersten Schritt der Analysephase. Aus dieser ergeben sich Auswirkungen auf die Digital-Strategie. Eine klare und sinnvoll aufgesetzte Strategie zur Digitalisierung ist die Grundlage für die Bereitstellung geeigneter IT-Services unter Beachtung wirtschaftlicher Aspekte. Sowohl die Sicherung der Betriebs- und Lieferfähigkeit des EVU als auch die Verbesserung der IT-Performance beschreiben deren Hauptziele. Während der Analyse sollten wesentliche Treiber festgehalten werden. Zudem werden in

der Digital-Strategie Vision sowie Mission festgelegt und darüber hinaus Stärken und Schwächen der bestehenden IT-Organisation aufgezeigt. Die sich daraus ergebenden Informationen sind Grundlage der strategischen IT-Planung und den daraus resultierenden Maßnahmen (Tiemeyer 2017). Verantwortlich dafür ist in der Regel die IT-Abteilung bzw. der IT-Leiter selbst (auch genannt CIO - Chief Information Officer) in Kooperation mit der Geschäftsführung, Fachbereichen und eventuell auch externen Experten.

3.1.2 Geschäfts- und Anwendungsarchitektur für Prozessklarheit und -transparenz

Themen der Energiewende und der damit einhergehenden Digitalisierung wie Smart Grid und Smart Meter, Sektorenkopplung oder die Verwaltung und Vernetzung dezentraler Energiesysteme stellen hohe Anforderungen an die Modernisierung der Geschäfts- und IT-Prozesse (Lünendonk 2014).

Die Geschäftsarchitektur als Teil der Unternehmensarchitektur, auch genannt Prozessarchitektur oder Businessarchitektur, befasst sich mit der Business-Strategie, Steuerungsmechanismen, der Organisation und Geschäftsprozessen. Die Zielsetzungen der Geschäftsarchitektur reichen von der Erhöhung der Transparenz und einer reinen Dokumentation der betrieblichen Abläufe, bis zur Unterstützung der Ausschreibung von Software und der Vollautomatisierung von Prozessen mittels geeigneter Anwendungssysteme durch detaillierte Kenntnis der einzelnen Geschäftsabläufe.

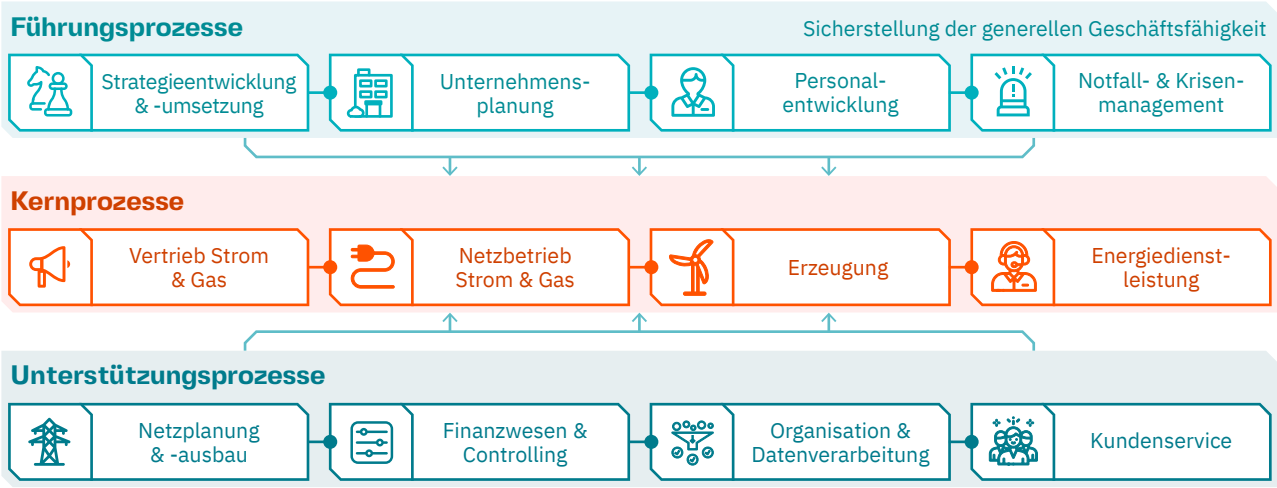
Ein Geschäftsprozess hat zum Ziel, ein bestimmtes Ergebnis wie ein Produkt oder eine Dienstleistung durch eine inhaltlich abgeschlossene, zeitliche und sachliche Abfolge von Aktivitäten zu erzeugen (Hinkelmann 2019). Für die Bestimmung eines Geschäftsprozessmodells müssen sich EVU die Frage stellen, was in welcher Reihenfolge von wem und mit welchen Ressourcen zu erledigen ist. Die Kenntnis der eigenen Prozesslandschaft ist eine notwendige Voraussetzung zum schrittweisen Aufbau von Prozessexzellenz. Für einen ersten Überblick über den Status quo der laufenden Prozesse bietet sich die Erarbeitung von Prozesslandkarten an. Auf der Basis solcher Prozesslandkarten, die sowohl für das gesamte Unternehmen als auch einzelne Bereiche erarbeitet werden, kann die detaillierte Modellierung konkreter Geschäftsprozesse erfolgen. In der Praxis findet man auf diese Art, nach Erfahrung der Autoren, in einem größeren Stadtwerk zwischen 500 und 700 einzelne Geschäftsprozesse (je nach Strukturierungsansatz und Umfang der Geschäftsfelder). Diese unterteilen sich in Führungs-, Kern- und Unterstützungsprozesse und sind für jedes EVU ähnlich, aber individuell ausgeprägt.

Die Führungsprozesse dienen zur Sicherstellung der generellen Geschäftstätigkeit und befinden sich branchenübergreifend beispielsweise in den Bereichen der Strategieentwicklung und -umsetzung, der Unternehmensplanung, der Personalentwicklung und dem Notfall- und Krisenmanagement. Vor allem bei EVU ist es aufgrund der digitalen Entwicklung der vergangenen Jahre und dem dadurch aufkommenden Marktdruck entscheidend, im Rahmen der Führungsprozesse nachhaltige Wettbewerbsvorteile durch eine grundlegende strategische Neuausrichtung und agile Geschäftsmodelle zu entwickeln (Vielhaber 2005).

Kernprozesse sind durch ihren erzeugten Wert entscheidend für das Unternehmen. Diese Prozesse umfassen bei EVU beispielsweise den Vertrieb und den Netzbetrieb von Strom und Gas (sowie ggf. Wärme), die Stromerzeugung und weitere Energiedienstleistungen. Ein Unternehmen sollte sich spätestens in der Analysephase darüber klar werden, welche Kernprozesse es ausführt und welche Rolle diese für den langfristigen Unternehmenserfolg spielen.

Ein unterstützender Prozess dient der Bereitstellung der Infrastruktur und der Erbringung interner

Abbildung 8: Beispiel einer Prozesslandkarte (hier Unternehmensprozesslandkarte) für ein EVU
Quelle: Eigene Darstellung



Dienstleistungen, die für die Kern- oder Führungsprozesse nötig sind. Bei EVU sind dies unter anderem i.d.R. kaufmännische Prozesse (z.B. im Rechnungs- und Finanzwesen oder Controlling), Betrieb und Management der IT, Recht und Compliance oder Regulierungsmanagement. Die Einführung moderner Softwareanwendungen und damit eine weitestgehende Automatisierung sind zentrale Themen bei der Digitalisierung des Unternehmens und die Grundlage für ein funktionierendes digitales IT-Management (Lünendonk 2014).

Die Erfüllung der Kernprozesse steht immer im Mittelpunkt – Führungsprozesse und Unterstützungsprozesse sollen in einem EVU daher so ausgerichtet sein, dass diese Erfüllung realisiert werden kann.

Wurden die konkreten Geschäftsprozesse, mit denen man sich im Rahmen der Digitalisierung beschäftigen will, festgelegt, erfolgt im nächsten Schritt die Modellierung, Analyse und Optimierung bestehender IST-Prozesse oder die Definition gänzlich neuer Geschäftsprozesse. Für die Geschäftsarchitektur sollten geeignete Anwendungssysteme eingesetzt werden, die relevante Daten und Funktionen von Geschäftsprozessen abbilden und dadurch den gesamten Zyklus integriert unterstützen. Solche Enterprise-Resource-Planning-Systeme (ERP-System) verwalten alle notwendigen Informationen über Material, Personal, Kapazitäten, Finanzen und Aufträge und können zudem branchenspezifische Erweiterungen beinhalten. Für die Analyse und Optimierung ist zudem das Erfassen geeigneter Kennzahlen unerlässlich. Weitere relevante Anwendungen sind neben ERP-Systemen Customer-Relationship-Management-(CRM-) Systeme für Marketing und Vertrieb, Supply-Chain-Management-Systeme für die Logistik oder Manufacturing-Execution-Systeme (MES) bzw. Produktionsplanungs- und Steuerungssysteme (PPS-Systeme) für die Fertigung, Portfoliomanagementsysteme (PMS) für Handel und Beschaffung oder Geografische Informationssysteme (GIS) für Netzplanung und -betrieb (Tiemeyer 2017). Das bekannteste ERP-System stammt vom gegenwärtigen Marktführer, dem deutschen Unternehmen SAP.

Die verschiedenen Informationssysteme werden übersichtlich in einer Applikations- bzw. Anwendungsarchitektur gesammelt (z.B. in Form einer IT-Landkarte) und deren Beziehung zu Kernprozessen des Unternehmens sowie zur Daten- und Infrastrukturebene dargestellt, Beziehungen und

Schnittstellen zwischen den Applikationen werden analysiert und festgehalten. Die Anwendungslandschaft in einem typischen Stadtwerk mit verschiedenen Geschäftsfeldern hat eine erhebliche Komplexität aus i.d.R. weit über 100 verschiedenen Softwaresystemen unterschiedlicher Größe, die es im Zusammenspiel mit der Prozesslandschaft zu managen gilt.

Prozessmanagement hilft nicht nur, Prozesse im Unternehmen besser nachvollziehen zu können, sondern auch Verantwortlichkeiten und Rollen eindeutig zuzuordnen und Transparenz über alle verbundenen Prozesse zu schaffen. Diese Transparenz sorgt für einen flüssigen Ablauf und ein zielgerichtetes Arbeiten und schafft ebenfalls Vertrauen und Motivation unter Angestellten. Aufgaben und deren Zweck bzw. Auswirkungen werden ersichtlich und verständlich, können effizienter gestaltet oder in ihrer Wichtigkeit geschärft werden.

Dabei ist es essenziell, zu Beginn neben der Identifikation der darzustellenden Geschäftsprozesse den gewünschten Detailgrad dieser Darstellungen festzulegen. Überschaubare, zusammengefasste Prozesse sorgen für einen schnellen Überblick und Eindruck der allgemeinen Unternehmensabläufe, können aber zur Vernachlässigung wichtiger Teilaspekte führen, welche eventuell essenziell für das Funktionieren der Gesamtstrategie sind. Zu komplexe Darstellungen aller Prozesse hingegen erfordern erheblichen Aufwand in der Erstellung und können bei unzureichender Pflege und Aktualisierung schnell an Sinnhaftigkeit verlieren. Es sollte daher ein Kompromiss gefunden werden, der so viele Prozesse wie möglich aufgreift, bei denen eine dauerhafte Pflege zu bewältigen ist und der gleichzeitig einen guten Überblick verschafft. Es sollte aber auch ermöglicht werden, in verschiedene Unterebenen von Unternehmensabläufen einzutauchen, um nachhaltig Prozesse anpassen, austauschen oder optimieren zu können. I.d.R. erhält man das gewünschte Resultat durch eine möglichst vollständige Darstellung der Unternehmens- und Bereichsprozesslandkarten (in denen die Prozesse zunächst strukturiert identifiziert werden) und die Detailmodellierung ausgewählter Prozesse aus diesen Prozesslandkarten. Auf diese wird in → *Kapitel 4* genauer eingegangen.

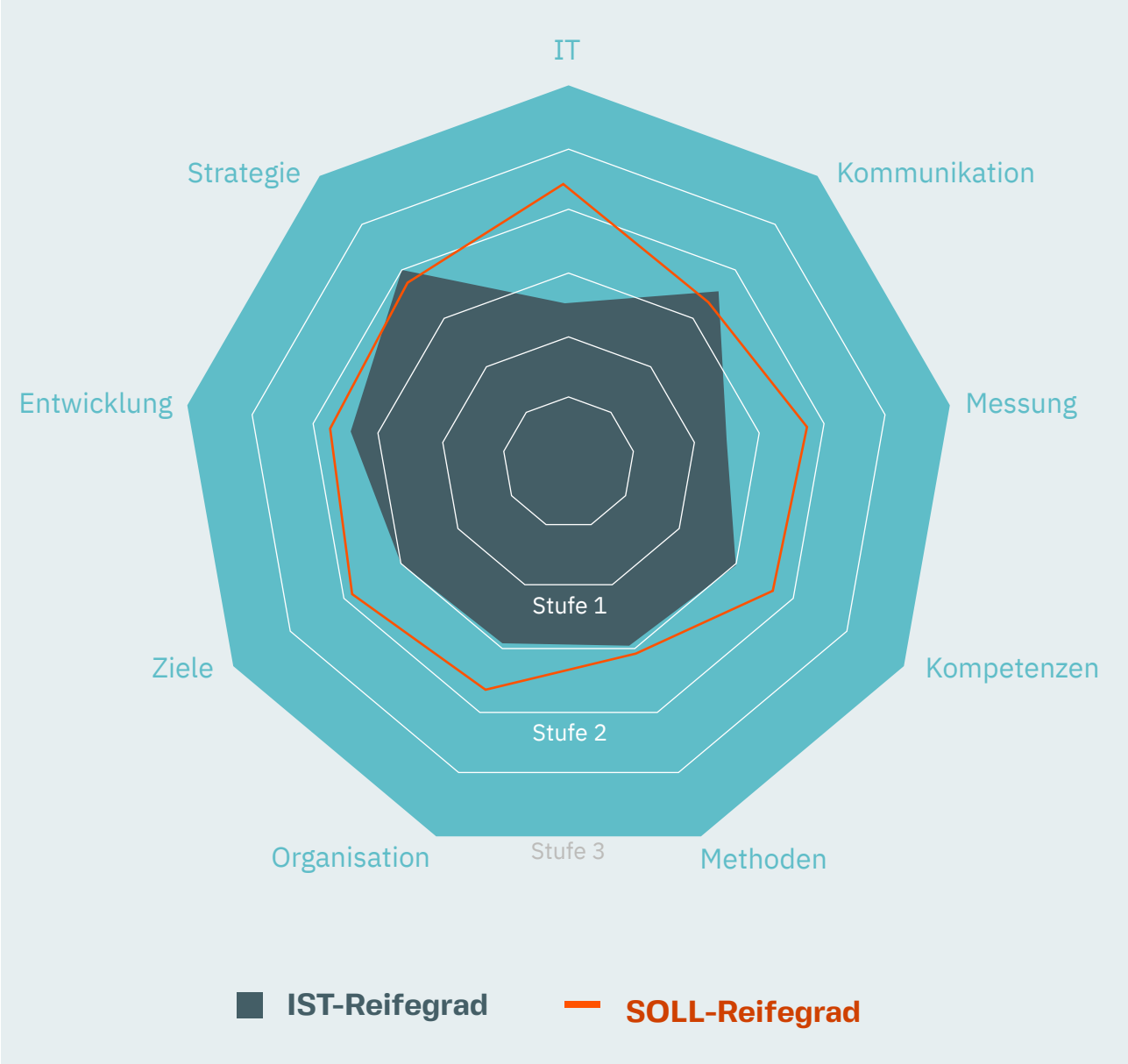
Nach Erstellung einer ausreichend komplexen Prozesslandkarte beziehungsweise Architekturlandschaft sollte eine Bewertung derselben stattfinden, beispielsweise durch eine SWOT-, Maturitäts-, Nutzwert- oder Gap-Analyse. So können Architekturen sinnvoll hinsichtlich ihrer Eignung zur Unterstützung der Geschäftsprozesse (i.d.R. die Erstellung von Produkten oder Dienstleistungen) betrachtet und bei Bedarf angepasst werden. Lücken in der Bebauung, Chancen und Risiken können dadurch leichter erfasst und zeitnah behoben werden. Insbesondere für eine strategische Planung eignet sich die visualisierte Darstellung der Anwendungslandschaft. Zusätzlich sollten ergänzende Angaben zu Anwendungssystemen und Schnittstellen strukturiert erfasst werden.

3.1.3 Reifegradbestimmung

Die Bestimmung des Reifegrads des IT-Einsatzes ist die Grundlage, um ein individuelles, angemessenes und nachhaltiges IT-Management verbunden mit einer digitalen Roadmap aufsetzen zu können. Durch die Erhebung des digitalen Reifegrads eines Unternehmens kann der Status quo der digitalen Transformation in verschiedenen Bereichen eines EVU erhoben und dadurch Stärken aber auch Schwachstellen identifiziert und bearbeitet werden. Viele bestehende Ansätze zielen auf die Analyse des Reifegrades von Prozessen, die für das IT-Management und die Digitalisierung relevant sind, ab. Dabei unterteilt man je nach Reifegradmodell in verschiedene Stufen, wobei die unterste Stufe diese Prozesse als chaotisch und undefiniert beschreibt und auf der höchsten Stufe Prozesse nicht nur geführt, sondern auch stetig optimierend ausgeführt werden. Die höchste Stufe kann, muss aber nicht Ziel sein. Die Reifegradbestimmung liefert zwar eine eindeutige Positionierung, die die

Reife beispielsweise der strategischen IT-Planung oder des Einsatzes von Geschäftsprozessmanagement darstellt, dennoch muss jedes EVU individuell und mit Blick auf die eigenen Ziele, den Markt und potenzielle Wettbewerber entscheiden, in welchen Dimensionen eine Verbesserung des Reifegrads am wichtigsten ist. Daher sollte nach Bestimmung des IST-Reifegrads ein SOLL-Reifegrad festgelegt werden. Mit der Führungsebene können anschließend Maßnahmen erarbeitet werden, mit welchen der SOLL-Reifegrad erreicht werden kann. Abbildung 9 stellt den IST- und SOLL-Reifegrad eines EVU beispielhaft dar. Aus der Darstellung kann man exemplarisch ablesen, dass im Bereich der IT der Reifegrad unter Stufe 1 liegt. Im SOLL-Zielbild muss er auf Stufe zwei oder höher klettern. Die Dimensionen der Reifegradanalyse und konkreten Fragestellungen je Dimension können individuell ausgeprägt werden.

Abbildung 9: IST- und SOLL-Reifegrad
Quelle: Eigene Darstellung



3.2 Stufe 2: Die Definitionsphase

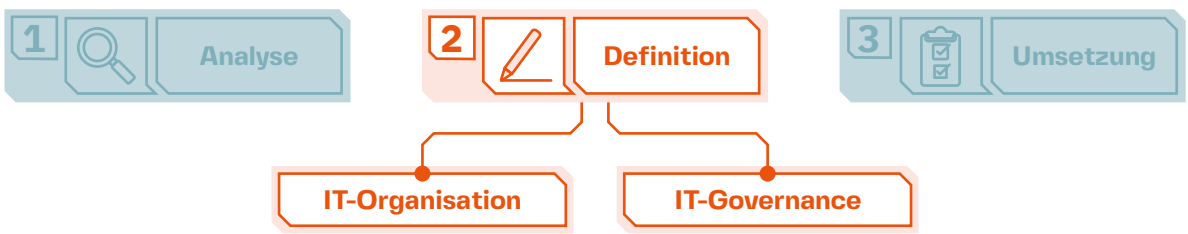
Die Bestimmung des Reifegrads in der Analysephase bildet die Grundlage für Schritt 2 – die Definition der IT-Organisation und der IT-Governance mit Hinblick auf die Etablierung eines zukunftsorientierten IT-Managements.

3.2.1 IT-Organisation

Die IT-Organisation stellt den Antrieb eines digitalisierten, dynamischen Unternehmens dar. Dafür muss sie eine neue, individuelle Rolle im Unternehmen einnehmen. Ziel einer idealen IT-Organisation ist allem voran das Erbringen der vereinbarten IT-Produkte und IT-Services zeitgerecht und wirtschaftlich in hoher Qualität für die (internen und externen) Kunden. Um dieses Ziel zu erreichen, sollte die Frage nach der organisatorischen Verankerung der IT-Funktionen sowie deren Vertretung in der Leitungsebene gestellt werden. Dabei stehen geeignete, also flexible Anpassungen an die jeweiligen aktuellen Bedürfnisse sowie modulare, sprich lose gekoppelte, separat anpassbare Architekturen aber auch Mitarbeiter mit entsprechenden Fähigkeiten und Begabungen sowie speziellen Ausbildungen im Mittelpunkt (Urbach und Ahlemann 2016). Es sollte beachtet werden, dass die IT-Organisation einem steten Wandel unterliegt und daher einer ständigen Prüfung zu unterziehen ist.

Die meisten IT-Organisationen arbeiten heutzutage nach dem Plan-Build-Run-Prinzip, welches hauptsächlich auf die Entwicklung und den Betrieb individueller Anwendungssysteme durch die eigene IT-Organisation setzt. Im Einzelnen wird die Bereitstellung neuer Technologien systematisch geplant, umgesetzt und die resultierenden Services effizient betrieben (Koch et al. 2016). Nach Erfahrung der Autoren verkürzen allerdings mehr und mehr Unternehmen ihre interne IT-Wertschöpfungskette und lagern Prozesse getreu dem Source-Make-Deliver Paradigma an externe Partner aus. Zudem liegt die Kernkompetenz eines EVU i.d.R. nicht in der eigenen Softwareentwicklung, sondern dem Einsatz von (ggf. angepasster) Standardsoftware, zunehmend mit einem steigenden Anteil von zu integrierenden Cloudanwendungen. In der Energiebranche werden – womöglich aufgrund des hohen Kostendrucks im Zusammenhang mit der Energiewende - im Vergleich zu anderen Branchen jedoch weniger externe Partner beschäftigt. Branchenübergreifend ist die Inanspruchnahme von Outsourcing-Anbietern bei Individualanwendungen, Standardanwendungen und Plattformen leicht rückgängig. Gerade bei Individualanwendungen wird vor allem auf die unternehmenseigene IT-Abteilung zurückgegriffen (Capgemini Consulting 2018). Der Fokus dieses Paradigmas bezieht sich primär auf das Management der Leistungsbeziehungen der IT zu Kunden und Lieferanten. Beide Paradigmen heben die Eigenständigkeit der IT-Wertschöpfungskette in den Vordergrund, was eine unabhängige Planung und Steuerung erfordert.

Abbildung 10: Phase 2 – Definition
Quelle: Eigene Darstellung



Das IT-Management kann sich dann auf Effizienz und Verlässlichkeit konzentrieren.

Zu aufwändige Planungsphasen bei immer schneller werdenden Innovationszyklen, ein zu starres und unflexibles IT-Gerüst mit zu langsamen Reaktionszeiten auf Markt- und Technologietrends sowie die Ignoranz von kurzfristigen externen marktorientierten oder technologischen Impulsen lassen das Plan-Build-Run-System ungeeignet erscheinen für die gegenwärtigen Entwicklungen der Digitalisierung. Auch Source-Make-Deliver, wo der Fokus verstärkt auf das Management der Lösungszulieferer und der Kundenbeziehung gerichtet wird, ist als eher reaktives Modell nur wenig geeignet, externe Impulse aufzunehmen und entsprechend schnell darauf zu reagieren (Capgemini Consulting 2018). IT ist im Rahmen der Digitalisierung ein zentraler Bestandteil neuer Produkte, Dienstleistungen und vollständiger Geschäftsmodelle. Deswegen muss die IT-Organisation frühzeitig und proaktiv mit den verschiedenen Fachbereichen kooperieren.

Ein neues Paradigma, in welchem die IT-Organisation nicht mehr reaktiv auf die Wünsche der Fachabteilungen wartet, wird notwendig.

Innovations-, Gestaltungs- sowie Transformationsfähigkeit stellen die Kernkompetenzen einer zukunftsgerichteten, digitalisierungswilligen IT-Organisation dar, woraus sich das neue Paradigma Innovate-Design-Transform ergibt. Eine enge Zusammenarbeit mit den jeweiligen Fachbereichen für eine gemeinsame Konzeption und Umsetzung von Geschäfts- und Wertschöpfungsmodell-Innovationen steht im Mittelpunkt. Die Entwicklung von Implementierungskompetenzen verliert in Zukunft an Relevanz; Kreativität, Flexibilität und Design-Kompetenz hingegen werden zunehmend bedeutender - gleichermaßen ein Kulturwandel im Unternehmen (ebd.).

Neben dem auf Innovation und Flexibilität ausgerichteten Paradigma bildet ein möglichst vereinheitlichte IT-Landschaft einen wichtigen Grundstein von zukunftsfähigen IT-Organisationen. Aus der vorangegangenen Analyse sollte dem Status quo der IT-Architektur eine hohe Relevanz zugeordnet werden. Gerade bei Energieversorgern treffen sehr viele Prozesse, Technologien und Produkte aufeinander, welche es zu managen gilt. Standards in der IT gewinnen zunehmend an Bedeutung, nicht zuletzt aufgrund jüngster Entwicklungen im Bereich des Datenschutzes und der IT-Sicherheit. Ein Standard ist ein gemeinsames Verständnis oder eine Vereinbarung Spezifikationen betreffend, welcher bestimmte Abläufe, Regeln oder Anforderungen umfasst. In der Energiewirtschaft sind das unter anderem technische Mindestanforderungen, Informationskaskaden sowie automatisierte Marktprozesse und Datenformate (BDEW 2016). Ziel einer Standardisierung ist allem voran die Kostenreduktion. Nebenbei können redundante Datenbestände, Medienbrüche sowie Dateninkonsistenzen reduziert werden. Zudem wird die überbetriebliche Kompatibilität mit den Systemen von Geschäftspartnern gefördert (Beimborn o. J.).

Das IT-Management als unterstützender Unternehmensbereich hängt bisweilen hinterher. Prozesse in der IT werden oftmals noch individuell gestaltet und nur zum Teil standardisiert erbracht (z.B. im Rahmen des IT-Servicemanagements). Deswegen ist in vielen Unternehmen eine transparente und dokumentierte Übersicht aller Prozesse nur in geringem Grad vorhanden und eine gezielte und strukturierte Anpassung an geänderte Bedingungen nur sehr begrenzt möglich, was im Rahmen einer agilen und iterativen Digitalisierungskultur vor dem Hintergrund aufkommender Wettbewerber von Nachteil ist (Zarnekow 2005). Die Geschwindigkeit der Entwicklung neuer Trends und Technologien bestimmt, wie lange Standards u.a. im Bereich Soft- und Hardware auch als Standard gelten, ob sie sich etablieren oder nach kurzer Zeit durch aktuellere Entwicklungen abgelöst werden. Diese Geschwindigkeit bei der Festlegung von Standards macht es daher für Energieversorger essenziell, stets auf dem neusten Stand zu sein und den

Digitalisierungsprozess als fortwährende Entwicklung und nicht als einmaliges Projekt zu begreifen.

Um nachhaltig und effizient eine Digitalisierung zu ermöglichen, sollten Unternehmen prüfen, ob es überhaupt eine Übersicht gibt, die alle eingesetzten Standards im Unternehmen verzeichnet. Oftmals beginnt damit der erste Schritt zu einer transparenten und reaktiven Prozessgestaltung in der IT-Organisation. Es sollte sich bewusst gemacht werden, welche Standards den Markt der Branche anführen und ob das Unternehmen in der Lage ist, sich schnell auf neue Standards einstellen zu können. Ist dies nicht der Fall, muss noch weiter vorn angegriffen und die Unternehmensstruktur sowie das Geschäftsmodell überdacht werden.

Im liberalisierten Energiemarkt existieren verschiedene digitale Lösungen, die unternehmensinterne Prozesse sowie Marktprozesse zwischen den einzelnen Energieversorgern oder Unternehmen anderer Branchen prozess- und kosteneffizient gestalten (BDEW 2016). Grundlage für moderne (betriebswirtschaftliche) Standardsoftware ist eine funktionierende Prozessorganisation. Software sollte möglichst direkt prozessorientiert implementiert werden, indem entweder im Rahmen der Anforderungserstellung die konkret abzubildenden Prozesse bereits definiert oder Standardprozesse der Anwendung für die Zielumgebung angepasst werden. Mit der Darstellung der Prozesslandschaft und der zugehörigen IT-Unterstützung sind die beteiligten Akteure (Geschäftsführung, Fachabteilungen und IT-Management) in der Lage, ein unternehmensübergreifendes Gesamtbild zu gestalten, welches für Transparenz und damit eine effiziente Realisierung der Geschäftsziele sorgt.

IT-Governance beschreibt die Verantwortung der IT und ihre Fähigkeit zur Erreichung der Unternehmensziele und ist damit Teil der Corporate Governance, also der Steuerung des gesamten Unternehmens. Sie beantwortet die Frage, was die IT für den Unternehmenserfolg leisten kann und welche Rahmenbedingungen hierfür durch das Management zu schaffen sind (Luber und Schmitz 2017). Bei der IT-Governance steht die Konformität und nicht die Performance im Vordergrund. IT-Systeme und damit verbundene organisatorische Strukturen und Prozesse sollten durch sie möglichst wirtschaftlich gestaltet werden. Durch eine klare IT-Governance können IT-Systeme und Applikationen konsolidiert, Anforderungen der Fachbereiche an die IT harmonisiert und Projekte zentral gesteuert werden.

Die Folgen einer nur unzureichend ausgeprägten oder nicht vorhandenen Governance sind eine Vielzahl verschiedener IT-Architekturen, eine mangelhaft gesteuerte Leistungserbringung sowie fehlende Skaleneffekte für die IT-Beschaffung, viele redundante IT-Lösungen und mangelnde Portfolio- und Projektsteuerung (Tiemeyer 2017).

Für die Definition einer bestehenden IT-Governance müssen verschiedene Entscheidungsprozesse hinterfragt werden. Dazu zählen die „Spielregeln“ für verschiedene Fragestellungen des IT-Einsatzes im Unternehmen (z.B. Ausrichtung und Leitung der IT, Beschaffung, Demandmanagement, Portfoliomanagement, Architekturmanagement, IT-Controlling) inkl. zugehöriger Verantwortlichkeiten. Bei der Definition sollte stets betrachtet werden, ob die IT-Governance zum Ziel hat, dass Chancen und Risiken der IT und mit der IT gemanagt werden (ebd.). Diese Position verschafft der IT eine aktive Rolle, in welcher sie zur Erreichung der Unternehmensziele effizient beitragen kann.

Das Framework COBIT[2] (Control Objectives for Information and Related Technology) eignet sich besonders für die Umsetzung einer IT-Governance. COBIT als ein umfassendes Framework stellt einen international anerkannten Standard für IT-Governance und IT- Controlling dar und deckt

2 https://www.isaca.org/resources/cobit

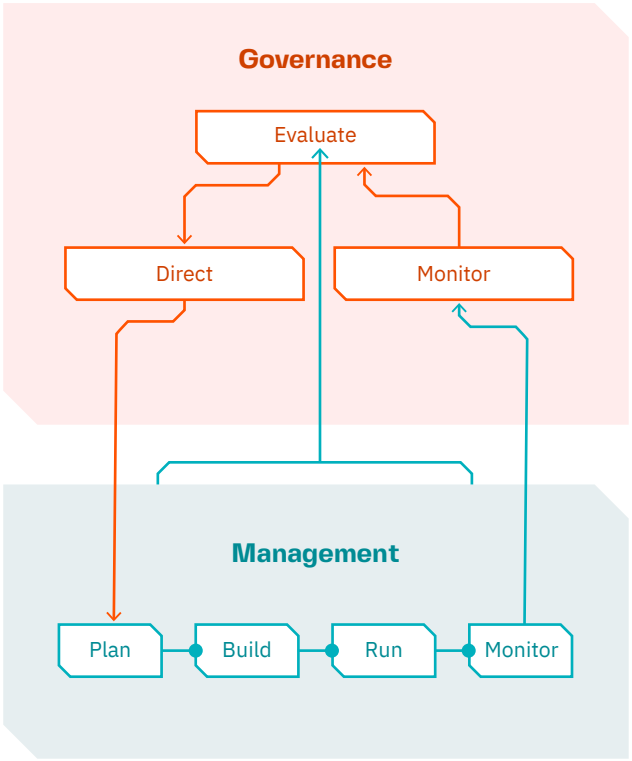
Prozesse der IT ganzheitlich ab. Für jeden COBIT Prozess werden eine Prozessbeschreibung, ein Prozessziel, wesentliche Aktivitäten und Messgrößen, Kontrollziele, Managementrichtlinien sowie Reifegradmodelle festgelegt. Ein Framework wie COBIT unterstützt den Aufbau eines internen Planungs-, Kontroll- & Steuerungssystems. Zentral hierbei sind die Schaffung einer Verbindung von IT und Geschäftsanforderungen, die Einbindung IT-bezogener Aktivitäten, die Identifikation zu steuernder IT-Ressourcen sowie die Definition zu berücksichtigender Kontrollziele. Ziel von COBIT ist die ganzheitliche Ausrichtung der IT auf Unternehmenslösungen, also der Übereinstimmung von Geschäfts- und Digital-Strategie sowie eine unternehmensweite Standardisierung und erhöhte IT-Verfügbarkeit durch die Einführung von Soft- und Hardware für mehr Flexibilität und Adaptionsfähigkeit der installierten IT-Systeme.

Das Framework erlaubt (in der aktualisierten Fassung von 2019) zudem eine individuelle Ausprägung aufgrund zuvor festgelegter Zielstellungen und Gestaltungsparameter, sodass EVU in der Lage sind, ihre IT-Governance flexibel zu gestalten und zusätzlich agile Elemente einfließen zu lassen.

Weiterhin soll durch das COBIT-Framework die Wirtschaftlichkeit der IT für das Gesamtunternehmen gewährleistet werden sowie besseres Innovations- und Investitionsmanagement sowie eine Vereinheitlichung und Vereinfachung der IT-Landschaft stattfinden. Auch das Minimieren von Risiken durch ein effizientes Risikomanagement spielt dabei eine Rolle.

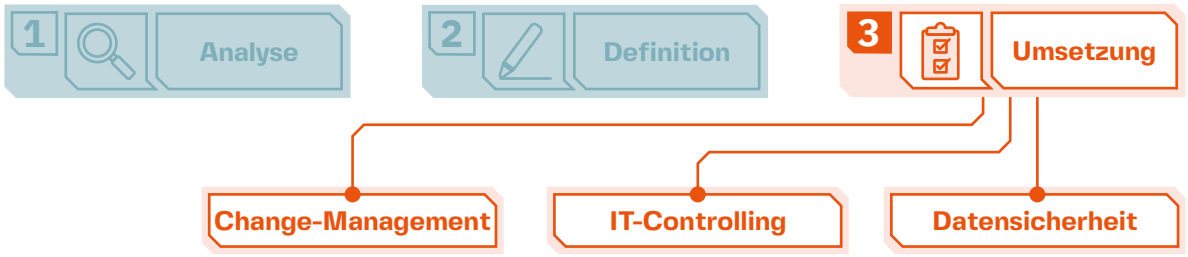
Das Framework unterteilt sich in Governance und Management-Domänen, die aufzeigen, welche Prozesse an welcher Stelle zu implementieren sind. Das Prinzip der Aufteilung ermöglicht eine genauere Zuweisung der Zuständigkeiten sowie die Vollständigkeit der Unternehmensressourcen, die die Erreichung der Unternehmensziele ermöglichen sollen, wie z.B. Prinzipien, Richtlinien und Rahmenwerke oder Kultur, Ethik und Verhalten etc. Die Governance-Domäne wird im COBIT-Kosmos EDM – Evaluieren, Vorgeben und Überwachen (englisch: evaluate, direct and monitor) genannt. Diese Prozesse stellen den Rahmen und die Regeln auf, denen die Managementprozesse folgen (Tiemeyer 2017). Sie beschäftigen sich mit dem Sicherstellen der Einrichtung und Pflege des Governance-Rahmenwerks, der Lieferung von Wertbeiträgen, der Risiko-Optimierung, der Ressourcenoptimierung sowie der Transparenz gegenüber Anspruchsgruppen (ISACA 2018).

Abbildung 11: Governance- & Managementprozesse
Quelle: nach COBIT



EVU stehen vor der Aufgabe, ihre IT-Governance auch auf neue Geschäftsmodelle, die wichtig für deren Weiterentwicklung sind, auszurichten. Dazu zählen zum Beispiel die organisatorische Verknüpfung der Softwareentwicklung mit Organisationsformen wie Kompetenz-Center im Umfeld energiewirtschaftlicher und technischer Systeme mit den Fachbereichen für eine schnellere Reaktion auf Geschäftsanforderungen (VKU 2017).

Abbildung 12: Schritt 3 – Umsetzung
Quelle: Eigene Darstellung



3.3 Stufe 3: Die Umsetzung

Auf Grundlage der in der Analysephase erfolgten Positionsbestimmung inkl. Ermittlung des Reifegrades des IT-Einsatzes und des in der Definitionsphase festgelegten Zielbildes erfolgt in der dritten Stufe des Vorgehensmodells die Umsetzung abgeleiteter Maßnahmen. Ziel ist es, das IT-Management so aufzustellen, dass eine erfolgreiche Digitalisierung ermöglicht wird. Für ein typisches EVU könnte dies beispielhaft bedeuten, dass:

- ↳ *eine IT-Strategie inkl. Digitalisierungsstrategie vorliegt,*
- ↳ *alle relevanten Entscheidungsprozesse den IT-Einsatz betreffend durch Vorgaben der IT- Governance definiert sind,*
- ↳ *das Geschäftsprozess- und Anwendungsarchitekturmanagement Fachbereiche und IT befähigen, gemeinsam und auf Augenhöhe Anforderungen an eine adäquate IT-Unterstützung zu formulieren,*
- ↳ *ein Portfolio- und Multiprojektmanagement etabliert ist,*
- ↳ *IT-Services hocheffizient erbracht werden,*
- ↳ *Informationssicherheit und Datenschutz explizit adressiert werden,*
- ↳ *innovative Technologien, Plattformen und Organisationsansätze laufend durch gewisse Monitoringprozesse auf ihre Eignung für den Einsatz im Unternehmen untersucht werden und*
- ↳ *strategische Partnerschaften eingegangen werden.*

In der Umsetzungsphase sollte das Hauptaugenmerk zusätzlich auf die Themen Change-Management, IT-Controlling sowie IT-Sicherheit gelegt werden.

3.3.1 Change-Management

Das Change-Management unterstützt dabei, notwendige Änderungen an den IT-Verfahren effektiv und effizient umzusetzen (Groß 2011). Basis für eine erfolgreiche Implementierung eines zukunftsfähigen IT-Managements bilden die Mitarbeiter eines EVU. Vor allem eine positive mentale Einstellung Veränderungen gegenüber und damit die Bereitschaft für die schnelle Adaption von Innovationen, aber auch eine gewisse Fehlertoleranz, machen wichtige Erfolgsfaktoren aus. Das wird am besten durch eine planvolle und flächendeckende Kommunikation erreicht.

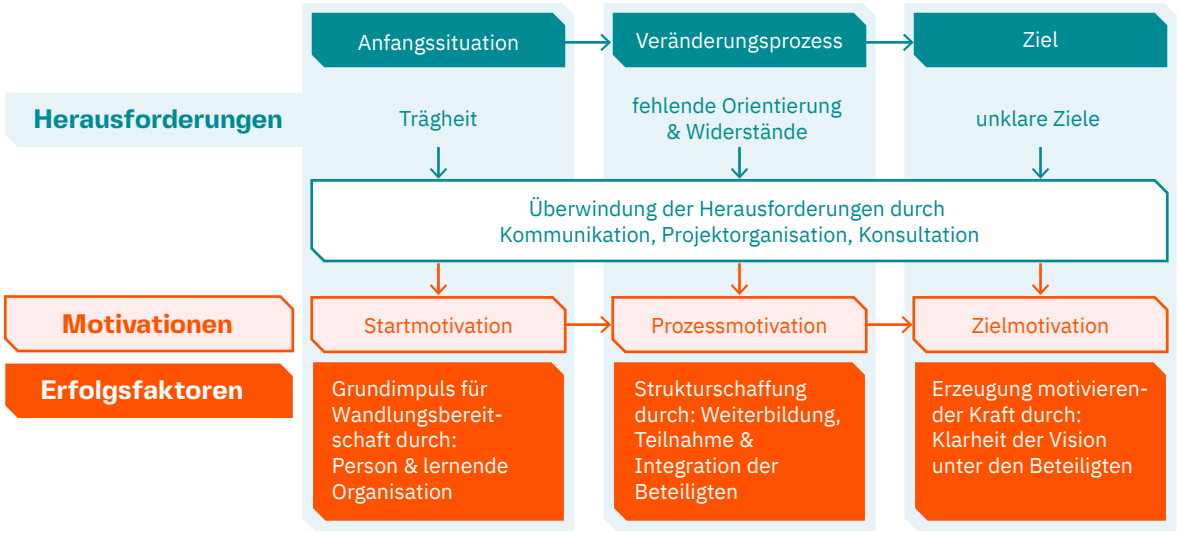
Wichtigstes Werkzeug dabei sind neben den Führungkräften sogenannte Change Manager, projekterfahrene Manager mit viel Expertenwissen im Change-Management, welche im Idealfall eine solide Kommunikationsfähigkeit, die Bereitschaft zur Kooperation und partnerschaftlichen Konfliktlösung,

Motivationsgabe und die Fähigkeit zur Organisation von Teamprozessen in sich vereinen (Capgemini Consulting 2015).

Das Change-Management kann in drei Phasen unterteilt werden, die sich unterschiedlichen Herausforderungen stellen müssen. Die Anfangssituation eines Unternehmens zu Beginn des Veränderungsprozesses steht vor allem einer allgemeinen Trägheit unter Mitarbeitern und damit etablierten Prozessen, Abläufen und Kulturen gegenüber. Um eine Startmotivation und einen Grundimpuls für Wandlungsbereitschaft unter den Beteiligten zu schaffen, ist es wichtig, mit dem Wandel beim Individuum und der sich transformierenden Organisation zu beginnen. Erst wenn unter den Personen des Unternehmens auch ein Wille zum Wandel und eine Bereitschaft zur aktiven Beteiligung geschaffen wurde, kann der Veränderungsprozess beginnen. Dieser läuft Gefahr, durch interne oder externe Widerstände aus verschiedenen Abteilungen und Ebenen aber auch einer fehlenden Orientierung innerhalb des Veränderungsprozesses zu scheitern. Eine intrinsische Motivation mit dem Selbstzweck als Ziel der Handlung muss an dieser Stelle geschaffen werden. Hilfreich dafür sind Methoden wie Kollaborationen zwischen Unternehmen, eine neue Selbstorganisation, Mitarbeiterzufriedenheitsanalysen und -motivation. Ein neues Change-Management fordert von Unternehmen, sich aktiv weiterzuentwickeln. Wichtig dabei ist, dass obwohl die Digitalisierung und Technisierung und damit neue Kompetenzen und Anwendungen zunächst im Vordergrund zu stehen scheinen, der Mensch bzw. Mitarbeiter jedoch an keiner Stelle außer Acht gelassen werden sollte und bei allen Veränderungen mit einbezogen wird. Nur durch ein aktives Veränderungsmanagement zusammen mit den Mitarbeitern kann eine digitale Transformation erfolgreich gemeistert werden (Wanner 2017).

So kann schließlich das Ziel der Transformation erreicht werden, sofern dies eindeutig definiert wurde. Eine Klarheit der Zielvision sollte bei allen Beteiligten vorherrschen (Lauer 2019).

Abbildung 13: Zielvision für Transformation im Change-Management
Quelle: Eigene Darstellung



Für die Überwindung der Herausforderungen im Change-Prozess sind in allen Phasen Kommunikation, Projektorganisation sowie Konsultation wichtige Erfolgsfaktoren. Durch eine ebenenübergreifende Kommunikation wird nachhaltig Transparenz und Orientierung für alle Beteiligten geschaffen. Sie dient dabei als Katalysator und schafft informatorische Transparenz, erkennt und schwächt Widerstände ab, verstärkt den Prozess im Sinne einer positiven Rückkopplung und fördert soziale Integration (Lauer 2019). Eine angemessene Kommunikationskultur spielt ebenfalls bei der Konsultation, sprich der Inanspruchnahme von externen oder auch hausinternen Beratungsleistungen eine Rolle. Im Rahmen von Strategie-, IT- oder Personalberatung kann der Change-Prozess unterstützt werden (ebd.). Auch Methoden des Projektmanagements helfen dem Change-Management, verschiedene Aufgaben für die Bewertung, Qualifizierung und kontrollierte Steuerung aller IT-Projekte übergreifend zu analysieren.

Durch ein solches Management kann eine sachgerechte Anforderungsdefinition für IT-Projekte stattfinden, damit nur gewinnbringende bzw. zielführende Projekte identifiziert und umgesetzt werden. Kosten, Nutzen, Risiken und Chancen werden gemeinsam betrachtet und der Projektaufwand durch die Betrachtung im Idealfall um 5 bis 10% reduziert (Tiemeyer 2017).

3.3.2 Strategisches IT-Controlling und Datensicherheit

Auch das IT-Controlling unterliegt einem Wandel durch die digitale Transformation.

Diente das Controlling vorher lediglich der Überwachung der Kosten, welche die IT verursachte, so stehen jetzt vor allem die Darstellung von Leistungen, Wertbeiträgen und der Nutzen der IT im Mittelpunkt.

Vor allem gewinnen Risikokennzahlen und zukunftsbezogene Informationskennzahlen (Prognosen) sowie systemgestützte szenarienbasierte Planungsrechnungen zur Ableitung konsistenter Strategien an Bedeutung (Rahmel et al. 2012). Für eine Überwachung der Zielerreichung müssen in diesem Zusammenhang Kennzahlen verwendet werden, um die Leistung verschiedener Prozesse sowie deren Qualität zu erheben und zu analysieren. Die Ziele eines angepassten zukunftsorientierten IT-Controllings umfassen Effizienz und Effektivität von Planung, Steuerung und Kontrolle aller IT-Prozesse (Tiemeyer 2017).

Mit Kennzahlen, die an Prozesse geknüpft sind, können Zielgrößen und Zielwerte operationalisiert und so genaue Vorgaben von festgelegten Zielen gemacht werden. Bei den großen EVU stehen ergebnisbasierte und wertorientierte Kennzahlen im Vordergrund. Kleine EVU konzentrieren sich hingegen eher auf die ergebnisbasierten Größen oder die Rohmarge (Rahmel et al. 2012). Der große Nutzen von Kennzahlen besteht vor allem darin, nach erfolgreicher Implementierung bestehende Soll- und Ist-Abweichungen zu analysieren und gegebenenfalls direkt anzupassen. Kennzahlen sind damit gut geeignet, bestehende Sachverhältnisse objektiviert darzulegen und an Akteure des Unternehmens weiterzugeben. Sie erfüllen daher nicht nur eine wichtige Kontroll- sondern auch Kommunikationsfunktion, welche durch Transparenz auch das Verständnis der beteiligten Mitarbeiter für vorliegende Prozesse schärft. Maßnahmen, die auf Basis von Kennzahlen zur Optimierung ergriffen werden müssen, sind damit verständlich und begründet für die relevanten Akteure zugänglich. Nicht nur mögliche Problemquellen, sondern ebenfalls Erfolge können damit sichtbar und eindeutig erhoben werden. Dafür ist die Nutzung eines Verhältnismaßstabes unabdinglich. Dies ist die Grundlage, um durch Prozessmodellierung tatsächlich einen Mehrwert für das Unternehmen zu generieren.

Wichtig dabei ist, eine angemessene Anzahl an Kennzahlen festzulegen, welche durchgängig erhoben und analysiert werden sollen. Zu viele Kennzahlen können schnell zu einer schwierig zu handhabenden Komplexität führen. Zu wenige hingegen begünstigen zwar die Verdichtung von Informationen, können aber auch wesentliche Einflussfaktoren und Ursachenquellen verschleiern (Helmke und Uebel 2016).

IT-Controlling sollte dabei in jeder der Phasen des Vorgehensmodells mitgedacht werden. Die Koordination des Informationsmanagements einer Organisation und die Information des Managements über die Effektivität und Effizienz der IT-Aktivitäten stehen hierbei im Mittelpunkt (Tiemeyer 2017). Das IT-Controlling kann als Stabsstelle, Parallelorganisation oder einer Kombination beider Formen im Unternehmen verankert sein. Im Gegensatz zum ergebnisverantwortlichen IT-Management ist das IT-Controlling für die Transparenz verantwortlich. Damit bietet es dem Management einen Informations-, Entscheidungs- und Koordinationsservice. Im Fall des Vorgehensmodells sollte das IT- Controlling sowohl im Rahmen der IT-Governance in der Definitionsphase als auch in der Umsetzung hinsichtlich des Change-Managements bedacht werden.

Auch das Thema IT- und Datensicherheit sollte mit besonderer Aufmerksamkeit behandelt werden. Neue Bedrohungen entwickeln sich mit fortschreitender Digitalisierung und der Abhängigkeit von Informations- und Telekommunikationssystemen. Ein Ausfall des Betriebs sowohl durch Angriffe, aber auch durch schlichte Unachtsamkeit oder lapidare Vorsichtsmaßnahmen kann verheerende Folgen haben. Nicht nur der Schutz zentraler Netzleit- und Netzführungssysteme, sondern auch anderer unternehmensinterner Systeme wie kaufmännische Anwendungen oder die Verarbeitung personenbezogener Kundendaten beispielsweise in Onlineportalen sollten eine zentrale Rolle spielen (BBH 2017).

Um diesen Herausforderungen zu begegnen, müssen Änderungen in der Organisation des IT-Betriebs und Investitionen zur Anpassung der IT-Landschaft stattfinden. Im Idealfall wird der Bereich der IT-Sicherheit und des Datenschutzes in der Geschäftsführungsebene verankert – schließlich muss dort gehaftet werden, wenn Probleme auftauchen. Eine entsprechende Positionierung sollte dabei schon in der Definitionsphase vorgesehen werden. So haben vor allem große Unternehmen eine zentrale und verantwortliche Instanz für Datensicherheit etabliert, bei den kleinen und mittleren Unternehmen sind es hingegen nur 70% (ebd.). Hier besteht unbedingt Nachholbedarf.

Die tadellose Umsetzung der neuen regulatorischen Datenschutz-Grundverordnung ist dabei zwingende Voraussetzung, genau wie die Einhaltung des IT-Sicherheitsgesetzes oder der Einsatz eines Information Security Management Systems (ISMS) zur Definition von Regeln und Methoden zur Gewährleistung der Informationssicherheit im Unternehmen. Wichtig dafür ist es, entsprechende Rollen und Verantwortlichkeiten fest zu verteilen. Auch die Hilfe externer Experten ist hierbei anzuraten. Für diese sollte stets im Mittelpunkt stehen, dass IT-Sicherheit angesichts flächendeckender digitaler Veränderungen geschäftsprozessübergreifend angegangen werden muss.

Auf das Thema IT-Sicherheit und Datenschutz wird genauer in in den Beiträgen → *drei* und → *vier* des Kompendiums eingegangen.

:// 4.
ABLEITUNG WICHTIGER BESTANDTEILE DES IT-MANAGEMENTS

Innovationspotenziale können nur voll ausgeschöpft werden, wenn im Unternehmen Flexibilität und Kreativität vorherrschen. Der Begriff „Agilität“ wird in diesem Zusammenhang oft verwendet. Um Agilität sinnhaft und nachhaltig umzusetzen, müssen gewisse Bereiche des IT-Managements selbst möglichst flexibel und anpassungsfähig sein. Diese Eigenschaften bilden gleichermaßen die Grundlage und Ziel des zukunftsfähigen IT-Managements.

Die wichtigsten Bestandteile des Vorgehensmodells entwickeln sich während des gesamten Prozesses der Digitalisierung – also im Idealfall zeitlich unbegrenzt – und passen sich an aktuelle Situationen schnell und bestenfalls automatisiert an. Dazu gehören zum einen aus IT-Sicht die IT-Landkarte und IT-Governance, zum anderen aus Business-Sicht das Geschäftsprozessmodell.

4.1 Flexible Geschäftsprozesse

Geschäftsprozesse und deren Optimierung sowie Automatisierung sind kein Produkt der Digitalisierung, sondern schon immer im Denken und Handeln von Geschäftsmodellen verankert und grundsätzlich ständigen Veränderungen unterworfen. Regelmäßige Anpassungen der Vorgaben durch die Regulierungsbehörde oder Gesetzgeber aber auch der technische Fortschritt und allem voran das Sammeln immens vieler Daten und die Notwendigkeit der Verarbeitung und Auswertung stärken die Relevanz einer neuen, digitalen Prozessgestaltung.

Treiber dieser neuen Geschäftsfelder sind u.a. Elektro-Mobilität, ganzheitliche Energieversorgungsangebote, Energiedienstleistungen, Energiemanagement, Energiespeicherung, dezentrale Erzeugung, Erzeugung aus Erneuerbaren Energien etc. (VKU 2015). Hinzu kommen veränderte Kundenerwartungen, Reaktionen auf sich ändernde und neue Wettbewerber, mobile Anwendungen aber auch der Optimierungsdruck im eigenen Unternehmen (BDEW 2015).

Im Rahmen der Digitalisierung haben sich Geschäftsprozesse und die Art und Weise ihrer Wirkung verändert. Sie veralten nun viel schneller, verlieren ihre Relevanz oder müssen sich kleinen Veränderungen schnell und flexibel anpassen. Das ist beispielsweise bei der Automatisierung wesentlicher Marktkommunikationsprozesse, der Kommunikation mit verschiedeneren Backendsystemen oder der Verarbeitung gemäß regulatorischer Vorgaben relevant. Langwierige, mehrmonatige IT-Projekte können das Ende für den Unternehmenserfolg bedeuten, denn es besteht immer die Gefahr, dass Wettbewerber durch neue agile und flexible Methoden schneller sind und Marktlücken besetzen. Um stets Aktualität zu besitzen, sollten Geschäftsprozesse deswegen kurzfristig an Änderungen angepasst werden können. Dazu gehört beispielsweise die Integration neuer Technologien oder die Nutzung von Plattformen. Daten müssen zudem übergreifend nutzbar und Geschäftsprozesse über funktionale Abteilungs- oder Bereichsgrenzen hinweg gestaltbar sein, Entwickler

oder Lösungsdesigner müssen Anwender aktiver mit in die Softwareentwicklung bzw. -anpassung einbeziehen und flexible Systeme zur anwendernahen Geschäftsprozessmodellierung und modernen und individualisierbaren Datenpräsentation bereitgestellt werden (VKU 2015).

Ein zukunftsorientiertes Geschäftsprozessmanagement lässt sich in folgenden Punkten zusammenfassen:

↳ *Implementierung eines iterativen und inkrementellen Ansatzes für eine flexible Berücksichtigung von Anforderungen und Optimierungspotenzialen während der Prozesserfassung und -ausführung*

↳ *Integration aller Prozessbeteiligten direkt in unterschiedliche Schritte des Geschäftsprozessmanagements*

↳ *Möglichkeit der Reaktion auf unvorhergesehene Änderungen, Iterationen von 2 bis 4 Wochen (Wiedmann 2016)*

↳ *stetige Überprüfung von Qualität und Akzeptanz der Geschäftsprozesse*

Grundlage bzw. nötige Maßnahmen für die Umsetzung eines digitalen Geschäftsprozessmanagements sind die Schulung der Mitarbeiter, die Schaffung von Voraussetzungen für eine Veränderungskultur (Change-Management) sowie eine gemeinsame übergreifende Prozessarchitektur und ein zentraler Bereich für Prozessmanagementangelegenheiten.

Prozessmanagement ist in diesem Zusammenhang nicht nur sinnvoll für eine Prozessoptimierung, sondern auch für eine unternehmensübergreifende Aufbau- und Ablauforganisation. Beim Prozessmanagement sollten Prozesse durch planerische, organisatorische sowie kontrollierende Maßnahmen unter Berücksichtigung von Qualität, Kosten, Zeit und Kundenzufriedenheit unterstützt werden. Wichtig dabei ist die Dauerhaftigkeit von Prozessen. Ein funktionierendes Prozessmanagement stützt sich auf die drei Säulen Prozessentwicklung, -führung sowie -kultur. In der Entwicklung sollten Visionen, Missionen und Strategien klar definiert sowie Prozessmodelle und Arbeitsanweisungen mit fester Rollenverteilung festgelegt werden. Bei der Prozessführung steht das Messen von Prozessen sowie die Festlegung von Verantwortlichkeiten, Kennzahlen und Instrumenten im Mittelpunkt. Die Prozesskultur beschreibt die Umsetzung aller Vorhaben (Microtech 2017).

4.2 IT-Governance – agile Frameworks für mehr Innovationsraum

Wie bereits in Abschnitt 3.2.2 erläutert, können Unternehmen für die Umsetzung der IT-Governance auf sogenannte Frameworks bzw. Referenzmodelle wie COBIT zurückgreifen.

Die Einführung eines unternehmensweiten Rahmenwerks für mehr Kontrolle und Transparenz ist zum einen förderlich für eine erste Transformation. Die IT-Governance läuft dabei allerdings auch Gefahr, zu einem starren Regelkonstrukt zu mutieren, was einem agilen System zunächst unzuträglich ist. Eine fortlaufende agile Anpassung an sich stetig ändernde Anforderungen wäre damit auf Dauer nicht gewährleistet. Technologie-Whitelists, die zwar für eine Standardisierung sorgen, aber zugleich den Einsatz neuer Technologien stark einschränken, zählen beispielsweise dazu. Ebenso fehlt durch die zentrale Steuerung die Möglichkeit für andere Akteure, Einfluss auf bestehende Vorgaben und damit Anpassung an digitale Prozesse vorzunehmen. Eine strikte Trennung zwischen Architektur und Entwicklung können ebenso gefährdend wirken.

Aus diesem Grund ist es wichtig, bewusst Raum für Innovation und Veränderung zu schaffen, welcher nicht durch ein starres Regelkonstrukt

eingeschränkt wird. Es sollte ein guter Mittelweg zwischen einer zentralistisch ausgeübten IT-Governance und der Ermöglichung von Innovationspotenzialen gefunden werden.

Um Einschränkungen der Innovationspotenziale zu verhindern, sollte eine zukunftsorientierte IT-Governance darauf achten, Gestaltungsverantwortungen bei den Mitarbeitern anzusiedeln, welche auch mit der Umsetzung von Prozessen betraut sind.

