Thema:

„Cyberrisiken und Sicherheitslücken für intelligente Energiesysteme: Eine Taxonomie und Archetypenanalyse“

Masterarbeit

zur Erlangung des akademischen Grades „Master of Science (M. Sc.)“ im Studiengang Wirtschaftswissenschaften der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Anders Vorname: Niklas Alexander

Prüfer: Prof. Dr. Michael H. Breitner
Betreuerin: M. Sc. Jana Gerlach

Hannover, den 30.September. 2022

Inhaltsverzeichnis

1. Einleitung

1.1 Motivation

Die Bundesregierung beschloss den Ausstieg aus der Kernenergie, sowie einen Kohleausstieg bis 2030. Dabei werden bereits die letzten Kernkraftwerke in Deutschland bis Ende 2022 abgestellt.[1] Erneuerbare Energien sind seitdem sehr gefragt, was die untere Abbildung verdeutlicht.