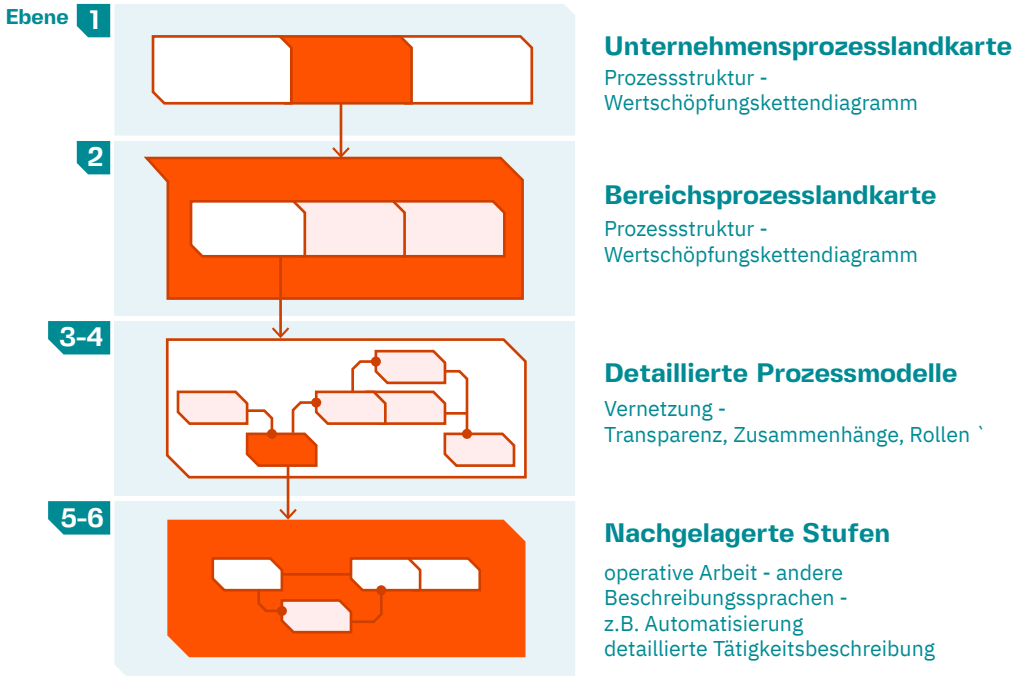
Bei Fehlern müssen Konsequenzen zwar vom Team selbst getragen werden, allerdings werden auch Räume für Optimierung und Effizienz geschaffen. Mitarbeiter müssen dahingehend geschult und für das Treffen solcher Entscheidungen kompetenztechnisch gerüstet werden. Dafür muss auch unternehmensübergreifend klar sein, wie die gemeinsamen Ziele und Strategien aussehen. So kann verhindert werden, dass Entscheidungen getroffen werden, die dem Unternehmen und seiner Weiterentwicklung offensichtlich schaden. Eine ausgereifte Kommunikationskultur ist dabei von großer Bedeutung genauso wie Vertrauen über alle Ebenen hinweg und das Gefühl, in seiner Meinung und seinen Entscheidungen ernst genommen zu werden (Mancke 2015).

Ansätze für eine agile IT-Governance sind beispielsweise Votingplattformen, Technologieratings, die Formulierung von Visionen und Leitsätzen, die Etablierung einer Unternehmenskommunikation, Teamreviews, Fortbildungs- und Schulungskonzepte, etc.

4.3 Darstellung und Kontrolle agiler IT-Landschaften durch IT-Landkarten

Die Optimierung der Geschäftsprozesse hat in den meisten Fällen direkte Auswirkungen auf die IT-Landschaft. Diese umfasst die gesamte unternehmensinterne IT wie Hardware, Software und Netzwerktechnik. Eine kontinuierliche Überwachung und Steuerung dieser Komponenten ist zentral für eine spätere Auswertung durch Kennzahlensysteme, die

Abbildung 14: Dokumentationsebenen einer Prozessarchitektur
Quelle: Eigene Darstellung auf Basis von Ropers 2013



an die jeweiligen Prozesse geknüpft sind. Entsprechende Bewertungen sollten nicht einmalig, sondern fortwährend stattfinden. Ändern sich Prozesse, so ändern sich Zusammenhänge und Abhängigkeiten, welche wiederum großen Einfluss auf die gesamte Unternehmensarchitektur haben können.

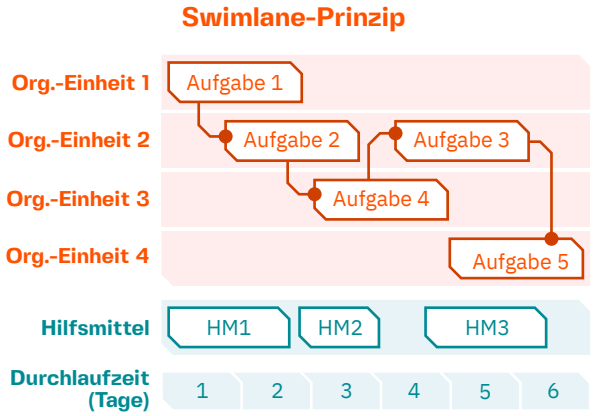
In Bezug auf Applikationen wird eine Übersicht der eingesetzten Anwendungssysteme und deren Interaktionen sowie Beziehungen zu Kerngeschäftsprozessen der Organisation sowie zur Daten- und Infrastrukturebene aufbereitet. Die Geschäftsarchitektur umfasst Objekte der Grundstrukturen des Geschäfts wie Geschäftsziele, Geschäftsprozesse, Organisationsstrukturen sowie Ressourcen wie Akteure oder Sachmittel. Dafür müssen ebenso Daten identifiziert und dokumentiert sowie mit ihren Beziehungen in einer Datenarchitektur beschrieben werden. In diesem Rahmen wird die Struktur des logischen und physischen Datenbestandes sowie Ressourcen zur Datenerhaltung erfasst.

IT-Landkarten sind ein wertvolles Werkzeug, um diese Anforderungen an eine detaillierte und strukturierte Unternehmensübersicht zu erfüllen.

Eine Variante dabei ist die Darstellung der Anwendungssysteme in einem grafischen Modell inkl. Schnittstellen und (optional) Nutzern sowie Standorten. Dabei werden übersichtlich alle Systeme des Unternehmens und Beziehungen zwischen diesen Systemen visualisiert und zu entsprechenden Funktionsbereichen zugeordnet (Lauschke 2005). Vorteil einer solchen Darstellung ist, dass sie bei Veränderungen in der IT wie der Implementierung neuer Soft- oder Hardware, Veränderungen von Prozessverläufen etc. eine stets aktuelle Übersicht über die IT im Unternehmen liefert. Vorausgesetzt, die Landkarte wird auch dementsprechend gepflegt und aktualisiert.

Eine andere Variante ist die Darstellung der IT-Landschaft als Prozessunterstützungskarte. Hierbei erfolgt eine Zuordnung von Anwendungssystemen

Abbildung 15: Darstellungsprinzipien für Prozesse
Quelle: Eigene Darstellung auf Basis von Ropers 2013



zu Prozessen. Die x-Achse enthält die Geschäftsprozesse bzw. Prozesscluster, auf der y-Achse werden die Anwendungssysteme dargestellt, ggf. noch weiter unterteilt, falls verschiedene Standorte existieren, die unterschiedliche Anwendungssysteme für die Geschäftsprozesse einsetzen (ebd.). Diese Art der Darstellung erlaubt es, bereichsübergreifend verwendete Anwendungen zu identifizieren. Die Dokumentation der Prozesse und zugehöriger Details wie Vernetzungen und Prozess-Schleifen ist dabei auf verschiedenen Ebenen möglich. Kennzahlen zur Prozesssteuerung lassen sich am besten auf den Ebenen 3 und 4 - der Feinstruktur - erarbeiten, weil die Informationsdichte gut überschaubar ist.

Um Prozessdokumentationen auf den Detailebenen mit mehr Informationen zu Verantwortlichen, Akteuren, Ressourcen etc. auszukleiden, bietet sich das Swimlane-Prinzip an (BPMN) (Ropers 2013).

Entsprechende Softwareanwendungen zum Geschäftsprozessmanagement helfen, komplexe Prozesse, die sich über die gesamte Organisation vom Vertrieb über das Marketing bis hin zum Accounting eines EVU erstrecken, anschaulich darzustellen, zu analysieren und zu optimieren, um Durchlaufzeiten und Kosten spezifischer Vorgänge sowie die fachbereichsübergreifende Kommunikation zu verbessern.

:// 5. ZUSAMMENFASSUNG

Die Digitalisierung ist selbst Forschungsgegenstand, Produkt und Anwendung sowie gleichermaßen Werkzeug zur Erschließung neuer Technologien und Geschäftsfelder. Die Energiewirtschaft ist in all ihren Bestandteilen wie jede andere Branche genauso von der digitalen Transformation betroffen, muss sich dem stetigen Wandel anpassen und eingeschlagene Wege gegebenenfalls nachjustieren.

Wichtig für Unternehmen der Branche vom kleinen EVU über Regionalversorger bis hin zu großen EVU ist es, neue Geschäftsmodelle zu finden, um sich damit gegenüber brancheninternen und branchenfremden Wettbewerbern behaupten zu können. Neue digitale Geschäftsmodelle bedeuten dabei nicht nur neue Akteure, Kunden und Verantwortliche, sondern gleichermaßen neue digitale Prozesse und hohe Datenmengen, welche es zu erschließen, zu dokumentieren, auszuwerten und anzupassen gilt.
Um diese Aufgaben sinnvoll, effizient, ressourcenschonend, kostensparend und zielerfüllend zu meistern, ist auch entsprechend das IT-Management digital aufzusetzen. Die IT als Unternehmensressource erhält neue Aufgaben und unterstützt das Unternehmen operativ und strategisch bei der Gestaltung und Entwicklung neuer Produkte und Dienstleistungen und wird damit zum direkten Wertbeitrag für die Steigerung des Unternehmenserfolgs. Wichtig ist es, dass EVU für diese Transformation die Unterstützung des Managements in Form von Ressourcen wie Know-how, Zeit und Budget erhalten.

Um das IT-Management bestmöglich für diese Aufgabe zu rüsten, bedarf es eines geeigneten Vorgehensmodells, welches sich in Analyse, Definition und Umsetzung gliedert.

In der ersten Phase sollten für Energieversorger das Aufsetzen einer Unternehmensstrategie und darauf aufbauenden digitalen Strategie sowie die Geschäfts- und Anwendungsarchitektur im Mittelpunkt stehen, welche schließlich zu einer Reifegradbestimmung zur Erschließung des IST- und des SOLL-Zustands des Unternehmens führt. In der Definitionsphase müssen eine möglichst innovative und flexible, auf Standards basierende IT-Organisation sowie eine im Idealfall durch ein entsprechendes Framework strukturierte IT-Governance in den Fokus der Betrachtung rücken. Im letzten Schritt erfolgt die Umsetzung in allen Bereichen, wobei ein proaktiv betriebenes Change-Management zusammen mit dem IT-Controlling und die stets stattfindende Rückkopplung den Schwerpunkt bilden.

Hervorzuhebende Faktoren eines funktionierenden IT-Managements sind vor allem digitalisierte Prozesse, die sich flexibel an neue Entwicklungen und Veränderung anpassen können, ohne andere Prozesse zu verlangsamen. Grundlage und Rahmen dafür bilden flexible Frameworks wie COBIT für mehr Kontrolle und Transparenz. Prozesse und damit verbundene Verantwortlichkeiten, Aufgaben aber auch Ressourcen wie Zeit und Kosten lassen sich dazu übersichtlich und transparent in einer passenden Prozessarchitektur darstellen und werden von Darstellungen der Anwendungslandschaft, die diese Geschäftsprozesse unterstützt, flankiert.

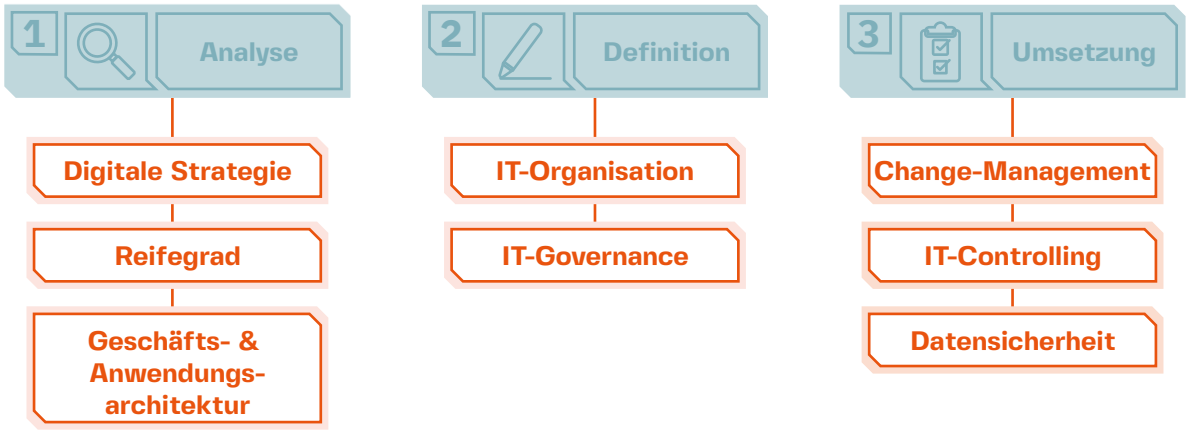
Diese Maßnahmen betreffen EVU unabhängig ihrer Größe. Tatsächlich schätzen Verantwortliche kleiner Versorgungsunternehmen ihre internen Prozesse als schnell und gut ein (A.T. Kearney, BDEW, IMP³rove 2019). EVU bewerten zudem die Prozessdigitalisierung im Bereich der IT im Vergleich zu anderen

Bereichen als besonders hoch. Die durchgeführten Experteninterviews sowie aktuelle Studien bestätigen, dass weniger die Größe des EVU, sondern vielmehr seine Vernetzung und Kooperationen zusammen mit der Orientierung an Best Practices entscheidend für ein Vorankommen auf dem Weg zur Digitalisierung sind. Vor allem Unternehmen vergleichbarer Größe und Großunternehmen als Vorreiter sowie Universitäten und Forschungseinrichtungen sind beliebte Partner, um die digitale Transformation im eigenen Unternehmen voranzutreiben.

Der Umgang mit Unternehmensprozessen und damit das Aufsetzen eines Vorgehensmodell für ein zukunftsfähiges IT-Management kosten das Unternehmen selbst Ressourcen sowie entsprechendes Know-how und Zeit bzw. Aufwand. Hier stehen jedoch die kleinen Vertreter der Energiebranche in der Umsetzung einer Herausforderung gegenüber. Praxisnähe, einfache Realisierbarkeit, aber minimales Kostenrisiko und die Bewahrung der Individualität eines EVU sind daher Eigenschaften, die ein IT-Management vor allem im Mittelstand erfüllen sollte (Mangiapane und Büchler 2015).

Bezüglich der notwendigen Prozessdigitalisierung sollte dabei immer der Fokus auf der Sinnhaftigkeit der Prozesse liegen. Ein zukunftsfähiges IT-Management hat die Kompetenz, Prozesse nicht nur zu sammeln und darzustellen, sondern auch zu optimieren, zu verkürzen oder wenn nötig auch zu entfernen. Erst dann können Prozesse sinnvoll miteinander verknüpft und neue und innovative Wertschöpfungsketten etabliert werden. Bei EVU liegen diese Chancen beispielsweise im Asset-Management bei der Verknüpfung von Prozessen zur Steuerung dezentraler Anlagen mit Steuerungsprozessen im Speicherbetrieb, was für das zukünftige Energiesystem eine hohe Bedeutung hat. Potenziale bei der Reduktion der Kosten sowie der Ableitung neuer Geschäftsmodelle tun sich dadurch geschäftsseitig auf und tragen zum Erfolg des Unternehmens bei (BDEW 2016). Durch diese unternehmensinternen Erfolge profitiert schlussendlich auch die Energiewende. Neue, digitale Technologien wie Smart Meter oder Energiemanagementsysteme erhalten die Chance, auch entsprechend ihrer Bestimmung nachhaltig und sinnvoll im Energiesystem integriert und digital gesteuert und überwacht zu werden.

Abbildung 16: Vorgehensmodell für ein zukunftsfähiges IT-Management
Quelle: Eigene Darstellung auf Basis von Ropers 2013



Literaturverzeichnis

A.T. Kearney, BDEW, IMP³rove (2019): Digital@EVU 2019. Wo steht die deutsche Energiewirtschaft?, S. 7, 15, 28.

Becker Büttner Held (BBH) (2017): Studie zur Digitalisierung der Energiewirtschaft, S. 26–27, z uletzt geprüft am 09.02.2021.

Beimborn, Daniel (o. J.): Standardisierung und Homogenisierung der Softwarelandschaft. Online verfügbar unter https://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/is-management/Management-von-Anwendungssystemen/Beschaffung-von-Anwendungssoftware/Standardisierung-und-Homogenisierung-der-Softwarelandschaft/index.html, zuletzt geprüft am 09.02.2021.

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen und Bundeskartellamt (BNA und BKA) (2020): Monitoringbericht 2019, S. 9.

Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) (2015): Strategiepapier: Digitalisierung in der Energiewirtschaft. Bedeutung, Treiber, und Handlungsempfehlungen für die IT-Architektur in den Unternehmen, S. 19, zuletzt geprüft am 10.02.2021.

Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) (2016): Die digitale Energiewirtschaft - Agenda für Unternehmen und Politik, S. 14, 48, 64, 66.

Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) (2017): Digitalisierung aus Kundensicht, S. 7., 10ff.

Capgemini Consulting (2015): Superkräfte oder Superteam? Wie Führungskräfte ihre Welt wirklich verändern können. Change Management Studie 2015, S. 18. Online verfügbar unter https://confio-beratung.de/wp-content/uploads/2017/04/change-management-studie-2015_4.pdf, zuletzt geprüft am 01.03.2021.

Capgemini Consulting (2018): Studie IT-Trends 2018, S. 6, 15, 33, zuletzt geprüft am 09.02.2021.

Deutsche Energie-Agentur GmbH (dena) (2021): Liberalisierung des Strommarktes. Online verfügbar unter https://www.dena.de/themen-projekte/energiesysteme/strommarkt/, zuletzt geprüft am 08.02.2021.

Doleski, Oliver D. (2017): Herausforderung Utility 4.0. Wiesbaden: Springer Fachmedien Wiesbaden.

Grashof, Katherina (2014): Monopole, Liberalisierung, Energiewende – (Dis)Kontinuitäten im Strommarktdesign. Online verfügbar unter https://www.fvee.de/fileadmin/publikationen/Themenhefte/th2014/th2014_04_03.pdf, zuletzt geprüft am 09.02.2021.

Grashof, Katherina (2015): Monopole, Liberalisierung, Energiewende – Strommarktdesign zwischen Wandel und Konstanz. In: Energiewirtschaftliche Tagesfrage 65 (9), S. 19–23.

Groß, Markus (2011): Im Mittelstand tummeln sich viele ITIL-Muffel. Online verfügbar unter https://www.computerwoche.de/a/im-mittelstand-tummeln-sich-viele-itil-muffel,2491559, zuletzt aktualisiert am 28.07.2011, zuletzt geprüft am 10.02.2021.

Helmke, Stefan; Uebel, Matthias (Hg.) (2016): Managementorientiertes IT-Controlling und IT-Governance. Wiesbaden: Springer Fachmedien Wiesbaden.

Hinkelmann, Knut (2019): Geschäftsprozess-Management: Einführung. Online verfügbar unter http://www.hinkelmann.ch/knut/lectures/gpm/GPM_Einfuehrung.pdf, zuletzt geprüft am 09.02.2021.

Institut für angewandte Arbeitswissenschaft (ifaa) (2019): Vorgehensmodelle zur Einführung und Umsetzung von Digitalisierungsmaßnahmen in der produzierenden Industrie. Online verfügbar unter https://www.arbeitswissenschaft.net/fileadmin/Downloads/Angebote_und_Produkte/Checklisten_Handlungshilfen/ifaa_2019_Vorgehensmodelle_Digitalisierung.pdf, zuletzt geprüft am 09.02.2021.

ISACA (2018): COBIT® 2019 Framework: Introduction and Methodology, S. 33. Online verfügbar unter https://community.mis.temple.edu/mis5203sec001sp2019/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf, zuletzt geprüft am 10.02.2021.

Koch, Petra; Ahlemann, Frederik; Urbach, Nils (2016): Die innovative IT-Organisation in der digitalen Transformation. In: Stefan Helmke und Matthias Uebel (Hg.): Managementorientiertes IT-Controlling und IT-Governance. Wiesbaden: Springer Fachmedien Wiesbaden, S. 177–196.

Lauer, Thomas (2019): Change Management. Berlin, Heidelberg: Springer Berlin Heidelberg.

Lauschke, Stephen (2005): Softwarekartographie: Analyse und Darstellung der IT-Landschaft eines mittelständischen Unternehmens. Bachelorarbeit. Technische Universität München, München, zuletzt geprüft am 10.02.2021.

Luber, Stefan; Schmitz, Peter (2017): Was ist IT-Governance. Online verfügbar unter https://www.security-insider.de/was-ist-it-governance-a-640525/, zuletzt aktualisiert am 07.09.2017, zuletzt geprüft am 09.02.2021.

Lünendonk GmbH (Lünendonk) (2014): Future Utility 2030. Energieversorger auf ihrem Weg in eine neue Zukunft, S. 10–13, zuletzt geprüft am 10.02.2021.

Mancke, Sebastian (2015): Crowdgovernance. Online verfügbar unter https://jaxenter.de/crowdgovernance-4-15981, zuletzt aktualisiert am 17.02.2015, zuletzt geprüft am 10.02.2021.

Mangiapane, Markus; Büchler, Roman P. (2015): Modernes IT-Management. Wiesbaden: Springer Fachmedien Wiesbaden.

Microtech (2017): Was ist Prozessmanagement? Online verfügbar unter https://www.microtech.de/erp-wiki/prozessmanagement, zuletzt aktualisiert am 26.05.2017, zuletzt geprüft am 10.02.2021.

Rahmel, Stefani; Völl, Wolfgang; Rönz, Malte (2012): Unternehmenssteuerung in der Energiewirtschaft in Zeiten eines tiefgreifenden Wandels. In: Controller Magazin. Ausgabe 1, Januar/Februar, S. 81, 84.

Ropers, Jens (2013): Operative Prozesse mit Kennzahlen zielorientiert steuern. In: Controller Magazin 38, Januar/Februar 2013 (11), S. 4–13, zuletzt geprüft am 10.02.2021.

Tiemeyer, Ernst (2017): Handbuch IT-Management. München: Carl Hanser Verlag GmbH & Co. KG, zuletzt geprüft am 09.02.2021.

Urbach, Nils; Ahlemann, Frederik (2016): IT-Management im Zeitalter der Digitalisierung. Berlin, Heidelberg: Springer Berlin Heidelberg.

Verband kommunaler Unternehmen e. V. (VKU) (2015): Stadtwerke-IT bei Energieversorgungsunternehmen, S. 21. Online verfügbar unter https://docplayer.org/459567-Stadtwerke-it-bei-energieversorgungsunternehmen.html, zuletzt geprüft am 02.03.2021.

Verband kommunaler Unternehmen e. V. (VKU) (2017): Digitalisierung. Handlungsoptionen für die Stadtwerke-IT, S. 42. Online verfügbar unter https://www.vku.de/fileadmin/user_upload/VKU_Broschuere-Digitalisierung.pdf, zuletzt geprüft am 02.03.2021.

Verband kommunaler Unternehmen e. V. (VKU) (2019): 2020. Zahlen, Daten, Fakten. Berlin/München: VKU Verlag, S. 6.

Vielhaber, Christoph (2005): Wertorientierte Unternehmenssteuerung in der Energiewirtschaft. Unter Mitarbeit von Technische Universität Dortmund.

Wanner, Markus F. (2017): Wie Sie mit agilem Change Management die digitale Transformation erfolgreich bewältigen. Online verfügbar unter https://www.tiba.de/magazin/wie-sie-mit-agilem-change-management-die-digitale-transformation-erfolgreich-bewaeltigen/, zuletzt aktualisiert am 01.2017, zuletzt geprüft am 10.02.2021.

Wiedmann, Peter C. K. (2016): Agiles Geschäftsprozessmanagement auf Basis gebrauchssprachlicher Modellierung. Dissertation. S. 88. Online verfügbar unter https://epub.uni-bayreuth.de/3257/, zuletzt geprüft am 10.02.2021.

Zarnekow, Rüdiger (2005): Integriertes Informationsmanagement. Berlin/Heidelberg: Springer-Verlag, zuletzt geprüft am 09.02.2021.

IT-SICHERHEIT FÜR KRITIS-UNTERNEHMEN IN DER DIGITALEN ENERGIE-WIRTSCHAFT

ABSTRACT

Der vorliegende Beitrag gibt einen Überblick über die rechtlichen Rahmenbedingungen von Betreibern kritischer Infrastruktur (KRITIS) und deren Auswirkungen auf die IT-Sicherheit am Beispiel der Energiewirtschaft. Vor dem Hintergrund der zunehmenden Vernetzung mit intelligenten Technologien und der steigenden Anzahl von Cyber-Angriffen, ist der Schutz von Energieversorgern und -erzeugern von besonders essenziellen Interesse für die Gesellschaft.

Ziel dieses Beitrags ist zum einen die Bewertung der derzeitige Sicherheitslage in der Energiewirtschaft und zum anderen die Abschätzung wie durchgängig dieses Sicherheitsniveau, im Rahmen der steigenden dezentralen Energieerzeugung und zunehmenden Digitalisierung mit intelligenten Technologien, ist. Um diese Frage zu beantworten wurde eine ausführliche Recherche in Bezug auf den aktuellen Entwicklungsstand der Energieerzeugung, der digitalen Strukturen in der Energiewirtschaft sowie den zukünftigen Prognosen durchgeführt und von Experten hinsichtlich ihres Sicherheitsniveaus bewertet. Die (IT-)Sicherheit wird dabei nicht als ein Zustand, sondern als kontinuierlicher Prozess betrachtet.

Wir zeigen, dass in den vergangenen Jahren große Fortschritte in den gesetzlichen Vorgaben und Sicherheitsstandards erreicht wurden. Dies betrifft allerdings nur einen Großteil an Netzbetreibern und einige wenige Betreiber von Energieerzeugungsanlagen. Im Hinblick auf die steigende Wichtigkeit von kleinen und dezentralen Erzeugern für die Versorgungssicherheit ist dabei kein durchgängiges und einheitliches Schutzniveau festzustellen.

Vor dem Hintergrund der zunehmenden dezentralen Energieerzeugung und der tendenziell steigenden Anzahl von dezentralen Energieerzeugungsanlagen mit niedrigerer Leistung, zeigt dieser Beitrag auf, dass die derzeitigen Sicherheitsvorgaben gerade für die Energieerzeugung, eine Schwachstelle für die Versorgungssicherheit darstellen.

AUTOREN

Stefan Brühl
(BBH Consulting AG)

Victor Stocker
(BBH Consulting AG)

Daniel Kaufmann
(BBH Consulting AG)

Abkürzungsverzeichnis

Abs	Absatz
AktG	Aktiengesetz
Art	Artikel
BDEW	Bundesverband der Energie- und Wasserwirtschaft
BMWi	Bundesministerium für Wirtschaft und Energie
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
bspw.	beispielsweise
CA	Certificate Authority
CLS	Cotrollable local systems
DDoS	Distributed Denial of Service (Dienstverweigerungs-Angriff)
DIN	Deutsches Institut für Normung
DS-GVO	Datenschutz Grundverordnung
e.V.	eingetragener Verein
EDV	Elektronische Datenverarbeitung
ehem.	ehemalig
EMT	Externer Marktteilnehmer
EN	Europäische Norm
ENTSO-E	Verband Europäischer Übertragungsnetzbetreiber
EnWG	Energiewirtschaftsgesetz
etc.	et cetera
EU	Europäisch
EU VNBO	Organisation der Verteilnetzbetreiberin der Union
EVU	Energieversorgungsunternehmen
GewO	Gewerbeordnung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GWA	Gateway Administrator
GWh	Gigawattstunde
GWH	Gateway Hersteller
Hs	Halbsatz
HS	Hochschule
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikations-technologien
ISMS	Informationssicherheits-managementsystem
ISO	International Organization for Standardization
IT	Informationstechnik
KRITIS	Kritische Infrastruktur
KritisV	Kritisverordnung
KWK	Kraft-Wärme-Kopplung
lit	littera
Mio	Million
MW	Megawatt
NIS	Netzwerk- und Informationssicherheit
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
OLG	Oberlandesgericht
PDCA	Plan Do Check Act
PKI	Public Key Infrastructure
S	Satz
s.o.	siehe oben
SM	Smart Meter
SMGW	Smart Meter Gateway
SOA	Statement of Applicability
sog.	sogenannte
TK	Telekommunikation
TWh	Terawattstunde
u.a.	unter anderem
VO	Verordnung
z.B.	zum Beispiel

1. EINLEITUNG 88

2. RECHTLICHE EINORDNUNG 89
2.1 Betreiber Kritischer Infrastruktur 90
2.2 Pflichten für KRITIS-Betreiber nach BSIG 92
2.3 Pflichten für Energieversorgungsunternehmen nach EnWG 93
2.4 Das unterschiedliche Regelungsregime im EnWG für Betreiber von Energieanlagen und Netzbetreiber 93
2.5 Analyse: KRITIS-Betreiber für Energieanlagen 94
2.6 Befreiung/Nicht-Anwendung der gesetzlichen Pflichten 95
2.7 Exkurs – Smart Meter-PKI: Sukzessive Erhöhung der IT-Sicherheit 96

3. ANFORDERUNGEN DER IT-SICHERHEITSKATALOGE 97

4. ANWENDUNG DES IT-SICHERHEITSKATALOGS UND IMPLEMENTIERUNG EINES INFORMATIONS-SICHERHEITSMANAGEMENTSYSTEMS (ISMS) 100
4.1 Definition des Geltungsbereichs 100
4.2 Einführung eines ISMS 101
4.3 Das Risikomanagement im ISMS 101

5. UP KRITIS UND DIE ALLIANZ FÜR CYBERSICHERHEIT 103

6. AUFSICHTS-MASSNAHMEN UND BUSSGELDER 104

7. DAS IT-SICHERHEITSGESETZ 2.0 105

8. EXKURS – WINTERPAKET: WEITERE REGELUNGEN ZUR CYBERSICHERHEIT AUF EU-EBENE 107

9. FAZIT 108

Literaturverzeichnis 109

:// 1. EINLEITUNG

Die Digitalisierung ist in vollem Gange und wird unsere Gesellschaft, Wirtschaft und Politik weiterhin grundlegend verändern. Innovative und digitale Technologien ermöglichen Unternehmen dabei auf der einen Seite, eine weiterführende Optimierung interner Prozesse zur Kostensenkung, sorgen jedoch gleichzeitig für eine steigende Abhängigkeit von IT-Systemen. Die Sicherheit der Informations- und Kommunikationstechnologien (IKT) in Unternehmen ist daher mehr denn je für die Wettbewerbsfähigkeit und den wirtschaftlichen Erfolg verantwortlich.

Dies gilt insbesondere für Energieversorgungsunternehmen (EVU), die zunehmend von intelligenten Technologien wie Smart Grids (intelligente Netze) oder Smart Meters (intelligente Messeinrichtungen) abhängig werden und durch ihre Dienstleistungen und Versorgungsinfrastruktur von großer Bedeutung für unsere moderne Gesellschaft sind. Fehlen Strom und Gas, könnten das öffentliche Leben und lebensnotwendige Dienstleistungen innerhalb kürzester Zeit zum Erliegen kommen, weshalb der öffentliche Versorgungssektor schon seit längerer Zeit im Fokus von Hackern und anderen Cyberkriminellen steht.

In Deutschland erleben Energieversorger und Betreiber von Energienetzen „jeden Tag unzählige Angriffe, die wir bisher glücklicherweise abwehren konnten“, sagt beispielsweise Hildegard Müller (ehem. Vorstandsmitglied bei Innogy, Leitung Netzgeschäft) (Müller 2019). Die Gefährdungslage ist bei 117,4 Mio. neuen Schadprogramm-Varianten und bis zu 20.000 täglichen Botinfektionen deutscher Systeme, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) im aktuellen Lagebericht zur IT-Sicherheit in Deutschland meldet, enorm (BSI 2020). Ein großflächiger Ausfall der Energieversorgung durch Cyberangriffe konnte hierzulande bisher zwar vermieden werden, völlig auszuschließen ist es aber nicht. Das zeigt der erfolgreiche Hackerangriff auf einen regionalen Stromversorger in Ludwigshafen im Mai 2020, bei dem die Angreifer Geschäfts- und Kundendaten kompromittieren konnten.[1]

Den wohl verheerendsten Angriff auf die Energieversorgung durch Cyberkriminelle erlebte jedoch eine Region in der Ukraine Ende Dezember 2015. Bei dem professionell organisierten Verbrechen fielen 27 Umspannwerke gleichzeitig aus, was dazu führte das 103 Städte über mehrere Stunden keinen Zugang zu Elektrizität hatten. Gleichzeitig wurden Telefon-Hotlines der betroffenen Firmen mit sog. DDoS-Attacken lahmgelegt, wodurch verhindert wurde, dass die Kunden ihren Stromlieferanten den Ausfall mitteilen konnten (Tanriverdi 2016).

Es muss daher in Zukunft davon ausgegangen werden, dass gut koordinierte Cyberangriffe eine unmittelbare Bedrohung darstellen und kritische Unternehmen im öffentlichen Interesse, wie Energieversorger, häufiger im Fokus stehen.

1 Heise – Hackerangriff auf Versorgungsunternehmen Technische Werke Ludwigshafen. Unter: https://www.heise.de/newsticker/meldung/Hackerangriff-auf-Versorgungsunternehmen-Technische-Werke-Ludwigshafen-4714059.html, aufgerufen am 23.06.2020.

:// 2. RECHTLICHE EINORDNUNG

Die EU-Richtlinie über „Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit“ (kurz NIS-Richtlinie) wurde daher im August 2016 als „zentraler Bestandteil der europäischen Sicherheitsstrategie“[2] verabschiedet. Ziel der Richtlinie ist es, Sicherheitsanforderungen und Meldepflichten nach dem aktuellen Stand der Technik einzuführen, sowie das Risikomanagement zu verbessern (Taeger 2016). In Deutschland ergänzt die NIS-Richtlinie das bereits im Juli 2015 in Kraft getretene IT-Sicherheitsgesetz, welches im Zuge der digitalen Agenda der Bundesregierung zur Verbesserung der Sicherheit informationstechnischer Systeme bei Unternehmen und zum Schutz von Kritischer Infrastruktur sowie den Bürgerinnen und Bürgern im Internet verabschiedet worden ist.

Dabei existiert das IT-Sicherheitsgesetz nicht als spezifisches Gesetz, sondern ist ein sog. Artikelgesetz. Das bedeutet, dass in anderen Gesetzen partielle Änderungen und Ergänzungen vorgenommen worden sind, wozu u.a. das BSI-, Atom-, Energiewirtschafts-, Telekommunikations- und das Telemediengesetz gehören. Die Betreiber von Kritischen Infrastrukturen (auch KRITIS-Betreiber genannt) erhalten innerhalb des IT-Sicherheitsgesetz einen besonderen Stellenwert. Sie werden verpflichtet einen gewissen Mindeststandard an IT-Sicherheit in ihren Unternehmen zu implementieren und regelmäßig dem Stand der Technik anzupassen.

Mit der Formulierung „Stand der Technik“ reagiert der Gesetzgeber bewusst auf den dynamischen Wandel im Zuge der Digitalisierung sowie immer kürzer werdende Produktlebenszyklen und gibt keine Vorgaben zur Umsetzung von bestimmten Technologien vor, wenngleich das BSI regelmäßig die sog. BSI-Standards in Bezug auf die IT-Sicherheit anpasst und veröffentlicht. Diese Richtlinien enthalten Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen zu unterschiedlichen Aspekten der Informationssicherheit. Somit sollen sich die Unternehmen der hohen Innovationsbereitschaft, die die Digitalisierung fordert, stellen und ihre Technik regelmäßig an die aktuellen Entwicklungen im Markt anpassen.

Die Steuerung und Kontrolle der KRITIS-Betreiber obliegt dabei dem BSI, welches nach § 4 Abs. 1 BSIG als „zentrale Meldestelle für die Zusammenarbeit der Bundesbehörden in Angelegenheiten der Sicherheit in der Informationstechnik“ genannt wird. Im Falle eines IT-Sicherheitsvorfalls bei einem KRITIS-Betreiber muss dieser unverzüglich nach § 8b Abs. 4 BSIG an das BSI gemeldet werden. Die gesammelten Informationen werden anschließend beim BSI ausgewertet und alsbald den KRITIS-Betreibern zur Verfügung gestellt, damit die Unternehmen den Schutz ihrer IT-Systeme verbessern können. Das BSI verfügt dadurch über eine zentrale Position als nationale IT-Sicherheitsbehörde mit einer verstärkten Beratungsfunktion.[3]

2 Kipker, Der BMI-Referentenentwurf zur Umsetzung der NIS-RL, MMR 2017, 143.

3 Deutscher Bundestag, Drucksache 18/4096, S.2.

2.1 Betreiber Kritischer Infrastruktur

Unter einer Kritischen Infrastruktur versteht man Einrichtungen, Anlagen oder Teile für bestimmte Sektoren im öffentlichen Interesse, bei denen ein Ausfall weitreichende und schwerwiegende Auswirkungen auf die Gesellschaft haben könnte. Nach § 2 Abs. 10 BSIG werden sieben Sektoren als kritisch eingestuft. Dazu zählen:

- *der Energiesektor*
- *der Wassersektor*
- *der Ernährungssektor*
- *die Informationstechnik und Telekommunikation*
- *der Gesundheitssektor*
- *das Finanz- und Versicherungswesen sowie*
- *der Transport- und Verkehrssektor*

Damit Einrichtungen, Anlagen oder Teile dieser Sektoren im Sinne des IT-Sicherheitsgesetzes als Kritische Infrastruktur betrachtet werden, müssen zusätzliche Bedingungen erfüllt sein.

In der Rechtsverordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG (auch BSI-Kritisverordnung oder kurz BSI-KritisV genannt) sind messbare Kriterien (Schwellenwerte) definiert worden, welche es den Betreibern erleichtern zu überprüfen, ob ihre Anlagen in den Regelungsbereich des IT-Sicherheitsgesetzes fallen oder nicht.

Im Zuge dieses Beitrags werden im Folgenden ausschließlich die Schwellenwerte für die Energieversorgung betrachtet. Die Kriterien der anderen kritischen Sektoren werden nicht berücksichtigt.

Schwellenwerte für Betreiber Kritischer Infrastruktur in der Stromversorgung:
Tabelle: Stromversorgung - Anlagenkategorien und Schwellenwerte,
Quelle: BSI-KritisV Anhang 1 Teil 3

Anlagenkategorie	Bemessungskriterium	Schwellenwert
Erzeugungsanlage	Installierte Netto-Nennleistung	420 MW
KWK-Anlage	Installierte Netto-Nennleistung	420 MW
Dezentrale Erzeugungsanlage	Installierte Netto-Nennleistung	420 MW
Speicheranlage	Installierte Netto-Nennleistung	420 MW
Anlage zur Steuerung/ Bündelung elektrische Leistung	Installierte Netto-Nennleistung	420 MW
Übertragungsnetz	Durch Letztverbraucher/Weiterverteiler entnommene Jahresarbeit	3.700 GWh/Jahr
Zentrale Anlage und Systeme für den Stromhandel	Handelsvolumen an der Börse	200 TWh/Jahr
Verteilernetz	Durch Letztverbraucher/Weiterverteiler entnommene Jahresarbeit	3.700 GWh/Jahr
Messstelle	Leistung der angeschlossenen Verbrauchsstelle bzw. Einspeisung	420 MW

Schwellenwerte für Betreiber Kritischer Infrastruktur in der Gasversorgung:
Tabelle 1: Gasversorgung - Anlagenkategorien und Schwellenwerte,
Quelle: BSI-KritisV Anhang 1 Teil 3

Anlagenkategorie	Bemessungskriterium	Schwellenwert
Gasförderanlage	Energie des geförderten Gases	5.190 GWh/Jahr
Gasspeicher	Entnommene Arbeit	5.190 GWh/Jahr
Fernleitungsnetz	Durch Letztverbraucher/Weiterverteiler entnommene Jahresarbeit	5.190 GWh/Jahr
Gasverteilernetz	Entnommene Arbeit	5.190 GWh/Jahr

Schwellenwerte für Betreiber Kritischer Infrastruktur in der Kraftstoff- und Heizölversorgung:
Tabelle 2: Kraftstoff- und Heizölversorgung - Anlagenkategorien und Schwellenwerte,
Quelle: BSI-KritisV Anhang 1 Teil 3

Anlagenkategorie	Bemessungskriterium	Schwellenwert
Ölförderanlage	Gefördertes Rohöl	4,4 Mio. Tonnen/Jahr
Raffinerie	Erzeugter Kraftstoff	420.000 Tonnen/Jahr
	Erzeugtes Heizöl	620.000 Tonnen/Jahr
Mineralölfernleitung	Transportierte Rohöl- oder Produktenmenge	4,4 Mio. Tonnen/Jahr
Öl- und Produktenlager	Umgeschlagene Rohölmenge	4,4 Mio. Tonnen/Jahr
	Umgeschlagene Menge Kraftstofft	420.000 Tonnen/Jahr
	Umgeschlagene Menge Heizöl	620.000 Tonnen/Jahr
Anlage zur standort-übergreifenden Steuerung	Transportierte Rohöl- oder Produktenmenge	4,4 Mio. Tonnen/Jahr
	Umgeschlagene Rohölmenge	4,4 Mio. Tonnen/Jahr
	Umgeschlagene Menge Kraftstofft	420.000 Tonnen/Jahr
	Umgeschlagene Menge Heizöl	620.000 Tonnen/Jahr
Anlage zum Vertrieb von Kraftstoff und Heizöl	Verteilte Menge Kraftstoff	420.000 Tonnen/Jahr
	Verteilte Menge Heizöl	620.000 Tonnen/Jahr
Anlage zum Vertrieb von Kraftstoff und Heizöl	Verteilte Menge Kraftstoff	420.000 Tonnen/Jahr
	Verteilte Menge Heizöl	620.000 Tonnen/Jahr
Anlage zur standort-übergreifenden Steuerung	Verteilte Menge Heizöl	620.000 Tonnen/Jahr

Schwellenwerte für Betreiber Kritischer Infrastruktur in der Fernwärmeversorgung:
Tabelle 3: Fernwärmeversorgung - Anlagenkategorien und Schwellenwerte,

Quelle: BSI-KritisV Anhang 1 Teil 3

Anlagenkategorie	Bemessungskriterium	Schwellenwert
Heizwerk	Ausgeleitete Wärmeenergie	2.300 GWh/Jahr
Gasspeicher	Ausgeleitete Wärmeenergie	2.300 GWh/Jahr
Fernleitungsnetz	Ausgeleitete Wärmeenergie	250.000

2.2 Pflichten für KRITIS-Betreiber nach BSIG

Erreicht bzw. überschreitet ein Unternehmen die Schwellenwerte aus der BSI-Kritisverordnung, ist es gesetzlich dazu verpflichtet, nach § 8a Abs.1 BSIG angemessene, organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme zu treffen. Hierfür sollen sich die Betreiber an dem aktuellen Stand der Technik orientieren oder sie schlagen branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen selbst vor (§ 8a Abs.2 BSIG). Diese müssen zunächst jedoch durch das BSI geprüft werden. Anschließend schreibt der Gesetzgeber in § 8a Abs.3 BSIG eine regelmäßige Überprüfung zur Erfüllung der Anforderungen aus § 8a Abs.1 BSIG vor und kann die Nachweise, welche in Form von Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen können, durch das BSI auch per Gesetz vom Unternehmen einfordern.

Der § 8b verpflichtet Betreiber Kritischer Infrastrukturen des Weiteren zur Benennung einer Kontaktstelle für das BSI und zu Meldungen im Störungsfall. Hierzu zählen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur führen könnte.[4] Weiterhin schreibt der Gesetzgeber vor, dass eine Meldung Angaben zu:

- *der Störung,*
- *den möglichen grenzübergreifenden Auswirkungen,*
- *den technischen Rahmenbedingungen,*
- *den vermuteten oder tatsächlichen Ursachen,*
- *der betroffenen Informationstechnik,*
- *der Art der betroffenen Einrichtung oder Anlage,*
- *der erbrachten kritischen Dienstleistung und*
- *den Auswirkungen der Störung auf diese Dienstleistung*

enthalten muss.

Die Regelungen des BSIG greifen jedoch nach § 8d Abs. 2 Satz 2 BSIG nicht für „Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes (EnWG) [..],

4 Siehe § 8b Abs. 4 S. 1,2 BSIG.

soweit sie den Regelungen des § 11 EnWG unterliegen.“ Demnach besitzt das EnWG für Betreiber von Kritischer Infrastruktur im Energiesektor grundsätzlich eine Vorrangstellung.

2.3 Pflichten für Energieversorgungsunternehmen nach EnWG

Erfüllt ein Energieversorgungsunternehmen die eben erwähnten Voraussetzungen nach § 11 Abs. 1a oder 1b EnWG, ist es ebenso gesetzlich dazu verpflichtet angemessene Schutzmaßnahmen gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu treffen, die für einen sicheren Netz- bzw. Anlagenbetrieb notwendig sind. Hierfür hat die Bundesnetzagentur die sog. IT-Sicherheitskataloge erstellt und veröffentlicht, an denen sich die betroffenen Unternehmen orientieren müssen.

Aktuell gibt es zwei verschiedene IT-Sicherheitskataloge:

- *IT-Sicherheitskatalog für Strom- und Gasnetze (Stand August 2015) gemäß § 11 Abs. 1a EnWG für den sicheren Betrieb von Energieversorgungsnetzen (Netzbetreiber) und*

- *IT-Sicherheitskatalog für Betreiber von Energieanlagen (Stand Dezember 2018) gemäß § 11 Abs. 1b EnWG für den sicheren Betrieb von Energieanlagen*

Der § 11 Abs. 1c EnWG verpflichtet zudem, wie das BSIG auch, Störungen über eine Kontaktstelle an das BSI zu melden, welche umgehend vom BSI an die Bundesnetzagentur weitergeleitet werden. Hierzu zählen ebenfalls Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen.

Weiterhin müssen Meldungen ebenso Angaben zu:

- *der Störung,*

- *den möglichen grenzübergreifenden Auswirkungen,*

- *den technischen Rahmenbedingungen,*

- *den vermuteten oder tatsächlichen Ursachen und*

- *der betroffenen Informationstechnik enthalten.*

2.4 Das unterschiedliche Regelungsregime im EnWG für Betreiber von Energieanlagen und Netzbetreiber

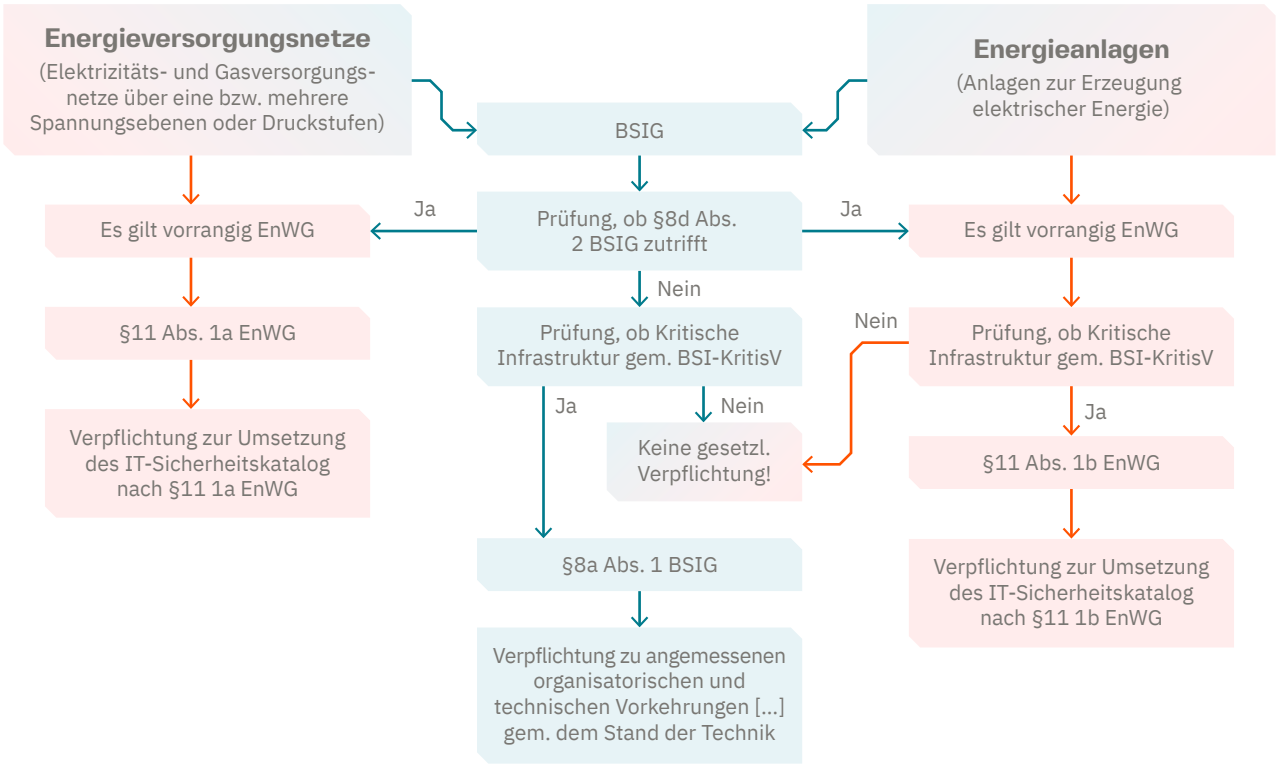
Die bereits angesprochene Vorrangstellung des EnWG für Betreiber Kritischer Infrastruktur im Energiesektor bedeutet, dass sie den Regelungen des § 11 EnWG unterliegen und der § 8a Abs. 1 BSIG zunächst keine Anwendung findet.

Dabei unterscheidet das EnWG zusätzlich zwischen Betreibern von Energieversorgungsnetzen sowie Betreibern von Energieanlagen. Bei ersteren handelt es sich um Elektrizitäts- und Gasversorgungsnetzbetreibern über eine bzw. mehrere Spannungsebenen oder Druckstufen, letztere betreiben Anlagen zur Erzeugung von elektrischer Energie.

Die verschiedenen Regelungen führen dabei innerhalb des EnWG zu einem unterschiedlichen Regelungsregime. Während für Betreiber von Energieversorgungsnetzen in der aktuellen Rechtsprechung nach § 11 Abs. 1a EnWG pauschal gilt, dass sie „einen angemessen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, […]“ gemäß dem IT-Sicherheitskatalog für Strom- und Gasnetze umsetzen müssen[5],

5 OLG Düsseldorf Beschl. v. 19.7.2017 – 3 Kart 109/16, BeckRS 2017, 132865.

Abbildung 1: Rechtliche Einordnung Kritischer Infrastruktur im Energiesektor
Quelle: eigene Darstellung



→ Rot erklärt das unterschiedliche Regelungsregime zwischen Energieversorgungsnetzen und Energieanlagen
→ Blau ist optional und erklärt die Stellung des BSIG

gilt dies für Betreiber von Energieanlagen erst, sobald sie „durch die Rechtsverordnung gemäß § 10 Abs. 1 BSIG als Kritische Infrastruktur bestimmt wurde [...]“. Das bedeutet, dass Energieanlagen zunächst den Schwellenwert von 420 MW (siehe → *Tabelle 1*) erreichen bzw. überschreiten müssen, damit sie gesetzlich dazu verpflichtet werden „einen angemessenen Schutz gegen Bedrohungen für ihre Telekommunikations- und elektronische Datenverarbeitungssysteme [...]“, gemäß dem IT-Sicherheitskatalog für Betreiber von Energieanlagen, umzusetzen. Damit verweist das EnWG speziell für Betreiber von Energieanlagen wieder auf die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG.

In Abbildung 1 ist die rechtliche Einordnung und das Verhältnis zwischen EnWG und BSIG nochmal grafisch erläutert.

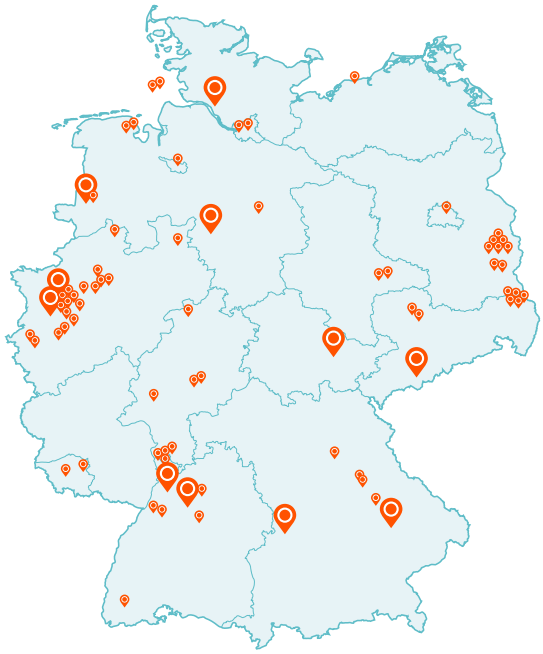
2.5 Analyse: KRITIS-Betreiber für Energieanlagen

Zur Veranschaulichung werden nachfolgend die Betreiber für Energieanlagen ermittelt und analysiert, welche nach der Rechtsverordnung (BSI-KritisV) als Kritische Infrastruktur bestimmt wurden. Hierfür wurde in der Kraftwerksliste der Bundesnetzagentur (Stand: 01.04.2020)[6] die Anzahl sämtlicher Energieanlagen ermittelt, welche den Schwellenwert von 420 MW aus der BSI-KritisV erreichen bzw. überschreiten.

Von den Anlagen, die sich aktuell im Betrieb befinden, werden lediglich 66 Energieanlagen als Kritische Infrastruktur klassifiziert. In Abbildung 2

6 Kraftwerksliste der BNetzA unter: https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/Erzeugungskapazitaeten/Kraftwerksliste/kraftwerksliste-node.html, aufgerufen am 10.01.2020.

Abbildung 2: KRITIS-Stromerzeuger (Stand: Nov. 2019) – Deutschlandkarte
Quelle: eigene Darstellung



ist eine Deutschlandkarte mit allen Energieanlagen, die unter die KRITIS-Verordnung fallen, dargestellt – darunter hauptsächlich Erdgasanlagen, Braun- und Steinkohlekraftwerke sowie einige wenige Pumpspeicherkraftwerke und Windparks.

Die gesamte Anzahl an Kritischer Infrastruktur unter den Energieanlagen in Deutschland entspricht demzufolge 3,40 Prozent, womit nur ein Bruchteil überhaupt die Schwellenwerte für Betreiber Kritischer Infrastruktur in der Energieerzeugung erreicht. Aufgrund ihrer Größe bzw. der installierten Nennleistung vereinen diese Anlagen immerhin 28,72 Prozent der gesamten deutschen Netto-Nennleistung und sind demnach verpflichtet die organisatorischen und technischen Maß-nahmen gemäß des IT-Sicherheitskatalog nach § 11 Abs. 1b EnWG umzusetzen und sich innerhalb einer Frist bis zum 31.03.2021 zertifizieren zu lassen.

Im Umkehrschluss bedeutet dies jedoch, dass es keine einheitliche Regelung in dem Umfang bzgl. der IT-Sicherheit für die restlichen 71,28 Prozent der Anlagenbetreiber gibt.

Zwar wird ein gewisses Maß zum Schutz der Telekommunikations- und elektronischen Datenverarbeitungssysteme durch Einzelmaßnahmen, wie dem Einsatz moderner Technologien oder dem allgemeinen Aufbau von Steuerungs- und Telekommunikationssystemen nach den Anforderungen des BDEW-Whitepapers, gewährleistet. Ein ganzheitlicher Ansatz wie ihn der IT-Sicherheitskatalog mithilfe eines Informationssicherheits-Managementsystem (ISMS), einem Risikomanagement und dem Aufbau einer Sicherheitsorganisation inkl. einer Meldestelle für das BSI in Unternehmen fordert, wird jedoch nicht umgesetzt.

2.6 Befreiung/Nicht-Anwendung der gesetzlichen Pflichten

Die gesetzlichen Vorschriften enthalten in der Regel keine entsprechenden Befreiungs- oder Ausnahmetatbestände für den Fall, dass der Netzbetreiber bestimmte IKT-Technologien einsetzt, die unter den Regelungsbereich des EnWG bzw. IT-Sicherheitskatalogs fallen. Falls der Netzbetreiber jedoch für den Betrieb seiner Anlagen nachweislich keine schützenswerte IKT-Technologie einsetzt, kann dieser gegenüber der Bundesnetzagentur eine „verbindliche Erklärung zur Nichtanwendbarkeit des IT-Sicherheitskatalogs“ abgeben. Nach entsprechender Prüfung der Netzstrukturdaten (Leitwarte, Schalthandlungen, Netzstrukturplan, etc.) entscheidet die Bundesnetzagentur, ob eine Nichtanwendbarkeit gerechtfertigt ist.

Der Netzbetreiber ist jedoch dazu verpflichtet, auch nach positiver Prüfung, bei jeder zukünftigen Veränderung der Netzinfrastruktur erneut zu überprüfen, ob eine Nichtanwendbarkeit berechtigt ist. Diese Verantwortung wird dem Netzbetreiber allein überlassen. Sollte sich anschließend herausstellen, dass – entgegen der getroffenen Aussagen und vorgelegten Unterlagen – der Netzbetreiber gleichwohl Systeme, Anwendungen oder Komponenten betreibt, auf die der IT-Sicherheitskatalog nach § 11 Abs. 1a EnWG anwendbar ist, könnte dies aufgrund der Nichtumsetzung des IT-Sicherheitskatalogs bei

einem Störfall haftungsrechtliche Konsequenzen nach sich ziehen.

2.7 Exkurs – Smart Meter-PKI: Sukzessive Erhöhung der IT-Sicherheit

Ein positiver Effekt für die IT-Sicherheit im Zuge der Digitalisierung und der zunehmenden Vernetzung zwischen Erzeugung, Verteilung und Verbrauch durch intelligente Technologien erfolgt durch den voranschreitenden Rollout von intelligenten Messsystemen (Smart Meter). Dabei liegt es zunächst nahe anzunehmen, dass hiermit eine weitere Möglichkeit für Cyberkriminelle geschaffen wird, sich Zugang zu kritischen Bereichen der Energieversorgung zu verschaffen. Und in der Tat bieten sich den Tätern auch weitere Angriffs flächen, die beispielsweise durch populäre Man-in-the-Middle-Angriffe[7] oder ähnlichen ausgenutzt werden könnten. Für diese Entwicklung haben die zuständigen Behörden jedoch frühzeitig mit Einführung der sog. Smart-Meter Public Key Infrastructure (kurz: SM-PKI) agiert und damit ein System implementiert, welches die automatisierte Kommunikation mit asymmetrischer Kryptographie nahezu vollständig absichert.

Allgemein gilt, dass mithilfe einer Public Key Infrastructure digitale Zertifikate für asymmetrische Verschlüsselungsverfahren ausgestellt, verteilt und geprüft werden. Für den sicheren Austausch der Daten zwischen zwei Teilnehmern kommt mit der sogenannten Root-CA[8] eine weitere Instanz hinzu, der alle an der PKI teilnehmenden Instanzen vertrauen.

Bei der SM-PKI fungiert das BSI als Vertrauensanker und zentrale Zertifizierungsstelle (Root-CA) mit darunterliegend privaten Unternehmen (Sub-CAs), welche die Betreuung der Marktteilnehmer übernehmen und zur Ausstellung von Zertifikaten für die Endnutzer autorisiert sind. Zu den Endnutzern selbst gehören:

- *Smart Meter Gateways (SMGW)*
- *Gateway Administratoren (GWA)*
- *Gateway Hersteller (GWH)*
- *Externe Marktteilnehmer (EMT)*

Bei Letzteren wird außerdem zwischen aktiven und passiven EMT unterschieden. Dabei nutzt ein aktiver EMT ein SMGW, um über dieses nachgelagerte Geräte (CLS) anzusprechen, während ein passiver EMT keine nachgelagerten Geräte steuert, sondern nur Daten empfängt und die eigenen Geschäftsprozesse fortführt. Um den sicheren Regelbetrieb von Smart Meter Gateways zukünftig zu gewährleisten und Schwachstellen auf ein Minimum zu reduzieren, müssen alle Teilnehmer der Smart Meter-PKI selbst ein gewisses Maß an IT-Sicherheit vorhalten und sich ggf. zertifizieren lassen. Dabei werden insbesondere für aktive EMT sowie die Root- und Sub-CAs hohe Sicherheitsstandards (u.a. Einführung eines ISMS) gemäß der Certificate Policy der Smart Metering PKI eingefordert, wobei diese Sicherheitskonzepte auch in abgeschwächter Form für die anderen Teilnehmer gelten. Mit voranschreitendem Rollout von intelligenten Messsystemen erhöht sich damit sukzessive die IT-Sicherheit in der Energiewirtschaft.

7 Der Angreifer erlangt die Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen einsehen und manipulieren.

8 Root-Certificate Authority (Wurzelzertifizierungsinstanz)

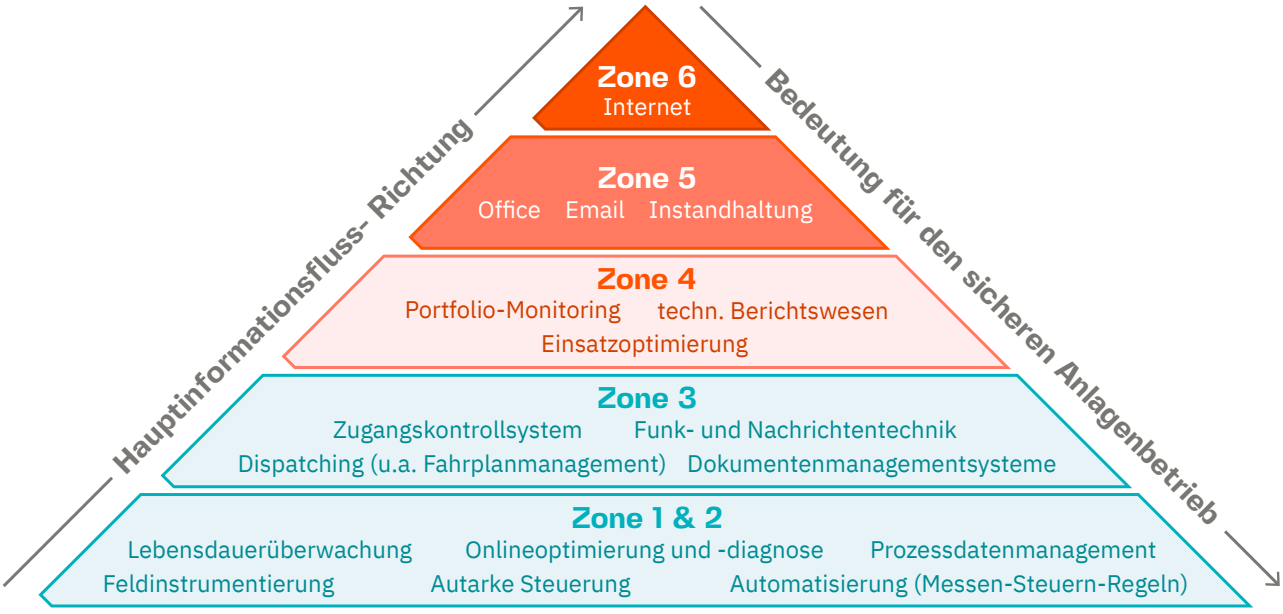
:// 3. ANFORDERUNGEN DER IT-SICHERHEITS-KATALOGE

Die IT-Sicherheitskataloge der Bundesnetzagentur sind beide nach einem ähnlichen Schema aufgebaut. Neben einer Einleitung werden zunächst die rechtlichen Grundlagen und Schutzziele bezüglich Verfügbarkeit, Integrität und Vertraulichkeit benannt und erklärt.

Anschließend wird der Geltungsbereich abgesteckt. Dieser umfasst generell alle zentralen und dezentralen Anwendungen, Systeme und Komponenten, die für einen sicheren Netz- bzw. Anlagenbetrieb notwendig sind. Bei Netzbetreibern zählen hierzu alle IT-Systeme, die direkt Teil der Netzsteuerung sind oder deren Ausfall die Sicherheit des Netzbetriebs gefährden könnten. Daher fallen darunter beispielsweise Trafo- und Netzkoppelstationen, aber auch Messeinrichtungen.

Für Energieanlagen werden die TK- und EDV-Systeme zusätzlich in sechs Zonen eingeteilt. (siehe Abbildung 3). Die Zonen 1-3 gelten dabei als zwingend und dauerhaft notwendig, während die Zonen 4-6 nur bedingt notwendig sind.

Abbildung 3: Zoneneinteilung von Anwendungen, Systemen und Komponenten in Energieanlagen
Quelle: IT-Sicherheitskatalog gem. § 11 Abs. 1b EnWG, S.11

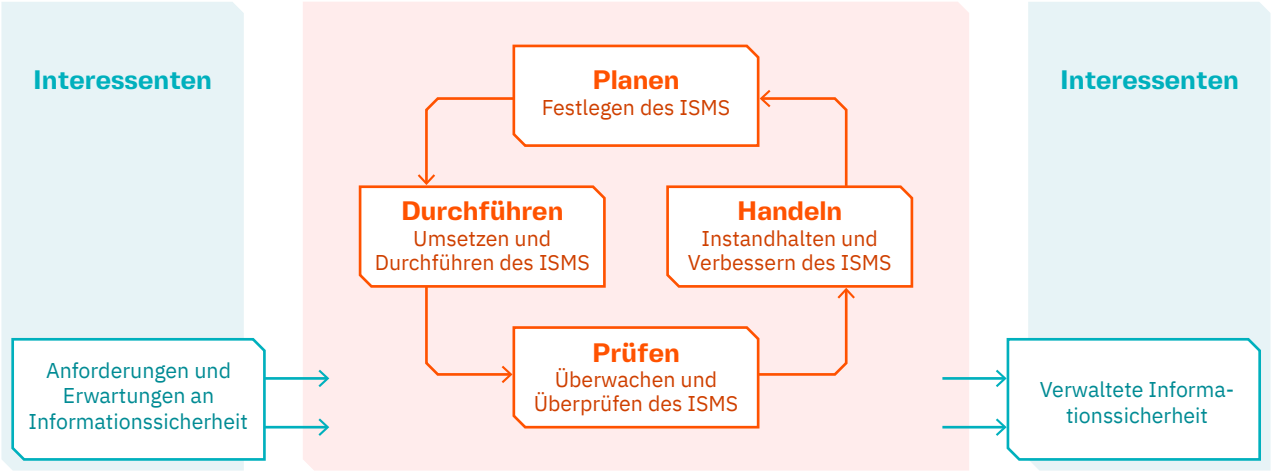


Zusätzlich werden im IT-Sicherheitskatalog Umsetzungsfristen angegeben, welche die jeweiligen Unternehmen einzuhalten haben. Dabei unterscheiden sich die Fristen für Netzbetreiber und Energieanlagen erheblich. Hat ein Netzbetreiber den IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG umzusetzen, musste das Unternehmen der Bundesnetzagentur bereits bis zum 31.01.2018 den Abschluss über die Umsetzung der Anforderungen aus dem IT-Sicherheitskatalog nachweisen. Im Dialog mit der Bundesnetzagentur war es zwar möglich eine Verlängerung der Frist zu beantragen, von denen die meisten jedoch im Jahr 2019 spätestens abgelaufen sind. Aufgrund der hohen Bußgelder sowie der Gefahr einer Schließung des Netzbetriebs bzw. des gesamten Unternehmens (siehe → *Kapitel 6*) ist davon auszugehen, dass grundsätzlich jeder Netzbetreiber zum aktuellen Zeitpunkt in Deutschland für seine IT-Systeme ein angemessenes Sicherheitsniveau nach dem IT-Sicherheitskatalog gemäß § 11 Abs.1a EnWG umgesetzt hat.

Die Betreiber von Energieanlagen hingegen, welche den IT-Sicherheitskatalog gemäß § 11 Abs. 1b EnWG umsetzen müssen, haben noch bis zum 31.03.2021 Zeit, geeignete technische Vorkehrungen zu treffen und diese zertifizieren zu lassen. Bei der Umsetzung der Anforderungen aus dem IT-Sicherheitskatalog ist es explizit nicht ausreichend bloße Einzelmaßnahmen, wie zum Beispiel den Einsatz von Antivirensoftware oder Firewalls, umzusetzen. Stattdessen ist zur Gewährleistung eines angemessenen Sicherheitsniveaus für IT-Systeme, ein ganzheitlicher Ansatz nötig, der kontinuierlich auf Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf anzupassen ist. Einen solchen ganzheitlichen Ansatz stellt wie bereits erwähnt das sog. Informationssicherheits-Managementsystem (ISMS) dar, welches explizit in den Kapiteln bzgl. der Sicherheitsanforderungen in beiden IT-Sicherheitskatalogen gefordert wird.

Prinzipiell umfassen alle Managementsysteme Regelungen, die für die Steuerung und Lenkung einer Institution sorgen und letztlich zur Zielerreichung führen, weshalb sich ein solches Managementsystem auch für die Informationssicherheit anbietet. Dementsprechend fordern beide IT-Sicherheitskataloge, sowohl von Netzbetreibern als auch von Energieanlagen, ein ISMS zu implementieren, das den Anforderungen der DIN EN ISO/IEC 27001 in der jeweils geltenden Fassung genügt.

Abbildung 4: PDCA-Modell nach IT-Sicherheitskatalog:
Quelle: Quelle: IT-SiKat 1a, S.9



Das ISMS legt fest, mit welchen Instrumenten und Methoden die Leitungsebene die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar plant, einsetzt, durchführt, überwacht und verbessert.[9]

Eine Kernforderung im IT-Sicherheitskatalog und der Einführung eines ISMS ist die kontinuierliche Überprüfung und Verbesserung der Wirksamkeit der Maßnahmen. Diese kann durch die Anwendung des „Plan-Do-Check-Act-Modells“ (PDCA-Modell) für die Prozesse erreicht werden. In → *Abbildung 4* ist dargestellt, wie sich die Bundesnetzagentur ein solches Modell für die Informationssicherheit vorstellt. Für konkrete Sicherheitsanforderungen im Detail verweist der IT-Sicherheitskatalog hauptsächlich auf die DIN EN ISO/IEC 27001 und benennt lediglich beispielsweise die Forderung eines ordnungsgemäßen Betriebs der betroffenen IKT-Systeme sowie die Rahmenbedingungen zur Risikoeinschätzung und Risikobehandlung.

9 BSI-Standard 200-1, S. 15.

:// 4. ANWENDUNG DES IT-SICHERHEITSKATALOGS UND IMPLEMENTIERUNG EINES INFORMATIONS-SICHERHEITSMANAGE-MENTSYSTEMS (ISMS)

Zusammengefasst umfassen die wesentlichen Anforderungen aus dem IT-Sicherheitskatalog:

- *die Definition des Geltungsbereichs,*
- *die Einführung eines Informations-sicherheitsmanagementsystems (ISMS),*
- *die Erstellung eines Netzstrukturplans,*
- *den Aufbau eines Risikomanagements (Risikoeinschätzung, -behandlung) und*
- *die Benennung eines Ansprechpartners IT-Sicherheit*

4.1 Definition des Geltungsbereichs

Der IT-Sicherheitskatalog gibt vor, alle zentralen und dezentralen Anwendungen, Systeme und Komponenten, die für einen sicheren Netzbetrieb notwendig sind in den Geltungsbereich aufzunehmen.

Entscheidend ist eine ausführliche Dokumentation des Geltungsbereiches. Dabei werden die einzelnen Anwendungen, Systeme und Komponenten in festen Assets (Werten) beschrieben und in einem sog. „Inventar der Werte“ aufgelistet.

Zu den sicherheitsrelevanten Anwendungen nach § 11 Abs. 1a EnWG gehören beispielsweise Leitsysteme und Komponenten für den Systembetrieb, Übertragungstechnik und Kommunikation, sowie Sekundär-, Automatisierungs- und Fernwirktechnik. Nach § 11 Abs. 1b EnWG gehören dazu Systeme und Komponenten aus den Zonen 1-3 (siehe Abbildung 3, Seite 97), wie beispielsweise die Automatisierungs-

Abbildung 5: Umfang des Geltungsbereiches
Quelle: Eigene Darstellung

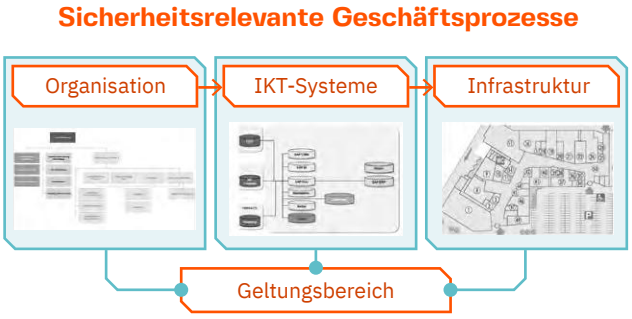


Abbildung 6: Umfang der Informationssicherheit
Quelle: Eigene Darstellung

technik bezüglich Messungen, Steuerung und Regelung oder das Zugangskontrollsystem.

Neben den IKT-Systemen werden außerdem bei beiden IT-Sicherheitskatalogen, die an den sicherheitsrelevanten Prozessen und Diensten maßgeblich beteiligten Organisationseinheiten, Dienstleister und Personen, als auch die notwendigen Standorte, Gebäude und Räume (Infrastruktur) in den Geltungsbereich mit aufgenommen.

Letztendlich ergibt sich der Geltungsbereich für ein ISMS, wie in Abbildung 5 dargestellt, aus den sicherheitsrelevanten IKT-Systemen und der dazugehörigen Organisation und Infrastruktur, weshalb sich die Informationssicherheit als ein Zusammenspiel von physisch-, organisatorisch- und informationstechnischer Sicherheit versteht (siehe Abbildung 6).

4.2 Einführung eines ISMS

Die Einführung eines Informationssicherheitsmanagementsystems (ISMS) nach DIN ISO 27001 ist generell mit einem mehrmonatigen Prozess verbunden. Für eine vollständige Implementierung einschließlich des dazugehörigen Zertifizierungsprozess benötigen Unternehmen je nach verfügbaren Ressourcen zwischen 6 und 12 Monaten.

Das ISMS-Team zur Einführung und Aufrechterhaltung des ISMS stellt sich aus mehreren Mitarbeitern aus unterschiedlichen Hierarchie-Ebenen zusammen. Mit der Geschäftsführung muss in der Regel zunächst eine Sicherheitsstrategie abgestimmt werden. Das Kernteam der IT-Sicherheit, bestehend aus ausgewählten Mitarbeitern (oftmals mit Führungsverantwortung), baut systematisch ein ISMS nach den Anforderungen der Norm im Einklang mit der Sicherheitsstrategie auf, leitet Maßnahmen zur Umsetzung ab und dokumentiert diese in verschiedenen Richtlinien und Anweisungen. Die Realisierung der Maßnahmen erfolgt anschließend in den Fachabteilungen (IT, Netzleitung, etc.) und durch die Belegschaft.

Eine gründliche Ausarbeitung von Schlüsseldokumenten ist bei der späteren Beweisführung in den Audits im Zertifizierungsprozess von großer Bedeutung und sollte daher mit entsprechender Sorgfalt umgesetzt werden. Beim Aufbau eines ISMS gehört daher, neben dem bereits kennengelernten „Inventar der Werte“, insbesondere die Erklärung zur Anwendbarkeit (Statement of Applicability, kurz: SOA). Sie stellt im Wesentlichen die Anforderungen aus der ISO 27001 sowie ISO 27019 dar und dient daher als ideale Übersicht über IST-Zustand des ISMS. Bei der Prüfung im Zertifizierungsprozess ist sie daher unerlässlich.

4.3 Das Risikomanagement im ISMS

Das Risikomanagement ist als zentraler Bestandteil für den Betrieb eines Informationssicherheitsmanagementsystem zu verstehen. Ziel ist es, Risiken zu identifizieren und geeignete Maßnahmen abzuleiten, um bestehende Risiken behandeln zu können. Zu diesem Zweck, werden mögliche Gefährdungen, ihre Eintrittswahrscheinlichkeiten, Schadenskategorien und mögliche Konsequenzen erhoben und protokolliert. Voraussetzung dafür ist ein vollständiges Inventar der Werte, welches alle sicherheitsrelevanten Anwendungen, Systeme und Komponenten für den sicheren Netz- bzw. Anlagenbetrieb enthält.

Definition der Rahmenbedingungen und Risikoeinschätzung

Daher müssen zunächst die Kriterien zur Bewertung von Risiken festgelegt werden. Im IT-Sicherheitskatalog werden hierfür qualitative Schadenskategorien vorgegeben und mögliche Bedrohungen den jeweiligen Eintrittswahrscheinlichkeiten zugeordnet.
Die Einordnung erfolgt dabei für Schadenskategorien der Assets (Werte) nach:

- *kritisch (Schadensauswirkungen können ein existenziell bedrohliches, katastrophalen Ausmaß erreichen),*
- *hoch (Schadensauswirkungen können beträchtlich sein) und*
- *mäßig (Schadensauswirkungen sind überschaubar).*

Für mögliche Bedrohungen wie typischerweise:

- *höhere Gewalt (z.B. Feuer, Wasserschäden, Krankheit),*
- *menschliche Fehlhandlungen (z.B. fehlerhafte Nutzung von IT),*
- *organisatorische Mängel (z.B. unbefugter Zutritt/Zugriff),*
- *technisches Versagen (z. B. Ausfall Strom oder Ausfall IT-System) und*
- *vorsätzliche Handlungen (z.B. Hacker, Viren, Trojaner).*

Werden Eintrittswahrscheinlichkeiten zugeordnet, die beispielsweise folgendermaßen aussehen könnten:

- *hoch (sehr wahrscheinlich),*
- *mittel (wahrscheinlich) und*
- *niedrig (unwahrscheinlich).*

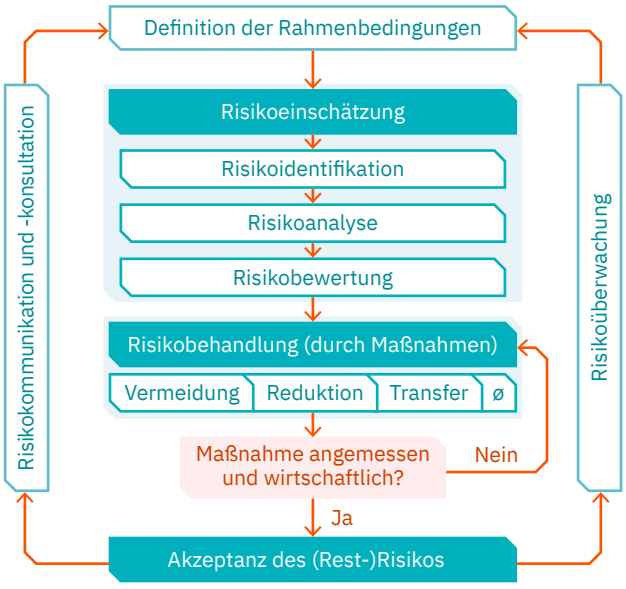
Zusammengerechnet ergeben die Schadenskategorien je Asset mit der möglichen Bedrohung je Eintrittswahrscheinlichkeit das Gesamtrisiko. Sämtliche Risikoeinschätzungen werden in einem sog. Verzeichnis für Risikoeinschätzungen protokolliert.

Risikobehandlung

Anschließend erfolgt durch das Kernteam die Behandlung des Risikos mithilfe von angemessenen Maßnahmen unter Berücksichtigung der Ergebnisse der Risikoeinschätzung und dem Stand der Technik. Die Wirtschaftlichkeit, Umsetzbarkeit und Gegenläufigkeit wird dabei geprüft, konsolidiert und bei der Auswahl der Maßnahmen berücksichtigt.

Die geplanten Maßnahmen werden anschließend in einem sog. Risikobehandlungsplan protokolliert und abgearbeitet. Die Auswirkungen der einzelnen Maßnahmen werden auf das Gesamtrisiko bzw. die Schadenskategorien und Eintrittswahrscheinlichkeiten angerechnet. Sind die Maßnahmen angemessen und wirtschaftlich wird das (Rest-)Risiko akzeptiert, ansonsten müssen neue Maßnahmen geplant werden. In Abbildung 7 wird das gesamte Verfahren im Risikomanagement schematisch dargestellt:

Abbildung 7: Ablauf Risikomanagement
Quelle: Eigene Darstellung



:// 5. UP KRITIS UND DIE ALLIANZ FÜR CYBERSICHERHEIT

Des Weiteren gibt es auf nationaler Ebene zwei Organisationen, die sich mit der Cybersicherheit vertieft befassen, UP KRITIS und die Allianz für Cybersicherheit. Der UP KRITIS ist eine öffentlich-rechtliche Kooperation. Leitgedanke der Kooperation ist es, in gemeinsamer Verantwortung von Wirtschaft und Staat, Kritische Infrastrukturen zu schützen und Versorgungssicherheit für die Bürger zu gewährleisten. Beteiligte sind die Betreiber Kritischer Infrastrukturen, deren Verbände und die zuständigen staatlichen Stellen. Im Januar 2017 zählte UP KRITIS mehr als 400 Beteiligte. Seit 2009 wurde ein Netzwerk zur Kommunikation und Austausch installiert, in dem u.a. Analysen durchgeführt und Empfehlungen erarbeitet werden. Zudem findet ein regelmäßiger Austausch über Vorfälle statt, um ein gemeinsames Lagebild zu erstellen. Durch die zusammenhängende und ressortübergreifende Arbeit werden Strukturen für eine koordinierte Krisenbewältigung geschaffen und regelmäßig geprobt (BSI 2017).

Zusätzlich – und auf ebenfalls auf freiwilliger Basis – gibt es die Allianz für Cybersicherheit[10]. Im Jahr 2012 zusammen mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) gegründet, ist es als Zusammenschluss aller wichtigen Akteure im Bereich der Cybersicherheit das Ziel, die allgemeine Widerstandsfähigkeit des Standortes Deutschland zu stärken (ebd.). Adressaten der Initiative sind Unternehmen und Institutionen, unabhängig davon, ob sie Kritische Infrastruktur sind. Zurzeit sind 4.802 Akteure registriert und beteiligt. Arbeitsgrundlage ist der Austausch von aktuellen Informationen, Wissen und Erfahrung, um Cyberrisiken zu erkennen und vorzubeugen.[11]

10 https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html, aufgerufen am 12.03.2021.

11 https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Ueber-uns/Teilnehmer/teilnehmer_node.html, aufgerufen am 12.03.2021.

:// 6. AUFSICHTS-MASSNAHMEN UND BUSSGELDER

Die Einhaltung der dargelegten gesetzlichen Vorgaben ist für eine sichere Versorgung durch Kritische Infrastrukturen essenziell. Daher werden im Folgenden die Mittel der Bundesbehörden bei Verstoß gegen die Anforderungen und die dazugehörigen Bußgelder dargestellt.

Wenn den Verpflichtungen aus dem EnWG nicht nachgekommen wird oder dem EnWG zuwidergehandelt wird, hat die Regulierungsbehörde (Bundesnetzagentur oder Landesregulierungsbehörde) nach § 65 Abs. 1 und 2 EnWG die Möglichkeit, Maßnahmen zur Einhaltung der Verpflichtung bzw. das Unterlassen eines bestimmten Verhaltens anzuordnen. Auf ein Verschulden (im Sinne eines schuldhaften Handelns) kommt es hierbei nicht an. Bei Verstoß gegen eine angeordnete vollziehbare Maßnahme kann dies als Ordnungswidrigkeit nach § 95 Abs. 1 Nr. 3a EnWG bewertet werden. Dieser kann mit einem Bußgeld von bis zu 100.000 Euro belegt werden, § 95 Abs. 2 S. 1 a. E. EnWG.

Bußgeldbewährtes Verhalten liegt u.a. nach § 95 Abs. 1 Nr. 2 a) und b) EnWG vor, wenn die Vorschriften aus § 11 Abs. 1 a bis c EnWG nicht gewahrt werden; also ein Verstoß gegen den jeweiligen Sicherheitskatalog oder gegen die Meldepflicht vorliegt. Dann ist eine Ordnungswidrigkeit gegeben. Vorsätzliches als auch fahrlässiges Handeln sind in diesem Rahmen bußgeldbewehrt.Das BSI kann gemäß § 8 a Abs. 3 S. 5 BSIG bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen. Wenn dieser Aufforderung nicht oder nicht ausreichend nachgekommen wird, kann das BSI ein Bußgeld gemäß § 14 Abs.1 Nr. 2 BSIG verhängen. Der Gesetzeswortlaut ist an dieser Stelle nicht eindeutig, jedoch kann aus dem Kontext geschlossen werden, dass ein Bußgeld bis zu einer Höhe von 100.000 Euro möglich sein kann.

Nach § 14 Abs. 1 BSIG sind Ordnungswidrigkeiten wie ein Verstoß gegen § 8 a Abs. 1 S. 1 BSIG i.V.m. § 10 Abs. 1 S. 1 BSI-Kritisverordnung bußgeldbewehrt. Für einen Verstoß gegen diese Norm reicht aus, dass die in § 8a Abs. 1 S.1 BSIG genannten Vorkehrungen (s.o.) nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig getroffen wurden. Weiter ist beispielsweise ein Bußgeld vorgesehen, wenn eine Kontaktstelle nicht oder nicht rechtzeitig benannt wurde gemäß § 8b Abs. 3 S.1 BSIG oder eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig gemacht wurde gemäß § 8b Abs. 4 Nr. 2 BSIG. Diese Verstöße können mit einem Bußgeld von bis zu 50.000 Euro geahndet werden, § 14 Abs. 2 S. 1 Hs. 2 BSIG.

Bei schwerwiegenden Verstößen gibt es – unter engen Voraussetzungen – die Möglichkeiten der Stilllegung von Betriebsteilen oder Anlagen, z. B. nach §§ 35, 51 GewO, und der Auflösung der Gesellschaft, z.B. nach § 396 AktG, § 62 GmbHG (Schulze 2014).

:// 7. DAS IT-SICHERHEITS-GESETZ 2.0

Das IT-Sicherheitsgesetz 2.0 wurde in seiner abschließenden Form noch nicht veröffentlicht, der Referentenentwurf vom 27. März 2019 zeigt jedoch deutlich, mit welchen Themen sich Unternehmen und Betreiber von Kritischen Infrastrukturen inhaltlich auseinandersetzen werden müssen - auch wenn einige Inhalte noch höchst umstritten sind.

Insbesondere das BSI soll in seiner zentralen Rolle als Anlaufstelle für IT-Sicherheit weiter gestärkt werden und eine massive Ausweitung der Befugnisse erhalten. Kernaufgabe bleibt es, Cyber-Angriffe abzuwehren und Sicherheitslücken zu schließen, um IT-Systeme von Staat, Bürgern und Wirtschaft besser zu schützen. Die Art und Weise diese Ziele zu verwirklichen ändert sich jedoch erheblich.

In Zukunft soll das BSI aktiv nach Sicherheitslücken suchen und dabei in Systeme eindringen, um Schwachstellen ausfindig zu machen und die Betroffenen anschließend zu benachrichtigen. Die Behörde wechselt damit von einer defensiv schützenden Rolle als Berater in den offensiven Angriffsmodus, wenn es um die IT-Sicherheit der Gesellschaft geht – manch Experte spricht daher bereits von einer zukünftigen „Hackerbehörde“. Des Weiteren kann das BSI zukünftig bei IT-Sicherheitsvorfällen Anordnungen zum Löschen und Melden an Provider erlassen. Dem BSI werden zudem Aufgaben des Verbraucherschutzes übertragen, wodurch die IT-Sicherheit von Produkten, mithilfe von sog. „IT-Sicherheitskennzeichen“, sichtbar gemacht werden soll. Für all diese neuen Befugnisse und Kompetenzen werden beim BSI aktuell schon mehr als 750 Planstellen geschaffen. Ab dem Wintersemester 2020/21 wird außerdem der Nachwuchs gezielt mit einem neuen Studiengang namens „Cyber-Security“ in Kooperation mit der Hochschule des Bundes (kurz HS-Bund) gefördert.[12]

Geplante Neuerungen für Betreiber Kritischer Infrastrukturen

Eine wesentliche Neuerung im IT-Sicherheitsgesetz 2.0 soll die Erweiterung des Adressatenkreis von Betreibern Kritischer Infrastrukturen um den Bereich der Entsorgung bzw. Abfallwirtschaft. Hintergrund dafür ist die Tatsache, dass Ausfälle oder Beeinträchtigungen im Bereich der Abfallwirtschaft nicht nur zu einer massiven Umweltverschmutzung, sondern auch zu einem Anstieg der Seuchengefahr führen würden.[13] Zudem soll das IT-Sicherheitsgesetz 2.0 auch für Infrastrukturen im besonderen öffentlichen Interesse gelten. Hierzu zählen:

- *Unternehmen der Rüstungsindustrie*
- *Unternehmen der Kultur und Medien sowie*

12 Pressemitteilung 10.01.2020, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Studiengang_Cyber_Security_100120.html, aufgerufen am 27.01.2020.

13 Bundesministerium des Innern, für Bau und Heimat (BMI) „Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit Informationstechnischer Systeme“ vom 16.12.2020 – B. Besonderer Teil zu Artikel 1 (Änderung des BSIG) zu Nr.1 zu Buchstabe e.

↳ *Unternehmen von erheblicher volkswirtschaftlicher Bedeutung*

Eine dazugehörige Rechtsverordnung mit Schwellenwerten wurde noch nicht veröffentlicht und erfolgt auch erst nach Verabschiedung des IT-Sicherheitsgesetzes 2.0, weshalb eine Einordnung von Unternehmen zum jetzigen Zeitpunkt noch nicht endgültig möglich ist.

Weiterhin werden zukünftig für die sog. KRITIS-Komponenten, welche unmittelbar für den Betrieb der kritischen Anlage notwendig sind oder deren Störung Auswirkungen auf den Betrieb haben, explizit Mindeststandards durch das BSI definiert. Es ist vorgesehen, dass dafür nur noch solche Komponenten von Herstellern und deren gesamten Zulieferketten verbaut werden, die über ein „BSI-Sicherheitskennzeichen“ verfügen.

Für den Fall von Cyber-Angriffen sollen zudem Krisenreaktionspläne herausgearbeitet werden, welche die an der Krisenreaktion beteiligten Behörden, Betreiber Kritischer Infrastrukturen und Betreiber weiterer Anlagen im besonderen öffentlichen Interesse in die Lage versetzen, im Notfall unverzüglich abgestimmte Entscheidungen zu treffen und angemessene Maßnahmen rechtzeitig durchzuführen. Im Vorfeld hierzu sollen vor allem Systeme zur Angriffserkennung und -bewältigung, um ein Informationssicherheitsmanagementsystem wirksam betreiben zu können, festgeschrieben werden. Das BSI macht künftig konkrete Anforderung zur Ausgestaltung solcher Systeme.

Eine weitere wesentliche Neuerung wird aller Voraussicht nach, eine Angleichung der Strafmaßnahmen und Bußgelder an das Niveau der Datenschutz-Grundverordnung (DSGVO). Während der Gesetzgeber bisher noch eine maximale Strafe von 100.000 Euro je Verstoß vorgesehen hatte, sind es zukünftig Geldbußen von bis zu 20.000.000 Euro oder bis zu vier Prozent des gesamten weltweit erzielten jährlichen Unternehmensumsatzes des vorangegangenen Geschäftsjahrs.

:// 8. EXKURS – WINTERPAKET: WEITERE REGELUNGEN ZUR CYBERSICHERHEIT AUF EU-EBENE

Mit der Verabschiedung des EU-Winterpakets sind noch weitere Aspekte zur Cybersicherheit im Energiesektor hinzugekommen, die hier der Vollständigkeit halber Erwähnung finden sollen. Sie betreffen insbesondere auch die kritische Infrastruktur, auch wenn sie nicht als solche in der jeweiligen Norm adressiert werden.

In der Elektrizitätsbinnenmarkt-Richtlinie[14] von Juni 2019 ist bei der Auflistung der Aufgaben der ÜNB nun auch konkret die Aufgabe der Cybersicherheit enthalten, Art. 40 Abs. 1 lit. m der Richtlinie.

In der ebenfalls mit dem Winterpaket erlassenen Elektrizitätsbinnenmarkt-Verordnung (Elektrizitätsbinnenmarkt-VO)[15] findet sich in Artikel 59 Abs. 2 lit. e Elektrizitätsbinnenmarkt-VO eine Befugnis für die Kommission einen Netzkodex zu erlassen, der „branchenspezifische Regeln für die Cybersicherheitsaspekte grenzüberschreitender Stromflüsse [enthält], einschließlich Regeln für gemeinsame Mindestanforderungen, Planung, Beobachtung, Berichterstattung und Krisenbewältigung“ enthalten soll.

Auch der Aufgabenkreis der ENTSO-E, dem Verband der europäischen Übertragungsnetzbetreiber, wird mit der Elektrizitätsbinnenmarkt-VO erweitert. Gemäß Art. 30 Abs. 1 lit. n der Verordnung muss die ENTSO-E die Cybersicherheit und den Datenschutz in Zusammenarbeit mit den maßgeblichen Behörden und regulierten Unternehmen fördern. Daneben erhält Europäische Organisation der Verteilnetzbetreiber (EU VNBO) die Aufgabe der Unterstützung des Ausbaus der Datenverwaltung, der Cybersicherheit und des Datenschutzes in Zusammenarbeit mit den maßgeblichen Behörden und regulierten Unternehmen, Art. 55 Abs. 1 lit. e Elektrizitätsbinnenmarkt-VO. Zudem soll die EU VNBO bei der Ausarbeitung von Netzkodizes beteiligt sein, Art. 55 Abs. 1 lit. f Elektrizitätsbinnenmarkt-VO.

Des Weiteren hat die Kommission im April 2019 eine Empfehlung zur Cybersicherheit im Energiesektor[16] herausgegeben. Darin werden – rechtlich unverbindlich – die zentralen Herausforderungen für die Cybersicherheit im Energiesektor dargestellt, insbes. Echtzeitanforderungen, Kaskadeneffekte und die Kombination älterer und modernster Technologien. Weiter werden darin auch wesentliche Schritte zur Umsetzung relevanter Vorsorgemaßnahmen aufgezeigt, vgl. Absatz 1 in den Ausführungen zum Gegenstand der Empfehlung.

14 Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU, ABl. L 158 S. 125, ber. 2020 ABl. L 15 S. 8, Celex-Nr. 3 2019 L 0944.

15 Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über den Elektrizitätsbinnenmarkt, ABl. L 158 S. 54, Celex-Nr. 3 2019 R 0943.

16 Empfehlung (EU) 2019/553 der Kommission vom 3. April 2019 zur Cybersicherheit im Energiesektor, Az. C(2019) 2400).

:// 9. FAZIT

KRITIS-Unternehmen in der Energiewirtschaft reagieren auf das erhöhte Cybersicherheitsrisiko, das eine zunehmend mit intelligenten Technologien vernetzte Versorgungsinfrastruktur mit sich bringt, mit großem Engagement. Dazu gehört neben der gesetzlich verpflichtenden Einführung von Informationssicherheitsmanagementsystemen (ISMS) auch der regelmäßige Austausch der Unternehmen mit dem BSI. Dies könnte sich in der Zukunft sogar noch intensivieren: Das geplante IT-Sicherheitsgesetz 2.0 sieht für das BSI zusätzliche Befugnisse vor, um die Betreiber kritischer Infrastruktur noch wirksamer unterstützen zu können.

Insgesamt konnte daher in den vergangenen Jahren eine positive Entwicklung und allgemeine Bewusstseinssteigerung für die Belange der Informationssicherheit innerhalb der Energiewirtschaft festgestellt werden.

:// IT-Sicherheit ist kein Zustand, sondern ein Prozess. //

Klar ist aber auch: Die Sicherheitsbedrohungen sind so dynamisch, dass eine vollumfängliche Absicherung von IT-Systemen nahezu unmöglich ist. Um hier Schritt halten zu können, müssen die Maßnahmen und Verbesserungsprozesse zur zeitnahen Schließung von Schwachstellen ebenso dynamisch und kontinuierlich verfolgt werden. Deshalb stellt die gesetzliche Verpflichtung für KRITIS-Unternehmen zur Einführung und dem fortlaufenden Betrieb der Sicherheitsprozesse eine sinnvolle Maßnahme dar.

Für die weitere Entwicklung stellt sich allerdings die Frage, ob die Reichweite der gesetzlichen Anforderungen auch zukünftig ausreichend ist. Vor dem Hintergrund des von der Regierung beschlossenen Atom- und Kohleausstiegs wird die Bedeutung dezentraler Erzeugungsanlagen für die Energieerzeugung in Deutschland sowie in Europa weiterhin wachsen. Dies birgt auch Auswirkungen auf die Cybersicherheit in der Energiewirtschaft.

:// Der Anteil der erneuerbaren Energien am Stromverbrauch wächst beständig: von rd. sechs Prozent im Jahr 2000 auf rund 38 Prozent im Jahr 2018 (BMWi). //

Durch den Zuwachs an dezentralen Erzeugungsanlagen fluktuiert die Einspeiseleistung; dies erfordert wiederum kurzfristige Regeleingriffe, um eine effiziente und zuverlässige Stromversorgung zu gewährleisten. Dies ist nur möglich durch ein Mehr an Kommunikation und Vernetzung innerhalb von intelligenten Netzen (Smart Grids) und gleichzeitig eine Erhöhung der IT-Sicherheit auf Ebene der dezentralen Energieerzeugung.

Die Analyse der Betreiber für Energieanlagen im Rahmen der Untersuchung bzgl. der KRITIS-Betreiber von Energieanlagen (→ *Kapitel 2.5*) zeigt auf, dass lediglich 3,40 Prozent sämtlicher Energieanlagen nach den aktuellen gesetzlichen Regelungen als KRITIS-Betreiber klassifiziert werden. Zwar vereinen diese aufgrund ihrer Größe 28,72 Prozent der gesamten installierten Erzeugungsleistung in Deutschland, jedoch bedeutet dies im Umkehrschluss, dass 71,28 Prozent der Energieanlagenbetreiber keinen ganzheitlichen Ansatz bei der

IT-Sicherheit verfolgen müssen. Im Kontext der Energiewende sowie der kurz- und mittelfristigen Abschaltung großer Erzeugungsanlagen ist davon auszugehen, dass zukünftig der Anteil der Anlagenbetreiber, die keinen gesetzlich verpflichtenden Ansatz in der IT-Sicherheit verfolgen, weiter zunehmen wird.

Die bisherigen Standards nach dem BDEW-Whitepaper für „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ oder der Einsatz neuer Technologien durch Smart Meter geben zwar ein definiertes Schutzniveau vor. Oftmals sind es jedoch softe Faktoren, Fahrlässigkeit oder mangelnde Kenntnis, die zu Schwachstellen führen und von Angreifern ausgenutzt werden können. Auch diese Einfallstore gilt es durch effektive Maßnahmen der Cybersicherheit zu schützen.

Grundsätzlich lässt sich festhalten, dass sich die Umsetzung der gesetzlichen Verpflichtungen das Schutzniveau der adressierten Unternehmen insgesamt deutlich erhöht hat. Mit der fortschreitenden Digitalisierung, der kontinuierlichen Automatisierung von Prozessen sowie der Heterogenisierung der Erzeugungslandschaft sollten Unternehmen prüfen, ob die Reichweite der bestehenden gesetzlichen Verpflichtungen und Schwellenwerte für die nahe Zukunft angemessen sein wird. Der Gesetzgeber wird auch zukünftig vor der Herausforderung stehen, eine Verhältnismäßigkeit zwischen angemessen Schutzniveau und effizienten Marktprozessen zu finden.

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2017): Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS, 2017, S. 19ff, 30. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf;jsessionid=9E1501ADB6A5BB03DC5068D3FF80A98B.internet081?__blob=publicationFile&v=1, zuletzt geprüft am 12.03.2021.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2020): Die Lage der IT-Sicherheit in Deutschland 2020. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2, zuletzt geprüft am 12.03.2021.

Müller, Benedikt (2019): Wie der Netzbetreiber Innogy den Cyber-Ernstfall probt. Hg. v. Süddeutsche Zeitung. Düsseldorf. Online verfügbar unter https://www.sueddeutsche.de/digital/innogy-hackerangriff-cyberwar-phishing-stromnetze-1.4456474, zuletzt geprüft am 12.03.2021.

Schulze, Hans-Georg (2014): Vermeidung von Haftung und Straftaten auf Führungsebene durch Delegation. In: NJW 48/2014, S. 3484–3488.

Taeger, Jürgen (2016): Die Entwicklung des IT-Rechts im Jahr 2016. In: NJW 69/2016, S. 3764–3770.

Tanriverdi, Hakan (2016): Bundesamt geht von Hackerangriff auf ukrainisches Stromnetz aus. Hg. v. Süddeutsche Zeitung. New York. Online verfügbar unter Bundesamt geht von Hackerangriff auf ukrainisches Stromnetz aus, zuletzt geprüft am 12.03.2021.

STUDIE ZUM EXEMPLARISCHEN ANWENDEN VON GEFÄHRDUNGS-SZENARIEN IN DER ENERGIE-DOMÄNE

ABSTRACT

Diese Studie liefert einen Beitrag für die praktische Anwendung von Gefährdungsszenarien in der Systementwicklung. Dafür wurde ein Anwendungsfall aus der Energiedomäne zum Thema virtuelle Kraftwerke im Rahmen einer Überlastsituation identifiziert und standardisiert mit dem Use Case-Template nach IEC 62559 erfasst. Der Anwendungsfall dokumentiert ein gewolltes Verhalten, bei dem Vertrauen in die ausgetauschten Daten besteht. Ein Angreifer hingegen möchte ein System zu einem nicht-gewollten Verhalten veranlassen und führt hierzu Angriffe auf das System durch. Solche Angriffe können in einem Misuse Case (MUC) Template dokumentiert werden, um dafür entsprechende Sicherheitsanforderungen zu identifizieren. Das MUC-Template wiederum basiert auf einem erweiterten 62559-2 Template und dokumentiert den Kontext eines ungewollten Verhaltens näher. Auf dieser Basis wurden in dieser Studie drei verschiedene Gefährdungsszenarien mit dem MUC-Template erfasst und analysiert, so dass systematisch verletzte Schutzziele und Sicherheitsanforderungen identifiziert werden konnten, die dann in einem zu implementierenden System als konkrete Sicherheitsmaßnahmen umgesetzt werden sollten.

AUTOREN

Christine Rosinger
(OFFIS)

Mathias Uslar
(OFFIS)

Abkürzungsverzeichnis

AMI	Advanced Metering Interface
APP	Anwendungen (BSI-Baustein)
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
CAPEC	Common Attack Pattern Enumeration and Classification
CON	Kryptokonzept (BSI-Baustein)
CPU	Central Processing Unit
DEM	Device Energy Management
DER	Dezentrale Energieressource, Im Kontext der Sicherheitsanforderungen: Detektion und Reaktion (BSI-Baustein)
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik
DMS	Distribution Management System
DMZ	Demilitarisierte Zone
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
ED	Edition
EDMS	Energiedatenmanagementsystem
EMS	Energiemanagementsystem
EnWG	Energiewirtschaftsgesetz
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnologie
iMSys	Intelligentes Messsystem
IND	Industrielle IT (BSI-Baustein)
INF	Infrastruktur (BSI-Baustein)
iOS	Mobiles Betriebssystem von Apple
IoT	Internet of Things
IP	Internet Protokoll
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Informationstechnologien
KEM	Kundenenergiemanagement
KPI	Key Performance Indikatoren
KRITIS	Kritische Infrastrukturen
LV	Low Voltage, Niederspannung
MDM	Mobile Device Management
MITM	Man-in-the-middle
MITRE CVE	Common Vulnerabilities and Exposures of the MITRE Corporation
MUC	Misuse Case
MV	Middle Voltage, Mittelspannung
NESCOR	National Electric Sector Cybersecurity Organization Resource
NET	Netze und Kommunikation (BSI-Baustein)
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
OpenLDAP	Offene Implementierung des Lightweight Directory Access Protocol
OPS	Betrieb (BSI-Baustein)
ORP	Organisation und Personal (BSI-Baustein)
OT	Operational Technology
OWASP	Open Web Application Security Project
PKI	Public Key Infrastructure
RTF	Rich Text Format
SAN	Storage Area Network
SBK	Schutzbedarfskategorie
SCADA	Supervisory Control and Data Acquisition
SGAM	Smart Grid Architecture Model

SMGW	Smart Meter Gateway
SNMP	Simple Network Management Protocol
SPS	Speicherprogrammierbaresteuerung
SQL	Structured Query Language, Datenbanksprache
SRD	System Reference Deliverable
SYS	IT-Systeme (BSI-Baustein)
TC	Technisches Komitee
TDoS	Telephone Denial of Service
TK	Telekommunikation
TR	Technische Richtlinie
UC	Use Case, Anwendungsfall
UCMR	Use Case Management Repository
UML	Unified Modeling Language
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e. V.
VK	Virtuelles Kraftwerk
VoIP	Voice over IP
VPN	Virtual Private Network
XLSM	Excel Spreadsheet Xml macro-enabled
XML	Extensible Markup Language

1. EINLEITUNG 115
1.1 Ziel und Motivation der Studie 115
1.2 Gliederung 115

2. IT-SICHERHEIT UND RESILIENZ IM ENERGIEKONTEXT 116

3. GEFÄHRDUNGSSZENARIEN AUS DER ENERGIEDOMÄNE 120
3.1 Gefährdungsszenarien 120
3.2 Angreifertypen 121
3.3 Typische Angriffsvektoren 122

4. METHODIK: IEC 62559 UND MISUSECASE-TEMPLATE 126
4.1 VDE 0175-110 – Richtlinie zur IT-Sicherheit und Resilienz für die Smart-Energy-Einsatzumgebung 126
4.2 IEC 62559 – Use Case Methodik 127
4.3 Misuse Case Template 128
4.4 Gefährdungskatalog nach BSI-Grundschutz 130
4.5 Attack Pattern Classification, Recommendations and Attack Conditions nach CAPEC 132
4.6 Gesamtmethodik 132

5. ANWENDUNG DER GESAMTMETHODIK 136
5.1 Beschreibung des Anwendungsfalls 136
5.2 Beschreibung des Misuse Cases 138
5.2.1 Beschreibung im MUC-Template 138
5.2.2 Risikoanalyse 140
5.2.3 Identifikation von Sicherheitsanforderungen 141

6. ZUSAMMENFASSUNG, DISKUSSION UND AUSBLICK 143
6.1 Zusammenfassung 143
6.2 Diskussion 143

Literaturverzeichnis 145

:// 1. EINLEITUNG

Dieser Abschnitt leitet diese Studie mit einer kurzen Ziel- und Motivationsbeschreibung in → *Abschnitt 1.1* ein. Weiterhin wird in → *Abschnitt 1.2* die Gliederung des weiteren Dokuments kurz erläutert.

1.1 Ziel und Motivation der Studie

Ziel dieses Beitrags ist die Untersuchung von Gefährdungen – häufig auch Bedrohungen genannt – und Gefährdungsszenarien, sowie die Analyse dieser, auf Basis eines Anwendungsfalls zu virtuellen Kraftwerken.

Die Gefährdungsanalyse ist Bestandteil einer Sicherheitsanalyse und wird meist vor der Risikoanalyse durchgeführt. Insgesamt dient dies bereits zu Beginn des Entwicklungsprozesses der Konzeptionierung und Umsetzung von Sicherheitsmaßnahmen für IT-Systeme und -Architekturen und fördert somit das Prinzip „Security-by-Design“[1].

Weiterhin wurde innerhalb dieses Ergebnisdokuments ein Überblick zu Gefährdungsszenarien aus der Energiedomäne, sowie die Erläuterung verschiedener Angreifertypen und typischer Angriffsvektoren geschaffen. Dabei wurden drei potenzielle Angriffsszenarien auf Basis der im Projekt entwickelten IT-Landkarte identifiziert. Dieser Anwendungsfall und die Gefährdungsszenarien wurden detailliert anhand verschiedener wissenschaftlicher und teilweise standardisierter Modelle und Methoden analysiert (siehe auch → *Abschnitt 4.6* „Gesamtmethodik“). Um entsprechende Gefährdungen zu vermeiden, wurden auf Basis der Analyse der Gefährdungsszenarien Sicherheitsanforderungen identifiziert, die wiederum bei der Implementierung des Anwendungsfalls in konkrete Sicherheitsmaßnahmen umgesetzt werden können.

1.2 Gliederung

Das weitere Dokument gliedert sich wie folgt: Zunächst werden in → *Abschnitt 2* die Begriffe IT-Sicherheit und Resilienz – als eine Säule der drei Schwerpunkte dieser Studie – im Kontext der Energiedomäne erläutert und eingeordnet. → *Abschnitt 3* gibt einen kurzen Überblick zu interessanten und bekannten Gefährdungsszenarien und Angreifertypen aus der Energiedomäne der Vergangenheit sowie einen Einblick in typische Angriffsvektoren. Danach werden in → *Abschnitt 4* die verschiedenen Bestandteile der hier verwendeten Methodik erläutert und dann zu einer Gesamtmethodik in → *Abschnitt 4.6* zusammengefügt. In → *Abschnitt 5* wird die vorher beschriebene Gesamtmethodik angewendet und textuell anhand eines beispielhaften Anwendungsfalls mit drei Angriffsszenarien zum Thema virtuelle Kraftwerke im Rahmen einer Überlastsituation beschrieben. Weiterhin werden die Gefährdungsszenarien in dem MUC-Template untersucht und ausgewertet. Der verwendete Anwendungsfall wurde mit dem Use Case-Template nach IEC 62559 erfasst. Das dazugehörige ausgefüllte Template ist im Anhang in → *Abschnitt 7.1* dargestellt. Die drei Angriffsszenarien auf diesen Anwendungsfall, die für diese Studie entwickelt wurden, werden im Anhang in → *Abschnitt 7.2* mittels eines Misuse Case-Templates, das ebenfalls an den IEC 62559 angelehnt ist, erfasst. Abschließend gibt es in → *Abschnitt 6* eine Zusammenfassung.

1 Das Prinzip „Security-by-Design“ verfolgt die durchgängige Berücksichtigung von Sicherheitsaspekten direkt von Beginn bis Ende des Designprozesses.

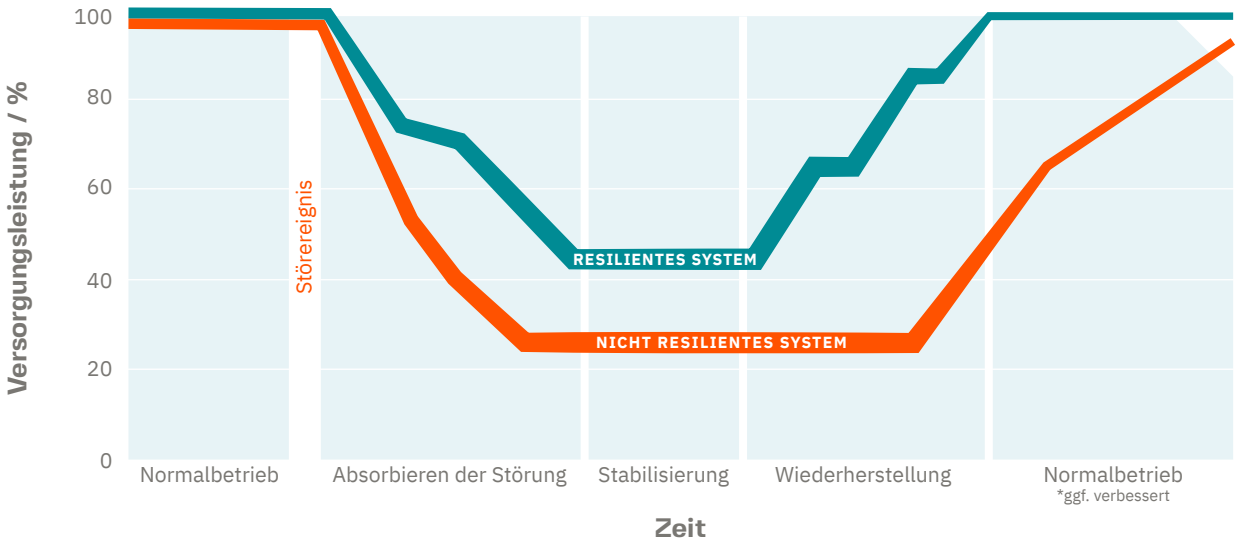
:// 2. IT-SICHERHEIT UND RESILIENZ IM ENERGIE-KONTEXT

Die Domäne Energie wird zu den kritischen Infrastrukturen (KRITIS) gezählt. Hierfür wurden in der „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ (BSI-KritisV) bestimmte Schwellenwerte festgelegt, um zu bestimmen, welche Bestandteile der Domäne in Bezug auf IT-Sicherheit besonders betrachtet werden müssen. Für die Energiedomäne bedeutet dies, dass nach BSI-KritisV, zum Beispiel Erzeugungsanlagen, die ungefähr 500.000 Personen versorgen (für Erzeugungsanlagen wurde hier z. B. der Schwellenwert von 420 MW installierte Netto-Nennleistung (elektrisch) festgelegt) zu den kritischen Infrastrukturen zählen und somit als besonders schützenswert gelten. Das BSI IT-Sicherheitsgesetz legt dabei fest, welche Maßnahmen ergriffen werden, um die Sicherheit von IT-Systemen zu erhöhen. Dies sind Folgende:

- *eine Kontaktstelle benennen,*
- *IT-Störfälle melden,*
- *den „Stand der Technik“ umsetzen und*
- *dies alle zwei Jahre dem BSI nachweisen.*

Um die Maßnahmen in der Energiedomäne umzusetzen wurden IT-Sicherheitskataloge von der Bundesnetzagentur (BNetzA) entwickelt. Hierbei

Abbildung 1: Vergleich zwischen resilientem (blau) und nicht resilientem (rot) System
Quelle: nach Babazadeh et al. (2018)



wird zwischen dem IT-Sicherheitskatalog für Betreiber von *Strom- und Gasnetzen* nach §11 Abs. 1a EnWG[2] und dem IT-Sicherheitskatalog für Betreiber von Energieanlagen nach §11 Abs. 1b EnWG, die nach BSI-Kritisverordnung als KRITIS eingeordnet wurden und an ein Energieversorgungsnetz angeschlossen sind, unterschieden. Der IT-Sicherheitskatalog für *Betreiber von Energieanlage*n nach §11 Abs. 1b EnWG[3] wurde im Jahr 2018 ergänzt, damit ein umfassender Schutz für den Netzbetrieb inklusive der Energieanlagen gewährleistet ist. „Betreiber von Energieanlagen, die mit dem öffentlichen Versorgungsnetz verbunden sind, werden verpflichtet, dort, wo eine Gefährdung für den Netzbetrieb möglich ist, ebenfalls Sicherheitsmaßnahmen zu ergreifen, um die Vorteile moderner IKT auch in Zukunft sicher nutzen zu können." Laut diesen beiden Katalogen müssen die entsprechenden Betreiber in ihrem System ein Informationssicherheitsmanagementsystem (ISMS) implementieren und zertifizieren, das den Anforderungen der ISO / IEC 27001 in der aktuell geltenden Fassung entspricht, um IT-sicherheitstechnische Mindeststandards zu erfüllen. Beide Sicherheitskataloge sind insgesamt sehr ähnlich angelegt, um einen gleichartigen Schutz für beide Bereiche umsetzen zu können.

Um solch eine KRITIS – neben den gesetzlichen Anforderungen – möglichst stabil und robust zu halten, wird zusätzlich versucht diese so resilient wie möglich zu konstruieren. Im zukünftigen Stromversorgungssystem ist Resilienz der effektivste Weg, um Ausfallsicherheit zu erreichen, denn die bisherige Robustheit lässt sich aufgrund der veränderten Struktur nicht eins zu eins fortführen. Außerdem kann hiermit die Geschäftskontinuität eines Unternehmens sichergestellt werden. Resilienz kann daher die Energieversorgung der Zukunft gegenüber Belastungen mit potenziell großen Schäden absichern (Hirschl et al. 2018), die sich sowohl schlecht quantifizieren und prognostizieren lassen als auch überraschend eintreffen. Für die Resilienz gilt nach Mayer et al. (2018) Folgendes:

> **:// Unter Resilienz eines Systems wird die Reaktionsfähigkeit des Systems auf seltene oder unerwartete gravierende Störereignisse verstanden. Man bezeichnet ein System als resilient, wenn seine Funktionsfähigkeit bei diesen Störungen möglichst wenig beeinträchtigt wird, es zu keinen größeren Schäden kommt und nach der Störung so schnell wie möglich wieder die volle Leistung zur Verfügung steht.[4] //**

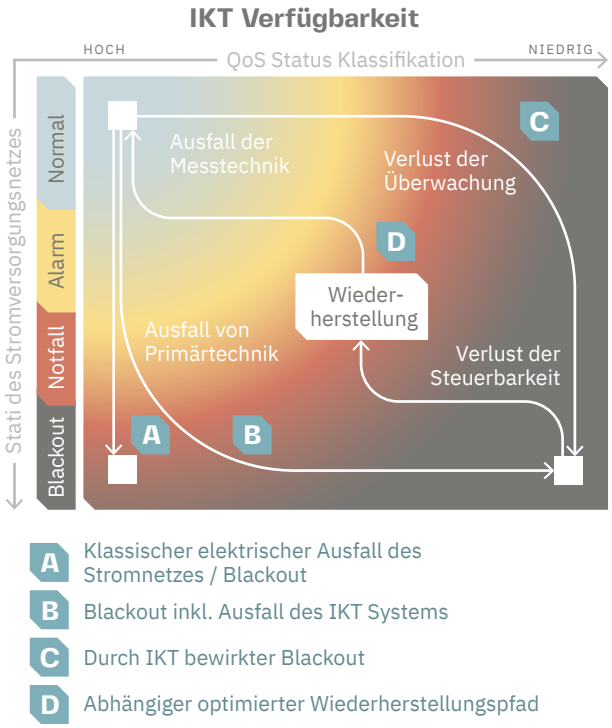
Für die bessere Veranschaulichung ist in → *Abbildung 1* (aus (Babazadeh et al. 2018)) der Vergleich zwischen einem resilienten System in Türkis und einem nicht-resilienten System in Orange bei der Wiederherstellung der Funktionsfähigkeit eines Systems nach einer Störung anhand der Versorgungsleistung in Prozent graphisch dargestellt. Dort ist zu erkennen, dass bereits in der ersten Phase nach der Störung bei einem resilienten System eine geeignete Reaktion erfolgt und somit das Absorbieren der Störung besser erfolgt. Daher steht hier dauerhaft eine höhere Versorgungsleistung trotz Störung als bei einem nicht-resilienten System zur Verfügung. Auch die Stabilisierungsphase kann mit einer höheren Versorgungsleistung erfolgen und auch die komplette Wiederherstellung der Funktionsfähigkeit erfolgt deutlich früher, wenn Maßnahmen für die Resilienz ergriffen wurden.

2 Siehe https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf.

3 Siehe https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_2018.pdf.

4 Ähnliche Definition auch in Babazadeh et al. 2018.

Abbildung 2: Resilienz und Cyber-Resilienz in der Stromversorgung übersetzt aus (Fischer 2018)
Quelle: Fischer (2018)



Weiterhin schließt nach VDE 0175-110 Resilienz

> :// **Sicherheitsmaßnahmen ein, mit denen Auswirkungen verringert werden können, und zwar nicht nur im Vorfeld von Zwischenfällen (feststellen und verhindern), sondern auch während dieser Zwischenfälle (erkennen und reagieren), sowie nach Behebung und deren Auswirkungen (wiederherstellen). //**

Dies bezieht sich auch auf den weiteren Begriff in diesem Themenfeld: die Cyber-Resilienz, die sich auf die Absicherung von IT-gestützten Prozessen fokussiert. Das cyber-resiliente Energiesystem soll damit auf unvorhergesehene Störungen in der Informations- und Kommunikationstechnik (IKT) in der Art reagieren, dass es dennoch seine grundlegende Funktionsfähigkeit erhält oder sie zumindest eigenständig wiedererlangt, so dass sich die Folgen etwaiger Störungen auf ein Minimum begrenzen. Für diese Selbstorganisation ist es notwendig, die IKT als integralen Bestandteil des Stromsystems zu begreifen und das Potenzial der Digitalisierung für die Erhöhung seiner Resilienz voll auszuschöpfen (Witte 2020). Nach Mayer et al. (2018) bedeutet Cyber-Resilienz folgendes:

> :// **Ein System ist dann cyber-resilient, wenn die IKT-Komponenten und die auf IKT basierenden Prozesse zusammen mit den energietechnischen Komponenten die Resilienz des Gesamtsystems erhöhen. Dazu gehören die Möglichkeiten, ein genaues Lagebild zu erzeugen und die Auswirkungen von Maßnahmen besser prognostizieren zu können. Ganz besonders leistet die Cyber-Resilienz auch eine Abschätzung, inwieweit sich Risiken durch ein Ereignis ändern, etwa indem nun andere Ereignisse deutlich wahrscheinlicher (etwa ein Erdschluss, da Leitungen aufgrund hoher Belastung stärker durchhängen) oder deutlich gefährlicher werden (etwa da aufgrund von IKT-Problemen nicht mehr ausreichend reagiert werden kann). //**

In Abbildung 2 ist eine cyber-resiliente Vorgehensweise zur „System Restauration“ in den ungestörten Betrieb beispielhaft dargestellt: Während Pfad (A) einen klassischen Blackout z. B. durch Ausfall von Primärtechnik (beispielsweise der Ausfall eines Transformators) repräsentiert, werden in Pfad (B) und (C) Blackouts durch IKT Ausfälle dargestellt. Hier erfolgte in Pfad (B) nach dem Ausfall der Primärtechnik ein zusätzlicher Ausfall des IKT-Systems und in Pfad (C) nach dem Ausfall

der Messtechnik, der Verlust der Überwachung *und letztendlich der Verlust der Steuerbarkeit, was in beiden Fällen (B) und (C) letztendlich ein Blackout des Stromversorgungsnetzes bewirkte und zu nicht vorhandener Verfügbarkeit der IKT führte. Pfad (D) stellt danach den Wiederherstellungspfad durch entsprechende Cyber-Resilienz-Maßnahmen dar. Die jeweiligen Pfade repräsentieren auf der x-Achse die IKT-Verfügbarkeit von hoch bis niedrig und auf der y-Achse die einzelnen Zustände des Stromversorgungsnetzes: Normal, Alarm, Notfall und Blackout.

Das heißt also ein resilientes System hat eine hohe Widerstandsfähigkeit gegenüber technischem oder menschlichem Versagen, aber auch höherer Gewalt oder gezielten Angriffen. Hierzu gehört auch das Aufdecken von Schwachstellen[5] (Vulnerabilitäten des (Gesamt-) Systems und seiner individuellen Komponenten), damit Angreifer entsprechende Lücken nicht ausnutzen können. Und auch das Analysieren von (Cyber-)Gefährdungen / Bedrohungen, wie beispielsweise Distributed-Denial-of-Service-Angriff, Viren, Phishing oder Man-in-the-middle-Attacken. Dies, also eine Gefährdungsanalyse für die Energiedomäne, wird Fokus dieses Dokuments sein.

5 „Eine Schwachstelle (englisch „vulnerability“) ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution.“, vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html. Solch ein Fehler eines IT-Systems kann beispielsweise ein Fehler im Programmiercode sein. Entsprechende Schwachstellen können durch Angreifer (z. B. Hacker) ausgenutzt werden, um das System zum Erliegen zu bringen (Angriff auf die Verfügbarkeit), Daten abzugreifen (Angriff auf die Vertraulichkeit) oder Daten zu manipulieren (Angriff auf die Integrität).

EXKURS

REDUNDANZ UND RESILIENZ

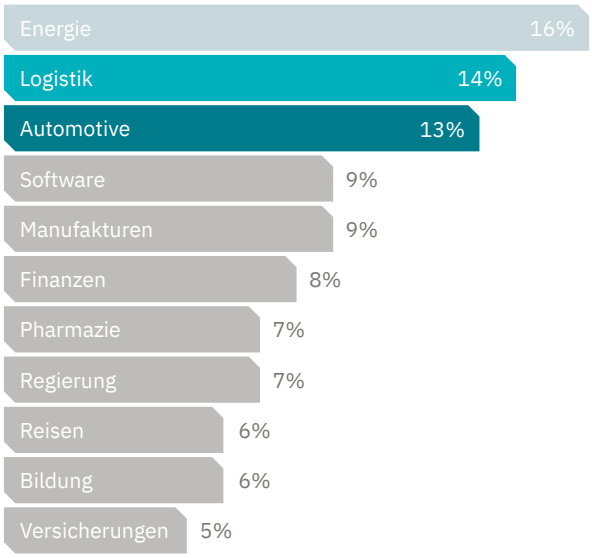
Redet man heutzutage über Energiesysteme, treten in der Diskussion oftmals die Begriffe Resilienz und Redundanz auf und werden häufig synonym genutzt, was jedoch nicht korrekt ist. Unter redundanten Systemen versteht man Systeme, von denen eine wichtige Komponente, die für den Betrieb mit ihrer Funktion dringend erforderlich ist, gedoppelt wird, als sogenannte „Fallback“ Lösung oder Reservekapazitäten. Dies kennt man aus dem Alltag, etwa, indem man Ersatzschlüssel für die Wohnungstür oder das Auto etwa bei Dritten, für den Fall, dass man sich ausgesperrt hat oder den Schlüssel verliert, hinterlegt. Auch im alltäglichen Leben gibt es diese Redundanz mittlerweile im technischen Alltag, ohne dass man sie bewusst wahrnimmt. Festplatten, seien es konventionelle oder auch SSD Datenträger, besitzen so genannten „Ersatzsektoren“. Speichert ein Computer physisch etwas, können mit der Zeit die Sektoren durch die Zugriffe physisch defekt werden – er ist also nur noch Zufall, ob eine 1 oder eine 0 gespeichert wird, was zu korrupten Daten führt. Die Festplatte mit ihrem Controller kann jedoch solche Lesefehler erkennen und Speicherzellen als „ungültig“ markieren und andere stattdessen heranziehen. Dies ist heutzutage ein übliches Verfahren für Redundanz. Wenn dann die Sektoren aufgebraucht sind und das Betriebssystem Fehler meldet, ist die Redundanz aufgebraucht.

Umgekehrt ist in diesem Beispiel auch zu sehen, dass die Redundanz das System resilient gegen Fehler und Umwelteinflüsse macht – gegen den Ausfall einzelner Zellen durch Abnutzung. Am Beispiel erkennt man aber auch, wie wichtig Resilienz, also die psychische Fähigkeit, schwierige Umgebungssituationen ohne anhaltende Beeinträchtigung zu überstehen, auch im Systementwurf ist. Eine klassische Festplatte mit rotierenden Massen hatte das Problem, dass man sie im Betrieb nicht bewegen sollte, da ansonsten der Lesekopf in einer Bewegung physisch die Platte treffen, sie zerkratzen und damit zerstören könnte – der so genannte Headcrash. Eine SSD hat diesen Kopf nicht mehr, sondern besteht nur aus mit Hauptspeicher vergleichbaren Zellen, die jedoch auch abnutzen können – sie ist resilienter gegen Bewegungen des Rechners, aber erkauft sich diesen Vorteil durch einen höheren Preis, eine geringere Speicherkapazität bei gleichem Formfaktor sowie einer schnelleren Abnutzung bei jedoch einer höheren Geschwindigkeit, da keine mechanischen Teile mehr den Betrieb begrenzen. Dennoch wiegen diese Nachteile nicht so schwer, als dass die klassischen Festplatten den Markt weiterhin dominieren könnten.

:// 3. GEFÄHRDUNGS-SZENARIEN AUS DER ENERGIEDOMÄNE

Der Energiesektor rückt als Ziel bedingt durch die Attraktivität von kritischen Infrastrukturen eines Landes zunehmend in den Fokus von Angreifern. Eine aktuelle Analyse der Hornetsecurity[6] zeigt in (Kreyenberg 2020), dass im Jahr 2019 der Energiesektor die Top 10 der angegriffenen Branchen mit 16 Prozent aller Attacken anführt, siehe auch Abbildung 3: Die Top 10 der angegriffenen Branchen in 2019 Quelle: Kreyenberg (2020).

Abbildung 3: Die Top 10 der angegriffenen Branchen in 2019
Quelle: Kreyenberg (2020)



6 Siehe auch https://www.hornetsecurity.com/de/security-informationen/cybersecurity-special-energiebranche/.

Dabei ist das Einfallstor mit knapp 47 Prozent aller Angriffe ein schädlicher Link, 32 Prozent aller Angriffe erfolgen über einen schädlichen Anhang, Phishing folgt mit 22 Prozent. Gezielter Betrug ist lediglich in 0,16 % aller Fälle zu sehen.

Das große Problem der Betreiber von kritischen Infrastrukturen ist die Asymmetrie: Ein Angreifer muss nur eine Schwachstelle finden, die er ausnutzen kann; der Betreiber muss hingegen einen ganzheitlichen Schutz gewährleisten, um sich in der Regel umfassend absichern zu können.

In diesem Abschnitt werden in diesem Zusammenhang zunächst in → *Abschnitt 3.1* Gefährdungsszenarien und in → *Abschnitt 3.2* Angreifertypen jeweils aus der Energiedomäne aufgezeigt. → *Abschnitt 3.3* gibt anschließend einen Einblick in typische Angriffsvektoren, hauptsächlich aus dem Projekt der OWASP Foundation.

3.1 Gefährdungsszenarien

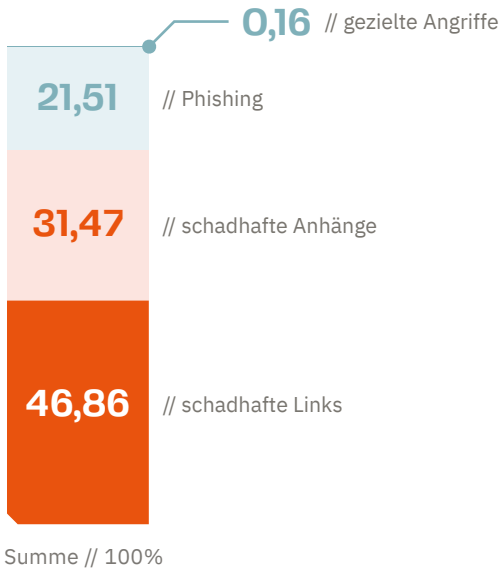
Über die Jahre fanden in der Energiewirtschaft verschiedene Cyberangriffe auf Infrastrukturen und Assets statt, meistens jedoch nicht als primäre Angriffe, sondern als kollaterale Cyberangriffe neben echten, physischen Angriffen, um zusätzlichen Schaden anzurichten, oder als Tests (sog. Probing, um Lücken in der Verteidigung zu finden). Im Folgenden werden beispielhaft drei Angriffe auf den Energiesektor beschrieben.

Eines der wenigen bekannten älteren Beispiele für eine erfolgreiche Cyber-Sabotage ist der Angriff auf eine australische Kläranlage in 2000, bei der ein Ex-Mitarbeiter mehrere Millionen Liter Abwasser in Flüsse, Parks und auf das Grundstück eines großen Hotels laufen ließ (Maroochy-Water-Services-Case-Study) (Marshall D. Abrams, Joe Weiss 2018).

Stuxnet ist ein Computerwurm, der im Juni 2010 entdeckt und zuerst unter dem Namen „RootkitTmphider“ beschrieben wurde (Langner 2013). Das Schadprogramm wurde speziell entwickelt zum Angriff auf ein System zur Überwachung und Steuerung (SCADA-System) des Herstellers Siemens – die Simatic S7. Dabei wurde eingegriffen in die Steuerung von Frequenzumrichtern der Hersteller Vacon aus Finnland und Fararo Paya in Teheran. Ein Frequenzumrichter dient beispielsweise dazu, die Geschwindigkeit von Motoren zu steuern. Solche Steuerungen werden vielfach eingesetzt, etwa in Industrieanlagen wie Wasserwerken, Klimatechnik oder Pipelines. Da bis Ende September 2010 der Iran den größten Anteil der infizierten Computer besaß und es zu außergewöhnlichen Störungen im iranischen Atomprogramm kam, lag es nah, dass Stuxnet hauptsächlich entstand, um die Leittechnik der Urananreicherungsanlage in Natanz (Iran) oder des Kernkraftwerks Buschehr (Iran) zu stören.

Im Dezember 2015 gelang Hackern mit BlackEnergy eine koordinierte Attacke auf mindestens drei Energienetzbetreiber in der Ukraine. Mutmaßlich kamen hier Spear-Phishing-E-Mails zum Einsatz, die Mitarbeiter zum Öffnen der schädlichen Anhänge bewogen haben. Die Cyberkriminellen spielten unter anderem Schadsoftware auf Systeme mit veralteten Softwareständen auf, löschten Daten auf Windows-Systemen und führten einen TDoS-Angriff (Telephone Denial of Service) auf mindestens ein Callcenter der Verteilnetzbetreiber durch, was eine Überlastung der Telefonleitungen zur Folge hatte. Rund 225.000 Einwohner waren von einem mehrstündigen Ausfall der Stromversorgung betroffen und hatten keine Möglichkeit, die Störung telefonisch zu melden.

Abbildung 4: Angriffsarten auf die Energiebranche
Quelle: Kreyenberg (2020)



3.2 Angreifertypen

Mittlerweile gibt es neben den klassischen Hackern als Einzeltäter, den unzufriedenen eigenen Mitarbeitern (Sabotage) auch ganze Hackergruppen, die sich auf Branchen spezialisiert haben. Im Energiebereich sind im Besonderen die Gruppen APT19, Dragonfly und Magic Hound zu nennen, die im Folgenden kurz beschrieben werden.

2017 nutzte APT19 drei verschiedene Angriffsmethoden. Anfang Mai starteten die Hacker Phishing-Angriffe mit infizierten RTF-Anhängen, die die als „MITRE CVE 2017-0199“ klassifizierte Schwachstelle von Microsoft Windows ausnutzten. Ende Mai änderten sie ihre Strategie und setzten stattdessen Microsoft-Excel-Dateien mit Makros (XLSM-Dokumente) ein. Die neuesten Versionen dieser XLSM-Dokumente konnten sich sogar selbst in Whitelists eintragen. Außerdem wurde mindestens eine Phishing-Kampagne beobachtet, bei der auf den infizierten Systemen die Malware „Cobalt Strike“ installiert wurde. Als Operationsbasis wird zumeist China angenommen.

Die Gruppe Dragonfly ist seit dem Jahr 2011 aktiv und war nach ihrer Enthüllung durch Symantec und andere Sicherheitsforscher im Jahre 2014 zunächst untergetaucht. Nach neuesten Erkenntnissen nehmen aber nun die gezielten Angriffs- und Sabotageversuche der sog. „Dragonfly 2.0“ auf westliche Energiekonzerne deutlich zu. Es wurden bereits erste Versuche unternommen, die Betriebssysteme von Energieunternehmen in Europa und den USA unter Kontrolle zu bringen oder sogar zu sabotieren.

Die Gruppe Magic Hound ist eine vom Iran gesponserte und vor allem im Nahen Osten operierende Gruppe, die bereits 2014 gegründet wurde. Das Team, das hinter der Kampagne steht, hat in erster Linie Organisationen in den Bereichen Energie, Regierung und Technologie ins Visier genommen, die entweder in Saudi-Arabien ansässig sind oder dort Geschäftsinteressen haben.

3.3 Typische Angriffsvektoren

Angriffsvektoren sind nach dem BSI wie folgt definiert[7]:„Als Angriffsvektor wird die Kombination von Angriffsweg und -technik bezeichnet, mit der sich ein Angreifer Zugang zu IT-Systemen verschafft.“ Meistens werden dafür bekannt gewordene Sicherheitslücken in dem angegriffenen System genutzt. Ein solches Ausnutzen bezeichnet man als (engl.) Exploit.

Es gibt verschiedenste Angriffsvektoren. Einige typische Angriffsvektoren werden im Folgenden aufgezählt und dabei beispielhaft erklärt:

↳ *Man-in-the-middle-attack (MITM-Angriff): Bei einem MITM-Angriff schaltet sich ein Angreifer logisch oder physisch zwischen zwei Parteien, die miteinander kommunizieren, um diese Kommunikation zu unterbrechen, abzuhören oder zu manipulieren.*

↳ *Sniffing: Ein Sniffer ist ein Softwaretool zur Netzwerkanalyse und kann von Angreifern zum Sniffing, d. h. zum Mithören des Netzwerkverkehrs, verwendet werden.*

↳ *Content Spoofing: Ein Angreifer modifiziert den Inhalt einer Nachricht so, dass er etwas anderes als das enthält, was der ursprüngliche Sender beabsichtigt hat, während die scheinbare Quelle des Inhalts unverändert bleibt.*

↳ *Injections: Injection steht für das Einschleusen von nicht vertrauenswürdigen Eingaben in ein Programm. Beispielsweise wird bei SQL-Injections eine SQL-Datenbank durch das Einschleusen von Datenbankbefehlen oder -abfragen, z. B. über eine fehlerhaft konfigurierte Eingabemaske, durch einen unautorisierten Angreifer ausgespäht, manipuliert oder sogar zerstört werden.*

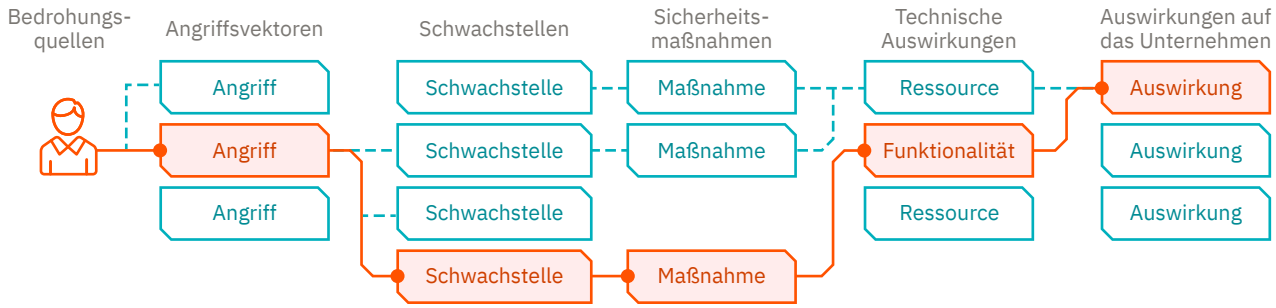
↳ *Buffer-Overflows: Bei einem Pufferüberlauf werden Speicherbereiche überschrieben, da im Programmcode der Speicherbereich für ein bestimmtes Datum zu klein reserviert wurde. Dabei kann es beispielsweise zum Programmabsturz oder Beschädigung der Datenstruktur kommen. Ein Pufferüberlauf entsteht durch Programmierfehler und kann meist nur durch einen Patch des Herstellers für ein entsprechendes Programm behoben werden.*

↳ *Portscans: Mit einem Portscanner kann überprüft werden, welche Dienste ein System über das Internetprotokoll anbietet. Damit kann ein Angreifer offene Ports eines Systems ausspionieren und anschließend darüber das System angreifen.*

↳ *Social Engineering: Bei Angriffen mittels Social Engineering versuchen Angreifer über das Ausspionieren persönlicher Informationen der Opfer z. B. vertrauenswürdige Informationen zu erbeuten oder monetäre Nutzen zu erzielen.*

7 Siehe BSI- Glossar der Cyber-Sicherheit unter: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817272.

Abbildung 5: OWASP Prozessklassifizierung Angriffsvektoren
Quelle: OWASP (2017)



Hierfür werden beispielsweise Identitäten vorgetäuscht, Obrigkeitshörigkeit oder auch Ängste ausgenutzt, um das Opfer dazu zu bringen, die notwendigen Informationen preiszugeben.

↳ *Physischer Zugriff: Ein Angriff mittels physischem Zugriff erfolgt direkt über die physischen Hardware-Schnittstellen eines Systems / Geräts, wie beispielsweise die WiFi-Schnittstelle, Speicherkarten, USB-Schnittstellen. So kann ein Angreifer z. B. Trojaner oder andere Schadsoftware auf einen USB-Stick oder eine Speicherkarte aufspielen, die dann von neugierigen Personen in das System eingesteckt werden, was dann direkt die Schadsoftware in das System einschleust, wie es beispielsweise beim Stuxnet-Angriff passiert ist.*

↳ *Identitätsdiebstahl: Beim Identitätsdiebstahl im digitalen Umfeld werden z. B. Login-Passwort-Kombinationen gestohlen, um diese weiterzuverwenden. Beispielsweise kann der Angreifer bei einem Onlinekaufhaus Waren erwerben, ohne diese zu bezahlen, oder bei einer Onlinebank Überweisungen tätigen. Eine Identität kann beispielsweise bei einem Social Engineering Angriff erbeutet werden.*

↳ *Phishing: Mittels Phishing versucht ein Angreifer über gefälschte Webseiten oder Emails an persönliche Informationen seines Opfers zu gelangen, um diese dann zu missbrauchen und beispielsweise Identitätsdiebstahl zu betreiben.*

↳ *Privilegienmissbrauch: Beim Privilegienmissbrauch kommt der Angreifer aus dem internen Bereich und ist mit mehr Privilegien, auch Rechte genannt, ausgestattet, als notwendig ist. Jeder Benutzer eines Systems oder auch Mitarbeiter in einer Firma sollte nur mit den Rechten ausgestattet werden, die für ihn notwendig sind, seine entsprechenden Tätigkeiten ausführen zu können. Dieses „Prinzip der geringsten Berechtigung“ („least priviledge“) führt zu einer Verringerung der Angriffsfläche.*

Es existieren zahlreiche Klassifikationen und Dokumentationen von Angriffsvektoren. Eine der bekanntesten ist dabei OWASP. Das Open Web Application Security Project ist eine Non-Profit-Organisation, die zum Ziel hat, für mehr Sicherheit in Anwendungen und Diensten des World Wide Webs zu sorgen.[8]

Die OWASP-Community weist auf Sicherheitsrisiken hin und schafft dadurch Transparenz für Endanwender oder Organisationen hinsichtlich

8 Weitere Informationen zu OWASP sind unter https://owasp.org/ zu finden.

Websecurity. Mitglieder sind Unternehmen, Bildungseinrichtungen und Einzelpersonen aus aller Welt. Die Arbeit von OWASP ist in die Bereiche Entwicklungs- und Dokumentationsprojekte unterteilt. Ergebnisse werden in Form von Dokumentationen, Informationsmaterialien, Vorgaben, Empfehlungen und Hilfsmitteln bereitgestellt. Eine bekannte Veröffentlichung ist die jährlich zusammengestellte Top 10 Liste der häufigsten Angriffe und größten Risiken im Bereich Webapplikationen. Die aktuellste Version ist dabei die 2017er Top 10 (OWASP 2017).[9]

In Abbildung 5 ist die OWASP Prozessklassifizierung von Angriffsvektoren dargestellt. Dort ist zu sehen, dass verschiedene Bedrohungsquellen, zumeist Angreifer, über einen Angriffsvektor Schwachstellen ausnutzen. Sind diese nicht durch geeignete Maßnahmen geschützt, hat dies zumeist technische Auswirkungen, die dann bewirken, dass bestimmte Funktionalitäten oder Ressourcen nicht mehr gegeben sind. Dies hat dann wiederum Auswirkungen auf das Unternehmen, so dass bestimmte Geschäftsprozesse geschädigt sind. Eine Schwachstelle ist dabei z. B. eine Lücke in einem Betriebssystem, die durch einen Zero-Day-Exploit[10] ausgenutzt werden kann. Weiterhin kann es aber auch eine Schwachstelle sein, in einem System Sicherheitsmaßnahmen zu nutzen, die nicht dem Stand der Technik entsprechen, wie beispielsweise zu schwache Verschlüsselungsverfahren oder zu kurze Schlüssellängen. Insgesamt besteht eine Asymmetrie zwischen den Angreifern und denen, die das System absichern müssen: Ein Angreifer muss nur eine einzige Schwachstelle finden, die er ausnutzen kann; der Betreiber einer kritischen Infrastruktur muss hingegen einen ganzheitlichen Schutz gewährleisten, um sich in der Regel umfassend absichern zu können. Somit kommt es zu einer Art Wettlauf zwischen den Betreibern und den Angreifern, dem nur mit einem kontinuierlichen Sicherheitsprozess beigekommen werden kann.

9 Weitere aktuelle Informationen sind unter https://owasp.org/www-project-top-ten/ zu finden.

10 Ein Zero-Day-Exploit nennt man einen Angriff, der vor dem Bekanntwerden der entsprechenden Lücke ausgenutzt wird. Die Entwickler haben also keine Zeit („null Tage“, zero day) einen Patch für die entsprechende Lücke bereitzustellen, damit der Angriff keine Wirkung mehr zeigt.

EXKURS

IT SECURITY IN A NUTSHELL – DIE LOW HANGING FRUITS.

Im Rahmen dieses Beitrags wurde aufgezeigt, dass zahlreiche Analysen und etablierte Verfahren unter der Verwendung von Standards und vorhandenen Sicherheitskatalogen ein geeignetes Risikomanagement für kritische Infrastrukturen ermöglichen und eine geeignete Antwort auf die beschriebenen Verfahren sind. Die analysierten Studien zeigen, dass sich die Natur der Angriffe immer mehr ändert und zumeist nicht ein physischer Zugang zu einem Port oder einem System ausgenutzt wird, sondern der Aspekt Social Engineering und Phishing immer mehr im Fokus der Angriffsvektoren steht.

Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um geheime Informationen oder unbezahlte Dienstleistungen zu erlangen. Häufig dient Social Engineering daher dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen; man spricht dann auch von Social Hacking. Dieses Hacking findet zumeist mit dem Vehikel der E-Mail statt. Mittels Phishing versucht man, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben. Ziel des Phishings ist es z. B. an persönliche Daten eines Systemnutzers zu gelangen oder ihn z. B. zur Ausführung einer schädlichen Aktion zu bewegen. In der Folge wird dann beispielsweise Identitätsdiebstahl begangen oder eine Schadsoftware installiert.

Dieses Einfallstor ist mit kulturellen Maßnahmen zu schließen, die darauf abzielen, die Fehlerquelle, in diesem Fall das Versagen des Erkennens eines Angriffs, durch Schulungen von Charakteristika zu verbessern. Die Mitarbeiter müssen erkennen, ob Datendiebe Firmengeheimnisse oder Mitarbeiterdaten abschöpfen wollen. Anfragen per Mail oder Telefon, indem sich Hacker als Mitarbeiter oder Geschäftspartner ausgeben, sollten frühzeitig erkannt und abgewehrt werden. Auch wenn es heutzutage fast üblich ist, sollten persönliche Daten nicht preisgegeben werden, da diese z. B. oftmals als Sicherheitsfragen für das Zurücksetzen von Accountdaten dienen (z. B. erstes Auto, Mädchenname der Mutter, Lieblingsfarbe, etc.). besonders zu COVID-19 Zeiten wird klar, dass BYOD („Bring Your Own Device“) und Home-Office mit ungeschützten Computern ein Problem darstellen kann. Analog trifft dies auf ungesicherte Rechner und Terminals an Airports oder Internetcafés auf Dienstreisen zu. Hier kann es auch zum Verlust eines schlecht gesicherten Rechners oder zum Verlust von sensiblen Daten kommen, weswegen diese stets geeignet aufbewahrt, vernichtet und verortet sein sollten. Der kurzfristige Zugang im Büro zu Rechner oder Handy sollte über Passwort, besser jedoch über biometrische Merkmale gesichert sein und mit kurzen Fristen hierfür versehen sein. Ebenso ist die Passwortpolitik von hoher Bedeutung sowie das Verbot, mittels Admin-Rechten Software aus unbekannten Quellen zu installieren. Nicht nur Endgeräte, sondern auch mobile Datenträger sollten passwortgeschützt oder verschlüsselt sein – wenn sie denn überhaupt erlaubt sind; eigene Geräte sollten grundsätzlich nur mit Erlaubnis in Gebrauch genommen werden. Häufige Wechsel und gute Regeln zur Erstellung neuer Passwörter, die nicht zu umständlich für den Endnutzer sind, aber auch angemessene Komplexität aufweisen, sind essenziell. Hier gibt es zahlreiche Best Practices, die erprobt sind und sich gut umsetzen lassen. Eine Sensibilisierung hierfür könnte über einen dedizierten Tag im Unternehmen zum Thema umgesetzt werden, in dem mittels Live-Hacks oder Postern in Gebäuden, der Kantine oder per Mail auf einzelne Maßnahmen hingewiesen wird. Einzelne Versorger gehen auch den Weg, die Kaffeetassen der Küchen im Gebäude durch passende Tassen mit IT-Hinweisen auszutauschen, oder diese einmal im Jahr an alle Mitarbeiter zu verteilen, die am Aktionstag teilnehmen. Dadurch sind die Hinweise im Alltag stets präsent.

:// 4. METHODIK: IEC 62559 UND MISUSECASE-TEMPLATE

In diesem Abschnitt wird die hier verwendete Methodik, um Gefährdungsszenarien in der Energiedomäne zu analysieren, beschrieben. Dafür werden in den folgenden Abschnitten die verschiedenen Standards, Methoden und Modelle kurz beschrieben und abschließend in → *Abschnitt 4.6* zu einer Gesamtmethodik kombiniert.

Als übergeordnetes Modell wird zunächst in → *Abschnitt 4.1* der VDE 0175-110 beschrieben. Danach wird der Standard IEC 62559, der das Thema Use Case Methodik definiert und ein Use Case Template vorgibt, in Abschnitt 4.2 erläutert. Mit diesem Standard lassen sich Anwendungsfälle systematisch erfassen und dokumentieren, was in dieser Studie anhand eines Beispiels für virtuelle Kraftwerke erfolgt ist. Für die Gefährdungsanalyse wird das Misuse Case Template verwendet, ebenfalls auch zur Erfassung und Dokumentation, dies wird in → *Abschnitt 4.3* beschrieben. Weiterhin sind für eine Gefährdungsanalyse mindestens ein Katalog mit Gefährdungen notwendig, in → *Abschnitt 4.4* wird der Gefährdungskatalog des BSI und in Abschnitt 4.5 ein Katalog mit gängigen Angriffsmustern der CAPEC beschrieben. Abschließend werden in→ *Abschnitt 4.6* die einzelnen Bestandteile zu einer Gesamtmethodik zusammengeführt.

4.1 VDE 0175-110 – Richtlinie zur IT-Sicherheit und Resilienz für die Smart-Energy-Einsatzumgebung

Bei der VDE 0175-110 mit dem Titel „Richtlinien zur IT-Sicherheit und Resilienz für die Smart-Energy-Einsatzumgebung“ handelt es sich um ein übergeordnetes Modell für das Software Engineering in der Energiedomäne. Diese Richtlinie wurde ebenfalls als IEC Technology Report mit dem Titel „Cyber security and resilience guidelines for the smart energy operational environment“ veröffentlicht und hat daher eine internationale Reichweite. Es definiert fünf zentrale Konzepte für IT-Sicherheit und Resilienz für die Domäne „Smart Energy“ und zeigt dazu im Anhang notwendige Standards auf, diese Konzepte umzusetzen. Bei den fünf Konzepten handelt es sich um folgende:

↳ *Resilienz als übergreifende Strategie zur Sicherstellung der Geschäftskontinuität,*

↳ *Security by Design als kosteneffektiver Sicherheitsansatz,*

↳ *Unterschiede zwischen Informationstechnologien („IT“) und Betriebstechnologien („OT“), die zu beachten sind,*

↳ *Risk assessment, also Risikobeurteilung, Risikoverringerung und die kontinuierliche Aktualisierung von Prozessen verbessern die Sicherheit und*

↳ *IT-Sicherheitsnormen und Richtlinien zu bewährten Verfahren für OT-Umgebungen im Energiebereich sollten angewendet werden, um den Risikomanagementprozess zu unterstützen und Sicherheitsprogramme und -richtlinien einzurichten.*

Diese Richtlinie verweist für die Umsetzung von IT-Sicherheit auf verschiedene IT-Sicherheitsstandards, z. B. die ISO / IEC 27000er-Reihe und soll als übergeordnetes Modell für die in diesem Beitrag verwendete und in den folgenden Abschnitten beschriebene Methodik dienen.

4.2 IEC 62559 – Use Case Methodik

Use Cases (dt. Anwendungsfälle) sind Grundbausteine für Anforderungs- und Systemspezifikationen in der Software- und Systementwicklung und Bestandteil der Modellierungssprache UML (Unified Modelling Language). Sie beschreiben die Funktionalitäten und das Verhalten des Projekts aus verschiedenen Blickwinkeln und unter Berücksichtigung unterschiedlicher Aspekte, so dass ein gemeinsames Verständnis aller beteiligten Entwickler- und Benutzerzielgruppen entstehen kann. An der Entwicklung und Umsetzung eines Projekts, beispielsweise im Bereich des Smart Grids, haben unter anderem Vertreter aus Unternehmen der Energiewirtschaft, Gerätehersteller, Elektrotechniker, Informatiker, IT-Sicherheitsbeauftragte und auch Gesetzgeber ihre Anteile und alle diese Nutzergruppen tragen ihre detaillierten Anforderungen an das Projekt heran und ihr eigenes spezielles Expertenwissen mit ein. Um eine Grundlage für das Vereinen dieser verschiedenen Sichtweisen und eine Kommunikationsgrundlage für ein gemeinsames Vorgehen und produktive Zusammenarbeit zu erreichen, werden Use Cases benötigt. Zudem helfen sie bei späteren Analysen des Vorgehens, wie beispielsweise einer Gefährdungs- oder Sicherheitsanalyse für Kommunikation innerhalb des Use Cases oder Gesamtsystems, zum Beispiel hinsichtlich der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit.

Aus dem Standard ISO/IEC 19505-2:2012[11] ins Deutsche übersetzt, ist ein Use Case: Eine Spezifikation einer Menge von Aktionen, die von einem System durchgeführt werden und ein beobachtbares Ergebnis erbringen, das typischerweise für einen oder mehrere Akteure oder Stakeholder des Systems von Wert ist.

Für einen Use Case müssen daher beteiligte Akteure[12] mitsamt ihren Zielen definiert und ihr detailliertes Vorgehen erläutert werden, welches zum Erreichen dieser Ziele oder auch zum Misserfolg führen kann. Diese verschiedenen Ausgänge, des in einem Use Case beschriebenen Vorgehens, werden in mehreren Szenarien mit klar definierten Schritten festgehalten. Jeder dieser Schritte spezifiziert eine Erzeugung, Bearbeitung oder Übertragung von Informationen durch einen oder mehrere Akteure.

Der IEC 62559 ist ein internationaler Standard mit dem Titel „Use Case Methodology“ und befasst sich damit, Vorgaben für die Anwendungsfallerfassung zu machen. Dafür wurde ein Use Case Template entwickelt, das die Anwendungsfallerfassung erleichtern soll. Der Standard besteht aktuell aus vier Teilen:

↳ *Teil 1 beschreibt das Konzept und den Prozess der Anwendungsfallerfassung mit dem Use Case Template (IEC TR 62559-1:2019 ED1 Use case methodology – Part 1: Concept and processes in standardization);*

↳ *Teil 2 definiert das Use Case Template für Anwendungsfälle, inkl. Akteurs- und Anforderungslisten (IEC 62559-2:2015 ED1 Use case methodology – Part 2: Definition of the templates for use cases, actor list and requirements list);*

11 Im Original lautet die Definition von Use Case: “A use case is the specification of a set of actions performed by a system, which yields an observable result that is, typically, of value for one or more actors or other stakeholders of the system.”.

12 Akteure sind Systeme oder Personen, die im Kontext des Use Cases aktiv sind.

↳ *Teil 3 definiert Artefakte für das Use Case Template in XML-Format (IEC 62559-3:2017 Edition 1.0 (2017-12-13) Use case methodology – Part 3: Definition of use case template artefacts into an XML serialized format); und*

↳ *Teil 4 definiert die Prozesse und Best Practices. (IEC SRD 62559-4:2020 Edition 1.0 (2020-03-27) Use case methodology – Part 4: Best practices in use case development for IEC standardization processes and some examples for application outside standardization).*

Der Standard IEC 62559 bietet ein standardisiertes und strukturiertes Verfahren zum Dokumentieren von Anwendungsfällen mit ihren verschiedenen Aspekten. Das dort entwickelte Template hat insgesamt acht Abschnitte, von denen die ersten beiden eine Kurzversion – das sogenannte Basistemplate – bilden. Die Abschnitte umfassen folgende Abschnitte

1. Beschreibung des Anwendungsfalls (Bestandteil Basistemplate)
2. Diagramme des Anwendungsfalls (Bestandteil Basistemplate)
3. Technische Einzelheiten
4. Schrittweise Analyse des Anwendungsfalls
5. Ausgetauschte Informationen
6. Anforderungen (optional)
7. Allgemeine Begriffe und Definitionen
8. Benutzerdefinierte Informationen (optional)

mit verschiedenen Unterabschnitten. Das Basistemplate der ersten zwei Abschnitte liefert eine kurze, wenig technische Übersicht über die grundlegenden Züge des Anwendungsfalls mit der Angabe von sogenannten Key Perfomance Indikatoren (KPI). Die folgenden Abschnitte beschäftigen sich mit den verschiedenen informationstechnischen Blickwinkeln und der Ausprägung der Einzelheiten. Ein vollständig ausgefülltes Template sollte einen ganzheitlichen Überblick über den Anwendungsfall, die beteiligten Akteure, ausgetauschten Informationen und technischen Ablauf geben. Die Granularität der Einträge muss je nach benötigtem Detailgrad im Voraus festgelegt werden.

Die grundlegenden Eckpunkte und Anforderungen für einen Anwendungsfall werden in der Regel von Experten und potenziellen Nutzern mit sehr differenziertem Hintergrundwissen herausgearbeitet. Es werden unterschiedliche Aspekte von den Entwicklern zu einer umfassenden standardisierten Darstellung des Anwendungsfalls zusammengefasst, um ein gemeinsames Verständnis und eine Diskussionsgrundlage zu ermöglichen. Im Laufe der Bearbeitung entsteht damit, aus groben Ideen und Geschäftszielen über das Definieren von Ablaufszenarien bis hin zu technischen Implementierungsdetails, eine Spezifikation des Anwendungsfalls in standardisierter Form.

Ein Beispiel für ein ausgefülltes Use Case Templates kann im Anhang in → *Abschnitt 7.1* eingesehen werden.

4.3 Misuse Case Template

Das Misuse Case (MUC) Template baut auf dem Use Case Template nach IEC 62559 auf, befasst sich aber mit missbräuchlichem Verhalten in dem entsprechenden Anwendungsfall. Dieser Abschnitt gibt einen Überblick über die Misuse Case (MUC) Methode, die das MUC Template verwendet und beschreibt zunächst die Motivation und Entstehung des MUC Templates. Das MUC Template beruht auf verschiedenen bestehenden Ansätzen zu diesem Themenfeld, die zusammengefügt wurden. Verwendet wird das MUC-Template

für einen bestimmten Anwendungsfall, an dem die Sicherheitsanalyse von Bedrohungen, die von Stakeholdern identifiziert wurden, durchgeführt werden soll.

Das Konzept der Misuse Cases sollte an dem Punkt nach der Anwendungsfallerfassung ansetzen, wobei nicht nur die gewünschte, sondern auch die unerwünschten Funktionalitäten im Mittelpunkt steht. Misuse Cases beschreiben anomales Verhalten und damit Systembedrohungen – im Vergleich zu den Anwendungsfällen, die die Funktionalität des Systems beschreiben. Es werden negative Szenarien modelliert, in denen z. B. unabsichtliches Verhalten, Unfälle oder Angriffe auf das System zu einer Sicherheitsverletzung führen könnten (Kure et al. 2018). Mit der MUC Methode werden solche Szenarien in grafischer Form dargestellt. Es ist auch hilfreich, sich in die Lage der Angreifer zu versetzen. Durch Analysieren und Erfassen aller möglichen Wege, die zu einem Systemausfall oder einem unerwarteten Fehler führen können, können die Entwickler das Systemdesign ändern, um die Auswirkungen des Ausfalls abzuschwächen (Peterson und Steven 2006). Das Template wird auch für die Analyse verwendet, welche Maßnahmen zur Vermeidung ergriffen werden sollten, um diese unerwünschte Funktionalität zu unterbinden. Für die Entwicklung der MUC Methode und des Templates wird hauptsächlich die Arbeit von Sindre und Opdahl (2005) betrachtet, die das Konzept der Misuse Cases für die Sicherheitsanalyse entwickelt haben. Weiterhin wird die Definition von Jacobson verwendet (Jacobson et al. 1995), der die Misuse Cases als eine Reihe von Interaktionen zwischen einem oder mehreren Akteuren definiert hat. Dabei definiert eine dieser Interaktionen ein Systemverhalten, das das gewünschte Ergebnis des Akteurs erreichen soll. Sindre und Opdahl erweitern diese Definition und definieren einen Misuse Case in der gleichen Weise, wie eine Funktion, die das System NICHT umsetzen soll. Das sollte es auch ermöglichen, den Mis-Akteur (analog zum Akteur) als eine Person oder ein System zu definieren, das – absichtlich oder unabsichtlich – einen Misuse Case hat, den das System nicht unterstützt.

Darüber hinaus wurde das IEC 62559-Template erweitert, um Misuse Cases erfassen zu können. Damit können nun zusätzliche Informationen zu gewonnen werden, was ein wichtiger Aspekt beim Systementwurf ist. Fehler im Prozess, z. B. bei einem Rollout eines bestimmten Dienstes im Smart Grid – mit harmlosen oder bösartigen Ursachen – können sowohl zu operationalen als auch physischen Konsequenzen führen. Um die Ursache eines (un-)beabsichtigten Missbrauchs herauszufinden, wurde im Misuse Case Template eine objektorientierte Modellierungstechnik (OOM) auf der Grundlage der Unified Modeling Language (UML) verwendet, gerade auch, um die Fehlerfolgen und ihre Ursachen zu analysieren, die auf dem tatsächlichen Modell basiert.

Mit der MUC Methode ist es nun möglich, brauchbare Sicherheitsanforderungen zu ermitteln, um sicherere Systeme zu bauen, indem man die Informationen aus MUC-Template zur Sicherheitsanalyse verwendet, um Sicherheitsrisiken zu mindern. Insgesamt geht es darum – als Bestandteil der Risikoanalyse – Bedrohungen zu modellieren und damit zu klären WAS soll VOR WEM und WIE LANGE geschützt werden.

Das Misuse Case Template (MUC-Template) beruht auf dem UC-Template aus dem IEC 62559 und besteht aus den folgenden Abschnitten:

1. Beschreibung des Misuse Cases (MUC): Der erste Abschnitt des MUC-Templates ist im Großen und Ganzen gleich, wie das UC-Template. Nur KPIs finden im MUC-Template keine Anwendung.

2. Diagramme des MUC: Auch dieser Abschnitt ist bei UC- und MUC-Template gleich gestaltet. Es macht hier evtl. Sinn andere Diagrammformen

zur Unterstützung der Analyse der Angriffsszenarien zu wählen. Das Zusammenspiel zwischen Use Cases und Misuse Cases, Actors und Misactors beispielsweise als UML Diagramm kann gut graphisch dargestellt werden. Dabei sollte auf die graphische Unterscheidung zwischen bösartigen und üblichen Komponenten geachtet werden.

3. Technische Details: Hier wird zu den regulären Akteuren eine Tabelle zu den Mis-Akteuren hinzugefügt. Der weitere Abschnitt zu „Referenzen“ bleibt wie im UC-Template bestehen

4. Schritt für Schritt Analyse des MUC: In diesem Abschnitt ist der Unterschied der beiden Templates am größten. Um zwischen absichtlichen und unabsichtlichen Situationen zu unterscheiden, werden hier zwei unterschiedliche Tabellen, zum einen für Fehlerszenarien und zum anderen für Angriffsszenarien, angeboten.

   Der → *Abschnitt 5* zu „ausgetauschte Informationen“ aus dem UC-Template findet im MUC-Template keine Anwendung, da es keinen absichtlichen Austausch von Informationen in diesen Szenarien gibt. Daher wird dieser → *Abschnitt 5* aus dem UC-Template ausgelassen.

   Aus diesem Grund hat die Tabelle zu den Szenarioschritten auch keine Spalten zu den Informationsobjekten, sowie zu Sendern und Empfängern, stattdessen aber ein Feld für die Dokumentation der Angriffe. Weiterhin können als präventive Maßnahme „Capture Points“ in einer zusätzlichen Tabelle eingesetzt werden.

   Die drei letzten Abschnitte sind wiederum identisch mit denen des UC-Templates und werden nur entsprechend ihrer Nummerierung angepasst. Daher bedürfen sie hier keiner weiteren Erläuterung.

5. Anforderungen

6. Allgemeine Begriffe und Definitionen

7. Benutzerdefinierte Informationen (optional)

Für die Zukunft ist es geplant ein gemeinsames Template für Use und Misuse Cases zu entwerfen, um direkt Angriffsszenarien und Fehlerfälle bei der Systementwicklung berücksichtigen zu können.

Das MUC-Template wird im Anhang in → *Kapitel 7.2* auf den in → *Kapitel 7.1* beschriebenen Anwendungsfall angewendet, was zum besseren Verständnis des MUC-Templates beitragen soll.

4.4 Gefährdungskatalog nach BSI-Grundschutz

Um innerhalb der Risikoanalyse eine Gefährdungs- oder Bedrohungsanalyse durchführen zu können, wird (mindestens) ein Katalog benötigt, der entsprechende Gefährdungen und Bedrohungen auflistet und beschreibt. In diesem Beitrag wird aufgrund des deutschen Kontextes der Gefährdungskatalog für Elementare Gefährdungen nach BSI-Grundschutz verwendet.

Die im Folgenden aufgelisteten und beschriebenen elementaren Gefährdungen, werden in den in dieser Studie untersuchten Gefährdungsszenarien verwendet. Alle elementaren Gefährdungen nach BSI-Grundschutz sind im Anhang in → *Abschnitt 7.1* aufgelistet, genauere Erklärungen zu den einzelnen Gefährdungen, siehe (BSI 2020):

↳ *G 0.14 Ausspähen von Informationen (Spionage): „Mit Spionage werden Angriffe bezeichnet, die das Ziel haben, Informationen über Unternehmen, Personen, Produkte oder andere Zielobjekte zu sammeln, auszuwerten und aufzubereiten. Die aufbereiteten Informationen können dann beispielsweise eingesetzt werden, um einem anderem Unternehmen bestimmte Wettbewerbsvorteile zu verschaffen,*

Personen zu erpressen oder ein Produkt nachbauen zu können.

Neben einer Vielzahl technisch komplexer Angriffe gibt es oft auch viel einfachere Methoden, um an wertvolle Informationen zu kommen, beispielsweise indem Informationen aus mehreren öffentlich zugänglichen Quellen zusammengeführt werden, die einzeln unverfänglich aussehen, aber in anderen Zusammenhängen kompromittierend sein können. Da vertrauliche Daten häufig nicht ausreichend geschützt werden, können diese oft auf optischem, akustischem oder elektronischem Weg ausgespäht werden."[13]

↳ *G 0.22 Manipulation von Informationen: „Informationen können auf vielfältige Weise manipuliert werden, z. B. durch fehlerhaftes oder vorsätzlich falsches Erfassen von Daten, inhaltliche Änderung von Datenbank-Feldern oder von Schriftverkehr. Grundsätzlich betrifft dies nicht nur digitale Informationen, sondern beispielsweise auch Dokumente in Papierform. Ein Täter kann allerdings nur die Informationen manipulieren, auf die er Zugriff hat. Je mehr Zugriffsrechte eine Person auf Dateien und Verzeichnisse von IT-Systemen besitzt bzw. je mehr Zugriffsmöglichkeiten auf Informationen sie hat, desto schwerwiegendere Manipulationen kann sie vornehmen. Falls die Manipulationen nicht frühzeitig erkannt werden, kann der reibungslose Ablauf von Geschäftsprozessen und Fachaufgaben dadurch empfindlich gestört werden.*

Archivierte Dokumente stellen meist schützenswerte Informationen dar. Die Manipulation solcher Dokumente ist besonders schwerwiegend, da sie unter Umständen erst nach Jahren bemerkt wird und eine Überprüfundann oft nicht mehr möglich ist."[14]

↳ *G 0.40 Verhinderung von Diensten (Denial of Service): „Es gibt eine Vielzahl verschiedener Angriffsformen, die darauf abzielen, die vorgesehene Nutzung bestimmter Dienstleistungen, Funktionen oder Geräte zu verhindern. Der Oberbegriff für solche Angriffe ist „Verhinderung von Diensten" (englisch: „Denial of Service"). Häufig wird auch die Bezeichnung „DoS-Angriff" verwendet.*

Solche Angriffe können unter anderem von verärgerten Mitarbeitern oder Kunden, aber auch von Mitbewerbern, Erpressern oder politisch motivierten Tätern ausgehen. Das Ziel der Angriffe können geschäftsrelevante Werte aller Art sein. Typische Ausprägungen von DoS-Angriffen sind

- *Störungen von Geschäftsprozessen, z. B. durch Überflutung der Auftragsannahme mit fehlerhaften Bestellungen,*
- *Beeinträchtigungen der Infrastruktur, z. B. durch Blockieren der Türen der Institution,*
- *Herbeiführen von IT-Ausfällen, indem z. B. Dienste eines Servers im Netz gezielt überlastet werden.*

Diese Art von Angriffen steht häufig im Zusammenhang mit verteilten Ressourcen, indem ein Angreifer diese Ressourcen so stark in Anspruch nimmt, dass sie den eigentlichen Nutzern nicht mehr zur Verfügung stehen. Bei IT-basierten Angriffen können z. B. die folgenden Ressourcen künstlich verknappt

13 Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrdungen/G_0_14_Aussp%C3%A4hen_von_Informationen__(Spionage).html.

14 Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrdungen/G_0_22_Manipulation_von_Informationen.html.

werden: Prozesse, CPU-Zeit, Arbeitsspeicher, Plattenplatz, Übertragungskapazität.“[15]

Anhand dieser Auswahl wurden für die Analyse Szenarien erarbeitet, die einige Gefährdungen beispielhaft untersucht haben.

Weiterhin können für Angriffe auf Webapplikationen die Gefährdungen nach OWASP oder für eine übergeordnete Betrachtung der Sicherheitsstandard IEC 62351-1[16], der sich mit „Daten- und Kommunikationssicherheit“ in der Energiedomäne befasst und einen guten Überblick zu Bedrohungen auf Basis der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit gibt, herangezogen werden.

4.5 Attack Pattern Classification, Recommendations and Attack Conditions nach CAPEC

Das Projekt Common Attack Pattern Enumeration and Classification (CAPEC) bietet einen öffentlich zugänglichen Katalog mit gängigen Angriffsmustern, der den Anwendern hilft zu verstehen, wie die Angreifer Schwächen in Anwendungen und anderen cybergestützten Fähigkeiten ausnutzen.

„Angriffsmuster“ sind Beschreibungen der gemeinsamen Attribute und Ansätze, die von Angreifern zur Ausnutzung bekannter Schwachstellen in cybergestützten Einsatzfeldern verwendet werden. Angriffsmuster definieren außerdem die Herausforderungen, denen ein Angreifer gegenüberstehen kann, und welche Wege er nutzt diese Herausforderungen zu lösen. Angriffsmuster leiten sich aus dem Konzept von Entwurfsmustern ab, die eher in einem konstruktiven als in einem destruktiven Kontext, wie bei Angriffsmustern, angewendet werden. Weiterhin wurden sie mit einer tiefgehenden Analyse zusammen mit spezifischen realitätsnahen Beispielen generiert.

Jedes Angriffsmuster beinhaltet das Wissen darüber, wie bestimmte Teile eines Angriffs entworfen und ausgeführt wurden, und gibt Hinweise darauf, wie die Effektivität des Angriffs verringert werden kann. Die Angriffsmuster helfen denjenigen, die Anwendungen entwickeln oder cybergestützte Einsatzfelder verwalten, die spezifischen Elemente eines Angriffs besser zu verstehen und zu erkennen und außerdem den Erfolg des Angriffs zu verhindern.[17] Für eine bessere Übersicht und Sortierung wurden die Angriffe in verschiedene Kategorien sortiert: zum einen die „Domänen des Angriffs“ (domains of attack[18]), die u.a. die Kategorien „Software“, „Hardware“ und „Kommunikation“ umfasst, und zum anderen die „Mechanismen des Angriffs“ (mechanism of attack[19]), die zum Beispiel die Kategorien „Missbrauch von Funktionalitäten“, „Manipulation von Datenstrukturen“ oder „Informationen sammeln und analysieren“ umfasst.

Die in dieser Studie verwendeten Angriffsvektoren aus dem CAPEC-Katalog sind im Anhang in → *Abschnitt 7.5* aufgelistet.

4.6 Gesamtmethodik

Dieser Abschnitt fasst die hier vorher beschriebenen Bestandteile in einer Gesamtmethodik zusammen. Diese Gesamtmethodik ist in → *Abbildung 6* schrittweise dargestellt und wird anhand

15 Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrdungen/G_0_40_Verhinderung_von_Diensten_(Denial_of_Service).html.

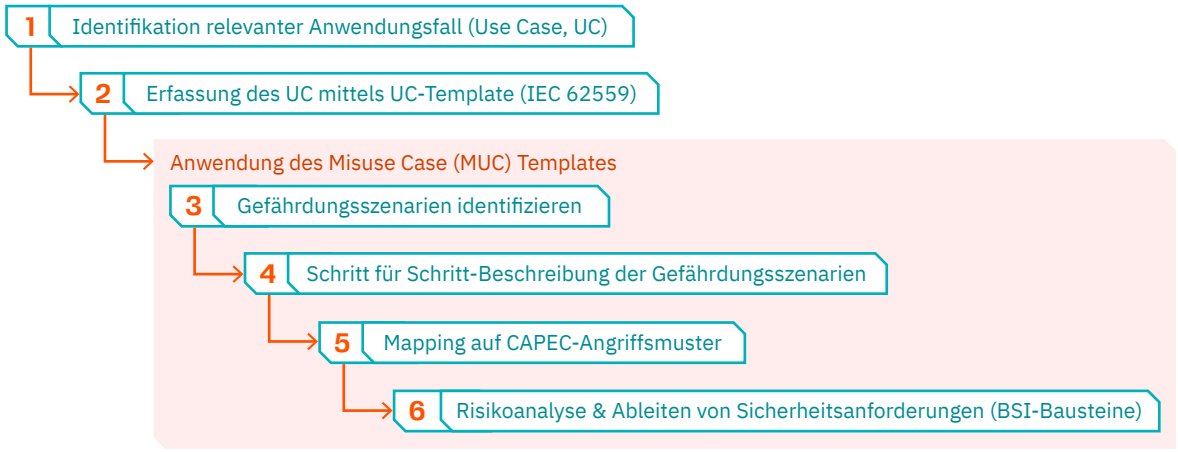
16 Der Titel des Sicherheitsstandards IEC TS 62351-1 lautet “Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues”.

17 Siehe auch https://capec.mitre.org/about/.

18 Die CAPEC „Domänen des Angriffs“ sind unter https://capec.mitre.org/data/definitions/3000.html aufgeführt.

19 Die CAPEC „Mechanismen des Angriffs“ sind unter https://capec.mitre.org/data/definitions/1000.html aufgeführt.

Abbildung 6: Schritte der Gesamtmethodik
Quelle: eigene Darstellung



dieser Abbildung in den folgenden Abschnitten beschrieben.

Zu Beginn des Projekts wurde zunächst ein relevanter Anwendungsfall identifiziert, siehe Schritt (1) in Abbildung 6, und mit dem UC-Template nach IEC 62559 systematisch erfasst, siehe Schritt (2) Abbildung 6. Durch die standardisierte Vorgehensweise unterstützen der Standard und sein Template allgemein Systementwicklungsprozesse. Im Rahmen der Analysen der Use Cases werden einzelne User Stories[20] weiter verdichtet und strukturiert aufbereitet. Diese Anwendungsfälle werden in einer formalisierten Art und Weise mit den IEC 62559-Anwendungsfalltemplates dokumentiert und zur Verfügung gestellt. Das Template ermöglicht es dabei vor allem, durch die kontrollierte Struktur und die vorgeschriebenen Informationen eine Wiederverwendung des Wissens in einem anderen Projektkontext zu gewährleisten. Ziel und Zweck des Templates ist jedoch die Dokumentation von Funktionalität, die einen Geschäftszweck verfolgt. Jedes Verhalten in einem Prozess bzw. die Funktionen eines Systems werden durch Aktionen Dritter ausgelöst. Das System zeigt auf einen gegebenen Input als Output ein beobachtbares Verhalten, welches ausgewertet werden kann. Angreifer versuchen ebenso wie Prozessverantwortliche, ein System zu einem Verhalten zu bringen. Das Fehlverhalten des Systems ist beobachtbar und somit auch der Erfolg eines Angreifers.

Daraus ergibt sich, dass sich auch ein Misuse eines Systems oder auch der Angriff auf ein System mit einem ähnlichen Template wie für einen Use Case abbilden lässt. Dadurch lassen sich Informationen über Angriffe und Motivationen von Angreifern als Auslöser in ähnlicher Form wie die bekannten Use Cases dokumentieren. Diese sind somit zugänglicher für die Fachexperten als ohne entsprechendes Template.

Bei der Anwendung des MUC-Templates werden zuerst Gefährdungsszenarien identifiziert und diese Gefährdungsszenarien dann systematisch mit dem Template erfasst, siehe Schritt (3) in Abbildung 6. Danach erfolgt die Schritt-für-Schritt-Beschreibung der Gefährdungsszenarien, ebenfalls im MUC-Template, siehe Schritt (4) in Abbildung 6. Um die Gefährdungsszenarien dann einzuordnen und zu systematisieren, werden

20 User Stories sind sehr kurz formulierte Softwareanforderungen, die in der agilen Softwareentwicklung verwendet werden.

diese dann Mustern in einem Gefährdungskatalog zugeordnet. In dieser Studie wurde dafür der CAPEC-Katalog und die BSI-Katalog zu elementaren Gefährdungen ausgewählt und daher die drei Gefährdungsszenarien passenden Angriffsmustern zugeordnet, siehe Schritt (5) in → *Abbildung 6*. Im abschließenden Schritt (6) in Abbildung 6 wird eine Risikoanalyse für die Angriffsszenarien durchgeführt und notwendige Sicherheitsanforderungen für die Vermeidung der entsprechenden Szenarien abgeleitet. Für die Auswahl der Sicherheitsanforderungen können wieder verschiedene Kataloge, wie beispielsweise die BSI-IT-Grundschutz-Bausteine oder der NISTIR 7628 verwendet werden. Abschließend kann im Misuse Case-Template bei Bedarf mittels so genannter „Stopp-Punkte“ (Capture Points) der entsprechende Angriff an bestimmten Punkten des Prozesses unterbrochen werden.

Insgesamt dient und unterstützt das UC-Template die allgemeine Systementwicklung und das MUC-Template wird für die Gefährdungsanalyse verwendet.

EXKURS

ENTSTEHUNGSGESCHICHTE DES UC-TEMPLATES

Das sogenannte IntelliGrid-Template zur Anforderungsanalyse für Smart Grid-Projekte war der erste strukturierte Versuch, domänenspezifische funktionale und nicht-funktionale Wege zu entwickeln, um Anforderungen für einen Anwendungsfall systematisch und einheitlich zu strukturieren.

Bereits in der Normungsstudie für die E-Energy-Projekte im Jahr 2009 wurde darauf hingewiesen, dass die Interoperabilität nicht nur technische Standards, sondern auch Verfahrensstandards erfordert. Die Arbeitsgruppe „sustainable processes“ (nachhaltige Prozesse) hat im Rahmen des M / 490 EU-Mandats eine geeignete Plattform auf europäischer Ebene geschaffen, um die von der deutschen DKE bereits geförderte Use-Case-Semantik auf europäischer Ebene weiter zu vereinheitlichen. Die Arbeiten aus dem Mandat führten zusammen mit Arbeiten aus dem sogenannten „Use Case Management Repository“ (UCMR) zu einer internationalen Standardisierung sowohl des funktionalen Templates als auch der Serialisierung. Daraus entwickelte sich in Zusammenarbeit mit dem Technische Komitee TC 8 der IEC (International Electrotechnical Commission) der Standard „IEC 62559 – Use case methodology“. Die Integration von Misuse Cases in das Use Case Template, zur Förderung der Analyse von Sicherheitsanforderungen, wurde daraufhin begonnen.

Zur Modellierung des Anwendungsfalls im IEC 62559 wird UML (unified modeling language) aus dem Bereich der Informatik als Modellierungssprache verwendet. UML umfasst verschiedene Arten von Diagrammen. Eines, das so genannte Anwendungsfalldiagramm, ermöglicht es auch Akteure aus anderen Disziplinen einzubeziehen, um den Systemkontext und die als Anwendungsfall zu definierende Funktionalität zu visualisieren. Durch die Zuordnung der Akteure zu den Anwendungsfällen ist es möglich, den unterschiedlichen Interessen der am System beteiligten Akteure gerecht zu werden und die Kommunikation mit den späteren Nutzern in der Spezifikationsphase zu erleichtern. Die Anwendungsfälle umfassen in erster Linie die funktionalen Anforderungen, also gewünschte Funktionalitäten, auf System- und Funktionsebene, aber auch spezielle Verweise auf nicht-funktionale Anforderungen, welche die Qualität der gewünschten Funktionalitäten beschreiben. Durch die Verwendung des Use Case Templates aus dem IEC 62559 können Benutzer von Textverarbeitungsprogrammen, wie Microsoft Word, ihre Daten austauschen. Dies vereinfacht die technische Zusammenarbeit der Anforderungsgeber nicht nur in Smart Grid-Projekten und der Standardisierung.

Parallel zu den Arbeiten der Gruppe „sustainable processes“ wurde in der Gruppe „Referenzarchitektur“ das Smart Grid-Architekturmodell (SGAM) erarbeitet. Zusammen mit der Use Case Methodik hilft das SGAM bei der strukturierten Dokumentation, zum einen bei Geschäftsprozessabläufen und zum anderen bei der Entwicklung zugehöriger Architekturen mit deren statischen Komponenten und deren Datenmodellen. Allerdings konzentriert sich diese Art der Modellierung in erster Linie auf die Funktionalitäten, während nicht-funktionale Anforderungen möglicherweise nicht ausreichend erfasst werden. Studien, wie beispielsweise (Buschermöhle et al. 2006), motivieren, dass durch die Anwendung dieser Anforderungen Probleme mit den vom Kunden gelieferten Systemen entstehen, weil die nicht-funktionalen Anforderungen im Entwicklungsprozess nicht ausreichend berücksichtigt werden.

:// 5. ANWENDUNG DER GESAMTMETHODIK

Die für diese Studie entwickelte Gesamtmethodik, die im vorherigen → *Abschnitt 4.6* beschrieben wurde, wird nun in diesem Kapitel angewendet. Dafür wird zunächst in → *Abschnitt 5.1* der identifizierte Anwendungsfall, der mittels UC-Template erfasst wurde, textuell vorgestellt und danach in → *Abschnitt 5.2* die analysierten Gefährdungsszenarien, die mit dem MUC-Template erfasst wurden, erläutert.

5.1 Beschreibung des Anwendungsfalls

Der untersuchte Anwendungsfall, auch Use Case (UC) genannt, fokussiert die Netzüberlast in einem Verteilnetz, infolgedessen die Einspeiseleistung reduziert werden muss, hier durch ein Virtuelles Kraftwerk (VK). Der UC basiert darauf, dass durch Sensoren eine Überlastsituation in einem entsprechenden Netzbereich festgestellt wurde, so dass das dazugehörige virtuelle Kraftwerk in Teilen seine Erzeugung reduzieren muss. Die einzelnen Schritte des Anwendungsfalls, die ebenfalls in Abbildung 7 dargestellt sind, werden im Folgenden genauer erläutert:

1. Netzsensoren geben Netzinformationen zurück, indem sie physikalische Phänomene im Netz messen. Solche Netzsensoren haben in einem entsprechenden Netzbereich eine Überlastsituation festgestellt und senden Informationen zu dieser Überlastsituation an das MV / LV SCADA-System, damit letztendlich die Überlastsituation durch die Abregelung von Lasten aufgelöst wird, in diesem Fall von einem virtuellen Kraftwerk (VK). SCADA steht dabei für Supervisory Control And Data Acquisition, also eine übergeordnete Steuerung und Datenerfassung. In diesem Fall handelt es sich um ein SCADA-System für die Mittel- und Niederspannung bzw. für die Betreiber der Mittel- und Niederspannung.

2. Das MV / LV SCADA-System informiert nun das Distribution Management System (DMS, ein Managementsystem für den Betrieb des Verteilnetzes) über die Überlastsituation und löst einen Alarm aus. Beim DMS handelt es sich um ein IT-System für Versorger, das in der Lage ist, Informationen über das Stromverteilungssystem in Echtzeit oder nahezu in Echtzeit zu verwalten, zu steuern, zu visualisieren, zu optimieren und zu automatisieren. Das DMS kann den Betreibern auch ermöglichen, komplexe Dienste für das Verteilnetz zu planen und auszuführen, um die Systemeffizienz zu erhöhen, den Leistungsfluss zu optimieren und Überlastungen zu verhindern.

3. Das DMS stellt nun eine Reduktionsanfrage an das DER-SCADA-System, damit die Energieversorgung gestoppt wird. DER-SCADA-Systeme (DER = Dezentrale Energieressource) sind Überwachungs- und Steuerungssysteme für Erzeuger von dezentralen Energieressourcen auf der Mittelspannungsebene, dies können beispielsweise auch Virtuelle Kraftwerke sein.

4. Das DER-SCADA-System informiert das Energiemanagementsystem (EMS) über den Versorgungsstopp und übersendet entsprechende Abschaltinformationen. Ein EMS dient den

Stromnetzbetreibern zur Überwachung, Steuerung und Optimierung der Leistung bei der Erzeugung und / oder der Übertragung im Stromnetz.

5. Das EMS muss nun einen neuen Versorgungszeitplan berechnen.

6. Dieser Versorgungszeitplan wird dann entsprechend an das Energiedatenmanagementsystem (EDMS) weitergeleitet. Das EDMS ist dabei ein System, das Energiedaten (z. B. Daten des EMS) speichert und entsprechend autorisierten Systemen zur Verfügung stellt.

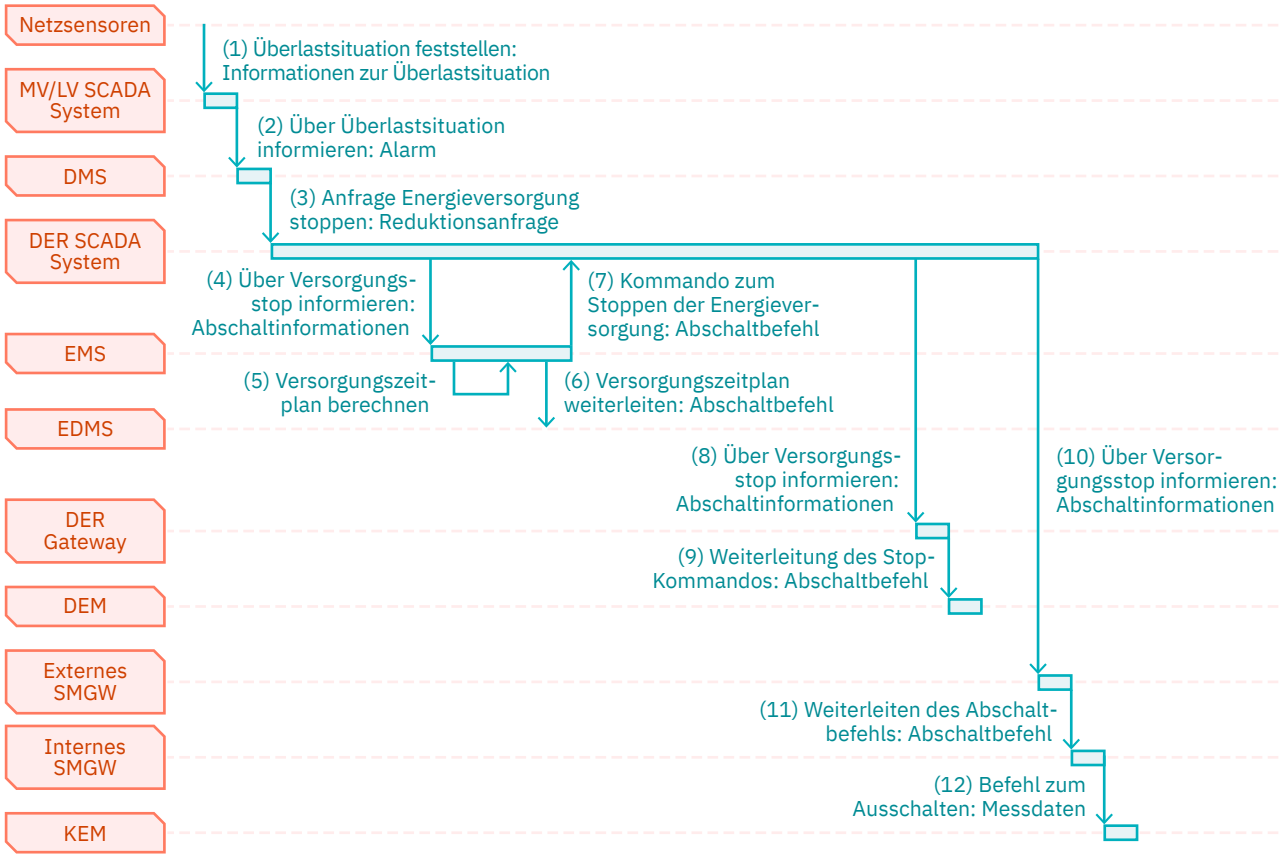
7. Wenn der neue Versorgungszeitplan berechnet und akzeptiert ist, wird vom EMS das Kommando zum Stoppen der Energieversorgung für das entsprechende VK an das DER-SCADA-System inkl. Abschaltbefehl gegeben.

8. Das DER-SCADA-System gibt nun den Abschaltbefehl an das DER-Gateway weiter. Das DER-Gateway fungiert dabei als Kommunikationsgateway zwischen dem Energiemanagementsystem und dem DER-SCADA-System.

9. Das Stopp-Kommando inkl. Abschaltbefehl wird dann an das Device Energy Management (DEM) weitergeleitet, das dann das komplette VK oder einzelne Lasten des VKs abregelt. Das DEM steuert also die DER-Geräte, um zu gewährleisten, dass die geforderte Produktion eingehalten wird.

10. Zusätzlich wird, um Systeme im Umfeld der entsprechenden DERs, die das Smart Metering

Abbildung 7: Sequenzdiagramm des Anwendungsfalls
Quelle: eigene Darstellung



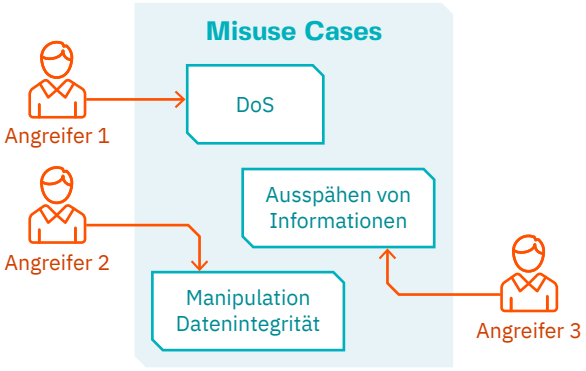
und Smart Home managen, zu informieren, vom DER-SCADA-System zunächst das externe Smart Meter Gateway (SMGW), dann das interne SMGW (11) und letztendlich das Kundenenergiemanagement (KEM) über den Versorgungsstopp informiert (12) und dabei die entsprechenden Abschaltinformationen und relevante Messwerte mitgesendet. Dabei erfüllt das externe Smart Metering Gateway die Kommunikationsfunktionen zwischen dem Smart Grid-Bereich und dem Smart Metering. Das interne Smart Metering Gateway erfüllt Kommunikationsfunktionen zwischen dem Smart Metering und dem Smart Home. Das KEM schließlich erfüllt Funktionen, die es ermöglichen, koordinierte Energiemanagementstrategien für eine oder mehrere zusammengehörige DEM in Abhängigkeit von Messdaten, Preisanreizen, Flexibilitätsanforderungen und zusätzlichen Informationen aus anderen Kanälen wie dem Internet zu definieren.

Die Beschreibung zielt darauf ab, den Prozess, sowie die ausgetauschten Nachrichten zu der durch den Alarm ausgelösten Leistungsreduktion inkl. der Quittierung und die Informationsweitergabe der aktuellen Netzsituation an die Systeme Dritter für die Implementierung zu dokumentieren. Die Dokumentation erfolgte in einem IEC 62559-2 konformen Template. Das mit diesem Anwendungsfall ausgefüllte Template ist im Anhang in → *Abschnitt 7.1* dargestellt.

5.2 Beschreibung des Misuse Cases

→ *Abschnitt 5.1* hat anhand des Anwendungsfalls mögliche Kommunikation und ausgetauschte Daten aufgezeigt. Der Anwendungsfall dokumentiert ein gewolltes Verhalten, bei dem Vertrauen in die ausgetauschten Daten besteht und lediglich technische Fehler betrachtet werden, falls diese eine mangelnde Qualität oder fehlende Antwortzeiten haben. Hier steht ein gewolltes Verhalten im Fokus. Ein Angreifer hingegen möchte ein System zu einem

Abbildung 8: Darstellung der Misuse Cases in einem Misuse Case Diagramm
Quelle: eigene Darstellung



nicht-gewollten Verhalten veranlassen und führt hierzu Angriffe auf das System durch. Solche Angriffe können in einem Misuse Case (MUC) Template dokumentiert werden. Das Misuse Case Template basiert auf einem erweiterten IEC 62559-2 Template und dokumentiert diesen Kontext eines ungewollten Verhaltens näher.

In dieser Studie wurden drei verschiedene Angriffsszenarien entwickelt, die je eines der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit angreifen. Diese sogenannten Misuse Cases sind in Abbildung 8 in einem Anwendungsfalldiagramm abgebildet. Die Akteure der Angreifer sind dabei in orange dargestellt und die Misuse-Cases in blau. Die Angriffe werden im Folgenden auf der Basis des in → *Abschnitt 5.1* erläuterten Anwendungsfalls zum virtuellen Kraftwerk beschrieben und sind nochmals als rote Blitze im Sequenzdiagramm in → *Abbildung 9* gezeigt.

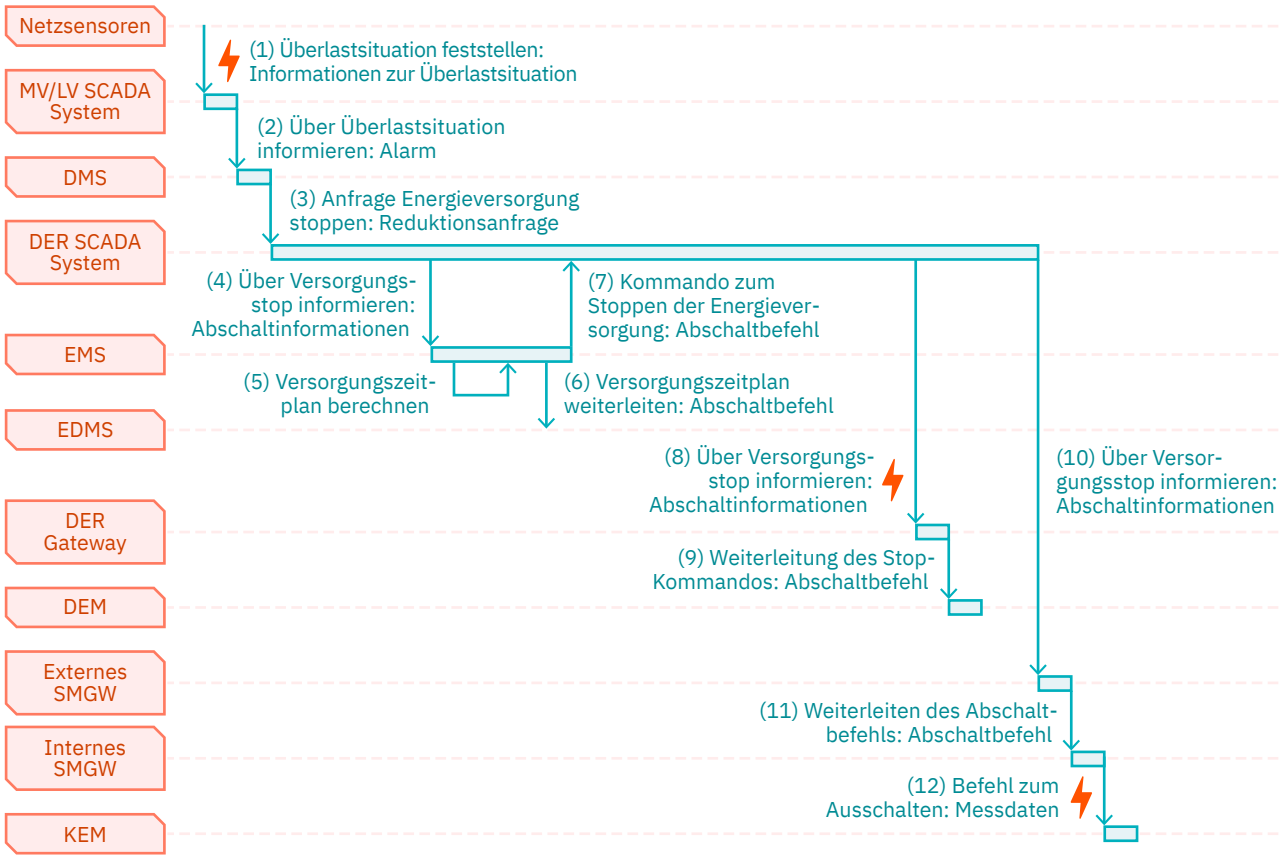
5.2.1 Beschreibung im MUC-Template

Das erste Szenario dokumentiert einen Angriff auf die Verfügbarkeit des MV / LV SCADA-Systems mittels Denial of Service-Angriff (DoS) und hat Einfluss auf Schritt (2) des Anwendungsfalls (siehe → *Abbildung 9*), so dass die Steuerung in der Mittel- / Niederspannungsebene gestört wird. Der Angreifer ist ein externer Hacker und Hackerkompetenz ist vorhanden, um den DoS-Angriff durchzuführen. Motivation

für diesen Angriff kann eine Konkurrenzsituation oder Vandalismus sein oder der Angreifer als Cyber-Hacker sucht Anerkennung oder eine Herausforderung oder hat auch einfach Spaß an der Technik. Für den Angriff spioniert der Angreifer das MV / LV SCADA-System aus, indem er einen Sniffing-Angriff durchführt. Dabei hört er beim Zielsystem den Netzwerkverkehr mit, um eine Schwachstelle zu identifizieren. Da das MV / LV SCADA-System den typischen Datenverkehr nicht überwacht, kann der Angreifer diese gefundene Schwachstelle für den DoS-Angriff nutzen, beispielsweise mittels Flooding, um eine Ressourcenüberlastung zu erwirken.
Er führt einen Flooding-Angriff durch, indem er das Zielsystem mit einer großen Zahl an Interaktionen flutet, so dass das Zielsystem seine eigentliche Aufgabe, nämliche die Meldung der Überlastsituation, nicht durchführen kann.

Das zweite Szenario dokumentiert einen Angriff auf Schritt (8) des Anwendungsfalls (Abbildung 9). Der Angriff erfolgt hier auf die Integrität der Informationsübermittlung, so dass die übermittelten Informationen verfälscht werden. In diesem Fall werden die Abschaltinformationen unterschlagen und stattdessen wird die entsprechende Anlage hochgeregelt, was dann zu Unterspannung im Stromnetz führt. Der Angreifer kommt aus dem internen Umfeld und hat Insiderwissen mit vollem Zugang zum System, um die Datenmanipulation durchzuführen. Die Motivation für diesen Angriff könnte beispielsweise Rache sein, da der Angreifer beispielsweise ein unzufriedener oder gar – bei kaum vorhandenen Sicherheitsprozessen im Unternehmen – ein ehemaliger gekündigter Arbeitnehmer sein könnte. Für den Angriff nutzt der Angreifer Content-Spoofing, um die Information über den Abschaltbefehl zu manipulieren

Abbildung 9: Darstellung der Angriffsszenarien in dem Sequenzdiagramm aus Abb. 7
Quelle: eigene Darstellung



und stattdessen die DER-Anlagen hoch zu regeln. Damit werden weitere Probleme verursacht, die dem Betreiber schaden.

Das dritte Szenario dokumentiert einen Angriff auf Schritt (12) des Anwendungsfalls (siehe → *Abbildung 9*). Der Angriff erfolgt hier auf die Vertraulichkeit der Informationsübermittlung. Der Angreifer hört Informationen (Messwerte etc.) mit bzw. spioniert sie aus und kann diese Informationen später selbst für die eigene Geschäftsstrategie nutzen. Der Angreifer ist ein externer Hacker mit Hackerkompetenz. Motivationen für diesen Angriff können neben der Konkurrenzsituation auch Diebstahl, Bereicherung oder auch der Wunsch nach Schaden für andere sein. Für den Angriff schaltet sich der Angreifer als Man-in-the-middle (MITM) zwischen das Interne SMGW und das KEM. Der Angreifer hört die Kommunikation zwischen dem internen SMGW und dem KEM mittels Sniffing-Angriff mit. Später leitet er aus den ausgespähten Daten für seine eigene Geschäftsstrategie neue Erkenntnisse ab.

Diese drei Angriffe, die Motivation der Angreifer sowie die vermuteten ausgenutzten Schnittstellen werden mit dem MUC-Template im Anhang in → *Kapitel 7.2* dokumentiert.

5.2.2 Risikoanalyse

Weiterhin erfolgt während der Erfassung der Gefährdungsszenarien im MUC-Template die Analyse der Szenarien. Dafür werden zunächst für die Risikoanalyse der einzelnen Szenarien der potenzielle Schaden (niedrig, mittel oder hoch) und die Eintrittswahrscheinlichkeit (normal, hoch oder sehr hoch) bestimmt, woraus dann wiederrum das Risiko nach der Risikomatrix in Tabelle 1 bestimmt werden kann (niedrig = hellblau, mittel = blau, hoch= rot). Das Risiko wird also, wie in der Risikoanalyse üblich, über folgende Formel bestimmt:

Risiko =
*Eintrittswahrscheinlichkeit * Potentieller Schaden*

Für die hier entwickelten drei Angriffsszenarien wurde die Eintrittswahrscheinlichkeit mit Hoch, also der mittleren Stufe, angenommen, da es sich um eine Art regionales Szenario handelt. Für die Ermittlung einer Eintrittswahrscheinlichkeit können verschiedene Faktoren miteinbezogen werden, wie beispielsweise die Angreifermotivation, die Angreifbarkeit der Schnittstelle oder die Zugriffszahlen. Der potenzielle Schaden ist bei A1 mit „Mittel“ angenommen worden, da es sich um ein System eines Betreibers der Mittel- und Niederspannung handelt und dementsprechend maximal ein mittelgroßer Ausfall zu befürchten ist. Die beiden anderen

Tabelle 1: Risikomatrix: Bewertungsschema für die Ermittlung des Risikos der Gefährdungsszenarien

Risikomatrix: unter 3 grün, ab 6 rot		**Potenzieller Schaden**		
		gering = 1	**mittel = 2**	**hoch = 3**
Eintritts-wahrscheinlichkeit	normal = 1	1	2	3
	hoch = 2	2	4	6
	sehr hoch = 3	3	6	9

Szenarien spielen sich regional sehr begrenzt ab, sozusagen auf Nachbarschafts- bzw. Haushaltsebene, so dass keine größeren Ausfälle zu befürchten sind. Da es sich in dem Anwendungsfall insgesamt mit einem virtuellen Kraftwerk um ein regional begrenztes Szenario handelt, ergeben sich für die Risiken der beschriebenen Szenarien A2 und A3 ein niedriges Risiko und für das Szenario A1 ein mittleres Risiko, da mit dem MV / LV SCADA-System bereits eine größere Zahl an virtuellen Kraftwerken gesteuert wird, was in Tabelle 2 dargestellt ist.
Dies lässt sich ebenfalls damit begründen, dass das Schutzziel Verfügbarkeit in der Energiedomäne die höchste Priorität der CIA-Schutzziele aufweist.

Aus dieser Risikoanalyse kann ein Entwickler für die konkrete Implementierung Schlüsse ziehen, um die Art, den Grad und die Menge der Sicherheitsmaßnahmen geeignet auszuwählen.

Die Festlegung des potenziellen Schadens und der Eintrittswahrscheinlichkeit erfolgt in der Schritt-für-Schritt-Analyse des Misuse Cases in → *Abschnitt 4* des MUC-Templates, das im Anhang in → *Kapitel 7.2* dokumentiert ist.

5.2.3 Identifikation von Sicherheitsanforderungen

Abschließend werden den einzelnen Schritten der Gefährdungsszenarien Sicherheitsanforderungen aus → *Abschnitt 5* des MUC-Templates zugeordnet, um die Gefährdungen zu vermeiden oder mindestens zu vermindern. Diese Zuordnung lässt sich aus den BSI-Kreuzreferenztabellen von elementaren Gefährdungen und Anforderungen ableiten und ist in der folgenden → *Tabelle 3* dargestellt. Dabei sind nur die Anforderungen aufgelistet, die in dem Anwendungsfall Verwendung finden. Die Bedeutungen der Anforderungen sowie entsprechende Referenzen sind im Anhang in → *Abschnitt 7.2.5* (in → *Abschnitt 5* des MUC-Templates) tabellarisch dargestellt.

Zusätzlich wurden für den Anwendungsfall folgende Sicherheitsanforderungen als notwendig erachtet: ISMS.1, ORP.5, CON.2, CON.5, CON.6, DER.3.1, DER.4, INF.1, INF.2, INF.3, INF.4, INF.5. Auch diese Anforderungen werden im Anhang in → *Abschnitt 7.2.5* (in → *Abschnitt 5* des MUC-Templates) genauer erläutert und tabellarisch dargestellt.

In der → *Tabelle 7.2.4.1* im Anhang werden für die bessere Verständlichkeit zu den identifizierten Sicherheitsanforderungen jeweils zwei Beispiele für die konkretere Umsetzung genannt. Diese Beispiele zielen sowohl auf organisatorische als auch auf technische Maßnahmen ab. Für den Angriff „A1-1 Ausspähen“ spielt beispielweise für die Absicherung ein gutes „Kryptokonzept“ (CON.1) eine Rolle, um damit dann geeignete kryptografische Verfahren auszuwählen und damit dann die Kommunikationsverbindung passend zu verschlüsseln.

Manche der genannten Sicherheitsanforderungen müssen nicht zwangsweise von den Entwicklern konkret realisiert werden, wenn die entsprechenden

Tabelle 2: Auswertung des Risikos der Angriffsszenarien aus dieser Studie

Angriffs-szenario Nr.	Angriffstyp	Eintrittswahr-scheinlichkeit	Potenzieller Schaden	Risiko
A1	Denial of Service-Angriff (DoS)	hoch = 2	mittel = 2	mittel = 4
A2	Manipulation der Datenintegrität	hoch = 2	niedrig = 1	niedrig = 2
A3	Ausspähen von Informationen	hoch = 2	niedrig = 1	niedrig = 2

Funktionalitäten / Dienstleistungen nicht in Anspruch genommen werden. Dann sind diese Sicherheitsanforderungen als optional zu betrachten.

Die identifizierten Sicherheitsanforderungen geben den Entwicklern Anhaltspunkte, welche Sicherheitsmaßnahmen konkret in der Implementierung notwendig sind, um ein möglichst hohes Sicherheitsniveau zu erreichen. Weiterhin muss bei dieser Auswahl der Sicherheitsmaßnahmen die entsprechende Risikoanalyse mitberücksichtigt werden. Falls eine Zertifizierung nach ISO 27000 nach IT-Grundschutz realisiert werden soll / muss, sollten ebenfalls die BSI-Bausteine angemessen umgesetzt werden.

Tabelle 3: Zuordnung von Sicherheitsanforderungen nach BSI-IT-Grundschutz-Bausteinen

Angriffsschritt	A1-1	A1-2	A2-1	A3-1	A3-2
Angriff	Ausspähen	DoS-Angriff	Content Spoofing	MITM-Angriff	Ausspähen
CAPEC-Katalog	Sniffing-Angriff (CAPEC-157)	Flooding (CAPEC-125)	Content-Spoofing (CAPEC-148)	Man-in-the-middle (MITM) (CAPEC-94)	Sniffing-Angriff (CAPEC-157)
BSI –Gefährdungskatalog	G 0.14 Ausspähen von Informationen (Spionage)	G 0.40 Verhinderung von Diensten (Denial of Service)	G 0.22 Manipulation von Informationen	G 0.43 Einspielen von Nachrichten	G 0.14 Ausspähen von Informationen (Spionage)
Zugehöriges Schutzziel	Vertraulichkeit	Verfügbarkeit	Integrität	Vertraulichkeit	Vertraulichkeit
Sicherheitsanforderungen (BSI-Bausteine)	ORP.1, ORP.2, ORP.3, ORP.4, CON.1, CON.8, CON.9, OPS.1.1.2, OPS.1.1.4, OPS.1.1.5, OPS.1.1.6, OPS.1.2.4, OPS.1.2.5, OPS.2.1, OPS.2.2, OPS.3.1, DER.2.3, APP.1.2, APP.2.1, APP.2.2, APP.3.3, APP.4.3, SYS.1.1, SYS.2.1, SYS.3.1, SYS.3.2.1, SYS.3.2.2, SYS.3.2.3, SYS.3.2.4, SYS.3.3, SYS.4.4, SYS.4.5, IND.1, IND.2.1, IND.2.2, IND.2.3, IND.2.4, IND.2.7, NET.1.2, NET.3.1, NET.3.2, NET.3.3, NET.4.1, INF.7, INF.8, INF.9, INF.10	CON.8, OPS.1.1.3, OPS.1.1.5, OPS.1.2.4, OPS.1.2.5, OPS.2.2, DER.1, DER.2.3, APP.1.2, APP.2.1, APP.2.2, APP.3.1, APP.3.2, APP.3.6, APP.4.3, APP.5.1, SYS.1.1, SYS.1.5, SYS.1.8, SYS.2.1, SYS.4.4, IND.2.1, NET.1.1, NET.1.2, NET.3.1, NET.3.2, NET.3.3, NET.4.2.	ORP.1, ORP.2, ORP.4, CON.1, CON.3, CON.4, CON.8, CON.9, OPS.1.1.2, OPS.1.1.5, OPS.1.2.2, OPS.1.2.4, OPS.1.2.5, OPS.2.1, OPS.2.2, OPS.3.1, DER.1, DER.2.1, DER.2.2, DER.2.3, APP.1.1, APP.1.2, APP.2.1, APP.2.2, APP.2.3, APP.3.1, APP.3.2, APP.3.6, APP.4.2, APP.4.3, APP.4.6, APP.5.2, SYS.1.1, SYS.1.2.2, SYS.1.3, SYS.1.5, SYS.1.7, SYS.1.8, SYS.2.1, SYS.2.2.2, SYS.2.3, SYS.3.1, SYS.3.2.1, SYS.3.2.2, SYS.3.2.3, SYS.3.3, SYS.4.1, SYS.4.3, SYS.4.5, IND.2.1, IND.2.2, IND.2.4, NET.1.1, NET.1.2, NET.3.1, NET.3.2, NET.3.3, NET.4.3, INF.7, INF.8, INF.9.	DER.2.3, APP.2.1, APP.2.2, APP.2.3, APP.3.1, APP.3.6, APP.4.3, SYS.1.1, SYS.1.5, SYS.2.1, SYS.3.2.1, IND.2.1, NET.1.1, NET.1.2, NET.3.1, NET.3.2, NET.3.3	Siehe Sniffing-Angriff A1 1, ganz links in dieser Tabelle.

:// 6. ZUSAMMENFASSUNG, DISKUSSION UND AUSBLICK

Diese Studie beschäftigte sich mit dem exemplarischen Anwenden von Gefährdungsszenarien in der Energiedomäne. Fokus war die Verwendung solcher Szenarien bereits in der Systementwicklung, um dem Thema Informationssicherheit insgesamt eine höhere Priorität zu geben, das Prinzip Security-by-Design weiterzuentwickeln und Systeme insgesamt sicherer zu machen. Hierfür wurde eine Gesamtmethodik aus verschiedenen standardisierten Vorgehensweisen entwickelt. Im Rahmen des Themenfeldes Resilienz soll mit dieser Methodik die Behandlung von Zwischenfällen im Vorfeld („feststellen und verhindern“) erfolgen. Gefährdungsszenarien werden hier mit einer Risikoanalyse bewertet und entsprechende Sicherheitsanforderungen für die Verhinderung identifiziert. Die Gesamtmethodik wurde in → *Abschnitt 4.6* vorgestellt und dann im Folgenden beispielhaft angewendet. Die textuelle Beschreibung der Anwendung der Gesamtmethodik erfolgte in → *Abschnitt 5*.

6.1 Zusammenfassung

Zu Beginn wurde ein Anwendungsfall aus der Energiedomäne, ein virtuelles Kraftwerk in einer Überlastsituation, als passendes Beispiel entwickelt. Dieser Anwendungsfall wurde dann mit dem Use Case-Template (UC-Template) nach IEC 62559 systematisch und standardisiert erfasst. Die Erfassung und Dokumentation im UC-Template erfolgte im Anhang in → *Abschnitt 7.1*. Für diesen Anwendungsfall wurden weiterhin drei verschiedene Gefährdungsszenarien entwickelt und mit dem Misuse Case-Template (MUC-Template), das an das UC-Template angelehnt ist, erfasst und dokumentiert. Im MUC-Template erfolgte danach ebenfalls die Analyse der Szenarien. Dafür wurden eine Risikoanalyse der Szenarien durchgeführt und standardisierte Sicherheitsanforderungen identifiziert, was das Ergebnis dieser Studie darstellt. Die Erfassung und Dokumentation im MUC-Template erfolgte im Anhang in → *Abschnitt 7.2*.

6.2 Diskussion

Als nächster Schritt nach der Analyse mit den Misuse Cases können die ermittelten Risiken und die identifizierten Sicherheitsanforderungen dann von den Entwicklern bei der realen Implementierung des Systems herangezogen werden, um die Sicherheitsanforderungen in einem angemessenen Grad auf Basis der Risikoanalyse in konkrete Sicherheitsmaßnahmen umzusetzen. Dies kann zu Herausforderungen führen, da eine angemessene Sicherheit auch immer eine Gradwanderung ist: Es sollen nicht übertrieben viele Mittel umgesetzt werden, was u.a. zu unnötigem Einsatz von Kapital führt, aber auch nicht zu wenig Maßnahmen ergriffen werden, was Angreifer anlocken könnte.

Insgesamt wird empfohlen ein System nach BSI-IT-Grundschutz, ISO 27000 oder entsprechenden domänenspezifischen Versionen abzusichern und damit ein ISMS für das entsprechende System für ein kontinuierliches Sicherheitsmanagement zu entwickeln. Das heißt, es wird ein standardisiertes

Verfahren verwendet, das mit individuellen Maßnahmen umgesetzt wird und daher immer eine maßgeschneiderte Anpassung an das dazugehörige System beinhaltet und zusätzlich ein kontinuierliches Controlling der Sicherheit im Unternehmen ermöglicht. Es sollte bereits bei der Identifikation von Sicherheitsanforderungen oder dann vor der Implementierung eine passende Auswahl von Sicherheitsstandards, z. B. aus der zugehörigen Domäne, erfolgen. In der Energiedomäne gibt es beispielsweise einen domänenspezifischen Standard aus der ISO 27k-Serie, den ISO/IEC 27019. Weiterhin können bei der technischen Umsetzung der IEC 62351, der Informationssicherheit in Energiemanagementsystemen und für den zugehörigen Datenaustausch beschreibt, herangezogen werden. Hier beschreibt beispielsweise der IEC 62351-8 Methoden für die Rollenbasierte Zugriffskontrolle oder der IEC 62351-9 das Schlüsselmanagement in der Energiedomäne.

Bei der konkreten Implementierung müssen für jede Sicherheitsanforderung Maßnahmen ergriffen werden. Die hier identifizierten Sicherheitsmaßnahmen sind mit Beispielen für die Umsetzung im Anhang in → *Kapitel 7.3* tabellarisch dargestellt. Zum Beispiel legt die Sicherheitsanforderung APP.3.3 für Fileserver nahe, Virenschutzprogramme einzusetzen und den Datenbestand zu verschlüsseln. Die Sicherheitsanforderungen CON.1 fordert ein Kryptokonzept. Hierfür müssen zum Beispiel sowohl Verschlüsselungsverfahren als auch an welchen Stellen diese eingesetzt werden sollen, und auch Schlüssellängen im Vorhinein festgelegt werden. Somit gibt es auch häufig eine Überschneidung der Maßnahmen für die einzelnen Sicherheitsanforderungen („Datenbestand verschlüsseln“ bei APP.3.3 und „Verschlüsselungsverfahren einsetzen“ bei CON.1). Abschließend müssen aber alle Sicherheitsanforderungen im implementierten System abgedeckt sein. Nach der Auswahl der Techniken müssen entsprechende Produkte, die es auf dem Markt gibt, ausgewählt oder eigene Entwicklungen angestoßen werden, um die Absicherungen in das zu entwickelnde System oder den operativen Betrieb übernehmen zu können.

6.3 Ausblick

Zukünftige Arbeiten in diesem Themenfeld werden sich damit befassen das UC- und das MUC-Template zu vereinigen, um direkt Angriffs- und Fehlerfälle bei der Systementwicklung mitbetrachten zu können. Dieses kombinierte Template soll dann im Anschluss in die Standardisierung als Norm eingebracht werden, um das Thema Security-by-Design voranzutreiben. Weiterhin wird der Fokus darauf liegen, zu untersuchen inwieweit Fehlerfälle eines Systems Gefährdungsszenarien begünstigen, da häufig Fehler oder Bugs in einem System den Angriff auf das System erst zulassen.

://shortcut
ANHANG
(Seiten 153-222)

Literaturverzeichnis

Babazadeh, Davood; Mayer, Christoph; Lehnhoff, Sebastian (2018): Cyber Resilienz – Schwarze Schwäne im Energiesystem. bulletin.ch, zuletzt geprüft am 12.02.2021.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2020): Katalog zu elementaren Gefährdungen. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrdungen/elementare_Gefaehrungen_Uebersicht_node.html, zuletzt geprüft am 12.02.2021.

Buschermöhle, Ralf; Eekhoff, Heike; Josko, Bernhard (2006): SUCCESS 2006 – Motivation, Vorgehensweise und Ergebnisse: Gesellschaft für Informatik e.V., S. 295–301, zuletzt geprüft am 12.02.2021.

Fischer, Lars (2018): Auf dem Weg zu einer quantitativen Analyse der Resilienzeffekte von IT-Sicherheitslücken in zukünftigen Energiesystemen. 1. internationale Konferenz über Infrastrukturresilienz, zuletzt geprüft am 12.02.2021.

Hirschl, Bernd; Aretz, Astrid; Bost, Mark; Tapia, Mariela; Gößling-Reisemann, Stefan (2018): Vulnerabilität und Resilienz des digitalen Stromsystems – Endbericht des Projekts „Strom-Resilienz. Bremen. Online verfügbar unter https://www.ioew.de/fileadmin/user_upload/BILDER_und_Downloaddateien/Publikationen/2018/Schlussbericht_Strom-Resilienz.pdf, zuletzt geprüft am 12.02.2021.

Jacobson, Ivar; Ericsson, Maria; Jacobson, Agneta (1995): The object advantage. Business process reengineering with object technology. Wokingham, England, Reading, Mass.: Addison-Wesley (ACM Press books).

Kreyenberg, Hannah (2020): Energiesektor steht im Fokus von Hackern (5/2020). In: ew, S. 56. Online verfügbar unter https://emagazin.ew-magazin.de/de/profiles/a21024e15cd4/editions/1920f3b9a2c62266cbfb, zuletzt geprüft am 03.03.2021.

Kure, Halima; Islam, Shareeful; Razzaque, Mohammad (2018): An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. In: Applied Sciences 8 (6), S. 898. DOI: 10.3390/app8060898.

Langner, Ralph (2013): To Kill a Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve. Online verfügbar unter https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf, zuletzt geprüft am 12.02.2021.

Marshall D. Abrams, Joe Weiss (2018): Malicious Control System Cyber Security Attack Case Study: Maroo-chy Water Services, Australia. Online verfügbar unter https://www.mitre.org/sites/default/files/pdf/08_1145.pdf, zuletzt geprüft am 12.02.2021.

Mayer, Christoph; Babazadeh, Davood; Lehnhoff, Sebastian (2018): Resilienz in digitalisierten Energiesystemen – Chance oder Risiko: DIV Deutscher Industrieverlag GmbH. In: gwf Gas + Energie (5/2018), zuletzt geprüft am 12.02.2021.

Open Web Application Security Project (OWASP) (2017): Die 10 kritischsten Sicherheitsrisiken für Webanwendungen. Online verfügbar unter https://wiki.owasp.org/images/9/90/OWASP_Top_10-2017_de_V1.0.pdf, zuletzt geprüft am 12.02.2021.

Peterson, Gunnar; Steven, John (2006): Defining Misuse within the Development Process. In: IEEE Secur. Privacy Mag. 4 (6), S. 81–84. DOI: 10.1109/MSP.2006.149.

IEC 62351-1, 2007-05: Power systems management and associated information exchange – Data and communications security.

VDE 0175-110, 12.2019: Richtlinien zur IT-Sicherheit und Resilienz für die Smart-Energy-Einsatzumgebung, zuletzt geprüft am 26.02.2021.

Sindre, Guttorm; Opdahl, Andreas L. (2005): Eliciting security requirements with misuse cases. In: Requirements Eng 10 (1), S. 34–44. DOI: 10.1007/s00766-004-0194-4.

Witte, Julika (Hg.) (2020): Zentrale und dezentrale Elemente im Energiesystem. Der richtige Mix für eine stabile und nachhaltige Versorgung : Stellungnahme. Stand: März 2020. München, Halle (Saale), Mainz: acatech - Deutsche Akademie der Technikwissenschaften e. V; Deutsche Akademie der Naturforscher Leopoldina e.V. - Nationale Akademie der Wissenschaften; Union der deutschen Akademien der Wissenschaften e. V (Stellungnahme / Deutsche Akademie der Naturforscher Leopoldina). Online verfügbar unter https://energiesysteme-zukunft.de/fileadmin/user_upload/Publikationen/PDFs/ESYS_Stellungnahme_zentral_dezentral.pdf.

://

ZUSAMMENFASSUNG UND SCHLUSSWORT

Die Digitalisierung stellt unsere Gesellschaft vor große Herausforderungen. Ihr transformatives Potential ist vergleichbar mit dem der Industrialisierung vor rund 200 Jahren. Immer mehr Teilbereiche unserer Gesellschaft verlagern sich in die digitale Sphäre, von kleinen Handlungen einzelner Menschen bis zu globalen Prozessen. Auch die Energiewirtschaft bleibt davon nicht unberührt. Im Energiewirtschaftssektor liegt das Hauptaugenmerk auf der Digitalisierung der Energienetze. Ein Großteil der erzielten Fortschritte bezieht sich auf die Funktionalität von Energiegeräten, die es Kunden ermöglichen, ihren Energieverbrauch zu überwachen und zu steuern, z. B. intelligente Zähler, intelligente Thermostate, intelligente Batterien und Ladegeräte.

Wie die Beiträge des Kompendiums gezeigt haben, birgt die Digitalisierung im Energiewirtschaftssektor besondere Risiken und Chancen: Als Teil der kritischen Infrastruktur ist der Energiewirtschaftssektor nicht nur besonders häufig von Angriffen betroffen, ein Ausfall der Energieversorgung hätte auch erhebliche Auswirkungen auf die Aufrechterhaltung zentraler gesellschaftlicher Funktionen. Das macht Sicherheit zu einem zentralen Aspekt der Digitalisierung in der Energiewirtschaft. Digitale Technologien bieten jedoch auch große Chancen für die Energie- und Mobilitätswende und damit für den Kampf gegen den Klimawandel. Durch die intelligente Vernetzung von Verbrauchern und Produzenten und die Nutzung von Big Data ermöglichen sie nicht nur die Hebung von großen Flexibilitäts- und Effizienzpotentialen, sondern sind auch Antwort auf die naturgemäße Volatilität von Erneuerbaren Energien. Die Digitalisierung macht die Energiebranche flexibler, so die Kernaussage der IFO-Studie "Energie im Zeitalter der Digitalisierung." Die Studie stellte fest, dass sich der Fokus des Wandels weg von der Effizienz und der Leistung von Anlagen hin zur digitalen Transformation der Energiewirtschaft verschiebt.

Um diese Transformation greifbar zu machen und um den Blick zu schärfen, für das was betrachtet und analysiert werden soll, wurden im ersten Beitrag verschiedene Aspekte der Digitalisierung beleuchtet. Ausgehend von den englischen Begriffen digitization, digitalization und digital transformation sowie von den deutschen Begriffen Digitalisierung und digitale Transformation, wurde nicht nur die Entwicklung der Digitalisierung nachgezeichnet, sondern es wurden auch unterschiedliche Kernbereiche der Digitalisierung herausgearbeitet. Genannt wurde die Umwandlung von Informationen in eine digitale Form (Daten) sowie die Vernetzung sämtlicher Bereiche unserer Gesellschaft und die Schaffung eines Mehrwerts, in Form eines wirtschaftlichen oder gesellschaftlichen Vorteils. Zusätzlich zu diesen Eigenschaften, wurde ein weiterer, für die Digitalisierung in der

Energiewirtschaft zentraler, Kernbereich identifiziert: die (Cyber- und Versorgungs-) Sicherheit.

Entlang der Aspekte Daten, Mehrwert und Sicherheit, hat sich das vorliegende Kompendium durch die Digitalisierung in der Energiewirtschaft gearbeitet. Vernetzung wird in keinem Teil gesondert besprochen, sie wird in allen Beiträgen mitbehandelt. Der erste Beitrag legte den Fokus, neben der Erarbeitung einer Definition, auf den Zugang und die Verwendung von Daten. Der Zugang zu digitalen Daten ist eine essenzielle Voraussetzung für Innovationen. Ohne Daten, beziehungsweise ohne die richtigen Daten (Datenart, -qualität, zeitliche Auflösung und Aggregationsgrad, etc.), ist die Entwicklung neuer Geschäftsmodelle nicht möglich. Dennoch weisen öffentliche Energiedaten hohe Zugangs- und Qualitätseinschränkungen auf und weiterhin ist unklar, welche Daten die unterschiedlichen Akteure am Energiemarkt tatsächlich benötigen. Was dagegen feststeht ist, dass hochaufgelöste Messdaten, zum Beispiel von Smart Metern, und personenbezogene Daten, zum Beispiel Nutzerverhalten, nicht nur für innovative Produkte unerlässlich sind, sondern auch für das Gelingen der Energiewende. Energiedaten von Verbrauchern und Erzeugern können – wenn sie einheitlich erhoben und allgemein verfügbar gemacht werden –den Übergang in eine digitale, klimaneutrale Energiewirtschaft ermöglichen.

Der zweite Kernbereich der Digitalisierung in der Energiewirtschaft, der ökonomische oder gesellschaftliche Mehrwert, stand im Fokus des zweiten Beitrags. Nach vielen Jahren der Stabilität müssen sich Energieversorgungsunternehmen (EVU) an eine sich verändernde Realität anpassen: Sowohl die Liberalisierung der Märkte in den 90er Jahren und der resultierende Wettbewerb als auch die Digitalisierungsfortschritte in der Energiewirtschaft, zwingen Energieversorgungsunternehmen (EVU) sich von ihrer Stabilitätsstrategie abzuwenden. Wenn sie weiterhin am Markt bestehen bleiben wollen, müssen sie dringend eine Digitalisierungsstrategie entwerfen. Die Autoren haben dazu ein dreistufiges Vorgehensmodell für ein zukunftsorientiertes IT- Management entwickelt, das EVU jeder Größe umsetzen können: Erstens, Analyse der Unternehmens- und Digitalisierungsstrategie. Zweitens, Definition der IT-Organisation und IT-Governance. Drittens, Umsetzung in allen Bereichen des Unternehmens. Für kleinere EVU ist es wichtig sicherzustellen, dass die Maßnahmen praxisnah, einfach umsetzbar und mit minimalem Kostenrisiko verbunden sind. Die Umsetzung der drei Schritte ist keine Garantie für deren Erfolg. Die Strategie muss flexibel auf sich verändernde Rahmenbedingungen reagieren können und darf nicht dazu führen, dass sich andere Prozesse verlangsamen. Zukunftsfähiges IT-Management muss Prozesse nicht nur sammeln, sondern auch optimieren, verkürzen und entfernen. Erst dann können innovative Wertschöpfungsketten gebildet werden. Die Chance, die für EVU in der Entwicklung eines zukunftsfähigen IT-Managements liegt, sind Asset-Management und die Verknüpfung von Prozessen zur Steuerung dezentraler Anlagen mit Steuerungsprozessen im Speicherbetrieb. Die Chance für die Energiewende liegt darin, dass Technologien nachhaltig und sinnvoll in das Energiesystem integriert werden.

Durch Smart Meter, Smart Grids und andere intelligente Technologien hängt unsere

Energieversorgung zunehmend von der IT-Sicherheit ab. Vor welchen Herausforderungen die Energiewirtschaft bei diesem Thema steht, hat der dritte Beitrag des Kompendiums beleuchtet. Unternehmen, die Teil der kritischen Infrastruktur sind (KRITIS-Unternehmen), haben in den vergangenen Jahren viel investiert, um ihre IT sicherer vor Bedrohungen zu machen. Gesetzliche Mindeststandards für KRITIS-Unternehmen und die Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), haben dazu beigetragen, dass das Sicherheitsniveau und das Bewusstsein für das Thema gestiegen sind. Gleichzeitig gibt es kein finales Sicherheitsziel, das erreicht werden kann. IT-Sicherheit bleibt ein stetiger Prozess, ein Rennen zwischen denen, die in die Systeme eindringen, und denen, die sie schützen wollen. Auch der Rechtsrahmen spielt für die IT-Sicherheit eine große Rolle. Er ist noch auf die alte Energiewelt, mit tendenziell eher wenigen, großen Kraftwerken ausgerichtet. In der neuen Energiewelt gibt es aber eine Vielzahl an kleinen Energieanlagen. Sie fallen laut aktuellem Recht aber nicht unter die kritische Infrastruktur. Nur 3,4 Prozent der Energieanlagen sind KRITIS-Betreiber. Das entspricht etwa 29 Prozent der gesamten installierten Leistung. Im Umkehrschluss bedeutet das, dass rund 71 Prozent der Leistung nicht zur kritischen Infrastruktur zählt und die Betreiber dort auch keinen ganzheitlichen Ansatz bei der IT-Sicherheit verfolgen müssen.

Wie notwendig ein hohes Maß an IT-Sicherheit im Energiesektor ist, zeigt die Statistik: 16 Prozent aller Hackerangriffe im Jahr 2019 erfolgten auf den Energiesektor – er ist damit der meistattackierte Sektor in Deutschland. Wie Gefährdungsszenarien konkret aussehen können, damit hat sich der vierte Beitrag des Kompendiums beschäftigt. Die Autoren haben drei konkrete Szenarien analysiert. Als Anwendungsfall diente ein virtuelles Kraftwerk in einer Überlastsituation. Durch die Standardisierung der Situation mit dem Use Case Template nach IEC 62559 und durch die Dokumentation des Angriffs mithilfe eines Misuse Case Template, konnten die drei Gefährdungsszenarien erfasst und analysiert werden. So konnten systematisch verletzte Ziele und Sicherheitsanforderungen identifiziert werden. Aus den Ergebnissen lassen sich konkrete Sicherheitsmaßnahmen ableiten, die Entwickler bei der realen Implementierung eines Systems heranziehen können. Auch hier wird deutlich, dass Sicherheit ein kontinuierlicher Prozess ist, der sich immer an neue Bedrohungen und Technologien anpassen muss. Absolute Sicherheit gibt es alleine schon deswegen nicht, weil die menschliche Komponente immer das schwächste Glied in der Kette ist. Bei den Hackerangriffen im Jahr 2019 handelte es sich in 47 Prozent der Fälle um schädliche Links, bei 32 Prozent um schädliche Anhänge, 22 Prozent Phishing und nur zu 0,16 Prozent um gezielte Angriffe. Die meisten Angreifer setzen auf menschliche Fehler: Ein falscher Klick reicht und auch das beste System ist ausgehebelt. Das zeigt, wie komplex die Sicherheitsfragen sind, die man sich selbst in so einem konkreten Fall, wie dem im vierten Beitrag untersuchten, stellen muss.

Der Zuwachs an Komplexität, der mit der Digitalisierung einhergeht, das wird in allen Beiträgen deutlich, ist eine große Barriere für Unternehmen, Gesetzgeber und Individuen. Die Digitalisierung schreitet in rasender Geschwindigkeit voran und mit ihr die unzähligen (neuen) Chancen und Risiken,

die durch sie entstehen: Die Corona-Pandemie hat unsere Arbeitswelt zwangsdigitalisiert. Durch die Arbeit im Homeoffice könnten Büroräume weniger werden und dadurch mehr Wohnraum in den Städten entstehen. Smart Grids und Smart Meter können unseren Energieverbrauch flexibler und damit effizienter gestalten und autonome Busse das Mobilitätsproblem auf dem Land lösen – nur um ein paar Beispiele zu nennen. Gleichzeitig ersetzt digitale Technik nicht die menschliche Komponente – wir alle sehnen uns danach, unsere Freunde und Verwandte, Kollegen und Kolleginnen in der echten Welt wieder zu sehen. Außerdem kann Hard- und Software nicht nur helfen den Energieverbrauch zu senken, sondern muss selbst erst aufwändig produziert und später mit Energie versorgt werden. Dafür sind viele seltene Erden und andere knappe Rohstoffe notwendig. Die Automatisierung des Verkehrs ist kein Selbstzweck und kann – wenn wir nicht aufpassen – auch zu einem höheren Verkehrsaufkommen führen.

Das alles passiert gleichzeitig, in allen Bereichen unseres Lebens. Letztlich ist Digitalisierung dann eine Chance, wenn wir sie als Hilfsmittel geschickt und bewusst einsetzen, und stellt dann ein Risiko dar, wenn wir sie unkontrolliert voranschreiten lassen. Es ist an uns, dem Staat und der Gesellschaft, die richtigen Weichen zu stellen, damit die Transformation dorthin führt, wo wir hinwollen. Was es deshalb braucht, ist Aufklärung darüber, wie die Technik funktioniert und was sie für Folgen hat. Der Staat muss seine Bürger informieren und ihnen damit eine aufgeklärte Entscheidung darüber ermöglichen, was sie für wünschenswert und was sie für nicht wünschenswert halten. Doch dazu müssen die Bürger erst einmal wissen, welche Möglichkeiten es heute überhaupt schon gibt. Hätten Sie zum Beispiel gewusst, dass es einen Algorithmus gibt, der selbstständig Texte schreibt, die nicht von Texten aus Menschenhand zu unterscheiden sind? Zwei Stellen dieses Schlusswortes wurden von so einem Algorithmus geschrieben – vielleicht erraten Sie, welche es sind.[1]

Dieses Kompendium will dazu einen aufklärerischen Beitrag leisten und die Digitalisierung in der Energiebranche greifbar machen. Klar ist, die Weichen für den Energiewirtschaftssektor von morgen werden schon längst digital gestellt.

Simon Schäfer-Stradowsky

1 Folgende Sätze sind von einer Maschine erstellt worden: Jeweils auf Seite 146: erster Absatz, die zwei letzten Sätze sowie zweiter Absatz, die letzten zwei Sätze.

://

Kurzbiographien der Autoren

Andreas Corusa

Andreas Corusa hat Versorgungstechnik sowie Energie- und Gebäudetechnik studiert. Von 2013 bis 2017 war er in Taiwan als Berater und Gründer im Start-Up Umfeld tätig. Seit Oktober 2017 ist er wissenschaftlicher Mitarbeiter und Projektmanager am Fachgebiet Energiesysteme der TU Berlin und arbeitet im WindNODE Energieprojekt an Querschnittsthemen wie der Digitalisierung und neuen Geschäftsmodellen in der Energiewirtschaft. Er ist der Hauptverantwortliche für dieses Kompendium.

Anne Walther

Frau Anne Walther absolvierte nach ihrem Bachelor der Medienkultur in Weimar ein Masterstudium in den Medien- und Kommunikationswissenschaften an der Martin-Luther-Universität Halle-Wittenberg mit Spezialisierung auf Marketing und Medienwirtschaft. Seit 2017 arbeitet Frau Walther im Bereich der Kommunikation und Marktforschung bei Conomic. Das Verfassen von Studien und Publikationen zu Themen der Digitalisierung und IT-Wirtschaft zählen zu den gegenwärtigen Schwerpunkten ihrer Arbeit.

Christian Sprengel

Herr Dr. Christian Sprengel arbeitete nach seinem Studium der Wirtschaftsinformatik an der Martin-Luther-Universität zunächst am Institut für Unternehmensforschung und Unternehmensführung, später am Institut für Wirtschaftsinformatik und Operations-Research. Während seiner Promotion war er seit 1999 als freiberuflicher IT- und Unternehmensberater mit den Schwerpunkten Geschäftsprozessmanagement sowie IT- und energiewirtschaftliche Prozessberatung tätig. Seit 2016 unterstützt Dr. Sprengel als Senior Consultant Conomic.

Christine Rosinger

Dipl.-Inform. Christine Rosinger ist Senior Researcher am OFFIS im Bereich Energie in der Gruppe „Entwurf und Bewertung standardisierter Systeme“. Ihr Forschungsschwerpunkt liegt auf dem Gebiet der Informationssicherheit in der Energiedomäne, wie bspw. Risikobewertungen und Bedrohungsanalysen. Sie arbeitet in verschiedenen Forschungsprojekten und unterstützt den Fortschritt des Security-by-Design-Prinzips sowie Interoperabilitätsaspekte. Zusätzlich ist sie in nationalen Standardisierungsaktivitäten (DKE/AK 952.0.15) beteiligt und seit 2014 IPMA Level D zertifiziert.

Daniel Kaufmann

Daniel Kaufmann hat Wirtschaftsingenieurwesen in Darmstadt und Bingen am Rhein studiert. Heute lebt der gebürtige Hesse in München und arbeitet bei der BBH Consulting AG als energiewirtschaftlicher Berater. Bereits während seines Studiums hat er sich umfangreich mit der Informationssicherheit und Energiewirtschaft auseinandergesetzt und beschäftigt sich daher auch bei BBH Consulting schwerpunktmäßig mit dem Aufbau von Informationssicherheitsmanagementsystemen (ISMS).

Elena Timofeeva

Dr. Elena Timofeeva, MBA ist wissenschaftliche Mitarbeiterin am Fachgebiet Energiesysteme der TU Berlin. Der Schwerpunkt ihrer Forschungsinteressen liegt auf der Anwendung digitaler Technologien in der Energiewirtschaft und insbesondere auf lokalen Strommärkten. Davor war sie als Senior Manager Energy & Climate Affairs bei einem energieintensiven Stromverbraucher sowie im Middle Office eines Energiehändlers tätig. Elena Timofeeva promovierte an der Freien Universität Berlin zu Unbundling in der Stromwirtschaft in einem rechtvergleichenden Kontext.

Falk Ritschel

Dr. Falk Ritschel ist seit 2009 Geschäftsführer der Conomic GmbH und betreut Projekte der Unternehmensberatung, der Marktforschung sowie der IT- und Prozessberatung. Sein aktueller Schwerpunkt liegt bei den Auswirkungen der Digitalisierung auf die Unternehmensstrategie. Zudem veröffentlichte Herr Dr. Ritschel mehrere Beiträge auf dem Gebiet der Innovation und Marktforschung.

Georg Erdmann

Prof. a.D. Dr. Georg Erdmann war zwischen 1995 und 2018 Inhaber des Lehrstuhls Energiesysteme an der Technischen Universität Berlin und sich schwerpunktmäßig mit den komplexen Wechselwirkungen zwischen energietechnischen, elektrotechnischen und institutionellen Innovationen einerseits und den verschiedenen Energiemärkten andererseits beschäftigt. Erdmann hatte im Laufe seiner Karriere zahllose Mandate bekleidet. Zu dem bedeutendsten gehörte die Berufung in das unabhängige Expertengremium der Bundesregierung „Energie der Zukunft“ (2011-2019).

Johannes Norbert Predel

Johannes Norbert Predel absolvierte ein Doppelmasterprogramm an der NTNU Trondheim (Norwegen) und TU Berlin. Während seiner Zeit als Student war er im WindNODE Verbundprojekt tätig. Seit seinem Abschluss im Jahre 2020 ist er Juniorberater bei der nymoen Strategieberatung. Der Schwerpunkt seiner Arbeiten liegt in den Bereichen der strategischen Ausrichtung von Unternehmen, der Produktentwicklung im Wärmemarkt, sowie Klimaschutzprojekten in der Immobilienwirtschaft.

Mathias Uslar

Dr.-Ing. Mathias Uslar ist Gruppenleiter im Bereich Systems Engineering und Assessment für Smart Grids am OFFIS - Institut für Informatik. Er hat an der Universität Oldenburg Informatik studiert und dort später in Energieinformatik promoviert. Neben seiner Tätigkeit in der Forschung ist er in zahlreichen IEC Gremien tätig. Dazu zählen IEC TC 57 WG 13,14, 16 und 21, IEC SyS Smart Energy WG 5 und IEC SyC Smart City sowie die deutschen Spiegelgremien. Er ist deutscher Sprecher des DKE K 901.

Simon Schäfer-Stradowsky

Simon Schäfer-Stradowsky ist Geschäftsführer des Instituts für Klimaschutz, Energie und Mobilität (IKEM) und Experte für innovatives Energie- und Klimaschutzrecht.Zu seinen Forschungsschwerpunkten zählen Förderregime für Erneuerbare Energien, die Flexibilisierung des Strommarktes und die Etablierung eines Rechtsrahmens für grünen Wasserstoff. Im Rahmen des Zertifikatslehrgangs „Regionale:r Energiesystem Manager:in“, ist er außerdem Dozent an der TH Köln.

Stefan Brühl

Stefan Brühl hat Wirtschaftsinformatik in Ulm und Flint (MI, USA) studiert. Seit mehr als 15 Jahren arbeitet er im Umfeld der Energiewirtschaft und Informationstechnologie. Er ist unter anderem Verbandsvertreter der Groupement Européen des entreprises et Organismes de Distribution d’Energie (GEODE) und auf nationaler und europäischer Ebene mit dem Schwerpunkten Informationssicherheit und Digitalisierung tätig.

Victor Stocker

Victor Stocker studierte Europäisches Recht und European Studies in Maastricht, Niederlande. Nach einer Anstellung im Automotive Sektor in Michigan (USA) zog es den gebürtigen Bayer zurück nach München. Dort ist er seit 2012 als energiewirtschaftlicher Berater bei der BBH Consulting AG tätig ist. Victor Stocker ist zertifizierter Datenschutzbeauftragter und geprüfter Information Security Officer und berät seit 2015 Unternehmen auf dem Gebiet der Informationssicherheit. Seine Expertise auf diesem Gebiet hat er in dieses Kompendium mit einfließen lassen.

:// 7. ANHANG

7.1 Erfassung eines Use Cases: Virtuelles Kraftwerk UC1

In diesem Abschnitt wird der für dieses Projekt erarbeitete Anwendungsfall (Use Case, UC) mittels des in Abschnitt 4.2 beschriebenen Use Case-Template nach IEC 62559 dokumentiert. Es handelt sich um einen Anwendungsfall im Themenfeld Virtuelles Kraftwerk (VK).

Dieser Use Case behandelt ein Virtuelles Kraftwerk im Rahmen einer Überlastsituation. Im Folgenden wird dieser Use Case im Use Case-Template nach IEC 62559 beschrieben. Die folgenden Abschnitte sind entsprechend des IEC 62559-Use Case-Templates durchnummeriert und benannt.

7.1.1 UC-Template Abschnitt „1 – Description of the use case"

7.1.1.1 UC-Template Abschnitt „1.1 – Name of use case"

Use case identification		
ID	Area Domain(s) / Zone(s)	Name of use case
UC1	SGAM Domains: Transmission, Distribution, DER, Customer Premises;	Virtuelles Kraftwerk
	SGAM Zones: Enterprise, Operation, Station, Field, Process	

7.1.1.2 UC-Template Abschnitt „1.2 – Version management"

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.5	03.12.2019	Christine Rosinger, OFFIS	Beschreibung des Use Cases	Draft
1.0	17.07.2020	Christine Rosinger, OFFIS	Finalisierung des UC	Final

7.1.1.3 UC-Template Abschnitt „1.3 – Scope and objectives of use case"

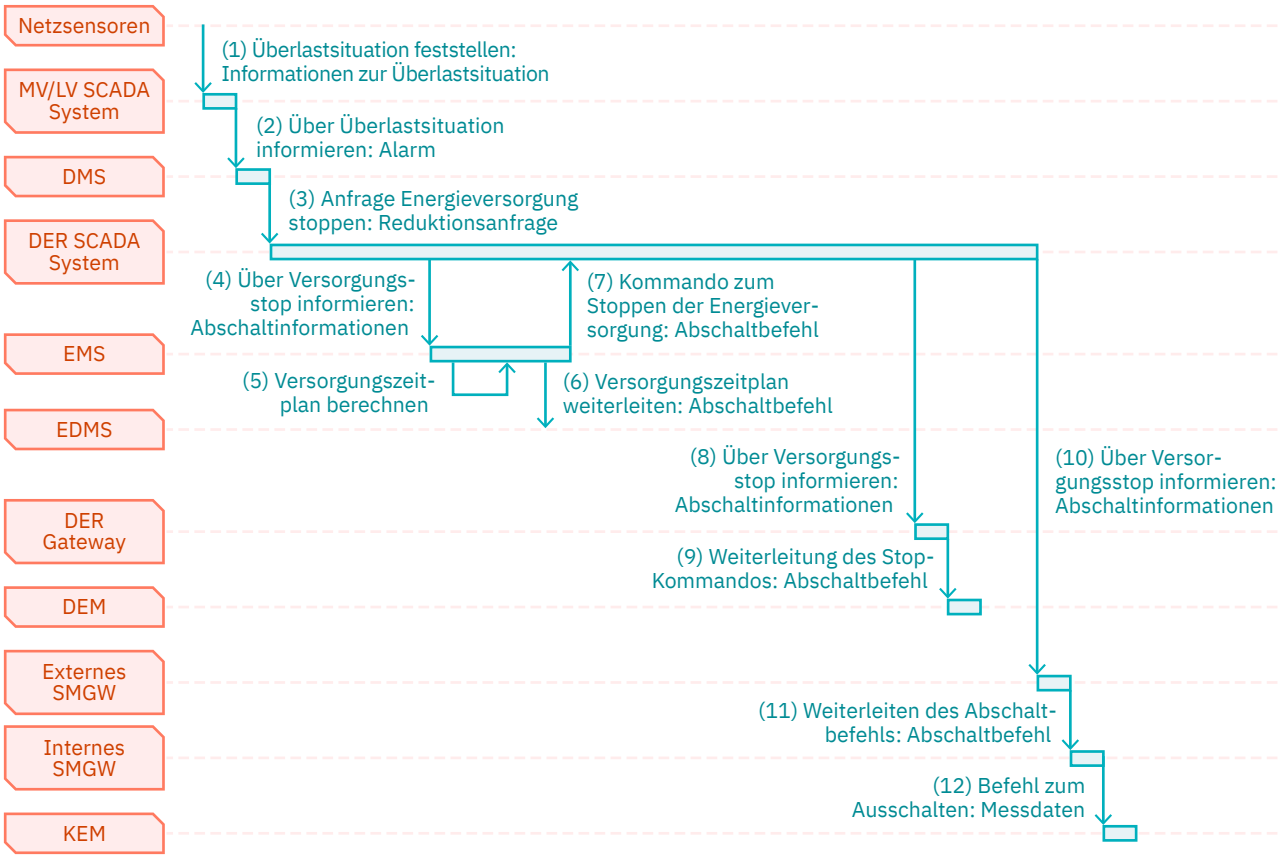
Scope and objectives of use case	
Scope	Dieser Anwendungsfall repräsentiert einen Anwendungsfall in einem virtuellen Kraftwerk. Sensoren haben eine Überlastsituation in dem entsprechenden Netzbereich festgestellt, so dass das virtuelle Kraftwerk seine Erzeugung reduzieren muss.
Objective(s)	Erfassung eines beispielhaften Anwendungsfalls für virtuelle Kraftwerke, um Gefährdungsszenarien zu identifizieren.
Related business case(s)	-

7.1.1.4 UC-Template Abschnitt „1.4 – Narrative of use case"

Narrative of use case
Short description
Ein Sensor im Netz hat eine Überlastsituation festgestellt. Es werden nun Mechanismen durchgeführt, die dazu führen, dass das virtuelle Kraftwerk (VK) seine Einspeisung reduziert.
Complete description
Die Beschreibung dieses Use Cases erfolgt anhand des Sequenzdiagramms in Abschnitt 2 dieses Use Case-Templates. Eine Beschreibung der dazugehörigen Akteure erfolgt in Abschnitt 3.1 dieses Use Case-Templates. Netzsensoren haben in einem entsprechenden Netzbereich eine Überlastsituation festgestellt und senden nun Informationen über diese Überlastsituation an das MV / LV SCADA-System (1), damit letztendlich die Überlastsituation durch die Abregelung von Lasten, in diesem Fall von einem virtuellen Kraftwerk (VK) aufgelöst wird. Das MV / LV SCADA-System informiert das Distribution Management System (DMS) über die Überlastsituation und löst einen Alarm aus (2). Das DMS stellt nun eine Reduktionsanfrage an das DER-SCADA-System, damit die Energieversorgung gestoppt wird (3). Das DER-SCADA-System informiert das Energiemanagementsystem (EMS) über den Versorgungsstopp und übersendet entsprechende Abschaltinformationen (4). Das EMS muss nun einen neuen Versorgungszeitplan berechnen (5) und den entsprechend an das Energiedatenmanagementsystem (EDMS) weiterleiten (6). Wenn der neue Versorgungszeitplan berechnet und akzeptiert ist, wird vom EMS das Kommando zum Stoppen der Energieversorgung für das entsprechende VK an das DER-SCADA-System inkl. Abschaltbefehl gegeben (7). Das DER-SCADA-System gibt nun den Abschaltbefehl an das DER-Gateway weiter (8). Das Stop-Kommando inkl. Abschaltbefehl wird dann an das Device Energy Management (DEM) weitergeleitet, das dann das komplette VK oder einzelne Lasten des VKs abregelt (9). Zusätzlich wird, um Systeme im Umfeld der entsprechenden DERs, die das Smart Metering und Smart Home managen, zu informieren, vom DER-SCADA-System zunächst das Externe Smart Meter Gateway (SMGW) (10), dann das Internet SMGW (11) und letztendlich das Kundenenergiemanagement (12) über den Versorgungsstop informiert und dabei die entsprechenden Abschaltinformationen und relevante Messwerte mitgesendet.

Die Abschnitte 1.5 bis 1.8 („1.5 Key performance indicators (KPI)", „1.6 Use Case conditions", „1.7 Further information ..." und „1.8 General remarks") wurden an dieser Stelle nicht aufgeführt, zum einen aus Platzgründen und zum anderen da sie für diesen Beitrag keine Relevanz haben.

7.1.2 UC-Template Abschnitt „2 – Diagrams of use case“



7.1.3 UC-Template Abschnitt „3 – Technical details“

7.1.3.1 UC-Template Abschnitt „3.1 – Actors“

Actors			
Actor name	**Actor type**	**Actor description**	**Further information specific to this use case**
Netzsensor	Sensor	Netzsensoren geben Netzinformationen zurück, indem sie physikalische Phänomene im Netz messen.	
MV / LV SCADA-System	SCADA-System	SCADA steht für Supervisory Control And Data Acquisition, also eine übergeordnete Steuerung und Datenerfassung. Hier handelt es sich um ein SCADA-System für die Mittel- und Niederspannung bzw. für die Betreiber der Mittel- und Niederspannung.	

Tabelle wird auf der nächsten Seite fortgesetzt →

Actors			
Distribution Management System (DMS)	Management-system	Beim DMS (Distribution Management System, also ein Managementsystem für den Betrieb des Verteilnetzes) handelt es sich um ein IT-System für Versorger, das in der Lage ist, Informationen über das Stromverteilungssystem in Echtzeit oder nahezu in Echtzeit zu verwalten, zu steuern, zu visualisieren, zu optimieren und zu automatisieren. Das DMS kann den Betreibern auch ermöglichen, komplexe Dienste für das Verteilnetz zu planen und auszuführen, um die Systemeffizienz zu erhöhen, den Leistungsfluss zu optimieren und Überlastungen zu verhindern.	
DER-SCADA-System	SCADA-System	DER-SCADA-Systeme (DER = Dezentrale Energieressource, SCADA = Supervisory Control And Data Acquisition) sind Überwachungs- und Steuerungssysteme für Erzeuger von dezentralen Energieressourcen auf der Mittelspannungsebene, dies können bspw. auch Virtuelle Kraftwerke sein.	
Energy Management System (EMS)	Management-system	Ein Energiemanagementsystem dient den Stromnetzbetreibern zur Überwachung, Steuerung und Optimierung der Leistung bei der Erzeugung und / oder der Übertragung im Stromnetz.	
Energy Data Management System (EDMS)	Management-system	Das EDMS ist ein System, das das Energiedaten (z. B. Daten des EMS) speichert und entsprechend autorisierten Systemen zur Verfügung stellt.	
DER-Gateway	Gateway	Das DER-Gateway fungiert als Kommunikationsgateway zwischen dem Energiemanagementsystem und dem DER-SCADA-System.	
Device Energy Management (DEM)	Management-system	Das DEM steuert die DER-Geräte, um zu gewährleisten, dass die geforderte Produktion eingehalten wird.	
Externes Smart Metering Gateway	Gateway	Das Externe Smart Metering Gateway erfüllt Kommunikationsfunktionen zwischen dem Smart Grid-Bereich und dem Smart Metering.	
Internes Smart Metering Gateway	Gateway	Das Interne Smart Metering Gateway erfüllt Kommunikationsfunktionen zwischen dem Smart Metering und dem Smart Home.	
Kunden Energy Management (KEM)	Management-system	Das KEM erfüllt Funktionen, die es ermöglichen, koordinierte Energiemanagementstrategien für eine oder mehrere zusammengehörige DEM in Abhängigkeit von Messdaten, Preisanreizen, Flexibilitätsanforderungen und zusätzlichen Informationen aus anderen Kanälen wie dem Internet zu definieren.	

Abschnitt 3.2 „References“ wird hier aufgrund der Nichtrelevanz für diesen Beitrag und aus Platzgründen nicht aufgeführt.

7.1.4 UC-Template Abschnitt „4 – Step by step analysis of use case"

7.1.4.1 UC-Template Abschnitt „4.1 – Overview of scenarios"

Scenario conditions						
No.	Scenario name	Scenario description	Primary actor	Triggering event	Pre-condition	Post-condition
1	Überlast-szenario	Es findet innerhalb eines Virtuellen Kraftwerks eine Überlastsituation statt	Netzsensor	Messung von Überlast	Eine Überlast-situation ist aufgetreten.	Das virtuelle Kraftwerk wurde abgeschaltet.

7.1.4.2 UC-Template Abschnitt „4.2 – Steps – Scenarios"

Scenario								
Scenario Name: Überlastszenario								
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information producer (actor)	Information receiver (actor)	IDs*	Require-ments R-ID
1		Überlast-situation feststellen	Ein Sensor misst den Überlastzustand im Netz und leitet ihn an das MV / LV SCADA-System weiter.	CREATE	Netzsensor	MV / LV SCADA-System	001	
2		Über Überlast-situation informie-ren	Das MV / LV SCADA-System informiert das DMS mit einen Alarm über die Netzüberlastung.	FOR-WARD	MV / LV SCADA-System	Distribution Management System (DMS)	002	Kommuni-kation (001)
3		Anfrage Energie-versorgung stoppen	Das DMS fordert das DER-SCADA-System auf, die DER-Ener-gieproduktion zu reduzieren.	CREATE	Distribution Management System (DMS)	DER-SCADA-System	003	Kommuni-kation(002) Kommuni-kation(003)
4		Über Versor-gungsstop informie-ren	Das DER-SCADA-System informiert das EMS über die Abschaltung.	INFORM	DER-SCADA-System	Energiema-nagement-system (EMS)	004	Kommuni-kation(004)

*Information exchanged (IDs)

Tabelle wird auf der nächsten Seite fortgesetzt →

Scenario								
Scenario Name: Überlastszenario								
5		Versorgungszeitplan berechnen	Das EMS berechnet einen neuen Zeitplan.	CALCULATE	EMS	EMS	005	Kommunikation (005)
6		Versorgungszeitplan weiterleiten	EMS leitet den neuen Zeitplan an EDMS weiter.	FORWARD	EMS	Energiedatenmanagementsystem (EDMS)	006	Kommunikation (006) Kommunikation (007)
7		Kommando zum Stoppen der Energieversorgung	Das EMS gibt den Befehl an das DER-SCADA-System die DERs abzuschalten.	COMMAND	EMS	DER-SCADA-System	007	Kommunikation (008)
8		Weiterleitung des Stopp-Kommandos	Das DER-SCADA-System leitet den Abschaltbefehl an das DER-Gateway weiter.	FORWARD	DER-SCADA-System	DER-Gateway	008	
9		Befehl zum Ausschalten	Das DER-Gateway gibt den Befehl dass das DEM die DERs abschalten soll.	COMMAND	DER-Gateway	Device-Energiemanagement (DEM)	009	Kommunikation (009)
10		Weiterleiten des Abschaltbefehls	Das DER-SCADA-System leitet den Abschaltbefehl an das externe Smart Meter Gateway weiter.	FORWARD	DER-SCADA-System	Externes Smart Metering Gateway	010	Kommunikation (010) Kommunikation (011)
11		Weiterleiten des Abschaltbefehls	Das externe Smart Meter Gateway leitet den Abschaltbefehl an das interne Smart Meter Gateway weiter.	FORWARD	Externes Smart Metering Gateway	Internes Smart Metering Gateway	011	
12		Befehl zum Ausschalten	Das interne Smart Meter Gateway gibt dem Kunden-Energiemanagement den Abschaltbefehl.	COMMAND	Internes Smart Metering Gateway	Kunden Energy Management (KEM)	012	Kommunikation (012)

7.1.5 UC-Template Abschnitt „5 – Information exchanged“

Information Exchanged			
Information exchanged ID	Name of information exchanged	Description of information exchanged	Requirements IDs
001	Informationen zur Überlastsituation	Informationen zur Überlastsituation	↳ SBK_Verfügbarkeit_Hoch (102) ↳ SBK_Integrität_Hoch (202) ↳ SBK_Vertraulichkeit_Normal (301)
002	Alarm	Alarm	↳ SBK_Verfügbarkeit_Hoch (102) ↳ SBK_Integrität_Hoch (202) ↳ SBK_Vertraulichkeit_Normal (301)
003	Reduktionsanfrage	Anfrage zur Reduzierung / Abschaltung der Erzeugung	↳ SBK_Verfügbarkeit_Hoch (102) ↳ SBK_Integrität_Hoch (202) ↳ SBK_Vertraulichkeit_Normal (301)
004	Abschaltinformationen	Abschaltinformationen	↳ SBK_Verfügbarkeit_Normal (101) ↳ SBK_Integrität_Normal (201) ↳ SBK_Vertraulichkeit_Normal (301)
005	Aktualisierter Versorgungszeitplan	Aktualisierter Versorgungszeitplan für die Erzeuger	↳ SBK_Verfügbarkeit_Normal (101) ↳ SBK_Integrität_Normal (201) ↳ SBK_Vertraulichkeit_Normal (301)
006	Abschaltbefehl	Abschaltbefehl	↳ SBK_Verfügbarkeit_Hoch (102) ↳ SBK_Integrität_Hoch (202) ↳ SBK_Vertraulichkeit_Normal (301)
007	Abschaltbefehl	Abschaltbefehl	↳ •SBK_Verfügbarkeit_Hoch (102) ↳ SBK_Integrität_Hoch (202) ↳ SBK_Vertraulichkeit_Normal (301)
008	Abschaltbefehl	Abschaltbefehl	↳ SBK_Verfügbarkeit_Hoch (102) ↳ SBK_Integrität_Hoch (202) ↳ SBK_Vertraulichkeit_Normal (301)

Tabelle wird auf der nächsten Seite fortgesetzt →

Information Exchanged			
009	Abschaltbefehl	Abschaltbefehl	↳ SBK_Verfügbarkeit_Hoch (102) ↳ SBK_Integrität_Hoch (202) ↳ SBK_Vertraulichkeit_Normal (301)
010	Abschaltbefehl	Abschaltbefehl	↳ SBK_Verfügbarkeit_Hoch (102) ↳ SBK_Integrität_Hoch (202) ↳ SBK_Vertraulichkeit_Normal (301)
011	Abschaltbefehl	Abschaltbefehl	↳ SBK_Verfügbarkeit_Hoch (102) ↳ SBK_Integrität_Hoch (202) ↳ SBK_Vertraulichkeit_Normal (301)
012	Messdaten	Messdaten	↳ SBK_Verfügbarkeit_Normal (101) ↳ SBK_Integrität_Hoch (202) ↳ SBK_Vertraulichkeit_Hoch (302)

7.1.6 UC-Template Abschnitt „6 – Requirements (optional)“

7.1.6.1 Kommunikation

Im Folgenden werden die in diesem Use Case Szenario verwendeten Kommunikationskanäle aufgelistet und beschrieben.

Categories ID	Category name for requirements	Category description
Kommunikation	Kommunikations-kanäle	Geräte und Netzwerke über die kommuniziert wird.
Requirement ID	**Requirement name**	**Requirement description**
Kommunikation (001)	Backhaulnetzwerk des Netzwerk-betreibers	Kommunikationsnetzwerk für die Netzautomatisierung
Kommunikation (002)	Intra-center Integration Bus	Kommunikations-Hub in einem Kontrollzentrum für den Betrieb der Energieversorgungs-Infrastruktur.
Kommunikation (003)	Backbonenetzwerk	Öffentliches Kommunikationsnetzwerk, auch Internet genannt.
Kommunikation (004)	Intra-center Integration Bus	Kommunikations-Hub in einem Kontrollzentrum für den Betrieb der Energieversorgungs-Infrastruktur.

Tabelle wird auf der nächsten Seite fortgesetzt →

Kommunikation (005)	Intra-center Integration Bus	Kommunikations-Hub in einem Kontrollzentrum für den Betrieb der Energieversorgungs-Infrastruktur.
Kommunikation (006)	Intra-center Integration Bus	Kommunikations-Hub in einem Kontrollzentrum für den Betrieb der Energieversorgungs-Infrastruktur.
Kommunikation (007)	Backbonenetzwerk	Öffentliches Kommunikationsnetzwerk, auch Internet genannt.
Kommunikation (008)	Intra-center Integration Bus	Kommunikations-Hub in einem Kontrollzentrum für den Betrieb der Energieversorgungs-Infrastruktur.
Kommunikation (009)	DER Integration Bus	Kommunikations-Hub in einem DER-System.
Kommunikation (010)	AMI Backhaul Netzwerk	Kommunikationsnetzwerk für die automatisierte Zählerinfrastruktur.
Kommunikation (011)	Backbonenetzwerk	Öffentliches Kommunikationsnetzwerk, auch Internet genannt.
Kommunikation (012)	Direktverbindung per Kabel	Punkt-zu-Punkt-Verbindung per Kabel zwischen zwei Geräten oder einem Gerät und einem Sensor.

7.1.6.2 Schutzbedarfskategorien

Im Folgenden werden die Schutzbedarfskategorien für die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit jeweils mit den Stufen normal, hoch und sehr hoch.

7.1.6.2.1 Verfügbarkeit

Requirements (optional)		
Categories ID	**Category name for requirements**	**Category description**
SBK_Verfügbarkeit	Schutzbedarfskategorie Verfügbarkeit	Schutzbedarfskategorien für das Schutzziel Verfügbarkeit, unterteilt in normal, hoch und sehr hoch.
Requirement ID	**Requirement name**	**Requirement description**
SBK_Verfügbarkeit_ Normal (101)	Normales Sicherheits-niveau für die Verfügbarkeit	Längere Ausfallzeiten, die zu Terminüberschreitungen führen, können nicht toleriert werden. Generell gilt: Die Folge eines Schadens ist eine Störung der Organisation.
SBK_Verfügbarkeit_ Hoch (102)	Hohes Sicherheitsniveau für die Verfügbarkeit	In zentralen Bereichen der Organisation werden zeitkritische Prozesse durchgeführt bzw. große Massen produziert, die ohne den Einsatz von IT nicht erledigt werden könnten. Nur sehr kurze Ausfallzeiten sind akzeptabel. Im Allgemeinen gilt Folgendes: Im Schadensfall können wichtige Bereiche der Organisation nicht mehr funktionieren; die Folge eines Schadens ist eine erhebliche Störung der Organisation oder betroffener Dritter.

Tabelle wird auf der nächsten Seite fortgesetzt →

Requirements (optional)		
SBK_Verfügbarkeit_ SehrHoch (103)	Sehr hohes Sicherheits-niveau für die Verfügbar-keit	In zentralen Bereichen der Organisation behandelt hauptsäch-lich zeitkritische Prozesse bzw. sehr große Massen produziert, die ohne den Einsatz von IT nicht erledigt werden könnten. Ausfallzeiten müssen schnellstmöglich behoben werden. Im Allgemeinen gilt Folgendes: Die Schadensauswirkungen können für die Organisation ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

7.1.6.2.2 Integrität

Categories ID	Category name for requirements	Category description
SBK_Integrität	Schutzbedarfskategorie Integrität	Schutzbedarfskategorien für das Schutzziel Integrität, unterteilt in normal, hoch und sehr hoch.
Requirement ID	**Requirement name**	**Requirement description**
SBK_Integrität_ Normal (201)	Normales Sicherheits-niveau für die Integrität	Die Informationen sollten korrekt sein. Kleinere Fehler können toleriert werden. Fehler, die die Zielerreichung wesentlich beeinträchtigen, müssen organisiert oder vermeidbar sein. Generell gilt: Die Folge eines Schadens ist eine Störung der Organisation.
SBK_Integrität _ Hoch (202)	Hohes Sicherheitsniveau für die Integrität	Die verarbeiteten Informationen sollten korrekt sein; etwaige Fehler sollten erkennbar und vermeidbar sein. Im Allgemeinen gilt Folgendes: Im Schadensfall können wichtige Bereiche der Organisation nicht mehr funktionieren; die Folge eines Schadens ist eine erhebliche Störung der Organisation oder betroffener Dritter.
SBK_Integrität _ SehrHoch (203)	Sehr hohes Sicherheits-niveau für die Integrität	Die verarbeiteten Informationen müssen korrekt sein; etwaige Fehler müssen erkennbar und vermeidbar sein. Fehler müssen schnellstmöglich behoben werden. Im Allgemeinen gilt Folgendes: Die Schadensauswirkungen können für die Organisation ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

7.1.6.2.3 Vertraulichkeit

Categories ID	Category name for requirements	Category description
SBK_Vertraulichkeit	Schutzbedarfskategorie Vertraulichkeit	Schutzbedarfskategorien für das Schutzziel Vertraulichkeit, unterteilt in normal, hoch und sehr hoch.

Requirement	Requirement name	Requirement description
SBK_Vertraulichkeit_ Hoch (302)	Hohes Sicherheitsniveau für die Vertraulichkeit	Der Schutz von Informationen, die nur für den internen Gebrauch bestimmt sind, muss gewährleistet sein. Der Schutz der persönlichen Daten muss gewährleistet sein. Andernfalls besteht die Gefahr, dass die soziale oder finanzielle Situation der Betroffenen beeinträchtigt wird. Generell gilt: Die Folge eines Schadens ist eine Störung der Organisation.
SBK_Vertraulichkeit_ Hoch (302)	Hohes Sicherheitsniveau für die Vertraulichkeit	Der Schutz vertraulicher Informationen muss gewährleistet sein und in kritischen Bereichen strenge Geheimhaltungsanforderungen erfüllen. Der Schutz der persönlichen Daten muss hohen Anforderungen genügen. Andernfalls besteht die Gefahr, dass die soziale oder finanzielle Situation der Betroffenen stark beeinträchtigt wird. Im Allgemeinen gilt Folgendes: Im Schadensfall können wichtige Bereiche der Organisation nicht mehr funktionieren; die Folge eines Schadens ist eine erhebliche Störung der Organisation oder betroffener Dritter.
SBK_Vertraulichkeit _ SehrHoch (303)	Sehr hohes Sicherheitsniveau für die Vertraulichkeit	Der Schutz vertraulicher Informationen muss gewährleistet sein und in kritischen Bereichen sehr strenge Geheimhaltungsanforderungen erfüllen. Der Schutz der persönlichen Daten muss sehr hohen Anforderungen genügen. Andernfalls besteht die Gefahr, dass die soziale oder finanzielle Situation der Betroffenen sehr stark beeinträchtigt wird. Im Allgemeinen gilt Folgendes: Die Schadensauswirkungen können für die Organisation ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Die Abschnitte 7 „Common Terms and Definitions“ und 8 „Custom information (optional)“ wurden aufgrund der Nichtrelevanz für diesen Beitrag und aus Platzgründen nicht aufgeführt.

7.2 Bedrohungsszenarien für UC1 mit dem Misuse Case Template

In diesem Abschnitt werden Angriffsszenarien für den Use Case UC1 mit dem Misuse Case Template, das in Abschnitt 4.3 erläutert wurde, beschrieben. Da dieses Template ebenfalls üblicherweise im Querformat verwendet wird, ist auch dieser Abschnitt im Querformat gehalten.

7.2.1 MUC-Template Abschnitt „1 – Description of the misuse case”

7.2.1.1 MUC-Template Abschnitt „1.1 – Name of misuse case”

Misuse case identification		
ID	Area Domain(s) / Zone(s)	Name of misuse case
MUC1		Beispielhafte Bedrohungen für ein Virtuelles Kraftwerk aus UC1

7.2.1.2 MUC-Template Abschnitt „1.2 – Version management“

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.5	09.03.2020	Christine Rosinger, OFFIS	Erster Entwurf	Draft
0.9	17.07.2020	Christine Rosinger, OFFIS	Vorversion	
1.0	01.10.2020	Christine Rosinger, OFFIS	Vervollständigung der Vorversion	Finale Version

7.2.1.3 MUC-Template Abschnitt „1.3 – Scope and objectives of misuse case”

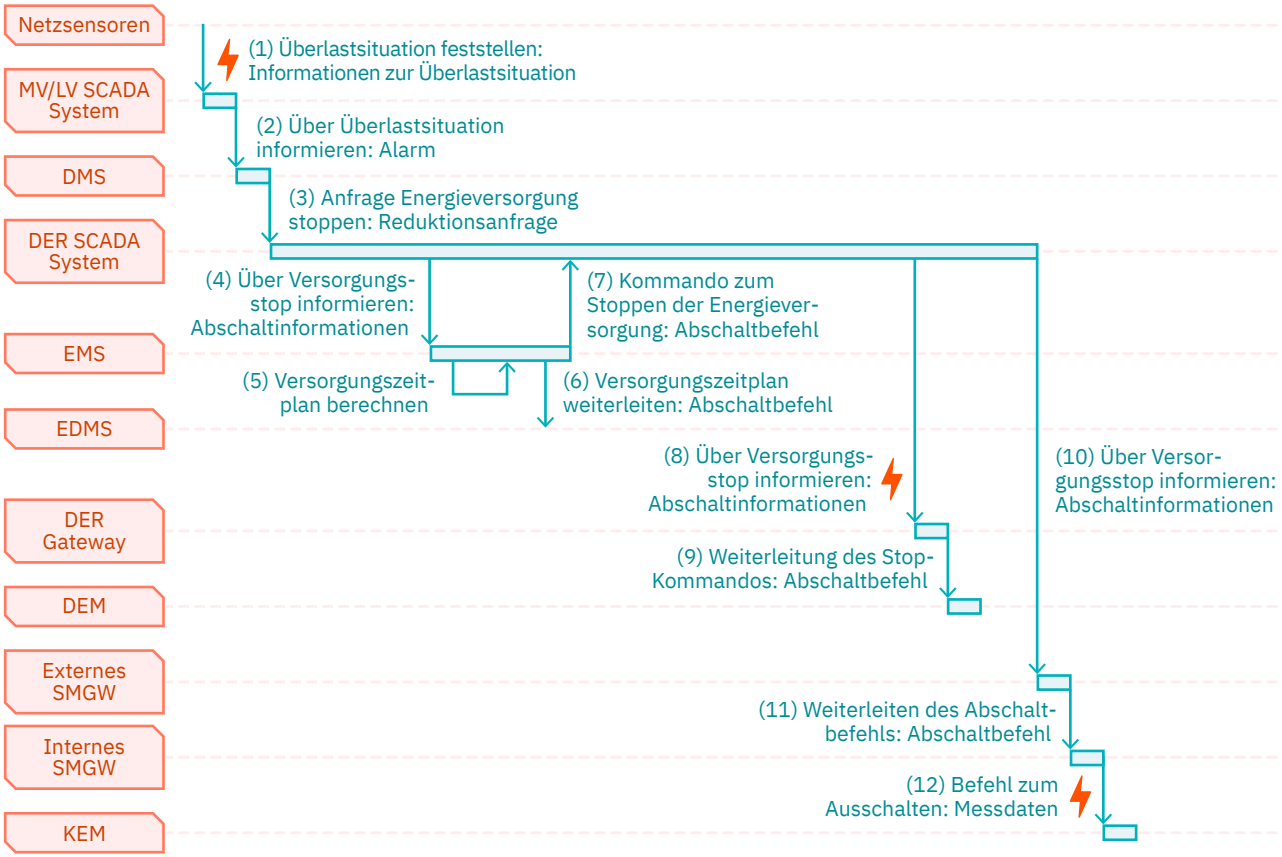
Scope and objectives of misuse case	
Scope	Bei diesem Misuse Case handelt es sich drei verschiedene Angriffe auf den Use Case UC1, so dass unterschiedliche Angriffsszenarien auf die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit abgedeckt werden.
Objective(s)	Ein Angreifer kann die Kommunikationsverbindung von zwei Akteuren abhören, verfälschen oder unterbrechen und bedroht damit die Ziele Vertraulichkeit, Integrität und Verfügbarkeit.
Related business case(s)	-

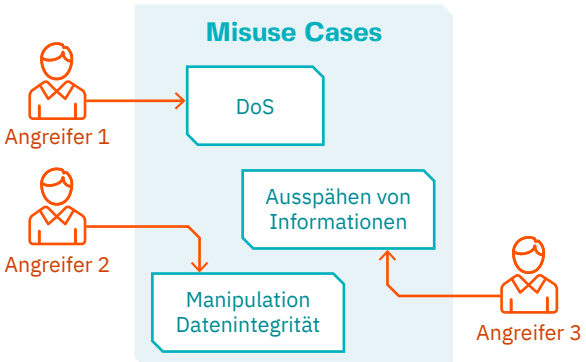
7.2.1.4 MUC-Template Abschnitt „1.4 – Narrative and condition of misuse case”

Narrative of use case
Short description
Drei verschiedene Angreifer starten einen Angriff auf den Anwendungsfall UC1 „Virtuelles Kraftwerk“.
Complete description
Es gibt drei verschiedene Angreifer, die je eins der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit angreifen. Die Angriffe werden im Rahmen des oben beschriebenen Anwendungsfalls zum Virtuellen Kraftwerk durchgeführt. Zu sehen sind die Angriffe in dem unten angefügten Sequenzdiagramm. Die roten Blitze symbolisieren dabei die drei möglichen Angriffe. Der erste rote Blitz symbolisiert einen Angriff auf die Verfügbarkeit des MV / LV SCADA-Systems mittels Denial of Service-Angriff (DoS), so dass die Steuerung in der Mittel- / Niederspannungsebene gestört wird. Der zweite rote Blitz symbolisiert einen Angriff auf Schritt 8 des Anwendungsfalls. Der Angriff erfolgt hier auf die Integrität der Informationsübermittlung, so dass die übermittelten Informationen verfälscht werden. In diesem Fall werden die Abschaltinformationen unterschlagen und stattdessen wird die entsprechende Anlage hochgeregelt, was dann zu Unterspannung im Stromnetz führt. Der dritte rote Blitz symbolisiert einen Angriff auf Schritt 12 des Anwendungsfalls. Der Angriff erfolgt hier auf die Vertraulichkeit der Informationsübermittlung. Der Angreifer hört Informationen (Messwerte etc.) mit bzw. spioniert sie aus und kann diese Informationen später selbst für die eigene Geschäftsstrategie nutzen.

Für diesen Misuse Case sind keine Voraussetzungen notwendig und es wurden auch keine Annahmen getroffen, daher wird der folgende Abschnitt „1.5 Misuse case conditions“ hier nicht aufgeführt. Auch die Abschnitte „1.6 Further information to the misuse case for classification / mapping” und „1.7 General remarks” sind nicht notwendig und wurden daher ausgespart.

7.2.2 MUC-Template Abschnitt „2 – Diagrams of misuse case“





7.2.3 MUC-Template Abschnitt „3 – Technical details"

7.2.3.1 MUC-Template Abschnitt „3.1 – Actor and Mis-Actor Profiles"

Die Akteure des Anwendungsfalls können dem UC-Template in Abschnitt 10.1 entnommen werden, daher wird die Tabelle mit den Akteuren hier nicht nochmal aufgeführt.

Mis Actors						
Grouping	Angreifer					
Group description	Die Angreifer, die das System angreifen wollen.					
Misactor name	Misactor type	Misactor Relationship	Misactor description	Intention / Motivation	Capability	Further information specific to this misuse case
Angreifer1	Menschlich (bösartig)	Extern	Angreifer, der einen DoS-Angriff ausführt.	↳ Vandalismus ↳ Cyber Hacker: Anerkennung, Spaß an der Technik, Herausforderung ↳ Konkurrenzsituation	Hackerkompetenz vorhanden	
Angreifer2	Menschlich (bösartig)	Intern	Angreifer mit Insiderwissen, der eine Datenmanipulation durchführt.	↳ Rache	Insiderwissen mit vollem Zugang zum System vorhanden.	↳ Unzufriedener Arbeitnehmer ↳ Gekündigter Arbeitnehmer
Angreifer3	Menschlich (bösartig)	Extern	Angreifer, der Informationen ausspäht.	↳ Diebstahl ↳ Bereicherung ↳ Schaden für andere	Hackerkompetenz vorhanden	

Der Abschnitt 3.2 „References" wird hier aus Platzgründen nicht aufgeführt und da er nicht für diesen Beitrag relevant ist.

7.2.4 MUC-Template Abschnitt „4 – Step by step analysis of misuse case"

Abschnitt 4.1 des Misuse Case-Templates umfasst und beschreibt Fehlerszenarien, die bspw. durch Fehler in der Programmierung entstanden sind. Diese Fehlerszenarien können bspw. von Angreifern ausgenutzt werden, um das entsprechende System anzugreifen. In diesem Misuse Case werden die Gefährdungen allerdings nicht durch Fehlerszenarien ausgelöst, so dass hier der Abschnitt 4.1 nicht aufgeführt wird.

7.2.4.1 MUC-Template Abschnitt „4.2 – General/Specific attack scenarios"

Attack Scenario Conditions						
Attack Scenario No.	Attack type	Attack target	Domains and Mechanism of Attack (CAPEC) / BSI Elem. Gefährdungen	Relevant Scenario No.	Likelihood (normal, hoch, sehr hoch)	Impact (Niedrig, Mittel, Hoch)
A1	Denial of Service-Angriff (DoS)	MV / LV SCADA-System	↳ Sniffing-Angriff (CAPEC-157) • BSI G 0.14 Ausspähen von Informationen (Spionage) ↳ Flooding (CAPEC-125) • BSI G 0.40 Verhinderung von Diensten (Denial of Service)	-	Hoch	Mittel
A2	Manipulation der Datenintegrität	DER-SCADA-System, DER-Gateway	↳ Content-Spoofing (CAPEC-148) • BSI G 0.22 Manipulation von Informationen		Hoch	Niedrig
A3	Ausspähen von Informationen	Internes SMGW, KEM	↳ Man-in-the-middle (CAPEC-94) • G 0.43 Einspielen von Nachrichten ↳ Sniffing-Angriff (CAPEC-157) • BSI G 0.14 Ausspähen von Informationen (Spionage)	-	Hoch	Niedrig

Tabelle wird auf den nächsten Seiten fortgesetzt →

Step No.	Name of process/ activity	Event	Description of process/ activity	Step of the Attack Scenario	CIA Threat	Requirements R-ID
A1-1	Aus-spähen	BSI G 0.14	Angreifer1 spioniert MV / LV SCADA-System aus, indem er einen Sniffing-Angriff (CAPEC-157) durch-führt, um es später mittels DoS-Angriff zu attackieren.	A-01	Vertrau-lichkeit	ORP.1, ORP.2, ORP.3, ORP.4, CON.1, CON.8, CON.9, OPS.1.1.2, OPS.1.1.4, OPS.1.1.5, OPS.1.1.6, OPS.1.2.4, OPS.1.2.5, OPS.2.1, OPS.2.2, OPS.3.1, DER.2.3, APP.1.2, APP.2.1, APP.2.2, APP.3.3, APP.4.3, SYS.1.1, SYS.2.1, SYS.3.1, SYS.3.2.1, SYS.3.2.2, SYS.3.2.3, SYS.3.2.4, SYS.3.3, SYS.4.4, SYS.4.5, IND.1, IND.2.1, IND.2.2, IND.2.3, IND.2.4, IND.2.7, NET.1.2, NET.3.1, NET.3.2, NET.3.3, NET.4.1, INF.7, INF.8, INF.9, INF.10
A1-2	DoS-Angriff	BSI G 0.40	Da das MV / LV SCADA-System den typischen Datenver-kehr nicht überwacht, kann Angreifer1 diese gefundene Schwach-stellen für den DoS-Angriff nutzen, bspw. mittels Flooding (CAPEC-125), um eine Ressourcenüber-lastung zu erwirken.	A-01	Verfüg-barkeit	CON.8, OPS.1.1.3, OPS.1.1.5, OPS.1.2.4, OPS.1.2.5, OPS.2.2, DER.1, DER.2.3, APP.1.2, APP.2.1, APP.2.2, APP.3.1, APP.3.2, APP.3.6, APP.4.3, APP.5.1, SYS.1.1, SYS.1.5, SYS.1.8, SYS.2.1, SYS.4.4, IND.2.1, NET.1.1, NET.1.2, NET.3.1, NET.3.2, NET.3.3, NET.4.2.
A2-1	Content Spoofing	BSI G 0.22	Angreifer2 ist ein unzufriedener Arbeit-nehmer des Betreibers mit Insiderinforma-tionen und Zugriff auf das System. Der Angreifer nutzt Content-Spoofing (CAPEC-148), um die Information über den Abschaltbefehl zu manipulieren und stattdessen die DER-Anlagen hoch-zuregeln. Damit werden weitere Probleme verursacht, die dem Betreiber schaden.	A-02	Inte-grität	ORP.1, ORP.2, ORP.4, CON.1, CON.3, CON.4, CON.8, CON.9, OPS.1.1.2, OPS.1.1.5, OPS.1.2.2, OPS.1.2.4, OPS.1.2.5, OPS.2.1, OPS.2.2, OPS.3.1, DER.1, DER.2.1, DER.2.2, DER.2.3, APP.1.1, APP.1.2, APP.2.1, APP.2.2, APP.2.3, APP.3.1, APP.3.2, APP.3.6, APP.4.2, APP.4.3, APP.4.6, APP.5.2, SYS.1.1, SYS.1.2.2, SYS.1.3, SYS.1.5, SYS.1.7, SYS.1.8, SYS.2.1, SYS.2.2.2, SYS.2.3, SYS.3.1, SYS.3.2.1, SYS.3.2.2, SYS.3.2.3, SYS.3.3, SYS.4.1, SYS.4.3, SYS.4.5, IND.2.1, IND.2.2, IND.2.4, NET.1.1, NET.1.2, NET.3.1, NET.3.2, NET.3.3, NET.4.3, INF.7, INF.8, INF.9.

A3-1	Man-in-the-middle (MITM) Angriff	G 0.43	Angreifer3 schaltet sich als Man-in-the-middle (MITM) zwischen das Interne SMGW und das KEM (CAPEC-94).	A-03	Vertrau-lichkeit	DER.2.3, APP.2.1, APP.2.2, APP.2.3, APP.3.1, APP.3.6, APP.4.3, SYS.1.1, SYS.1.5, SYS.2.1, SYS.3.2.1, IND.2.1, NET.1.1, NET.1.2, NET.3.1, NET.3.2, NET.3.3
A3-2	Ausspä-hen	BSI G 0.14	Angreifer3 hört die Kommunikation zwischen dem Internen SMGW und dem KEM mittels Sniffing-Angriff (CAPEC-157) mit. Später leitet er aus den ausgespähten Daten für seine eigene Geschäftsstrategie neue Erkenntnisse ab.	A-03	Vertrau-lichkeit	Siehe Sniffing-Angriff A1 1, weiter oben.

7.2.4.2 MUC-Template Abschnitt „4.3 – Overview of Capture point (optional)"

Capture Point - Scenarios			
Step No.	Description of the capture point	Attack Step No.	Role-Based Access control (RBAC) information

7.2.5 MUC-Template Abschnitt „5 – Requirements"

Requirements		
Categories ID	Category name for requirements	Category description
SecReq	Sicherheitsanforderungen (Security Requirements)	Sicherheitsanforderungen, nach den Bausteinen des BSI IT-Grund-schutz-Kompendiums, die in dem entsprechenden Schritten umgesetzt sein sollten, um die entsprechende Gefährdung zu vermeiden.

Tabelle wird auf den nächsten Seiten fortgesetzt →

Requirement ID	Requirement name	Requirement description
ISMS	**Sicherheits-management**	
ISMS.1	Sicherheits-management	„Mit (Informations-)Sicherheitsmanagement wird die Planungs-, Lenkungs- und Kontrollaufgabe bezeichnet, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen. Ein funktionierendes Sicherheitsmanagement muss in die existierenden Managementstrukturen jeder Institution eingebettet werden. Daher ist es praktisch nicht möglich, eine für jede Institution unmittelbar anwendbare Organisationsstruktur für das Sicherheitsmanagement anzugeben. Vielmehr werden häufig Anpassungen an spezifische Gegebenheiten erforderlich sein.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ISMS/ISMS_1_Sicherheitsmanagement.html.
ORP	**Organisation und Personal**	
ORP.1	Organisation	„Jede Institution benötigt für die Regelung und Steuerung des allgemeinen Betriebs, sowie für die Planung, Organisation und Durchführung aller Verwaltungsdienstleistungen, eine zuständige Dienststelle. Die meisten Institutionen haben hierfür eine Organisationseinheit, die dieses Zusammenspiel der verschiedenen Rollen und Einheiten mit den entsprechenden Geschäftsprozessen und Ressourcen steuert. Bereits auf dieser übergreifenden Ebene sind Aspekte der Informationssicherheit einzubringen und verbindlich festzulegen.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_1_Organisation.html.
ORP.2	Personal	„Das Personal eines Unternehmens bzw. einer Behörde hat einen entscheidenden Anteil am Erfolg oder Misserfolg einer Institution. Die Mitarbeiterinnen und Mitarbeiter haben dabei die wichtige Aufgabe, Informationssicherheit umzusetzen. So können die aufwendigsten Sicherheitsvorkehrungen ins Leere laufen, wenn sie im Arbeitsalltag nicht gelebt werden. Die elementare Bedeutung von Informationssicherheit für eine Institution und ihre Geschäftsprozesse muss daher für das Personal transparent und nachvollziehbar aufbereitet sein.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_2_Personal.html.
ORP.3	Sensibilisierung und Schulung	„Mitarbeiter sind ein wichtiger Erfolgsfaktor für ein hohes Maß an Informationssicherheit in einer Institution. Daher ist es wichtig, dass sie die Sicherheitsziele kennen, die Sicherheitsmaßnahmen verständlich sind und jeder einzelne Mitarbeiter bereit ist, diese umzusetzen. Die Voraussetzung dafür ist, dass es ein Sicherheitsbewusstsein innerhalb der Institution gibt. Darüber hinaus sollte eine Sicherheitskultur aufgebaut und im Arbeitsalltag mit Leben gefüllt werden. Mitarbeiter müssen für relevante Gefährdungen sensibilisiert werden und wissen, wie sich diese auf ihre Institution auswirken können. Ihnen muss bekannt sein, was von ihnen im Hinblick auf Informationssicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollen.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html.

ORP.4	Identitäts- und Berechtigungs-management	Der Zugang zu schützenswerten Ressourcen einer Institution ist auf berechtigte Benutzer und berechtigte IT-Komponenten einzuschränken. Benutzer und IT-Komponenten müssen zweifelsfrei identifiziert und authentisiert werden. Die Verwaltung der dafür notwendigen Informationen wird als Identitätsmanagement bezeichnet. Beim Berechtigungsmanagement geht es darum, ob und wie Benutzer oder IT-Komponenten auf Informationen oder Dienste zugreifen und diese benutzen dürfen, ihnen also basierend auf dem Benutzerprofil Zutritt, Zugang oder Zugriff zu gewähren oder zu verweigern ist. Berechtigungsmanagement bezeichnet die Prozesse, die für Zuweisung, Entzug und Kontrolle der Rechte erforderlich sind. Die Übergänge zwischen den beiden Begriffen sind fließend, daher wird in diesem Baustein der Begriff Identitäts- und Berechtigungsmanagement (englisch Identity and Access Management, IAM) benutzt. Zur besseren Verständlichkeit wird in diesem Baustein der Begriff "Benutzerkennung" bzw. "Kennung" synonym für "Benutzerkonto", "Login" und "Account" verwendet. In diesem Baustein wird der Begriff "Passwort" als allgemeine Bezeichnung für "Passphrase", "PIN" oder "Kennwort" verwendet. Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html.
ORP.5	Compliance Management (Anforderungs-management)	„In jeder Institution gibt es gesetzliche, vertragliche, strukturelle und interne Richtlinien und Vorgaben, die beachtet werden müssen. Viele dieser Vorgaben haben direkte oder indirekte Auswirkungen auf das Informationssicherheitsmanagement. Die Anforderungen unterscheiden sich dabei je nach Branche, Land und anderen Rahmenbedingungen. Darüber hinaus unterliegt beispielsweise eine Behörde anderen externen Regelungen als eine Aktiengesellschaft. Die Leitungsebene der Institution muss die Einhaltung der Anforderungen („Compliance“) durch angemessene Überwachungsmaßnahmen sicherstellen. Je nach Größe einer Institution kann diese verschiedene Managementprozesse haben, die sich mit unterschiedlichen Aspekten des Risikomanagements beschäftigen. Dazu zählen beispielsweise Informationssicherheitsmanagement, Datenschutzmanagement, Compliance Management und Controlling. Die verschiedenen Einheiten sollten vertrauensvoll zusammenarbeiten, um Synergieeffekte zu nutzen und Konflikte frühzeitig auszuräumen.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_5_Compliance_Management_(Anforderungsmanagement).html.

CON	Konzeption und Vorgehensweise	
CON.1	Kryptokonzept	„Die Verschlüsselung von Informationen ist ein weit verbreitetes Mittel, um die Informationssicherheit in den Schutzzielen Vertraulichkeit, Integrität und Authentizität zu gewährleisten. Mit Hilfe von kryptografischen Verfahren werden Informationen verschlüsselt, sodass deren Inhalt ohne den zugehörigen Schlüssel nicht lesbar ist. Dabei können symmetrische Verfahren, d.h. es wird der selbe Schlüssel zum Verschlüsseln und Entschlüsseln verwendet, sowie asymmetrische Verfahren, d.h. es wird ein Schlüssel zum Verschlüsseln und ein anderer Schlüssel zum Entschlüsseln verwendet, eingesetzt werden. In einer heterogenen Umgebung können dabei lokal gespeicherte Daten und auch die zu übertragenden Daten einer Institution wirkungsvoll durch kryptografische Verfahren und Techniken geschützt werden. Darüber hinaus werden weitergehende Maßnahmen auf organisatorischer und prozessualer Ebene benötigt. Der alleinige technische Einsatz von kryptografischen Verfahren genügt nicht, um die Vertraulichkeit, Integrität und Authentizität der verschlüsselten Informationen zu gewährleisten. Die Gesamtheit der eingesetzten kryptografischen Verfahren und damit verbundenen Maßnahmen wird im Rahmen eines Kryptokonzeptes gebündelt betrachtet. Nur durch eine ganzheitliche Betrachtung der Thematik wird ein effektiver Schutz durch Kryptografie ermöglicht. Eine Besonderheit stellen Kryptomodule dar, die für kryptografische Verfahren bei erhöhtem Schutzbedarf eingesetzt werden können. Mit einem Kryptomodul ist ein Produkt gemeint, das die im Kryptokonzept dargelegte Sicherheitsfunktion bietet. Ein solches Produkt kann dabei aus Hardware, Software, Firmware oder aus einer Kombination daraus bestehen. Hinzu kommen noch notwendige Bauteile wie Speicher, Prozessoren, Busse und die Stromversorgung, um die Kryptoprozesse umzusetzen. Ein Kryptomodul kann in unterschiedlichen IT- oder Telekommunikationssystemen verwendet werden, um sensible Daten bzw. Informationen zu schützen.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_1_Kryptokonzept.html.
CON.2	Datenschutz	„Aufgabe des Datenschutzes ist es, Personen davor zu schützen, dass sie durch die Nutzung ihrer personenbezogenen Daten durch Dritte in der Ausübung von Grundrechten beeinträchtigt werden. Das Grundgesetz für die Bundesrepublik Deutschland gewährleistet das Recht von Bürgerinnen und Bürgern, grundsätzlich selbst über die Verwendung ihrer personenbezogenen Daten zu bestimmen. Die Datenschutzgesetze des Bundes und der Bundesländer nehmen darauf Bezug, wenn sie den Schutz des Rechts auf informationelle Selbstbestimmung hervorheben. Die EU-Grundrechtecharta formuliert in Artikel 8 unmittelbar das Recht auf den Schutz personenbezogener Daten (Absatz 1), hebt die Notwendigkeit einer Rechtsgrundlage zur Datenverarbeitung hervor (Absatz 2) und schreibt die Überwachung der Einhaltung von Datenschutzvorschriften durch eine unabhängige Stelle vor (Absatz 3). Die Datenschutz-Grundverordnung (DSGVO) führt diese Anforderungen der Grundrechtecharta näher aus. Von zentraler Bedeutung ist dabei der Artikel 5 DSGVO, der die Grundsätze für die Verarbeitung personenbezogener Daten auflistet, die teilweise als Schutzziele ausgewiesen sind. Das Standard-Datenschutzmodell (SDM) bietet eine Methode, um diese geforderte Umsetzung von Datenschutzvorschriften auf der Grundlage von sieben Schutz- bzw. Gewährleistungszielen systematisch überwachen zu können.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_2_Datenschutz.html.

CON.3	Datensicherungskonzept	„Institutionen speichern immer mehr Daten und sind gleichzeitig immer stärker auf sie angewiesen. Gehen Daten verloren, z. B. durch defekte Hardware, Malware oder versehentliches Löschen, können gravierende Schäden entstehen. Durch regelmäßige Datensicherungen lassen sich solche Auswirkungen jedoch minimieren. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_3_Datensicherungskonzept.html.
CON.4	Auswahl und Einsatz von Standardsoftware	„Unter Standardsoftware wird Software verstanden, die auf dem Markt angeboten und in der Regel über den Fachhandel oder Onlineportale bezogen wird. Sie zeichnet sich dadurch aus, dass Institutionen sie selbst installieren und mit wenig Aufwand anpassen können. Hierbei muss auch die Informationssicherheit über den gesamten Lebenszyklus der Standardsoftware von der Planung bis zur Aussonderung hinweg berücksichtigt werden. So müssen Institutionen einen Anforderungskatalog für Standardsoftware erstellen, ein geeignetes Produkt auswählen und es sicher installieren. Außerdem müssen sie die Lizenzen geeignet verwalten und das Produkt auch wieder sicher deinstallieren können.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_4_Auswahl_und_Einsatz_von_Standardsoftware.html.
CON.5	Entwicklung und Einsatz von Individualsoftware	„Viele Institutionen stehen vor Herausforderungen, die sie nicht mehr hinreichend mit Standardsoftware lösen können. Die mit diesen Herausforderungen verbundenen Aufgabenstellungen bedürfen häufig Softwarelösungen, die auf die individuellen Bedürfnisse der Institutionen zugeschnitten sind, im Folgenden Individualsoftware genannt. Hierzu können einerseits Basislösungen, die aus einer Grundmenge an typischen Funktionen bestehen, eingesetzt und individualisiert werden. Die Grundfunktionen werden hierbei für den individuellen Einsatzzweck der Institution angepasst und um individuell benötigte Funktionen erweitert. Gängige Beispiele hierfür sind IT-Anwendungen wie ERP- (Enterprise Resource Planning), CMS- (Content Management Systeme) oder IDM-Systeme (Identity Management). Individualsoftware kann auch vollständig neu von der Institution selbst oder von Dritten entwickelt werden. Von essentieller Bedeutung ist es hierbei, dass bereits bei der Planung und Konzeptionierung der Individualsoftware auch die benötigten Sicherheitsfunktionen bedacht werden und die Informationssicherheit in dem gesamten Lebenszyklus der Individualsoftware berücksichtigt wird. Fehler in der Planung oder fehlende Sicherheitsfunktionen können im laufenden Betrieb nicht oder nur mit hohem zusätzlichen Aufwand ausgeglichen werden. Gängige Beispiele für Individualsoftware sind Anwendungen zur Geschäftsprozesssteuerung oder individuell angepasste Fachanwendungen, wie Personalverwaltungssoftware, Verfahren zur Verwaltung von Sozialdaten oder Meldedaten.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_5_Entwicklung_und_Einsatz_von_Individualsoftware.html.

CON.6	Löschen und Vernichten	„Damit Informationen nicht in falsche Hände geraten, ist eine geregelte Vorgehensweise erforderlich, um Daten und Datenträger vollständig und zuverlässig zu löschen oder zu vernichten. Dabei müssen schutzbedürftige Informationen, die auf analogen und digitalen Datenträgern gespeichert sind, berücksichtigt werden. Wenn nicht oder nur unzureichend gelöschte Datenträger weitergegeben, verkauft oder ausgesondert werden, können dadurch unbeabsichtigt schützenswerte Informationen in falsche Hände gelangen. Dadurch können erhebliche Schäden entstehen. Jede Institution muss deshalb eine Vorgehensweise zum sicheren Löschen und Vernichten von Informationen etablieren.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_6_L%C3%B6schen_und_Vernichten.html.
CON.8	Software-Entwicklung	„Institutionen stehen häufig vor Herausforderungen, die nicht mehr hinreichend mit Standardsoftware behandelt werden können. Nur durch individuell entwickelte bzw. angepasste Software, die auf die Anforderungen der Institution zugeschnitten ist, können diese Herausforderungen effektiv gelöst werden. Beispiele hierfür sind hochspezifische Software-Lösungen für Branchenspezialisten (wie zur Steuerung von Produktionsanlagen), an die eigenen Geschäftsprozesse angepasste IT-Anwendungen (wie Content-Management-Systeme oder Identity-Management-Systeme) oder Altsysteme, die angepasst werden müssen, jedoch nicht mehr vom ursprünglichen Hersteller weitergepflegt werden. Hierbei kann (Individual-) Software durch die Institution selbst oder von einem Dritten komplett neu entwickelt werden. Ebenso kann es erforderlich sein, eine Basis-Lösung an die eigenen Anforderungen anzupassen und durch zusätzliche individuelle Funktionen zu erweitern. In beiden Fällen nimmt die Software-Entwicklung eine zentrale Rolle ein, indem aus den Anforderungen der Institution ein Programm-Code entwickelt bzw. angepasst wird. Hierbei ist es von essentieller Bedeutung, dass die Informationssicherheit über den gesamten Software-Entwicklungsprozess hinweg berücksichtigt wird, da nur auf diese Weise die Informationssicherheit der zu entwickelnden Software-Lösung und im Rahmen des Entwicklungsprojektes selbst gewährleistet werden kann. Es ist in der Regel viel aufwändiger, wenn Informationssicherheit erst in einer späten Phase der Software-Entwicklung betrachtet wird. Außerdem besteht die Gefahr, dass bereits fertig entwickelte Bestandteile der Software angepasst oder neu entwickelt werden müssen.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_8_Software-Entwicklung.html.
CON.9	Informationsaustausch	„In diesem Baustein wird der sichere Austausch von Informationen betrachtet. Der Fokus liegt dabei weniger auf konkreten Datenträgern und Übertragungswegen, sondern auf konzeptionellen Vorgaben. Informationen können auf verschiedensten Wegen übermittelt werden. Neben der Übertragung über Datennetze oder mit Hilfe von Wechseldatenträgern können Informationen auch bei persönlichen Treffen, Telefonaten oder auf Papier ausgetauscht werden. Eine Institution muss sicherstellen, dass vertrauliche Informationen nicht an unberechtigte Empfänger weitergegeben werden. Falls Informationen an Dritte weitergegeben werden, muss die Institution regeln, unter welchen Bedingungen dies geschehen darf.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_9_Informationsaustausch.html.

OPS	Betrieb	
OPS1.1.2	Ordnungsgemäße IT-Administration	„Die fortlaufende Administration von IT-Systemen und -Komponenten ist für den IT-Betrieb grundlegend. Die Systemadministratoren richten dabei IT-Systeme und Anwendungen ein, beobachten den Betrieb und reagieren mit Maßnahmen, welche die Funktion und die Leistungsfähigkeit der IT-Systeme erhalten. Darüber hinaus passen sie die IT-Systeme an veränderte Bedürfnisse an. Dabei erfüllen Systemadministratoren auch eine Reihe von Aufgaben für die Sicherheit, sie sorgen nicht nur dafür, dass die IT-Systeme verfügbar bleiben, sondern setzen auch Sicherheitsmaßnahmen um und überprüfen, ob sie wirksam sind. Dazu verfügen sie über sehr weitreichende Berechtigungen, sodass es für die Sicherheit des Informationsverbunds auch sehr wichtig ist, die Systemadministration selbst vor unbefugten Zugriffen abzusichern.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_2_Ordnungsgem%C3%A4%C3%9Fe_IT-Administration.html.
OPS1.1.3	Patch- und Änderungsmanagement	„Die immer schnellere Entwicklung in der Informationstechnik und die steigenden Anforderungen der Benutzer stellen viele Behörden und Unternehmen vor große Herausforderungen. Eine davon ist die Aufgabe, die Komponenten ihrer Informationstechnik korrekt und zeitnah zu aktualisieren. Auch zeigt sich in der Praxis, dass vorhandene Sicherheitslücken oder Betriebsstörungen häufig auf mangelhafte oder fehlende Patches und Änderungen zurückzuführen sind. Ein fehlendes oder vernachlässigtes Patch- und Änderungsmanagement führt aber schnell zu Sicherheitslücken in den einzelnen Komponenten und damit zu möglichen Angriffspunkten. Aufgabe des Patch- und Änderungsmanagements ist es allgemein, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozesse und Verfahren steuer- und kontrollierbar zu gestalten.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_3_Patch-_und_%C3%84nderungsmanagement.html.

OPS1.1.4	Schutz vor Schadprogrammen	„Schadprogramme sind Programme, die in der Regel ohne Wissen und Einwilligung des Benutzers schädliche Funktionen auf einem IT-System ausführen. Diese Schadfunktionen können ein breites Feld abdecken, das von Spionage über Erpressung (sogenannte Ransomware) bis hin zur Sabotage und Zerstörung von Informationen oder gar Geräten reicht. Schadprogramme können grundsätzlich auf allen Betriebssystemen und IT-Systemen ausgeführt werden. Dazu gehören neben klassischen IT-Systemen wie Clients und Servern auch mobile Geräte wie Smartphones. Netzkomponenten, wie Router, Industriesteuerungsanlagen, und sogar IoT-Geräte, wie vernetzte Kameras, sind heutzutage ebenfalls vielfach durch Schadprogramme gefährdet. Schadprogramme verbreiten sich auf klassischen IT-Systemen zumeist über E-Mail-Anhänge, manipulierte Webseiten (Drive-by-Downloads) oder Datenträger. Smartphones werden in der Regel über die Installation von schädlichen Apps infiziert, auch Drive-by-Downloads sind möglich. Darüber hinaus sind offene Netzschnittstellen, fehlerhafte Konfigurationen und Softwareschwachstellen häufige Einfallstore auf allen IT-Systemen. In diesem Baustein wird der Begriff „Virenschutzprogramm“ verwendet. „Viren“ stehen dabei als Synonym für alle Arten von Schadprogrammen. Gemeint ist mit „Virenschutzprogramm“ demnach ein Programm zum Schutz vor jeglicher Art von Schadprogrammen.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_4_Schutz_vor_Schadprogrammen.html.
OPS1.1.5	Protokollierung	„Damit ein verlässlicher IT-Betrieb gewährleistet ist, sollten IT-Systeme und Anwendungen entweder alle oder zumindest ausgewählte betriebs- und sicherheitsrelevante Ereignisse protokollieren, d. h. sie automatisch speichern und für die Auswertung bereitstellen. Eine Protokollierung wird in vielen Institutionen eingesetzt, um Hard- und Softwareprobleme sowie Ressourcenengpässe rechtzeitig entdecken zu können. Aber auch Sicherheitsprobleme und Angriffe auf die betriebenen Netzdienste können anhand von Protokollierungsdaten nachvollzogen werden. Ebenso können mit solchen Daten durch forensische Untersuchungen Beweise gesichert werden, nachdem ein Angriff auf IT-Systeme bekannt wurde. In jedem Informationsverbund werden lokal Protokollierungsdaten von einer Vielzahl von IT-Systemen und Anwendungen generiert. Um jedoch einen Gesamtüberblick über einen Informationsverbund zu erhalten, können die von verschiedenen IT-Systemen und Anwendungen generierten Protokollinformationen an eine dedizierte Protokollierungsinfrastruktur gesendet und dort zentral gespeichert werden. Nur so lassen sich die Protokollierungsdaten an einer zentralen Stelle auswählen, filtern und systematisch auswerten.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_5_Protokollierung.html.

OPS1.1.6	Software-Tests und -Freigaben	„Der Einsatz von IT in Institutionen setzt voraus, dass die maschinelle Datenverarbeitung soweit wie möglich fehlerfrei funktioniert, da die Einzelergebnisse in den meisten Fällen nicht mehr kontrolliert werden können. Deswegen muss Software jeglicher Art schon vor Inbetriebnahme im Rahmen von Software-Tests überprüft werden. In diesen Tests muss nachgewiesen werden, dass die Software die erforderlichen Funktionen zuverlässig bereitstellt und darüber hinaus keine unerwünschten Nebeneffekte aufweist. Mit der anschließenden Freigabe der Software durch die fachlich zuständige Organisationseinheit wird die grundsätzliche Erlaubnis erteilt, die Software produktiv in der Institution zu nutzen. Gleichzeitig übernimmt diese Organisationseinheit damit auch die Verantwortung für das IT-Verfahren, das durch die Software unterstützt wird. Software kann an unterschiedlichen Stellen ihres Lebenszyklus getestet werden. So können Software-Tests bereits bei der Entwicklung, vor der Freigabe für den Produktivbetrieb oder im Zuge des Patch- und Änderungsmanagements notwendig werden. Die Software-Tests und -Freigaben sind sowohl für Individualsoftware als auch beim Einsatz von Standardsoftware durchzuführen. Dieser Baustein beschreibt den Test- und Freigabeprozess für individuell entwickelte oder angepasste Software sowie für Standardsoftware. Der Test- und Freigabeprozess zeichnet sich dadurch aus, dass dieser je nach Ergebnis mehrmals durchlaufen werden kann.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_6_Software-Tests_und_-Freigaben.html.
OPS.1.2.4	Telearbeit	„Unter Telearbeit wird jede auf die Informations- und Kommunikationstechnik gestützte Tätigkeit verstanden, die ganz oder teilweise außerhalb der Geschäftsräume und Gebäude des Arbeitgebers verrichtet wird. Bei der heimbasierten Telearbeit arbeiten die Arbeitnehmer regelmäßig tages- oder stundenweise abwechselnd an ihrem Arbeitsplatz beim Arbeitgeber und am häuslichen Arbeitsplatz.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_2_4_Telearbeit.html.
OPS.1.2.5	Fernwartung	„Mit dem Begriff Fernwartung wird ein räumlich getrennter Zugriff auf IT-Systeme und die darauf laufenden Anwendungen bezeichnet. Der Zugriff kann z. B. dazu dienen, Konfigurations-, Wartungs- oder Reparaturarbeiten durchzuführen. Die Fernwartung kann aktiv oder passiv geschehen. Bei der aktiven Fernwartung werden die Tastatur- und Maussignale vom System eines Administrators an ein entferntes System übertragen. Das entfernte System überträgt die Bildschirm- oder Konsolenausgabe an das System des Administrators. Der Administrator führt Aktionen auf dem entfernten System aus, als wenn er selbst vor Ort wäre. Bei der passiven Fernwartung werden nur die Bildschirminhalte eines Systems zum Administrator übertragen. Der Administrator erteilt einem Benutzer vor Ort Anweisungen, die von ihm ausgeführt und vom Administrator beobachtet werden. Da sich viele IT-Systeme außerhalb der Reichweite ihrer Administratoren befinden (z. B. in entfernten Rechenzentren, Industrieanlagen oder einem Außenstandort ohne IT-Personal), wird Fernwartung in vielen Institutionen eingesetzt. Aufgrund der tiefgreifenden Eingriffsmöglichkeiten in IT-Systeme, ist die Absicherung von Fernwartungskomponenten von besonderer Bedeutung.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_2_5_Fernwartung.html.

OPS2.1	Outsourcing für Kunden	„Beim Outsourcing lagern Institutionen (Outsourcing-Kunden) Geschäftsprozesse und Dienstleistungen ganz oder teilweise zu externen Dienstleistern (Outsourcing-Dienstleistern) aus. Outsourcing kann die Nutzung und den Betrieb von Hard- und Software betreffen, wobei die Leistung in den Räumlichkeiten des Auftraggebers oder in einer externen Betriebsstätte des Outsourcing-Dienstleisters erbracht werden kann. Typische Beispiele sind der Betrieb eines Rechenzentrums, einer Applikation oder einer Webseite. Outsourcing ist ein Oberbegriff, der oftmals durch weitere Begriffe ergänzt wird, wie Hosting, Housing oder Colocation. Unabhängig davon, was ausgelagert wird, bindet jede Auslagerung den Kunden an den externen Dienstleister und dessen Dienstleistungsquantität sowie -qualität. Dieses Verhältnis ist insbesondere für den Kunden nicht nur mit Chancen, sondern auch mit erheblichen Risiken verbunden. Dazu gehören eine starke Abhängigkeit, der Verlust von eigenem Wissen sowie von Kontroll- und Steuerungsmöglichkeiten. Informationssicherheitsaspekte müssen daher während des kompletten Lebenszyklus einer Auslagerung angemessen berücksichtigt werden.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_2_1_Outsourcing_f%C3%BCr_Kunden.html.
OPS2.2	Cloud-Nutzung	„Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software. Cloud Computing bietet viele Vorteile: Die IT-Dienste können bedarfsgerecht, skalierbar und flexibel genutzt und je nach Funktionsumfang, Nutzungsdauer und Anzahl der Benutzer abgerechnet werden. Auch kann auf spezialisierte Kenntnisse und Ressourcen des Cloud-Diensteanbieters zugegriffen werden, wodurch interne Ressourcen für andere Aufgaben freigesetzt werden können. In der Praxis zeigt sich jedoch häufig, dass sich die Vorteile, die Institutionen von der Cloud-Nutzung erwarten, nicht vollständig auswirken. Die Ursache dafür ist meistens, dass wichtige kritische Erfolgsfaktoren im Vorfeld der Cloud-Nutzung nicht ausreichend betrachtet werden. Daher müssen Cloud-Dienste strategisch geplant sowie (Sicherheits-)Anforderungen, Verantwortlichkeiten und Schnittstellen sorgfältig definiert und vereinbart werden. Auch das Bewusstsein und Verständnis für die notwendigerweise geänderten Rollen, sowohl auf Seiten des IT-Betriebs als auch der Benutzer der nutzenden Institution, ist ein wichtiger Erfolgsfaktor. Zusätzlich sollte bei der Einführung von Cloud-Diensten auch das Thema Governance berücksichtigt werden (Cloud Governance). Kritische Bereiche sind beispielsweise die Vertragsgestaltung, die Umsetzung von Mandantenfähigkeit, die Sicherstellung von Portabilität unterschiedlicher Services, die Abrechnung genutzter Service-Leistungen, das Monitoring der Service-Erbringung, das Sicherheitsvorfallmanagement und zahlreiche Datenschutzaspekte.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_2_2_Cloud-Nutzung.html.

OPS3.1	Outsourcing für Dienstleister	„Beim Outsourcing übernehmen Outsourcing-Dienstleister Geschäftsprozesse und Dienstleistungen ganz oder teilweise von auslagernden Institutionen, den Outsourcing-Kunden. Outsourcing kann die Nutzung und den Betrieb von Hard- und Software betreffen, wobei die Leistung in den Räumlichkeiten des Outsourcing-Kundens oder in einer externen Betriebsstätte des Outsourcing-Dienstleisters erbracht werden kann. Typische Beispiele sind der Betrieb eines Rechenzentrums, einer Applikation oder einer Webseite. Outsourcing ist ein Oberbegriff, der oftmals durch weitere Begriffe ergänzt wird wie Hosting, Housing oder Colocation. Unabhängig davon, welche Dienstleistungen übernommen werden, ist eine enge Bindung zwischen dem Outsourcing-Dienstleister und dem Outsourcing-Kunden notwendig. So bleibt der Outsourcing-Dienstleister nicht von den Risiken der Outsourcing-Beziehung verschont. Zudem muss er die vom Outsourcing-Kunden festgelegten risikomindernden Sicherheitsanforderungen umsetzen (siehe Baustein OPS.2.1 Outsourcing für Kunden). Denn es liegt auch im Interesse des Outsourcing-Dienstleisters, die vereinbarte Leistung zu erbringen und das vereinbarte Sicherheitsniveau einzuhalten. Werden an ihn gestellte Anforderungen nicht erfüllt, drohen mitunter hohe Vertragsstrafen und gegebenenfalls weitere juristische Folgen. Diese können nicht nur finanzielle Auswirkungen haben, sondern auch die Reputation nachhaltig schädigen.“ Weitere Informationen siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_3_1_Outsourcing_f%C3%BCr_Dienstleister.html.
DER	**Detektion und Reaktion**	
DER.1	Detektion von sicherheitsrelevanten Ereignissen	„Um IT-Systeme schützen zu können, müssen sicherheitsrelevante Ereignisse rechtzeitig erkannt und behandelt werden. Dazu ist es notwendig, dass Institutionen im Vorfeld geeignete organisatorische, personelle und technische Maßnahmen planen, implementieren und regelmäßig üben. Denn wenn auf ein vorgegebenes und erprobtes Verfahren aufgesetzt werden kann, lassen sich Reaktionszeiten verkürzen und vorhandene Prozesse optimieren. Als sicherheitsrelevantes Ereignis wird ein Ereignis bezeichnet, das sich auf die Informationssicherheit auswirkt und die Vertraulichkeit, Integrität oder Verfügbarkeit beeinträchtigen kann. Typische Folgen solcher Ereignisse sind ausgespähte, manipulierte oder zerstörte Informationen. Die Ursachen dafür sind dabei vielfältig: So spielen unter anderem Malware, veraltete IT-Systeminfrastrukturen oder Innentäter eine Rolle. Angreifer nutzen aber auch oft Zero-Day-Exploits aus, also Sicherheitslücken in Programmen, bevor es für diese einen Patch gibt. Eine weitere ernstzunehmende Gefährdung sind sogenannte Advanced Persistent Threats (APT). Dabei handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen Zugriff in der Folge auf weitere IT-Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten auf Seiten der Angreifer aus und sind oft schwer zu detektieren.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_1_Detektion_von_sicherheitsrelevanten_Ereignissen.html.

DER.2.1	Behandlung von Sicherheitsvorfällen	„Um Schäden zu begrenzen und um weitere Schäden zu vermeiden, müssen erkannte Sicherheitsvorfälle schnell und effizient bearbeitet werden. Dafür ist es notwendig, ein vorgegebenes und erprobtes Verfahren zur Behandlung von Sicherheitsvorfällen zu etablieren (Security Incident Handling oder auch Security Incident Response). Ein Sicherheitsvorfall kann sich stark auf eine Institution auswirken und große Schäden nach sich ziehen. Solche Vorfälle sind beispielsweise Fehlkonfigurationen, die dazu führen, dass vertrauliche Informationen offengelegt werden, oder kriminelle Handlungen, wie z. B. das Hacking von Servern, der Diebstahl von vertraulichen Informationen sowie Sabotage oder Erpressung mit IT-Bezug. Die Ursachen für Sicherheitsvorfälle sind vielfältig: So spielen unter anderem Malware, veraltete Systeminfrastrukturen oder Innentäter eine Rolle. Angreifer nutzen aber auch oft Zero-Day-Exploits aus, also Sicherheitslücken in Programmen, für die es noch keinen Patch gibt. Eine weitere ernstzunehmende Gefährdung sind sogenannte Advanced Persistent Threats (APT). Außerdem könnten sich Benutzer, Administratoren oder externe Dienstleister falsch verhalten, sodass Systemparameter sicherheitskritisch geändert werden oder sie gegen interne Richtlinien verstoßen. Weiter ist als Ursache denkbar, dass Zugriffsrechte verletzt werden, dass Software und Hardware geändert oder schutzbedürftige Räume und Gebäude unzureichend gesichert werden.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_2_1_Behandlung_von_Sicherheitsvorf%C3%A4llen.html.

DER.2.2	Vorsorge für die IT-Forensik	„IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Datennetzen zur Aufklärung von Sicherheitsvorfällen in IT-Systemen. IT-Sicherheitsvorfälle forensisch zu untersuchen, ist immer dann notwendig, wenn entstandene Schäden bestimmt, Angriffe abgewehrt, zukünftige Angriffe vermieden und Angreifer identifiziert werden sollen. Ob ein IT-Sicherheitsvorfall forensisch untersucht wird, entscheidet sich, während der Vorfall behandelt wird. Eine IT-forensische Untersuchung im Sinne dieses Bausteins besteht aus den folgenden Phasen: ↳ Strategische Vorbereitung: In dieser Phase werden Prozesse geplant und aufgebaut, die sicherstellen, dass eine Institution IT-Sicherheitsvorfälle forensisch analysieren kann. Sie ist auch dann notwendig, wenn die Institution über keine eigenen Forensik-Experten verfügt. ↳ Initialisierung: Nachdem die verantwortlichen Mitarbeiter entschieden haben, einen IT-Sicherheitsvorfall forensisch zu untersuchen, werden die vorher geplanten Prozesse angestoßen. Des Weiteren wird der Untersuchungsrahmen festgelegt und es werden Erstmaßnahmen durchgeführt. ↳ Spurensicherung: Hier werden die zu sichernden Beweismittel ausgewählt und die Daten forensisch gesichert. Dabei wird zwischen Live-Forensik und Post-Mortem-Forensik unterschieden: Die Live-Forensik stellt sicher, dass flüchtige Daten, wie z. B. Netzverbindungen oder RAM, von einem laufenden IT-System gesichert werden. Bei der Post-Mortem-Forensik hingegen werden forensische Kopien von Datenträgern erstellt. ↳ Analyse: Die gesammelten Daten werden forensisch analysiert. Dabei werden die Daten sowohl für sich als auch im Gesamtzusammenhang betrachtet. ↳ Ergebnisdarstellung: Die relevanten Untersuchungsergebnisse werden zielgruppengerecht aufbereitet und vermittelt.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_2_2_Vorsorge_f%C3%BCr_die_IT-Forensik.html.

DER.2.3	Bereinigung weitreichender Sicherheitsvorfälle	„Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen. Dabei verschafft sich ein Angreifer dauerhaften Zugriff zu einem Netz und weitet diesen Zugriff auf weitere IT-Systeme aus. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und umfassende technische Fähigkeiten auf Seiten der Angreifer aus. Angriffe dieser Art sind in der Regel schwierig zu detektieren. Nachdem ein APT-Angriff entdeckt wurde, stehen die Verantwortlichen in den betroffenen Institutionen vor großen Herausforderungen. Denn sie müssen eine Bereinigung durchführen, die über das übliche Vorgehen zur Behandlung von IT-Sicherheitsvorfällen hinausgeht. Es ist davon auszugehen, dass die entdeckten Angreifer bereits seit längerer Zeit auf die betroffene IT-Infrastruktur zugreifen können. Außerdem nutzen sie komplexe Angriffswerkzeuge, um die Standard-Sicherheitsmechanismen zu umgehen und diverse Hintertüren zu etablieren. Zudem besteht die Gefahr, dass die Angreifer die infizierte Umgebung genau beobachten und auf Versuche zur Bereinigung reagieren, indem sie ihre Spuren verwischen und die Untersuchung sabotieren. In diesem Baustein wird von einer hohen Bedrohungslage durch einen gezielten Angriff hochmotivierter Täter mit überdurchschnittlichen Ressourcen ausgegangen. Grundsätzlich sollte bei einem solchen Vorfall immer auch ein (zertifizierter) Forensikdienstleister hinzugezogen werden, wenn die Institution selbst nicht über entsprechende eigene Forensik-Experten verfügt. Forensik-Dienstleister sollten dabei bereits in der Phase der forensischen Analyse herangezogen werden. Der Dienstleister sollte jedoch auch bei der Bereinigung zumindest beratend einbezogen werden. Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_2_3_Bereinigung_weitreichender_Sicherheitsvorf%C3%A4lle.html.
DER.3.1	Audits und Revisionen	„Audits und Revisionen sind grundlegend für jedes erfolgreiche Managementsystem für Informationssicherheit (ISMS). Nur wenn etablierte Sicherheitsmaßnahmen und -prozesse regelmäßig daraufhin überprüft werden, ob sie noch wirksam, vollständig, angemessen und aktuell sind, lässt sich der Gesamtzustand der Informationssicherheit beurteilen. Audits und Revisionen sind somit ein Werkzeug, um ein angemessenes Sicherheitsniveau festzustellen, zu erreichen und aufrechtzuerhalten. Durch Audits und Revisionen ist es möglich, Sicherheitsmängel und Fehlentwicklungen zu erkennen und entsprechende Gegenmaßnahmen zu ergreifen. Als Audit (audire = hören, zuhören) wird eine systematische, unabhängige Prüfung von Aktivitäten und deren Ergebnissen bezeichnet. Dabei wird geprüft, ob definierte Anforderungen wie Normen, Standards oder Richtlinien eingehalten werden. In einer Revision (revidieren = kontrollieren, prüfen) wird untersucht, ob Dokumente, Zustände, Gegenstände oder Vorgehensweisen korrekt, wirksam und angemessen sind. Im Gegensatz zum Audit muss die Revision nicht unbedingt unabhängig erfolgen. Zudem kann die Revision im Sinne einer Wartung auch bereits die Nachbesserung umfassen.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_3_1_Audits_und_Revisionen.html.

DER.4	Notfallmanagement	„In Notfällen müssen Institutionen weiter auf Informationen zugreifen können, um einen Geschäftsprozess, ein IT-System oder eine Fachaufgabe wiederherstellen zu können. Um die Informationssicherheit auch in einem Notfall aufrechterhalten zu können, sollten deshalb entsprechende Prozesse geplant, etabliert und überprüft werden. Nur wenn geplant und organisiert vorgegangen wird, ist eine optimale Notfallvorsorge und Notfallbewältigung möglich. Ein professioneller Prozess zum Notfallmanagement reduziert die Auswirkungen eines Notfalls und sichert somit den Betrieb und Fortbestand der Institution. Es sind geeignete Maßnahmen zu identifizieren und umzusetzen, durch welche zeitkritische Geschäftsprozesse und Fachaufgaben zum einen robuster und ausfallsicherer werden. Zum anderen sollten diese Maßnahmen ermöglichen, einen Notfall schnell und zielgerichtet zu bewältigen. Die Aufrechterhaltung der Informationssicherheit im Notfall ist in ein übergreifendes Notfallmanagement, idealerweise in ein Notfallmanagementsystem, einzubinden. Das Notfallmanagement hat jedoch einen eigenen Prozessverantwortlichen, den Notfallbeauftragten, der sich mit dem Informationssicherheitsbeauftragten abstimmt.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_4_Notfallmanagement.html.
APP	**Anwendungen**	
APP.1.1	Office-Produkte	„Die Gruppe der Office-Produkte umfasst in erster Linie solche Anwendungen, die dazu dienen, Dokumente zu betrachten, zu bearbeiten oder zu erstellen. Dazu zählen unter anderem die freie Anwendung LibreOffice und die proprietäre Anwendung Microsoft Office, die in vielen Institutionen genutzt werden. Office-Produkte gehören für die meisten Institutionen zur notwendigen IT-Grundausstattung. Sie umfassen unter anderem Programme zur Textverarbeitung, Tabellenkalkulation und Erstellung von Präsentationen sowie Zeichenprogramme und einfache Datenbanksysteme. Die Nutzung von Office-Anwendungen ermöglicht und vereinfacht es, Informationen zu erheben und zu verarbeiten.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_1_1_Office-Produkte.html.

APP.1.2	Web-Browser	„Webbrowser sind Anwendungsprogramme, die (Hypertext-)Dokumente, Bilder, Video-, Audio- und andere Datenformate aus dem Internet abrufen, verarbeiten, darstellen, ausgeben und auf lokalen IT-Systemen speichern können. Ebenso können Webbrowser auch Daten ins Internet übertragen. Stationäre und mobile Client-Systeme sind heute ohne Webbrowser nicht vorstellbar, weil sehr viele private und geschäftliche Anwendungen entsprechende Inhalte nutzen. Gleichzeitig werden diese Inhalte im Internet immer vielfältiger. Immer weniger Webseiten kommen ohne eingebettete Videos, animierte Elemente und andere aktive Inhalte aus. Moderne Webbrowser decken zudem eine große Bandbreite an Zusatzfunktionen ab, indem sie Plug-ins und externe Bibliotheken einbinden. Hinzu kommen Erweiterungen für bestimmte Funktionen, Datenformate und Inhalte. Die Komplexität moderner Webbrowser bietet ein hohes Potenzial für gravierende konzeptionelle Fehler und programmtechnische Schwachstellen. Sie erhöht nicht nur die möglichen Gefahren für Angriffe aus dem Internet, sondern birgt zusätzliche Risiken durch Programmier- und Bedienungsfehler. Die Folgen für die Vertraulichkeit und Integrität von Daten sind erheblich. Ebenso ist die Verfügbarkeit des gesamten IT-Systems durch solche Schwachstellen bedroht. Internetinhalte müssen demzufolge aus Sicht des Webbrowsers grundsätzlich als nicht vertrauenswürdig angesehen werden.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_1_2_Web-Browser.html.
APP.2.1	Allgemeiner Verzeichnisdienst	„Ein Verzeichnisdienst stellt in einem Datennetz Informationen über beliebige Objekte in einer definierten Art zur Verfügung. In einem Objekt können zugehörige Attribute gespeichert werden, zum Beispiel können zu einer Benutzerkennung der Name und Vorname des Benutzers, die Personalnummer und der Rechnername abgelegt werden. Diese Daten können dann gleichermaßen von verschiedenen Applikationen verwendet werden. Der Verzeichnisdienst und seine Daten werden in der Regel von zentraler Stelle aus verwaltet. Einige typische Anwendungsgebiete von Verzeichnisdiensten sind: ↳ Verwaltung von Adressbüchern, z. B. für Telefonnummern, E-Mail-Adressen und Zertifikate für elektronische Signaturen ↳ Ressourcen-Verwaltung, z. B. für IT-Systeme, Drucker, Scanner und andere Peripherie-Geräte ↳ Benutzerverwaltung, z. B. zur Verwaltung von Benutzerkonten und Benutzerberechtigungen ↳ Authentisierung, z. B. zur Anmeldung an Betriebssystemen oder Anwendungen Verzeichnisdienste sind auf Lesezugriffe hin optimiert, da Daten aus dem Verzeichnisdienst typischerweise abgerufen werden. Schreibzugriffe, bei denen Einträge erstellt, geändert oder gelöscht werden, sind seltener notwendig.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_2_1_Allgemeiner_Verzeichnisdienst.html.

APP.2.2	Active Directory	„Active Directory (AD) ist ein von Microsoft entwickelter Verzeichnisdienst, der mit dem Betriebssystem Windows 2000 Server erstmalig eingeführt wurde. Ausgehend von den Active-Directory-Funktionen des Betriebssystems Microsoft Windows 2000 Server wurden dem Active-Directory-Dienst mit jedem Release der Windows-Server-Familie weitere Schlüsselfunktionen hinzugefügt. Active Directory wird hauptsächlich in IT-Netzen mit Microsoft-Komponenten eingesetzt. Ein AD speichert Informationen über Objekte innerhalb eines Netzes, z. B. über Benutzer oder IT-Systeme. Es erleichtert es Anwendern und Administratoren, diese Informationen bereitzustellen, zu organisieren, zu nutzen und zu überwachen. Als ein objektbasierter Verzeichnisdienst ermöglicht Active Directory die Verwaltung von Objekten und deren Beziehung untereinander, was die eigentliche Netzumgebung auszeichnet. Active Directory stellt zentrale Steuerungs- und Kontrollmöglichkeiten des jeweiligen Netzes bereit. Der Einsatz eines solchen Verzeichnisdienstes bietet sich vor allem dort an, wo z. B. die Anzahl der im Netz eingesetzten Clients eine dezentrale Verwaltung erschwert. Ohne einen Verzeichnisdienst könnte nicht mehr gewährleistet werden, dass lokal vorzunehmende Einstellungen, wie z. B. die Vorgaben aus Sicherheitsrichtlinien, aufgrund des hohen Aufwandes zuverlässig erledigt werden. Verwaltungsaufgaben innerhalb des Netzes wie z. B. Passwortänderungen, Kontenerstellung und Zugriffsrechte können effizienter durchgeführt werden, wenn ein Verzeichnisdienst eingesetzt wird.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_2_2_Active_Directory.html.
APP.2.3	OpenLDAP	OpenLDAP ist ein frei verfügbarer Verzeichnisdienst, der in einem Datennetz Informationen über beliebige Objekte, beispielsweise Benutzer oder IT-Systeme, in einer definierten Art zur Verfügung stellt. Die Informationen können einfache Attribute wie die Namen oder Nummern von Objekten oder auch komplexe Formate wie Fotos oder Zertifikate für elektronische Signaturen umfassen. Typische Einsatzgebiete sind zum Beispiel Adressbücher oder Benutzerverwaltungen. OpenLDAP stellt eine Referenz-Implementierung für einen Server-Dienst im Rahmen des Lightweight Directory Access Protocols (LDAP) dar. Als Open-Source-Software kann OpenLDAP auf einer Vielzahl von Betriebssystemen installiert werden und gilt als einer der am meisten verbreiteten Verzeichnisdienste. Zur Besonderheit von OpenLDAP gehören die Overlays. Overlays erweitern den Funktionsumfang von OpenLDAP um zahlreiche Funktionen und werden auch für grundlegende Funktionen wie Protokollierung, Replikation und die Wahrung der Integrität verwendet. Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_2_3_OpenLDAP.html.

APP.3.1	Webanwendungen	„Webanwendungen stellen Funktionen und dynamische Inhalte zur Verfügung. Sie nutzen dazu das Internetprotokoll HTTP (Hypertext Transfer Protocol) bzw. HTTPS. Bei HTTPS wird die Verbindung durch die Protokolle SSL (Secure Socket Layer) oder TLS (Transport Layer Security) verschlüsselt und zusätzlich gesichert. Webanwendungen erstellen auf einem Server Dokumente und Benutzeroberflächen, z. B. Eingabemasken, und liefern diese an entsprechende Clientprogramme, wie etwa Webbrowser. Webanwendungen werden gewöhnlich auf der Grundlage von Frameworks entwickelt. Diese stellen ein Rahmenwerk für häufig wiederkehrende Aufgaben zur Verfügung, z. B. für Sicherheitskomponenten. Um eine Webanwendung zu betreiben, sind in der Regel mehrere Komponenten notwendig. Hierzu gehören üblicherweise ein Webserver, um Daten auszuliefern und ein Applikationsserver, um die eigentliche Anwendung zu betreiben. Außerdem sind zusätzliche Hintergrundsysteme nötig, die oft als Datenquellen über unterschiedliche Schnittstellen angebunden sind, z. B. Datenbanken oder Verzeichnisdienste. Webanwendungen werden sowohl in öffentlichen Datennetzen als auch in Institutionsnetzen (Intranet) eingesetzt, um Daten und Anwendungen bereitzustellen. Je nach Zweck der Webanwendungen werden diese in der Regel von Anwendern genutzt, die sich im Vorfeld authentisieren müssen. Dabei müssen Webanwendungen Sicherheitsmechanismen umsetzen, die den Schutz der Daten gewährleisten und deren Missbrauch verhindern. Typische Sicherheitskomponenten bzw. -mechanismen sind: Authentisierung, Autorisierung, Eingabevalidierung, Ausgabekodierung, Session-Management, Fehlerbehandlung und Protokollierung.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_3_1_Webanwendungen.html.
APP.3.2	Webserver	„Ein Webserver ist die Kernkomponente jedes Webangebotes: Er nimmt Anfragen der Clients über einen Browser entgegen und liefert die entsprechenden Inhalte zurück. Der Transport der Daten erfolgt in der Regel über das Hypertext Transfer Protocol (HTTP) oder dessen mit Transport Layer Security (TLS) verschlüsselte Variante HTTP Secure (HTTPS). Da Webserver eine einfache Schnittstelle zwischen Serveranwendungen und Benutzern bieten, werden sie auch häufig für interne Informationen und Anwendungen in Institutionsnetzen, wie dem Intranet, eingesetzt. Webserver sind in der Regel direkt im Internet verfügbar und bieten somit eine exponierte Angriffsfläche. Deswegen müssen sie durch geeignete Schutzmaßnahmen abgesichert werden.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_3_2_Webserver.html.

APP.3.3	Fileserver	„Ein Fileserver (oder auch Dateiserver) ist ein Server in einem Netz, der Dateien von (internen) Festplatten oder Netzfestplatten für alle zugriffsberechtigten Benutzer bzw. Clients zentral bereitstellt. Die Datenbestände können von zugriffsberechtigten Benutzern genutzt werden, ohne sie z. B. auf Wechseldatenträgern zu transportieren oder per E-Mail zu verteilen. Dadurch, dass die Daten zentral vorgehalten werden, können sie strukturiert und in verschiedenen Verzeichnissen und Dateien bereitgestellt werden. Bei Fileservern können Zugriffsrechte auf die Dateien zentral vergeben werden. Auch die Datensicherung kann vereinfacht werden, wenn sich alle Informationen an einer zentralen Stelle befinden. Ein Fileserver verwaltet meistens Massenspeicher, die mit ihm über Schnittstellen wie SCSI (Small Computer System Interface) oder SAS (Serial Attached SCSI) verbunden sind. Die Speicher befinden sich entweder direkt im Gehäuse des Fileservers oder sind extern angeschlossen. Letzteres wird oft als Directly Attached Storage (DAS) bezeichnet. Ein Fileserver kann auf herkömmlicher Server-Hardware oder einer dedizierten Appliance betrieben werden. Oft können bei großen Datenmengen auch zentrale Storage-Area-Network (SAN)-Speicher über Host-Bus-Adapter (HBA) im Server und an SAN-Switches angebunden werden.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_3_3_Fileserver.html.
APP.3.6	DNS-Server	„Domain Name System (DNS) ist ein Netzdienst, der dazu eingesetzt wird, Hostnamen von IT-Systemen in IP-Adressen umzuwandeln. Üblicherweise wird über DNS zu einem Hostnamen die entsprechende IP-Adresse gesucht (Vorwärtsauflösung). Ist hingegen die IP-Adresse bekannt und der Hostname wird gesucht, wird dies als Rückwärtsauflösung bezeichnet. DNS kann mit einem Telefonbuch verglichen werden, das Namen nicht in Telefonnummern, sondern in IP-Adressen auflöst. Welche Namen zu welchen IP-Adressen gehören, wird im Domain-Namensraum verwaltet. Dieser ist hierarchisch aufgebaut und wird von DNS-Servern zur Verfügung gestellt. DNS-Server verwalten den Domain-Namensraum im Internet, werden aber auch häufig im internen Netz einer Institution eingesetzt. Auf den IT-Systemen der Benutzer sind standardmäßig sogenannte Resolver installiert. Darüber werden die Anfragen an DNS-Server gestellt. Als Antwort liefern diese Informationen über den Domain-Namensraum zurück. Die Bezeichnung DNS-Server steht im eigentlichen Sinne für die verwendete Software, wird jedoch meist auch als Synonym für das IT-System benutzt, auf dem diese Software betrieben wird. DNS-Server können nach ihren Aufgaben unterschieden werden. Dabei gibt es grundsätzlich zwei verschiedenen Typen: Advertising DNS-Server und Resolving DNS-Server. Advertising DNS-Server sind üblicherweise dafür zuständig, Anfragen aus dem Internet zu verarbeiten. Resolving DNS-Server hingegen verarbeiten Anfragen aus dem internen Netz der Institution. Ein Ausfall eines DNS-Servers kann sich gravierend auf den Betrieb einer IT-Infrastruktur auswirken. Dabei ist nicht direkt das ausgefallene DNS-System problematisch, sondern die daraus resultierende Einschränkung DNS-basierter Dienste. Unter Umständen sind Webserver oder E-Mail-Server nicht mehr erreichbar oder die Fernwartung funktioniert nicht mehr. Da DNS von sehr vielen Netzanwendungen benötigt wird, müssen laut Spezifikation (RFC 1034) mindestens zwei autoritative DNS-Server (Advertising DNS-Server) für jede Zone betrieben werden.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_3_6_DNS-Server.html.

APP.4.3	Relationale Datenbanksysteme	„Datenbanksysteme (DBS) sind ein oft genutztes Hilfsmittel, um IT-gestützt große Datensammlungen zu organisieren, zu erzeugen, zu verändern und zu verwalten. Ein DBS besteht aus dem so genannten Datenbankmanagementsystem (DBMS) und einer oder mehreren Datenbanken. Eine Datenbank ist eine Zusammenstellung von Daten samt ihrer Beschreibung (Metadaten), die dauerhaft im Datenbanksystem abgelegt werden. Da Datenbanksysteme eine zentrale Bedeutung in einer IT-Infrastruktur einnehmen, ergeben sich an sie wesentliche Sicherheitsanforderungen. Meist sind Kernprozesse einer Institution von den Informationen aus den Datenbanken abhängig. Dadurch ergeben sich entsprechende Verfügbarkeitsanforderungen. Zusätzlich bestehen oft hohe Anforderungen an die Vertraulichkeit und Integrität der in den Datenbanken gespeicherten Informationen.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_4_3_Relationale_Datenbanksysteme.html.
APP.5.1	Allgemeine Groupware	„Als Groupware (auch kollaborative Software genannt) werden Anwendungen und Systeme bezeichnet, mit denen mehrere Personen (Gruppen) über räumliche bzw. zeitliche Distanzen hinweg zusammenarbeiten können. Mithilfe von Groupware-Systemen können Gruppen untereinander und miteinander kooperieren und Termine abstimmen. Dokumente und Daten lassen sich durch Groupware von mehreren Benutzern gleichzeitig verwenden und bearbeiten, wodurch der Informationsfluss effizienter gestaltet wird. Unter dem Begriff Groupware-Systeme werden unter anderem der Groupware-Server, die zugehörigen Groupware-Clients und die erforderlichen Groupware-Dienste zusammengefasst. Neben den Basisfunktionen, wie z. B. Projektmanagement, E-Mail, Kalender oder Notizbuch, bieten neuere Applikationen auch Social-Media-Erweiterungen an, durch die Mitarbeiter noch besser kommunizieren und kooperieren können.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_5_1_Allgemeine_Groupware.html.
APP.5.2	Microsoft Exchange und Outlook	„Microsoft Exchange ist eine Groupware-Lösung für mittlere bis große Institutionen. Mit ihr können elektronisch Nachrichten übermittelt werden und sie verfügt über weitere Dienste, um Workflows zu unterstützen. Nachrichten, wie E-Mails, können mit Microsoft Exchange zentral verwaltet, zugestellt, gefiltert und versendet werden. Ebenso können typische Groupware-Anwendungen, wie Notizen, Kontaktlisten, Kalender und Aufgabenlisten angeboten und verwaltet werden. Um die Funktionen von Microsoft Exchange nutzen zu können, ist neben dem Server-Dienst eine zusätzliche Client-Software oder ein Web-Browser nötig. Die Kombination aus Microsoft Exchange-Servern und Outlook-Clients wird hier als Microsoft Exchange-System bezeichnet. Microsoft Outlook ist ein Client, der durch die Installation des Office-Pakets von Microsoft oder durch Integration in die Betriebssysteme von mobilen Geräten direkt zur Verfügung gestellt wird. Darüber hinaus ermöglicht die Webanwendung „Outlook Web App" (OWA) über den Browser z. B. auf E-Mails, Kontakte und den Kalender zuzugreifen. Diese Funktion ist im Microsoft Exchange-Paket bereits enthalten.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_5_2_Microsoft_Exchange_und_Outlook.html.

SYS	IT-Systeme	
SYS.1.1	Allgemeiner Server	„Als „Allgemeiner Server“ werden IT-Systeme mit einem beliebigen Betriebssystem bezeichnet, die Benutzern und anderen IT-Systemen Dienste bereitstellen. Diese Dienste können Basisdienste für das lokale oder externe Netz sein, aber auch den E-Mail-Austausch ermöglichen oder Datenbanken und Druckerdienste anbieten. Server haben eine zentrale Bedeutung für die Informationstechnik und damit für funktionierende Arbeitsabläufe einer Institution. Oft erfüllen Server Aufgaben im Hintergrund, ohne dass Benutzer direkt mit ihnen im Austausch stehen. Auf der anderen Seite gibt es Serverdienste, die direkt mit den Benutzern interagieren und nicht auf den ersten Blick als Serverdienst wahrgenommen werden. Ein bekanntes Beispiel sind X-Server unter Unix.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_1_1_Allgemeiner_Server.html.
SYS.1.5	Virtualisierung	„Bei der Virtualisierung von IT-Systemen werden ein oder mehrere virtuelle IT-Systeme auf einem physischen IT-System ausgeführt. Ein solches physisches IT-System wird als „Virtualisierungsserver“ bezeichnet. Mehrere Virtualisierungsserver können zu einer virtuellen Infrastruktur zusammengefasst werden. Darin können die Virtualisierungsserver selbst und die auf ihnen betriebenen virtuellen IT-Systeme gemeinsam verwaltet werden. Die Virtualisierung von IT-Systemen bietet viele Vorteile für den IT-Betrieb in einem Informationsverbund. So können beispielsweise Kosten für Hardwarebeschaffung, Strom und Klimatisierung eingespart werden, wenn die Ressourcen der physischen IT-Systeme effizienter genutzt werden. Allerdings ist die Virtualisierung auch eine Herausforderung für den Betrieb des Informationsverbunds. Da durch die eingesetzte Virtualisierungstechnik unterschiedliche Bereiche und Arbeitsfelder im Informationsverbund berührt werden, müssen Wissen und Erfahrungen aus diesen Bereichen zusammengeführt werden. Zudem können sich Probleme auf einem Virtualisierungsserver auch auf alle anderen virtuellen IT-Systeme, die auf dem selben Virtualisierungsserver betrieben werden, auswirken. Ebenso können sich virtuelle IT-Systeme gegenseitig in ihrem Betrieb stören.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_1_5_Virtualisierung.html.

SYS.1.8	Speicherlösungen	„Das stetige Wachstum digitaler Informationen und die zunehmende Menge unstrukturierter Informationen führen dazu, dass innerhalb von Institutionen zentrale Speicherlösungen eingesetzt werden. Dabei unterliegen die Anforderungen an solche Speicherlösungen einem stetigen Wandel, der sich beispielsweise an folgenden Aspekten beobachten lässt: ↳ Die Daten einer Institution sollen jederzeit, an jedem Ort und für unterschiedliche Anwendungsszenarien verfügbar sein. Dadurch gelten für moderne Speicherlösungen häufig gestiegene Verfügbarkeitsanforderungen. ↳ Die zunehmende Digitalisierung sämtlicher Informationen in einer Institution macht es notwendig, dass weitreichende rechtliche Vorgaben (Compliance-Anforderungen) beachtet und eingehalten werden müssen. ↳ Speicherlösungen sollen dynamisch an die sich stetig ändernden Anforderungen anpassbar sein und Speicherplatz zentral bereitstellen können. In der Vergangenheit wurden Speicherlösungen oft umgesetzt, indem Speichermedien direkt an einen Server angeschlossen wurden. Diese sogenannten Direct-Attached-Storage(DAS)-Systeme können die aktuellen und zukünftigen Anforderungen jedoch oft nicht mehr erfüllen. Daher sind die heute weitverbreiteten zentralen Speicherlösungen und deren Bestandteile notwendig, die sich wie folgt unterscheiden lassen: ↳ Speicherlösungen: Eine Speicherlösung besteht aus einem oder mehreren Speichernetzen sowie mindestens einem Speichersystem. ↳ Speichernetze: Speichernetze ermöglichen einerseits den Zugriff auf die Speichersysteme, andererseits die Replikation von Daten zwischen Speichersystemen. ↳ Speichersysteme: Als Speichersystem wird die zentrale Instanz bezeichnet, die für andere IT-Systeme Speicherplatz zur Verfügung stellt. Ein Speichersystem erlaubt außerdem den zeitgleichen Zugriff mehrerer IT-Systeme auf den vorhandenen Speicherplatz.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_1_8_Speicherl%C3%B6sungen.html.
SYS.2.1	Allgemeiner Client	„Als „Allgemeiner Client“ wird ein IT-System mit einem beliebigen Betriebssystem bezeichnet, das die Trennung von Benutzern zulässt und nicht dazu dient, Server-Dienste bereitzustellen. Auf einem Client sollten mindestens eine Administrator- und eine Benutzer-Umgebung eingerichtet werden können. Typischerweise ist ein solches IT-System vernetzt und in ein Client-Server-Netz eingebunden. Das IT-System kann auf einer beliebigen Plattform betrieben werden. Dabei kann es sich beispielsweise um einen PC mit oder ohne Festplatte, um ein mobiles oder stationäres Gerät, aber auch um eine Linux-Workstation oder einen Apple Mac handeln. Das IT-System verfügt in der Regel über Laufwerke für auswechselbare Datenträger, weitere Schnittstellen für den Datenaustausch sowie andere Peripheriegeräte.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_2_1_Allgemeiner_Client.html.

SYS.3.1	Laptops	„Ein Laptop (oder auch Notebook) ist ein PC, der mobil genutzt werden kann. Er hat eine kompakte Bauform, integriert Peripheriegeräte wie Tastatur und Bildschirm, ist über Akkus zeitweise unabhängig von einer externen Stromversorgung und besteht oft aus speziell für den mobilen Einsatz konzipierten Hardware-Komponenten. Laptops können mit allen üblichen Betriebssystemen wie Microsoft Windows, Apple macOS oder Linux betrieben werden. Die Geräte sind in den meisten Institutionen verbreitet und ersetzen für einige Mitarbeiter den klassischen Desktop-PC. Da Laptops häufig mobil genutzt werden, sind sie oft nicht permanent am LAN der Institution angeschlossen. Stattdessen können sie sich in der Regel per Virtual Private Network (VPN) über das Internet oder andere Datennetze verbinden, um so auf die Ressourcen des LANs zuzugreifen. Auch die Infrastruktur einer klassischen Büroumgebung, wie kontrollierbare Umwelteinflüsse, eine stabile Stromversorgung oder zutrittsgeschützte Bereiche kann für den mobilen Einsatz von Laptops nicht vorausgesetzt werden.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_1_Laptops.html.
SYS.3.2.1	Allgemeine Smartphones und Tablets	„Smartphones sind Mobiltelefone, die mit einem großen, üblicherweise berührungsempfindlichen Bildschirm (Touch-Display) ausgestattet sind. Smartphones vereinen neben der Telefonie beispielsweise Media-Player, Personal Information Manager und Digitalkamera in einem Gerät und bieten den Benutzern darüber hinaus viele weitere Anwendungen und Funktionen, wie Web-Browser, E-Mail-Client oder GPS. Zudem sind sie mit Mobilfunk-, WLAN- und Bluetooth-Schnittstellen ausgestattet. Tablets sind, vereinfacht gesagt, Smartphones mit großem Formfaktor, mit denen in der Regel nicht über das Mobilfunknetz telefoniert werden kann. Als Phablets werden Hybridgeräte aus Smartphone und Tablet bezeichnet. Sie werden in diesem Baustein nicht gesondert hervorgehoben.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_2_1_Allgemeine_Smartphones_und_Tablets.html
SYS.3.2.2	Mobile Device Management (MDM)	„Smartphones, Tablets und Phablets sind für viele Mitarbeiter ein nicht mehr wegzudenkender Teil ihrer Arbeit. Die IT-Abteilungen müssen jedoch immer mehr solcher Geräte in vielen unterschiedlichen Ausführungen bereitstellen und dabei gleichzeitig für eine angemessene Sicherheit sorgen. Hinzu kommt, dass mobile Endgeräte (Mobile Devices) besonderen Gefahren ausgesetzt sind und die Administration sich in grundlegenden Punkten von anderen IT-Systemen unterscheidet. Deswegen ist ein Mobile Device Management (MDM) besonders in Institutionen mit einer größeren Anzahl von Smartphones, Tablets und Phablets unabdingbar für einen geregelten und sicheren Betrieb dieser Geräte. Mit einer entsprechenden Software für das MDM können die Endgeräte zentral verwaltet werden, es lassen sich Sicherheitsregeln durchsetzen und es können Notfallaktionen ausgelöst werden. Ein MDM gewährleistet somit auf allen Geräten einen gleichen oder zumindest vergleichbaren Sicherheitsstandard.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_2_2_Mobile_Device_Management_(MDM).html.

SYS.3.2.3	iOS (for Enterprise)	„Mobilgeräte sind ständige Begleiter in der heutigen Informationsgesellschaft. Sie sind fast ununterbrochen online, das heißt mit dem Internet oder dem internen Institutionsnetz (Intranet) verbunden, und ermöglichen damit jederzeit den Zugriff auf digitale Informationen. Die Geräte können über diverse Schnittstellen kommunizieren, zum Beispiel über Mobilfunk, WLAN oder Bluetooth. Aufgrund von modernen, einfachen Bedienkonzepten sowie ihrer hohen Leistungsfähigkeit sind Smartphones und Tablets heutzutage weit verbreitet. Dazu zählen auch die von der Firma Apple produzierten Mobilgeräte iPhone und iPad mit dem Betriebssystem iOS. Ursprünglich wurden diese Geräte für den privaten Gebrauch konzipiert. Durch die Umgestaltung der Infrastrukturen und die Art der Informationserhebung und -verarbeitung werden sie jedoch immer häufiger auch im beruflichen Umfeld verwendet und lösen teilweise sogar Notebooks ab. Durch die Integration von Business-Funktionen wurde iOS seit der Version 4 schrittweise für den Einsatz in Unternehmen und Behörden ausgebaut und Funktionen für die Verwaltung aus Sicht einer Institution integriert. Hierzu gehören die Möglichkeit zur zentralisierten Geräteregistrierung (Apple Business Manager) sowie Optionen wie Single Sign-On (SSO).“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_2_3_iOS_(for_Enterprise).html.
SYS.3.2.4	Android	„Mobile Geräte sind ständige Begleiter in der heutigen Informationsgesellschaft. Sie sind fast ununterbrochen online, das heißt, mit dem Internet oder dem internen Institutionsnetz (Intranet) verbunden, und ermöglichen damit jederzeit den Zugriff auf digitale Informationen. Die Geräte können über diverse Schnittstellen kommunizieren, z. B. über Mobilfunk, WLAN oder Bluetooth. Aufgrund von modernen, einfachen Bedienkonzepten sowie ihrer hohen Leistungsfähigkeit sind Smartphones und Tablets heutzutage weit verbreitet. Ursprünglich wurden diese Geräte für den privaten Gebrauch konzipiert. Heute werden sie jedoch auch im beruflichen Umfeld immer häufiger verwendet. Ein oft genutztes Betriebssystem für Smartphones und Tablets ist Android von Google. Seit Version 4 wurde Android schrittweise für den Unternehmenseinsatz ausgebaut. So wurden z. B. Funktionen integriert, die es Institutionen erleichtern, Android-Geräte zu verwalten. Auch steigt die Zahl der von Android unterstützten Verwaltungsrichtlinien mit jeder Version und es gibt herstellerspezifische Erweiterungen, die zusätzliche Richtlinien erlauben.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_2_4_Android.html.
SYS.3.3	Mobiltelefon	„Die in diesem Baustein betrachteten Mobiltelefone, die auch „Feature-Phones“ oder „Dumbphones“ genannt werden, besitzen weniger Eigenschaften als ein Smartphone, bieten aber mehr Funktionen als nur die reine Telefonfunktion. So können diese Mobiltelefone zusätzlich mit einer Kamera für Videos und Fotos, einem Terminplaner, E-Mail-Programmen, Spielen, einem MP3-Player oder einem Radioempfänger ausgestattet sein. „Klassische“ Mobiltelefone verfügen in der Regel nicht über einen Touchscreen und ein Betriebssystem, auf das zusätzliche Apps installiert werden können. Diese fehlenden Funktionen unterscheidet das Mobiltelefon von einem Smartphone. Mobiltelefone sind durch eine international eindeutige Seriennummer (International Mobile Equipment Identity, IMEI) gekennzeichnet. Die Identifizierung der Benutzer des Mobiltelefons erfolgt durch die SIM-Karte, die bei Vertragsabschluss vom Mobilfunkanbieter zugeteilt wird.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_3_Mobiltelefon.html.

SYS.4.1	Drucker, Kopierer und Multifunktionsgeräte	„Moderne Drucker, Kopierer und Multifunktionsgeräte sind komplexe Geräte, die neben mechanische Komponenten eigene Betriebssysteme enthalten und Serverdienste und -funktionen bereitstellen. Da die Geräte oft vertrauliche Informationen verarbeiten, müssen sie bzw. die gesamte Druck- und Scan-Infrastruktur geschützt werden. Für viele Geschäftsprozesse wird auch heute noch Papier als Informationsträger benutzt. Damit sind Drucker, Kopierer oder Multifunktionsgeräte wichtige Komponenten in der IT-Infrastruktur. Fallen die Geräte aus oder werden verfälschte Dokumente ausgedruckt, kann sich das mitunter auf kritische Prozesse auswirken und zu erheblichen wirtschaftlichen Schäden führen.“
SYS.4.3	Eingebettete Systeme	Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_4_1_Drucker,_Kopierer_und_Multifunktionsger%C3%A4te.html.
IND	**Industrielle IT**	
IND.1	Betriebs- und Steuerungstechnik	„Betriebstechnik (Operational Technology, OT) ist Hard- und Software, die physische Geräte, Prozesse und Ereignisse in der Institution überwacht und steuert. In der Industrie, zu der unter anderem auch die Kritischen Infrastrukturen gehören, zählen dazu insbesondere industrielle Steuerungssysteme (Industrial Control Systems, ICS) und Automationslösungen, die dort Steuerungs- und Regelfunktionen aller Art übernehmen. Weitere Beispiele sind Laborgeräte, z. B. automatisierte Mikroskope oder Analysewerkzeuge, Logistiksysteme, wie Barcodescanner mit Kleinrechner, oder Gebäudeleittechnik. Die in der Vergangenheit übliche physische Trennung der OT von anderen IT-Systemen und Datennetzen in Büroanwendungen ist heute aufgrund zunehmender Integrationsanforderungen nur in Ausnahmefällen bei erhöhtem Schutzbedarf anwendbar. Mehrstufige Produktionsschritte und deren übergreifende Steuerung sowie regulatorische Anforderungen machen es zunehmend notwendig, die OT auch über Organisationsgrenzen hinweg zu öffnen. Diese Entwicklung wird durch den Trend zur Optimierung von Fertigungsprozessen noch beschleunigt, vor allem im Rahmen der Industrie 4.0. Neben OT-spezifischen Komponenten werden zunehmend auch IT-Komponenten und Entwicklungen aus der Office-IT in der OT eingesetzt. Daher ist die OT inzwischen vergleichbaren Gefährdungen ausgesetzt. Zugleich weist die OT gegenüber der klassischen IT aber auch wesentliche Unterschiede auf, die es erschweren, dort etablierte Sicherheitsverfahren anzuwenden. So kann es Restriktionen aufgrund von Herstellervorgaben oder gesetzlichen Anforderungen geben, die Veränderungen an IT-Komponenten verhindern oder erschweren. Ein Beispiel dafür sind die Anwendung von Sicherheitsupdates oder nachträgliche Härtungsmaßnahmen. Die OT unterliegt zudem meist deutlich längeren Lebenszyklen, auch über die Herstellerunterstützung hinaus. Dadurch kann zum Beispiel nicht gewährleistet werden, dass Sicherheitsupdates durchgehend verfügbar sind. Ein wesentlicher Unterschied ergibt sich für die OT auch aus den oft hohen Verfügbarkeits- und Integritätsanforderungen, während im Vergleich zur Office-IT die Vertraulichkeit häufig von nachrangiger Bedeutung ist. Störungen von OT-Systemen können Gefährdungen von Leib, Leben und Umwelt nach sich ziehen und sind zumeist nicht durch einen Neustart zu beheben.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_1_Betriebs-_und_Steuerungstechnik.html.

IND.2.1	Allgemeine ICS-Komponente	„Eine ICS-Komponente ist eine elektronische Komponente, die eine Maschine oder Anlage steuert oder regelt. Sie ist damit Bestandteil eines industriellen Steuerungssystems (engl. Industrial Control System, ICS) oder allgemeiner einer Betriebstechnik (engl. Operational Technology, OT). Solche Komponenten können Speicherprogrammierbare Steuerungen (SPS) (engl. Programmable Logic Controller, PLC), Sensoren, Aktoren, eine Maschine oder andere Teile eines ICS sein. Aufgrund der im OT-Umfeld typischen hohen Verfügbarkeitsanforderungen und der oft extremen Umgebungsbedingungen wie Hitze oder Kälte, Staub, Vibration oder Korrosion wurden ICS-Komponenten schon immer als robuste Geräte mit hoher Zuverlässigkeit und langer Lebensdauer konstruiert. ICS-Komponenten werden normalerweise über Spezialsoftware des jeweiligen Herstellers konfiguriert bzw. programmiert. Das wird entweder über sogenannte Programmiergeräte z. B. als Anwendung unter Windows oder Linux oder über eine Engineering-Station durchgeführt, welche die Anwendungsprogramme in die Speicherprogrammierbaren Steuerungen lädt. Die Rolle des Informationssicherheitsbeauftragten für den Bereich der industriellen Automatisierung wird je nach Art und Ausrichtung der Institution anders genannt. Eine weitere Bezeichnung neben ICS-Informationssicherheitsbeauftragter (ICS-ISB) ist auch Industrial Security Officer.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_2_1_Allgemeine_ICS-Komponente.html.
IND.2.2	Speicherprogrammierbare Steuerung (SPS)	„Eine Speicherprogrammierbare Steuerung (SPS, engl. Programmable Logic Controller, PLC) ist eine ICS-Komponente. Sie übernimmt Steuerungs- und Regelaufgaben in der Betriebstechnik (engl. Operational Technology, OT). Die Grenzen zwischen verschiedenen Geräteklassen und Bauformen sind heute fließend, so kann z. B. auch ein Fernwirkgerät (engl. Remote Terminal Unit, RTU) die Funktionen einer SPS übernehmen oder ein Programmable Automation Controller (PAC) kann versuchen, die Vorteile einer SPS und eines Industrie-PCs zu vereinen. Jedoch ist die SPS immer noch das klassische Automatisierungsgerät, sodass in diesem Baustein die Begriffe SPS, RTU und PAC synonym verwendet werden. Eine SPS verfügt über digitale Ein- und Ausgänge, ein Echtzeitbetriebssystem (Firmware) sowie weitere Schnittstellen für Ethernet oder Feldbusse. Die Verbindung zu Sensoren und Aktoren erfolgt über die analogen oder digitalen Ein- bzw. Ausgänge oder über einen Feldbus. Die Kommunikation mit Prozessleitsystemen erfolgt meist über die Ethernet-Schnittstelle und IP-basierte Netze. Die möglichen Realisierungen sind vielfältig, eine Speicherprogrammierbare Steuerung kann als Baugruppe, Einzelgerät, PC-Einsteckkarte (Slot-SPS) oder als Software-Emulation (Soft-SPS) eingesetzt werden. Am häufigsten anzutreffen sind modulare Speicherprogrammierbare Steuerungen, die aus verschiedenen funktionalen Steckmodulen zusammengesetzt werden. Zunehmend werden auch weitere Funktionen wie das Visualisieren, Alarmieren und Protokollieren durch die SPS übernommen. Aufgrund der im OT-Umfeld typischen hohen Verfügbarkeitsanforderungen und der oft extremen Umgebungsbedingungen wie Hitze oder Kälte, Staub, Vibration oder Korrosion wurden ICS-Komponenten schon immer als robuste Geräte mit hoher Zuverlässigkeit und langer Lebensdauer konstruiert. Eine SPS wird normalerweise über Spezialsoftware des jeweiligen Herstellers konfiguriert bzw. programmiert. Das wird entweder über sogenannte Programmiergeräte, z. B. als Anwendung unter Windows oder Linux, oder über eine Engineering-Station durchgeführt, welche die Daten über ein Netz verteilt.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_2_2_Speicherprogrammierbare_Steuerung_(SPS).html.

IND.2.3	Sensoren und Aktoren	„Sensoren sind als elektronische Komponente mit Mikroprozessor und Software ausgeführte Messumformer, die eine physikalische Größe in einen elektrischen Ausgabewert wandeln. Dieser wird als normiertes Einheitssignal (häufig 4 bis 20mA, 0 bis 10V) an einer seriellen Schnittstelle oder als digitale Informationen, die über einen Feldbus oder Ethernet-Protokolle übertragen werden, bereitgestellt. Messumformer stellen neben den Messwerten häufig noch Schnittstellen bereit, über die eine Diagnose und Parametrierung erfolgt. So kann ein Sensor neben einem elektronischen Ausgabewert auch noch über weitere Schnittstellen verfügen, z. B. WLAN-, Bluetooth- oder Wireless-HART-Schnittstellen für Parametrierung und Diagnose. Auf dem Markt gibt es viele unterschiedliche Sensoren, z. B. um physikalische Größen zu messen. Je nach Aufgabe variieren der Funktionsumfang und die Leistungsfähigkeit eines Sensors stark. Die Bandbreite umfasst einerseits Sensoren, die lediglich Messwerte liefern und nicht konfiguriert werden müssen. Es gibt aber auch solche, die eine Kalibrierung, Konfiguration oder Vorverarbeitung von Daten bis hin zur vollständigen Signalverarbeitung ermöglichen (intelligente Sensoren, smart sensors).“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_2_3_Sensoren_und_Aktoren.html.
IND.2.4	Maschine	„Eine Maschine ist eine technische Vorrichtung, die automatisierte Aufgaben durchführt. Ein typisches Beispiel dafür ist eine Werkzeugmaschine, die Produkte auf eine vorgegebene Art bearbeitet. Dabei wird sie von einem IT-System mithilfe eines Programms gesteuert, das die entsprechenden Arbeitsanweisungen und -schritte vorgibt. Solche Maschinen werden auch als Automaten bezeichnet. Meistens werden Maschinen von Maschinenbauern konstruiert und mit bestimmten vordefinierten Funktionen ausgestattet. Der Betreiber der Maschine kann allerdings noch die Parameter bestimmen, nach denen sie arbeiten soll. So lassen sich beispielsweise Formen, die gefräst werden sollen, oder Kalibrierungen für bestimmte Materialien einstellen. Damit der Betreiber die Parameter verändern kann, verfügen Maschinen über verschiedene Schnittstellen, z. B. für Wechseldatenträger, spezialisierte Programmiergeräte oder Netzzugriffe. Häufig werden von Maschinenbauern auch Fernwartungsdienstleistungen angeboten, um frühzeitigen Verschleiß zu erkennen oder bei Problemen schnell reagieren zu können.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_2_4_Maschine.html.

IND.2.7	Safety Instrumented Systems	„Safety Instrumented Systems (SIS) bilden eine Untergruppe der Industrial Control Systems (ICS). SIS werden eingesetzt, um Gefahren für technische Anlagen, die Umwelt und Personen abzuwehren. Der prinzipielle Aufbau von SIS unterscheidet sich kaum von den konventionellen Automatisierungssystemen. Der wesentliche Unterschied liegt in den erhöhten Anforderungen an die Zuverlässigkeit, mit der die von einem SIS auszuführenden Sicherheitsfunktionen (SIF) vollzogen werden. Das Maß an Zuverlässigkeit wird mit Hilfe des vierstufigen Sicherheits-Integritätslevels (SIL) ausgedrückt, diese werden in der IEC 61508 definiert. SIL1 ist hierbei die geringste und SIL4 die höchste Anforderung an die Zuverlässigkeit. Abhängig von der SIL-Stufe gelten unterschiedliche Anforderungen an die zulässige Ausfallrate von Komponenten, die Hardware-Fehlertoleranz der Architektur, die Unabhängigkeit von Prüfern sowie weitere sicherheitsrelevante Punkte. Der gesamte Lebenszyklus eines SIS ist organisatorisch in ein Functional Safety Management (FSM) eingebettet. Dieser Baustein ist unabhängig von der jeweiligen SIL-Stufe eines SIS umzusetzen. Die Informationssicherheit ist in jeder Lebensphase zu berücksichtigen, von der Entwicklung der Komponenten bis hin zu deren Anwendung, Betrieb und Außerbetriebnahme. Dabei ist zu beachten, dass die Sicherstellung der Integrität der SIS die höchste Priorität hat. Ein weiteres wesentliches Merkmal von SIS ist die Unabhängigkeit und die Trennung von umgebenden IT-Systemen und von der Betriebstechnik (Operational Technology, OT). Das bedeutet, dass die Verfügbarkeit und Integrität des SIS nicht von ihnen beeinflusst werden dürfen.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_2_7_Safety_Instrumented_Systems.html.
NET	**Netze und Kommunikation**	
NET.1.1	Netzarchitektur und -design	„Ein zuverlässiges Netzmanagement ist Grundvoraussetzung für den sicheren und effizienten Betrieb moderner Netze. Dazu ist es erforderlich, dass das Netzmanagement alle Netzkomponenten umfassend integriert. Außerdem müssen geeignete Maßnahmen umgesetzt werden, um die Netzmanagement-Kommunikation und -infrastruktur zu schützen. Das Netzmanagement umfasst viele wichtige Funktionen wie z. B. die Netzüberwachung, die Konfiguration der Komponenten, die Behandlung von Ereignissen und die Protokollierung. Eine weitere wichtige Funktion ist das Reporting, das als gemeinsame Plattform für Netz und IT-Systeme angelegt werden kann. Alternativ kann es dediziert als einheitliche Plattform oder als Bestandteil der einzelnen Netzmanagement-Komponenten realisiert werden. Die Netzmanagement-Infrastruktur besteht aus zentralen Management-Systemen, wie z. B. einem SNMP-Server, Administrations-Endgeräten mit Software für Managementzugriffe und dezentralen Managementagenten. Außerdem gehören dedizierte Managementwerkzeuge wie z. B. Probes bzw. spezifische Messgeräte sowie Managementprotokolle wie z. B. SNMP oder SSH dazu. Auch Managementschnittstellen wie dedizierte Ethernet-Ports oder Konsolen-Ports sind Bestandteil einer Netzmanagement-Infrastruktur.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_1_2_Netzmanagement.html.

NET.1.2	Netzmanagement	„Ein zuverlässiges Netzmanagement ist Grundvoraussetzung für den sicheren und effizienten Betrieb moderner Netze. Dazu ist es erforderlich, dass das Netzmanagement alle Netzkomponenten umfassend integriert. Außerdem müssen geeignete Maßnahmen umgesetzt werden, um die Netzmanagement-Kommunikation und -infrastruktur zu schützen. Das Netzmanagement umfasst viele wichtige Funktionen wie z. B. die Netzüberwachung, die Konfiguration der Komponenten, die Behandlung von Ereignissen und die Protokollierung. Eine weitere wichtige Funktion ist das Reporting, das als gemeinsame Plattform für Netz und IT-Systeme angelegt werden kann. Alternativ kann es dediziert als einheitliche Plattform oder als Bestandteil der einzelnen Netzmanagement-Komponenten realisiert werden. Die Netzmanagement-Infrastruktur besteht aus zentralen Management-Systemen, wie z. B. einem SNMP-Server, Administrations-Endgeräten mit Software für Managementzugriffe und dezentralen Managementagenten. Außerdem gehören dedizierte Managementwerkzeuge wie z. B. Probes bzw. spezifische Messgeräte sowie Managementprotokolle wie z. B. SNMP oder SSH dazu. Auch Managementschnittstellen wie dedizierte Ethernet-Ports oder Konsolen-Ports sind Bestandteil einer Netzmanagement-Infrastruktur.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_1_2_Netzmanagement.html.
NET.3.1	Router und Switches	„Router und Switches bilden das Rückgrat heutiger IT-Netze. Ein Ausfall eines oder mehrerer dieser Geräte kann zum kompletten Stillstand der gesamten IT-Infrastruktur führen. Sie müssen daher besonders abgesichert werden. Router arbeiten auf der OSI-Schicht 3 (Netzschicht) und vermitteln Datenpakete anhand der Ziel-IP-Adresse im IP-Header. Router sind in der Lage, Netze mit unterschiedlichen Topographien zu verbinden. Sie werden verwendet, um lokale Netze zu segmentieren oder um lokale Netze über Weitverkehrsnetze zu verbinden. Ein Router identifiziert eine geeignete Verbindung zwischen dem Quellsystem bzw. Quellnetz und dem Zielsystem bzw. Zielnetz. In den meisten Fällen geschieht dies, indem er die Datenpakete an den nächsten Router weitergibt. Switches arbeiteten ursprünglich auf der OSI-Schicht 2, mittlerweile sind sie jedoch mit unterschiedlichen Funktionen erhältlich. Hersteller kennzeichnen die Geräte meist mit dem OSI-Layer, der unterstützt wird. Dadurch entstanden die Begriffe Layer-2-, Layer-3- und Layer-4-Switch, wobei es sich bei Layer-3- und Layer-4-Switches eigentlich funktional bereits um Router handelt. Die ursprünglich unterschiedlichen Funktionen von Switches und Routern werden somit heute oft auf einem Gerät vereint.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_1_Router_und_Switches.html.

NET.3.2	Firewall	„Eine Firewall ist ein System aus soft- und hardwaretechnischen Komponenten, das dazu eingesetzt wird, IP-basierte Datennetze sicher zu koppeln. Dazu wird mithilfe einer Firewall-Struktur der technisch mögliche Informationsfluss auf die in einer Sicherheitsrichtlinie als vorher sicher definierte Kommunikation eingeschränkt. Sicher bedeutet hierbei, dass ausschließlich die erwünschten Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen werden. Um Netzübergänge abzusichern, wird oft nicht mehr eine einzelne Komponente verwendet, sondern eine ganze Reihe von IT-Systemen, die unterschiedliche Aufgaben übernehmen, z. B. ausschließlich Pakete zu filtern oder Netzverbindungen mithilfe von Proxy-Funktionen strikt zu trennen. Der in diesem Baustein verwendete Begriff „Application Level Gateway“ (ALG) bezeichnet eine Firewall-Komponente, die Datenströme auf Basis von Sicherheitsproxies regelt. Eine Firewall wird am zentralen Übergang zwischen unterschiedlich vertrauenswürdigen Netzen eingesetzt. Unterschiedlich vertrauenswürdige Netze stellen dabei nicht unbedingt nur die Kombination aus Internet und Intranet dar. Vielmehr können auch zwei institutionsinterne Netze einen unterschiedlich hohen Schutzbedarf besitzen. So hat z. B. das Netz der Bürokommunikation meistens einen geringeren Schutzbedarf als das Netz der Personalabteilung, in dem besonders schützenswerte, personenbezogene Daten übertragen werden.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_2_Firewall.html.
NET.3.3	VPN	„Mithilfe von Virtuellen Privaten Netzen (VPNs) können schutzbedürftige Daten über nicht-vertrauenswürdige Netze wie das Internet übertragen werden. Ein VPN ist ein Netz, das physisch innerhalb eines anderen Netzes betrieben wird, jedoch logisch von diesem Netz getrennt ist. VPNs können mithilfe kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten schützen. Die sichere Authentisierung der Kommunikationspartner ist auch dann möglich, wenn mehrere Netze oder IT-Systeme über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_3_VPN.html.
NET.4.1	TK-Anlagen	„Mit einer Telekommunikationsanlage, kurz TK-Anlage, können die Telefone einer Institution intern verbunden und extern an ein öffentliches Telefonnetz angeschlossen werden. Durch die zunehmende Verzahnung von IT und Telekommunikation können TK-Anlagen dabei sowohl analog als auch IP-basiert aufgebaut sein. Hybrid-Anlagen sind eine Kombination aus einer klassischen Telekommunikationslösung und einem VoIP-System. Mit einer Hybrid-Anlage können klassische digitale und analoge Telefonie sowie VoIP gleichzeitig betrieben werden. Neben der Sprachtelefonie können, abhängig von den angeschlossenen Endgeräten, weitere Dienste genutzt werden. So ist es möglich, mittels TK-Anlagen Daten, Texte, Grafiken und Bewegtbilder zu übertragen. Die Informationen können dabei analog oder digital über drahtgebundene oder drahtlose Übertragungsmedien weitergeleitet werden. Je nach Anbindung und genutzten Datennetzen können in einer Institution verschiedenste Telekommunikationsanlagen eingesetzt werden.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_4_1_TK-Anlagen.html.

NET.4.2	VoIP	„Voice over IP (VoIP) bezeichnet das Telefonieren über Datennetze, insbesondere über das Internet. Um Signalisierungsinformationen zu übertragen, beispielsweise bei einem Anruf, werden spezielle Signalisierungsprotokolle eingesetzt. Die eigentlichen Nutzdaten wie Sprache oder Video werden mit Hilfe eines Medientransportprotokolls übermittelt. Beide Protokolle werden jeweils benötigt, um eine Multimediaverbindung aufzubauen und aufrechtzuerhalten. Bei einigen Verfahren wird nur ein Protokoll sowohl für die Signalisierung als auch für den Medientransport benötigt.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_4_2_VoIP.html.
INF	**Infrastruktur**	
INF.1	Allgemeines Gebäude	„Ein Gebäude umfasst alle stationären Arbeitsplätze, die verarbeiteten Informationen sowie die aufgestellte Informationstechnik. Es gewährleistet somit einen äußeren Schutz. Daher ist nicht nur das Bauwerk an sich, also Wände, Decken, Böden, Dach, Fenster sowie Türen zu betrachten, sondern auch alle gebäudeweiten Infrastruktur- und Versorgungseinrichtungen wie Strom, Wasser, Gas, Heizung und Kühlung. Betrachtet wird ein Gebäude, das von einer oder mehreren Organisationseinheiten einer Institution genutzt wird. Diese können unterschiedliche Sicherheitsansprüche haben. Zudem muss in alle Überlegungen einfließen, dass ein Gebäude fast immer auch von institutionsfremden Personen, wie Bürgern, Kunden oder Lieferanten, betreten wird. Wenn ein Gebäude von verschiedenen Parteien genutzt wird, dann müssen Gestaltung und Ausstattung des Gebäudes und das Nutzungskonzept für das Gebäude zueinander passen. Es soll eine optimale Umgebung für die dort tätigen Menschen sichergestellt werden. Unberechtigte sollen dort keinen Zutritt erhalten, wo sie die Sicherheit beeinträchtigen könnten. Die im Gebäude stationierte Technik soll zudem sicher und effizient betrieben werden können.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_1_Allgemeines_Geb%C3%A4ude.html.

INF.2	Rechenzentrum sowie Serverraum	„Heute werden fast alle strategischen und operativen Funktionen und Aufgaben durch Informationstechnik (IT) maßgeblich unterstützt oder sind ohne IT nicht ausführbar. Dadurch steigen die Anforderungen an die Leistungsfähigkeit und Verfügbarkeit der IT-Systeme und deren Anbindung an die Netzumgebung stetig. Um diesem Leistungsbedarf gerecht zu werden, um entsprechende Reserven vorzuhalten und um die IT auch wirtschaftlich betreiben zu können, konzentrieren Institutionen jeglicher Größe ihre IT-Landschaft in Rechenzentren. Ein Rechenzentrum (RZ) ist wie folgt definiert: 1. Wird die IT der Institution innerhalb eines Gebäudes oder einer Liegenschaft verteilt in mehreren Bereichen betrieben und sind diese Bereiche untereinander und zu den IT-Benutzern hin durch hauseigene LAN-Verbindungen angeschlossen, ist mindestens der funktional bedeutendste dieser Bereiche als RZ zu behandeln. Des Weiteren sind Bereiche, von deren ordnungsgemäßem Betrieb 50 % und mehr Nutzer abhängig sind oder aus denen heraus 50 % und mehr an Diensten und Daten (gemessen an der Gesamtheit der Bereiche) bereitgestellt werden, als RZ zu behandeln. 2. Hat eine IT-nutzende Institution nur einen zentralen IT-Betriebsbereich, ist dieser gemeinsam mit den erforderlichen Supportbereichen grundsätzlich immer wie ein RZ entsprechend dem Schutzbedarf zu behandeln. Unter „IT-Betriebsbereich“ sind Räume zu verstehen, in denen die Hardware aufgebaut ist und betrieben wird, die der Bereitstellung von Diensten und Daten dient. Das RZ umfasst neben dem IT-Betriebsbereich alle weiteren technischen Supportbereiche (z. B. Stromversorgung, Kälteversorgung, Löschtechnik, Sicherheitstechnik), die dem bestimmungsgemäßen Betrieb und der Sicherheit des IT-Betriebsbereichs dienen. 3. Ist die IT-nutzende Institution an mehreren räumlich voneinander getrennten Standorten angesiedelt und sind diese durch andere als hauseigene LAN-Verbindungen miteinander gekoppelt, ist jeder der Standorte entsprechend (1) separat zu betrachten und zu behandeln. 4. Ein IT-Betriebsbereich, in dem für kritische Geschäftsprozesse (Prozesse, deren Störung oder Ausfall zu wesentlichen Beeinträchtigungen der Erledigung primärer Aufgaben einer Institution führen) erforderliche IT angesiedelt ist, ist immer als RZ zu behandeln, unabhängig von Größe oder Anteilsregeln aus Nummer (2). 5. IT-Betriebsbereiche, aus denen heraus Dienste oder Dienstleistungen für Dritte erbracht werden, sind immer als Teil eines RZ zu betrachten. Dabei ist es unerheblich, ob dies gegen Entgelt erfolgt oder nicht. 6. Besteht ein begründetes Interesse, einen IT-Betriebsbereich gemeinsam mit seinem Supportbereich abweichend von den vorgenannten Regelungen als Serverraum zu behandeln, ist dies samt den sich daraus ergebenden Reduzierungen von Sicherheitsanforderungen zu begründen. Weicht ein Rechenzentrum von dieser Definition ab, wird der betrachtete IT-Betriebsbereich als Serverraum bezeichnet. Diese Definition orientiert sich ausschließlich an der Bedeutung der IT-Struktur für die Aufgabenerfüllung der nutzenden Institution und steht damit im methodischen Einklang mit der DIN EN 50600. Soll ein Serverraum abgesichert werden, können die Anforderungen dieses Bausteins entsprechend reduziert werden. Dies muss jedoch stichhaltig und nachvollziehbar begründet werden (6) und es müssen mindestens die Basis-Anforderungen umgesetzt werden.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_2_Rechenzentrum_sowie_Serverraum.html.

INF.3	Elektro-technische Verkabelung	„Die elektrotechnische Verkabelung von IT-Systemen und anderen Geräten umfasst alle Kabel und Verteilungen im Gebäude vom Einspeisepunkt des Verteilungsnetzbetreibers bis zu den Elektro-Anschlüssen der Verbraucher. Die ordnungsgemäße und normgerechte Ausführung der elektrotechnischen Verkabelung ist Grundlage für den sicheren IT-Betrieb.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_3_Elektrotechnische_Verkabelung.html.
INF.4	IT-Ver-kabelung	„Die IT-Verkabelung umfasst alle Kommunikationskabel und passiven Komponenten wie Rangier- bzw. Spleißverteiler oder Patchfelder innerhalb einer Institution. Sie bildet also die physikalische Grundlage der internen Kommunikationsnetze. Die IT-Verkabelung reicht von Übergabepunkten aus einem Fremdnetz, z. B. dem Anschluss eines TK-Anbieters oder der DSL-Anbindung eines Internet-Providers, bis zu den Anschlusspunkten der Netzteilnehmer.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_4_IT-Verkabelung.html.
INF.5	Raum sowie Schrank für technische Infrastruktur	„Ein Raum für technische Infrastruktur enthält technische Komponenten, die nur selten direkt vor Ort bedient werden müssen. Sie sind aber unabdingbar für die Gebäudeinfrastruktur und damit auch für die IT-Infrastruktur. Dabei kann es sich z. B. um Verteiler für die Energieversorgung, Sicherungskästen, Lüftungsanlagen, TK-Anlagenteile, Patchfelder, Switches oder Router handeln. Dieser Raum ist kein ständiger Arbeitsplatz und wird in der Regel nur zu Wartungszwecken betreten bzw. geöffnet. Wenn die zu schützende technische Infrastruktur nicht in einem separaten Raum untergebracht werden kann oder sich der Raum nicht entsprechend der beschriebenen Anforderungen einrichten lässt, kann die technische Infrastruktur auch in einem eigens dafür ausgerüsteten Schrank untergebracht werden. Das kann auch sinnvoll sein, wenn für die Unterbringung der technischen Infrastruktur ein Schrank die wirtschaftlichste Alternative darstellt. Die Anforderungen an den Raum sind dann möglichst wirkungsgleich auf den Schrank und dessen Hülle zu übertragen.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_5_Raum_sowie_Schrank_f%C3%BCr_technische_Infrastruktur.html.
INF.7	Büroarbeits-platz	„Ein Büroraum ist der Bereich innerhalb einer Institution, in dem sich ein oder mehrere Mitarbeiter aufhalten, um dort ihre Aufgaben zu erfüllen. In diesem Baustein werden die typischen Gefährdungen und Anforderungen bezüglich der Informationssicherheit für einen Büroraum beschrieben.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_7_B%C3%BCroarbeitsplatz.html.

INF.8	Häuslicher Arbeitsplatz	„Telearbeiter, freie Mitarbeiter oder Selbstständige arbeiten typischerweise von häuslichen Arbeitsplätzen aus. Im Gegensatz zum Arbeitsplatz im Büro nutzen diese Mitarbeiter einen Arbeitsplatz in der eigenen Wohnung. Dabei muss ermöglicht werden, dass die berufliche Umgebung hinreichend von der privaten getrennt ist. Wenn Mitarbeiter häusliche Arbeitsplätze dauerhaft benutzen, müssen zudem diverse rechtliche Anforderungen erfüllt sein, beispielsweise müssen die Arbeitsplätze arbeitsmedizinischen und ergonomischen Bestimmungen entsprechen. Bei einem häuslichen Arbeitsplatz kann nicht die gleiche infrastrukturelle Sicherheit vorausgesetzt werden, wie sie in den Büroräumen einer Institution anzutreffen ist. So ist z. B. der Arbeitsplatz oft auch für Besucher oder Familienangehörige zugänglich. Deshalb müssen Maßnahmen ergriffen werden, mit denen sich ein Sicherheitsniveau erreichen lässt, das mit einem Büroraum vergleichbar ist.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_8_H%C3%A4uslicher_Arbeitsplatz.html.
INF.9	Mobiler Arbeitsplatz	„Eine gute Netzabdeckung sowie leistungsfähige IT-Geräte, wie z. B. Laptops, Smartphones oder Tablets, ermöglichen es Mitarbeitern, nahezu an jedem Platz bzw. von überall zu arbeiten. Das bedeutet, dass dienstliche Aufgaben häufig nicht mehr nur in den Räumen und Gebäuden der Institution erfüllt werden, sondern an wechselnden Arbeitsplätzen in unterschiedlichen Umgebungen, z. B. in Hotelzimmern, in Zügen oder bei Kunden. Die dabei verarbeiteten Informationen müssen angemessen geschützt werden. Das mobile Arbeiten verändert einerseits die Dauer, Lage und Verteilung der Arbeitszeiten. Andererseits erhöht es die Anforderungen an die Informationssicherheit, da in mobilen Arbeitsplatz-Umgebungen keine sichere IT-Infrastruktur vorausgesetzt werden kann, so wie sie in einer Büroumgebung anzutreffen ist.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_9_Mobiler_Arbeitsplatz.html.
INF.10	Besprechungs-,Veranstaltungs- und Schulungsraum	„In der Regel hat jede Institution einen oder mehrere Räume, in denen Besprechungen, Schulungen oder sonstige Veranstaltungen durchgeführt werden können. Hierfür sind oft speziell ausgestattete Räume vorgesehen. Besprechungs-, Veranstaltungs- und Schulungsräume zeichnen sich im Wesentlichen dadurch aus, dass sie von wechselnden Personen bzw. Personenkreisen und Besuchern in der Regel nur für einen begrenzten Zeitraum genutzt werden. Mitgebrachte IT-Systeme werden dabei häufig gemeinsam mit Geräten der Institution betrieben, wie beispielsweise institutionsfremde Laptops an fest verbauten Beamern. Aus diesen unterschiedlichen Nutzungsszenarien heraus ergibt sich eine besondere Gefährdungslage, die in anderen Räumen der Institution in dieser Weise nicht existiert.“ Weitere Informationen, siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_10_Besprechungs-_Veranstaltungs-_und_Schulungsr%C3%A4ume.html.

7.2.6 MUC-Template Abschnitt „6 – Common Terms and Definitions”

Hier können Abkürzungen und Definitionen aufgelistet werden. Da dieses Dokument bereits zu Beginn ein Abkürzungsverzeichnis beinhaltet, wird diese Tabelle hier nicht aufgeführt.

7.2.7 MUC-Template Abschnitt „7 – Custom information (optional)“

Die in Abschnitt 7 aufgeführte Tabelle ist für diese Studie nicht notwendig und wird daher hier ausgespart.

7.3 Übersicht Beispiele für identifizierte Sicherheitsanforderungen

ID	Anforderungsname	Beispiele
ISMS.1	Sicherheits-management	Benennung eines Informationssicherheitsbeauftragten, Dokumentation Sicherheitsprozess
ORP.1	Organisation	Vergabe von Berechtigungen, Geräteverwaltung
ORP.2	Personal	Geregelte Einarbeitung Mitarbeiter, Vertraulichkeitsvereinbarung
ORP.3	Sensibilisierung und Schulung	Ansprechpartner zu Sicherheitsfragen, Sicherheitseinweisung Mitarbeiter für die IT
ORP.4	Identitäts- und Berech-tigungsmanagement	Aufgabenverteilung und Funktionstrennung, Identifikation und Authentisierung
ORP.5	Compliance Manage-ment (Anforderungs-management)	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen, Konzeption und Organisation des Compliance Managements
CON.1	Kryptokonzept	Auswahl geeigneter kryptografischer Verfahren, Verschlüsselung der Kommunikationsverbindungen
CON.2	Datenschutz	Umsetzung Standard-Datenschutzmodell
CON.3	Datensicherungskon-zept	Regelmäßige Datensicherung, Verpflichtung der Mitarbeiter zur Datensicherung
CON.4	Auswahl und Einsatz von Standardsoftware	Sicherstellen der Integrität von Standardsoftware, sichere Installation und Konfiguration von Standardsoftware
CON.5	Entwicklung und Einsatz von Individualsoftware	Festlegung benötigter Sicherheitsfunktionen der Individualsoftware, geeignete Steuerung der Anwendungsentwicklung
CON.6	Löschen und Vernichten	Regelung der Vorgehensweise für die Löschung und Vernichtung von Informationen, Beseitigung von Restinformationen
CON.8	Software-Entwicklung	Sicheres Systemdesign, Verwendung von Bibliotheken aus vertrauenswürdigen Quellen, Sicherer Einsatz der Test- und Entwicklungsumgebungen
CON.9	Informationsaustausch	Regelung des Informationsaustausches, Verschlüsselung und Signatur
OPS1.1.2	Ordnungsgemäße IT-Administration	Personalauswahl für administrative Tätigkeiten, Regelungen für Wartungs- und Reparaturarbeiten
OPS1.1.3	Patch- und Änderungs-management	Konfiguration von Autoupdate-Mechanismen, Sicherstellung der Integrität und Authentizität von Softwarepaketen
OPS1.1.4	Schutz vor Schad-programmen	Nutzung systemspezifischer Schutzmechanismen, Sensibilisierung und Verpflichtung der Benutzer

Tabelle wird auf den nächsten Seiten fortgesetzt →

ID	Anforderungsname	Beispiele
OPS1.1.5	Protokollierung	Zugriffsschutz für Protokollierungsdaten, Verschlüsselung der Protokollierungsdaten
OPS1.1.6	Software-Tests und -Freigaben	Durchführung von funktionalen Software-Tests, Personalauswahl der Software-Tester
OPS.1.2.4	Telearbeit	Sicherheitstechnische Anforderungen an den Telearbeitsrechner, Sensibilisierung und Schulung der Telearbeiter
OPS.1.2.5	Fernwartung	Absicherung der Schnittstellen zur Fernwartung, sichere Protokolle bei der Fernwartung
OPS2.1	Outsourcing für Kunden	Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben, Vereinbarung über Datenaustausch zwischen den Outsourcing-Partnern
OPS2.2	Cloud-Nutzung	Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung, Einsatz von Verschlüsselung bei Cloud-Nutzung
OPS3.1	Outsourcing für Dienstleister	Festlegung der möglichen Kommunikationspartner, Vereinbarung über die Anbindung an Netze der Outsourcing-Partner
DER.1	Detektion von sicherheitsrelevanten Ereignissen	Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen, automatische Reaktion auf sicherheitsrelevante Ereignisse
DER.2.1	Behandlung von Sicherheitsvorfällen	Eskalationsstrategie für Sicherheitsvorfälle, Nachbereitung von Sicherheitsvorfällen
DER.2.2	Vorsorge für die IT-Forensik	Erstellung eines Leitfadens für Beweissicherungsmaßnahmen bei IT-Sicherheitsvorfällen, sichere Verwahrung von Originaldatenträgern und Beweismitteln
DER.2.3	Bereinigung weitreichender Sicherheitsvorfälle	Sperrung und Änderung von Zugangsdaten und kryptografischen Schlüsseln, gezielte Systemhärtung
DER.3.1	Audits und Revisionen	Überprüfung des Risikobehandlungsplans, Dokumentation der Revisionsergebnisse
DER.4	Notfallmanagement	Erstellung eines Notfallkonzepts, regelmäßige Überprüfung und Verbesserung der Notfallmaßnahmen
APP.1.1	Office-Produkte	Sicherstellen der Integrität von Office-Produkten, Schutz gegen nachträgliche Veränderungen von Dokumenten
APP.1.2	Web-Browser	Verwendung von vertrauenswürdigen Zertifikaten, Zwei-Browser-Strategie
APP.2.1	Allgemeiner Verzeichnisdienst	Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste, sicherer Betrieb von Verzeichnisdienste
APP.2.2	Active Directory	Härtung des Active Directory, Trennung von Administrations- und Produktionsumgebung
APP.2.3	OpenLDAP	Konfiguration der durch OpenLDAP verwendeten Datenbank, Konfiguration der durch OpenLDAP verwendeten Datenbank

ID	Anforderungsname	Beispiele
APP.3.1	Webanwendungen	Sichere Anbindung von Hintergrundsystemen, Einsatz von Web Application Firewalls
APP.3.2	Webserver	Penetrationstest und Revision, Schutz vor Denial-of-Service-Angriffen
APP.3.3	Fileserver	Einsatz von Viren-Schutzprogrammen, Verschlüsselung des Datenbestandes
APP.3.6	DNS-Server	Sichere Grundkonfiguration eines DNS-Servers, Einsatz von DNSSEC
APP.4.3	Relationale Datenbanksysteme	Zeitnahes Einspielen von Sicherheitsupdates, Überwachung des Datenbankmanagementsystems
APP.5.1	Allgemeine Groupware	Sicherer Betrieb von Groupware-Systemen, Umgang mit Spam durch Benutzer
APP.5.2	Microsoft Exchange und Outlook	Absicherung der Kommunikation zwischen Microsoft Exchange-Systemen, Einsatz von Outlook Anywhere
SYS.1.1	Allgemeiner Server	Einrichtung lokaler Paketfilter, aktive Verwaltung der Wurzelzertifikate
SYS.1.5	Virtualisierung	Einsatz einer PKI, Kapselung der virtuellen Maschinen
SYS.1.8	Speicherlösungen	Einsatz einer hochverfügbaren SAN-Lösung, Absicherung eines SANs durch Segmentierung
SYS.2.1	Allgemeiner Client	Rollentrennung, Kompatibilitätsprüfung von Software
SYS.3.1	Laptops	Zugriffsschutz am Laptop, geeignete Aufbewahrung von Laptops
SYS.3.2.1	Allgemeine Smartphones und Tablets	Verhaltensregeln bei Sicherheitsvorfällen, Nutzung von PIM-Containern
SYS.3.2.2	Mobile Device Management (MDM)	Verteilung der Grundkonfiguration auf mobile Endgeräte, Auswahl und Freigabe von Apps
SYS.3.2.3	iOS (for Enterprise)	Verwendung der Gerätecode-Historie, keine Verbindung mit Host-Systemen
SYS.3.2.4	Android	Deaktivieren der Entwickler-Optionen, Verwendung einer Firewall
SYS.3.3	Mobiltelefon	Sperrmaßnahmen bei Verlust eins Mobiltelefons, sichere Datenübertragung über Mobiltelefone
SYS.4.1	Drucker, Kopierer und Multifunktionsgeräte	Verschlüsselung von Informationen bei Druckern, Konfiguration von Druckern
SYS.4.3	Eingebettete Systeme	Hardware-Realisierung von Funktionen eingebetteter Systeme, Einsatz kryptografischer Prozessoren bzw. Koprozessoren bei eingebetteten Systemen
SYS.4.4	Allgemeines IoT-Gerät	Deaktivierung und Deinstallation nicht benötigter Komponenten, Schutz der Administrationsschnittstellen
SYS.4.5	Wechseldatenträger	Datenträgerverschlüsselung, Integritätsschutz durch Checksummen oder digitale Signaturen

ID	Anforderungsname	Beispiele
IND.1	Betriebs- und Steuerungstechnik	Dokumentation der OT-Infrastruktur, Änderungsmanagement im OT-Betrieb
IND.2.1	Allgemeine ICS-Komponente	Zentrale Systemprotokollierung und –überwachung, Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen
IND.2.2	Speicherprogrammierbare Steuerung (SPS)	Erweiterte Systemdokumentation für Speicherprogrammierbare Steuerungen, Zeitsynchronisation
IND.2.3	Sensoren und Aktoren	Installation von Sensoren, Kalibrierung von Sensoren
IND.2.4	Maschine	Fernwartung durch Maschinen- und Anlagenbauer, Betrieb nach Ende der Gewährleistung
IND.2.7	Safety Instrumented Systems	Verankerung von Informationssicherheit im Functional Safety Management, Absicherung der Daten- und Signalverbindungen
NET.1.1	Netzarchitektur und -design	DMZ-Segmentierung für Zugriffe aus dem Internet, Netzplanung
NET.1.2	Netzmanagement	Beschränkung der SNMP-Kommunikation, grundsätzliche Nutzung von sicheren Protokollen
NET.3.1	Router und Switches	Schutz vor Fragmentierungsangriffen, Bogon- und Spoofing-Filterung
NET.3.2	Firewall	Einrichten geeigneter Filterregeln am Paketfilter, Absicherung von grundlegenden Internetprotokollen
NET.3.3	VPN	Planung der technischen VPN-Realisierung, sichere Anbindung eines externen Netzes
NET.4.1	TK-Anlagen	Änderung voreingestellter Passwörter, Absicherung von Remote-Zugängen
NET.4.2	VoIP	Einschränkung der Erreichbarkeit über VoIP, Trennung des Daten- und VoIP-Netzes
INF.1	Allgemeines Gebäude	Sicherheitskonzept für die Gebäudenutzung, unabhängige elektrische Versorgungsstränge
INF.2	Rechenzentrum sowie Serverraum	Perimeterschutz für das Rechenzentrum, Überspannungsschutzeinrichtung
INF.3	Elektrotechnische Verkabelung	Auswahl geeigneter Kabeltypen, Planung der Kabelführung
INF.4	IT-Verkabelung	Fachgerechte Installation, Redundanzen für die Verkabelung
INF.5	Raum sowie Schrank für technische Infrastruktur	Schutz vor Einbruch, Vermeidung sowie Schutz vor elektromagnetischen Störfeldern
INF.7	Büroarbeitsplatz	Geschlossene Fenster und abgeschlossene Türen, geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger

ID	Anforderungsname	Beispiele
INF.8	Häuslicher Arbeitsplatz	Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz, Umgang mit dienstlichen Unterlagen bei erhöhtem Schutzbedarf am häuslichen Arbeitsplatz
INF.9	Mobiler Arbeitsplatz	Arbeiten mit fremden IT-Systemen, zeitnahe Verlustmeldung
INF.10	Besprechungs-, Veranstaltungs- und Schulungsraum	Sichere Konfiguration von Schulungs- und Präsentationsrechnern, Mitführverbot von Mobiltelefonen

7.4 Gefährdungskatalog nach BSI-Grundschutz

- *G 0.1 Feuer*
- *G 0.2 Ungünstige klimatische Bedingungen*
- *G 0.3 Wasser*
- *G 0.4 Verschmutzung, Staub, Korrosion*
- *G 0.5 Naturkatastrophen*
- *G 0.6 Katastrophen im Umfeld*
- *G 0.7 Großereignisse im Umfeld*
- *G 0.8 Ausfall oder Störung der Stromversorgung*
- *G 0.9 Ausfall oder Störung von Kommunikationsnetzen*
- *G 0.10 Ausfall oder Störung von Versorgungsnetzen*
- *G 0.11 Ausfall oder Störung von Dienstleistern*
- *G 0.12 Elektromagnetische Störstrahlung*
- *G 0.13 Abfangen kompromittierender Strahlung*
- ***G 0.14 Ausspähen von Informationen (Spionage):*** *„Mit Spionage werden Angriffe bezeichnet, die das Ziel haben, Informationen über Unternehmen, Personen, Produkte oder andere Zielobjekte zu sammeln, auszuwerten und aufzubereiten. Die aufbereiteten Informationen können dann beispielsweise eingesetzt werden, um einem anderem Unternehmen bestimmte Wettbewerbsvorteile zu verschaffen, Personen zu erpressen oder ein Produkt nachbauen zu können.*

Neben einer Vielzahl technisch komplexer Angriffe gibt es oft auch viel einfachere Methoden, um an wertvolle Informationen zu kommen, beispielsweise indem Informationen aus mehreren öffentlich zugäng-

lichen Quellen zusammengeführt werden, die einzeln unverfänglich aussehen, aber in anderen Zusammenhängen kompromittierend sein können. Da vertrauliche Daten häufig nicht ausreichend geschützt werden, können diese oft auf optischem, akustischem oder elektronischem Weg ausgespäht werden."[1]

↳ *G 0.15 Abhören*

↳ *G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten*

↳ *G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten*

↳ *G 0.18 Fehlplanung oder fehlende Anpassung*

↳ *G 0.19 Offenlegung schützenswerter Informationen*

↳ *G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle*

↳ *G 0.21 Manipulation von Hard- oder Software*

↳ ***G 0.22 Manipulation von Informationen:*** *„Informationen können auf vielfältige Weise manipuliert werden, z. B. durch fehlerhaftes oder vorsätzlich falsches Erfassen von Daten, inhaltliche Änderung von Datenbank-Feldern oder von Schriftverkehr. Grundsätzlich betrifft dies nicht nur digitale Informationen, sondern beispielsweise auch Dokumente in Papierform. Ein Täter kann allerdings nur die Informationen manipulieren, auf die er Zugriff hat. Je mehr Zugriffsrechte eine Person auf Dateien und Verzeichnisse von IT-Systemen besitzt bzw. je mehr Zugriffsmöglichkeiten auf Informationen sie hat, desto schwerwiegendere Manipulationen kann sie vornehmen. Falls die Manipulationen nicht frühzeitig erkannt werden, kann der reibungslose Ablauf von Geschäftsprozessen und Fachaufgaben dadurch empfindlich gestört werden.*

Archivierte Dokumente stellen meist schützenswerte Informationen dar. Die Manipulation solcher Dokumente ist besonders schwerwiegend, da sie unter Umständen erst nach Jahren bemerkt wird und eine Überprüfung dann oft nicht mehr möglich ist."[2]

↳ *G 0.23 Unbefugtes Eindringen in IT-Systeme*

↳ *G 0.24 Zerstörung von Geräten oder Datenträgern*

↳ *G 0.25 Ausfall von Geräten oder Systemen*

↳ *G 0.26 Fehlfunktionen von Geräten oder Systemen*

↳ *G 0.27 Ressourcenmangel*

1 Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrdungen/G_0_14_Aussp%C3%A4hen_von_Informationen__(Spionage).html.

2 Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrdungen/G_0_22_Manipulation_von_Informationen.html.

↳ *G 0.28 Software-Schwachstellen oder -Fehler*

↳ *G 0.29 Verstoß gegen Gesetze oder Regelungen*

↳ *G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen*

↳ *G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen*

↳ *G 0.32 Missbrauch von Berechtigungen*

↳ *G 0.33 Personenausfall*

↳ *G 0.34 Anschlag*

↳ *G 0.35 Nötigung, Erpressung oder Korruption*

↳ *G 0.36 Identitätsdiebstahl*

↳ *G 0.37 Abstreiten von Handlungen*

↳ *G 0.38 Missbrauch personenbezogener Daten*

↳ *G 0.39 Schadprogramm*

↳ ***G 0.40 Verhinderung von Diensten (Denial of Service):*** *„Es gibt eine Vielzahl verschiedener Angriffsformen, die darauf abzielen, die vorgesehene Nutzung bestimmter Dienstleistungen, Funktionen oder Geräte zu verhindern. Der Oberbegriff für solche Angriffe ist "Verhinderung von Diensten" (englisch: "Denial of Service"). Häufig wird auch die Bezeichnung "DoS-Angriff" verwendet.*
Solche Angriffe können unter anderem von verärgerten Mitarbeitern oder Kunden, aber auch von Mitbewerbern, Erpressern oder politisch motivierten Tätern ausgehen. Das Ziel der Angriffe können geschäftsrelevante Werte aller Art sein. Typische Ausprägungen von DoS-Angriffen sind

- *Störungen von Geschäftsprozessen, z. B. durch Überflutung der Auftragsannahme mit fehlerhaften Bestellungen,*
- *Beeinträchtigungen der Infrastruktur, z. B. durch Blockieren der Türen der Institution,*
- *Herbeiführen von IT-Ausfällen, indem z. B. Dienste eines Servers im Netz gezielt überlastet werden*

Diese Art von Angriffen steht häufig im Zusammenhang mit verteilten Ressourcen, indem ein Angreifer diese Ressourcen so stark in Anspruch nimmt, dass sie den eigentlichen Nutzern nicht mehr zur Verfügung stehen. Bei IT-basierten Angriffen können z. B. die folgenden Ressourcen künstlich verknappt werden:

Prozesse, CPU-Zeit, Arbeitsspeicher, Plattenplatz, Übertragungskapazität."[3]

↳ *G 0.41 Sabotage*

↳ *G 0.42 Social Engineering*

↳ *G 0.43 Einspielen von Nachrichten*

↳ *G 0.44 Unbefugtes Eindringen in Räumlichkeiten*

↳ *G 0.45 Datenverlust*

↳ *G 0.46 Integritätsverlust schützenswerter Informationen*

↳ *G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe*

7.5 CAPEC Katalog: verwendete Angriffsvektoren

Im Folgenden werden die Inhalte der für diese Studie ausgewählten Angriffsvektoren aus dem CAPEC-Katalog aufgelistet.

7.5.1 CAPEC-94: Man in the Middle Attack

↳ *Description: This type of attack targets the communication between two components (typically client and server). The attacker places themself in the communication channel between the two components. Whenever one component attempts to communicate with the other (data flow, authentication challenges, etc.), the data first goes to the attacker, who has the opportunity to observe or alter it, and it is then passed on to the other component as if it was never observed. This interposition is transparent leaving the two compromised components unaware of the potential corruption or leakage of their communications. The potential for Man-in-the-Middle attacks yields an implicit lack of trust in communication or identify between two components. MITM attacks differ from sniffing attacks since they often modify the communications prior to delivering it to the intended recipient. These attacks also differ from interception attacks since they may forward the sender's original unmodified data, after copying it, instead of keeping it for themselves.*

↳ *Execution Flow*

- *Experiment*

1. The attacker probes to determine the nature and mechanism of communication between two components looking for opportunities to exploit.

3 Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrdungen/G_0_22_Manipulation_von_Informationen.html.

2. The attacker inserts themself into the communication channel initially acting as a routing proxy between the two targeted components. The attacker may or may not have to use cryptography.

- *Exploit*

1. The attacker observes, filters or alters passed data of its choosing to gain access to sensitive information or to manipulate the actions of the two target components for their own purposes.

↳ *Prerequisites:*

- *There are two components communicating with each other.*
- *An attacker is able to identify the nature and mechanism of communication between the two target components.*
- *An attacker can eavesdrop on the communication between the target components.*
- *Strong mutual authentication is not used between the two target components yielding opportunity for attacker interposition.*
- *The communication occurs in clear (not encrypted) or with insufficient and spoofable encryption.*
- *Mitigations:*
- *Get your Public Key signed by a Certificate Authority.*
- *Encrypt your communication using cryptography (SSL,...).*
- *Use Strong mutual authentication to always fully authenticate both ends of any communications channel.*
- *Exchange public keys using a secure channel.*

7.5.2 CAPEC-125: Flooding

↳ *Description: An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target. This type of attack generally exposes a weakness in rate limiting or flow. When successful this attack prevents legitimate users from accessing the service and can cause the target to crash. This attack differs from resource depletion through leaks or allocations in that the latter attacks do not rely on the volume of requests made to the target but instead focus on manipulation of the target's operations. The key factor in a flooding attack is the number of requests the adversary can make in a given period of time. The greater this number, the more likely an attack is to succeed against a given target.*

↳ *Prerequisites: Any target that services requests is vulnerable to this attack on some level of scale.*

↳ *Mitigations:*

- *Ensure that protocols have specific limits of scale configured.*
- *Specify expectations for capabilities and dictate which behaviors are acceptable when resource allocation reaches limits.*
- *Uniformly throttle all requests in order to make it more difficult to consume resources more quickly than they can again be freed.*

7.5.3 CAPEC-148: Content Spoofing

↳ *Description: An adversary modifies content to make it contain something other than what the original content producer intended while keeping the apparent source of the content unchanged. The term content spoofing is most often used to describe modification of web pages hosted by a target to display the adversary's content instead of the owner's content. However, any content can be spoofed, including the content of email messages, file transfers, or the content of other network communication protocols. Content can be modified at the source (e.g. modifying the source file for a web page) or in transit (e.g. intercepting and modifying a message between the sender and recipient). Usually, the adversary will attempt to hide the fact that the content has been modified, but in some cases, such as with web site defacement, this is not necessary. Content Spoofing can lead to malware exposure, financial fraud (if the content governs financial transactions), privacy violations, and other unwanted outcomes.*

↳ *Prerequisites: The target must provide content but fail to adequately protect it against modification.The adversary must have the means to alter data to which they are not authorized. If the content is to be modified in transit, the adversary must be able to intercept the targeted messages.*

7.5.4 CAPEC-157: Sniffing Attacks

↳ *Description: In this attack pattern, the adversary intercepts information transmitted between two third parties. The adversary must be able to observe, read, and/or hear the communication traffic, but not necessarily block the communication or change its content. Any transmission medium can theoretically be sniffed if the adversary can examine the contents between the sender and recipient. Sniffing Attacks are similar to Man-In-The-Middle attacks (CAPEC-94), but are entirely passive. MITM attacks are predominantly active and often alter the content of the communications themselves.*

↳ *Prerequisites: The target data stream must be transmitted on a medium to which the adversary has access.*

↳ *Mitigations: Encrypt sensitive information when transmitted on insecure mediums to prevent interception.*

7.6 UC-Template nach IEC 62559

Dieser Abschnitt zeigt das Use Case-Template (UC-Template) nach IEC 62559 in unausgefüllter Form.

7.6.1 UC-Template Abschnitt „1 – Description of the use case"

7.6.1.1 UC-Template Abschnitt „1.1 – Name of use case"

Use case identification		
ID	Area Domain(s) / Zone(s)	Name of use case

7.6.1.2 UC-Template Abschnitt „1.2 – Version management"

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status

7.6.1.3 UC-Template Abschnitt „1.3 – Scope and objectives of use case"

Scope and objectives of use case	
Scope	
Objective(s)	
Related business case(s)	

7.6.1.4 UC-Template Abschnitt „1.4 – Narrative of use case"

Narrative of use case
Short description
Complete description

7.6.1.5 UC-Template Abschnitt „1.5 – Key performance indicators (KPI)"

Key performance indicators			
ID	Name	Description	Reference to mentioned use case objectives

7.6.1.6 UC-Template Abschnitt „1.6 – Use case conditions"

Use case conditions
Assumptions
Prerequisites

7.6.1.7 UC-Template Abschnitt „1.7 – Further information to the use case for classification / mapping"

Classification Information
Relation to other use cases
Level of depth
Prioritisation
Generic, regional or national relation
Nature of the use case
Further keywords for classification

7.6.1.8 UC-Template Abschnitt „1.8 – General remarks"

General remarks

7.6.2 UC-Template Abschnitt „2 – Diagrams of use case"

Diagram(s) of use case

7.6.3 UC-Template Abschnitt „3 – Technical details"

7.6.3.1 UC-Template Abschnitt „3.1 – Actors"

Actors			
Grouping		Group description	
Actor name	Actor type	Actor description	Further information specific to this use case

7.6.3.2 UC-Template Abschnitt „3.2 – References"

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

7.6.4 UC-Template Abschnitt „4 – Step by step analysis of use case“

7.6.4.1 UC-Template Abschnitt „4.1 – Overview of scenarios“

Scenario conditions						
No.	Scenario name	Scenario description	Primary actor	Triggering event	Pre-condition	Post-condition

7.6.4.2 UC-Template Abschnitt „4.2 – References“

Scenario								
Scenario name :								
Step No.	Event	Name of process/ activity	Descrip-tion of process/ activity	Service	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Require-ments R-ID

7.6.5 UC-Template Abschnitt „5 – Information exchanged“

Information Exchanged			
Information exchanged ID	Name of information exchanged	Description of information exchanged	Requirements IDs

7.6.6 UC-Template Abschnitt „6 – Requirements (optional)“

Requirements (optional)		
Categories ID	Category name for requirements	Category description
Requirement ID	Requirement name	Requirement description

7.6.7 UC-Template Abschnitt „7 – Common Terms and Definitions”

Common terms and definitions	
Term	Definition

7.6.8 UC-Template Abschnitt „8 – Custom information (optional)“

Custom information (optional)		
Key	Value	Refers to section

7.7 MUC-Template angelehnt an IEC 62559

Dieser Abschnitt zeigt das Misuse Case-Template (MUC-Template), das an das UC-Template nach IEC 62559 angelehnt und erweitert wurde, in unausgefüllter Form.

7.7.1 MUC-Template Abschnitt „1 – Description of the misuse case"

7.7.1.1 MUC-Template Abschnitt „1.1 – Name of misuse case"

Misuse case identification		
ID	Area Domain(s)/ Zone(s)	Name of misuse case

7.7.1.2 MUC-Template Abschnitt „1.2 – Version management"

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status

7.7.1.3 MUC-Template Abschnitt „1.3 – Scope and objectives of misuse case"

Scope and objectives of misuse case	
Scope	
Objective(s)	
Related business case(s)	

7.7.1.4 MUC-Template Abschnitt „1.4 – Narrative and condition of misuse case"

Narrative of misuse case
Short description
Complete description

7.7.1.5 MUC-Template Abschnitt „1.5 – Misuse case conditions"

Misuse case conditions
Assumptions
Prerequisites

7.7.1.6 MUC-Template Abschnitt „1.6 – Further information to the misuse case for classification / mapping"

Classification Information
Relation to other use cases and misuse cases
Level of depth
Prioritisation
Generic, regional or national relation
Nature of the misuse case
Further keywords for classification

7.7.1.7 MUC-Template Abschnitt „1.7 – General remarks"

General remarks

7.7.2 MUC-Template Abschnitt „2 – Diagrams of misuse case"

Diagram(s) of misuse case

7.7.3 MUC-Template Abschnitt „3 – Technical details"

7.7.3.1 MUC-Template Abschnitt „3.1 – Actor and Mis-Actor Profiles"

Actors					
Grouping					
Group description					
Actor name	Actor type	Actor description	Intention/ Motivation	Capability	Further information specific to this use case

Mis Actors					
Grouping					
Group description					
Misactor name	Misactor type	Misactor Relationship	Misactor description	Intention/ Motivation	Further information specific to this misuse case

7.7.3.2. MUC-Template Abschnitt „3.2 – References"

References						
No.	References type	Reference	Status	Impact on misuse case	Originator / organisation	Link

7.7.4 MUC-Template Abschnitt „4 – Step by step analysis of misuse case"

7.7.4.1 MUC-Template Abschnitt „4.1 – Overview of Failure scenarios"

Failure Scenario Conditions					
Scenario No :					
Scenario name :					
Scenario description					
Failure Scenario No.	Triggering Event	Pre-Condition	Worst case threat	Reason of benign Scenario	Relation to other (Mis-) Use case
Step No.	Name of process/ activity	Description of process/ activity	Step of the Failure Scenario	CIA Threat	Require-ments R-ID

7.7.4.2 MUC-Template Abschnitt „4.2 – General/Specific attack scenarios"

Attack Scenario Conditions						
Attack Scenario No.	Attack type	Attack target	Domains and Mechanism of Attack (CAPEC)	Relevant Scenario No.	Likelihood	Relation to other (Mis-) Use case
Step No.	Name of process/ activity	Event	Description of process/ activity	Step of Attack Scenario	CIA Threat	Require-ments R-ID

7.7.4.3 MUC-Template Abschnitt „4.3 – Overview of Capture point (optional)"

Capture Point - Scenarios			
Step No.	Description of the capture point	Attack Step No.	Role-Based Access control (RBAC) information

7.7.5 MUC-Template Abschnitt „5 – Requirements"

Requirements		
Categories ID	Category name for requirements	Category description
Requirement ID	Requirement name	Requirement description

7.7.6 MUC-Template Abschnitt „6 – Common Terms and Definitions"

Common terms and definitions	
Term	Definition

7.7.7 MUC-Template Abschnitt „7 – Custom information (optional)"

Custom information (optional)		
Key	Value	Refers to section

Autoren
Andreas Corusa *(TU Berlin)*
Georg Erdmann *(TU Berlin)*
Elena Timofeeva *(TU Berlin)*
Johannes Norbert Predel
(TU Berlin/nymoen Strategieberatung)
Falk Ritschel *(Conomic GmbH)*
Christian Sprengel *(Conomic GmbH)*
Anne Walther *(Conomic GmbH)*
Daniel Kaufmann *(BBH Consulting AG)*
Stefan Brühl *(BBH Consulting AG)*
Victor Stocker *(BBH Consulting AG)*
Christine Rosinger *(OFFIS e.V.)*
Mathias Uslar *(OFFIS e.V.)*
Simon Schäfer-Stradowsky *(IKEM e.V.)*

Design
Ellery Studio
Brady Kuehl, Mursal Nasr,
Hannah Schrage, Gaja Vičič
David Ramirez Fernandez

DOI Nummer
→ 10.14279/depositonce-11849

Förderkennziffer
03SIN537

Lizenz
Das Kompendium „Digitalisierung in der Energiewirtschaft“ und die darin beinhalteten Einzelbeiträge unserer Partner sowie alle Illustrationen von Ellery Studio GbR. stehen unter der Creative Commons Lizenz Namensnennung 4.0 International (CC-BY 4.0). Um eine Kopie der Lizenz zu sehen besuchen Sie https://creativecommons.org/licenses/by/4.0/

Herausgeber
Technische Universität Berlin
Institut für Energietechnik
Fachgebiet Energiesysteme

Hauptverantwortlicher für Koordination und Inhalt
Andreas Corusa
(andreas.corusa@tu-berlin.de)

Mit freundlicher Unterstützung durch
die Wirtschaftswissenschaftliche Fakultät
Institut für Infrastruktur und
Ressourcenmanagement (IIRM)
Professur für Energiemanagement und Nachhaltigkeit

Acknowledgement
Dieses Dokument beruht auf Arbeiten, die mit Unterstützung des Bundesministeriums für Wirtschaft und Energie (BMWi) im Rahmen des SINTEG-Programms „Schaufenster intelligente Energie - Digitale Agenda für die Energiewende“ im Schaufenster WindNODE erstellt wurden.
Es wurde vor seiner Veröffentlichung den WindNODE-Partnern zur Durchsicht und Kommentierung zur Verfügung gestellt. Die hier enthaltenen Ansichten der Verfasser spiegeln nicht notwendigerweise die Ansichten des BMWi oder der übrigen WindNODE-Partner wider.

Da dieses Kompendium aus verschiedenen Beiträgen besteht, kann es durch die Entscheidung einzelner Autor*innen dazu kommen, dass das generische Maskulinum verwendet wird. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint, soweit es für die Aussage erforderlich ist.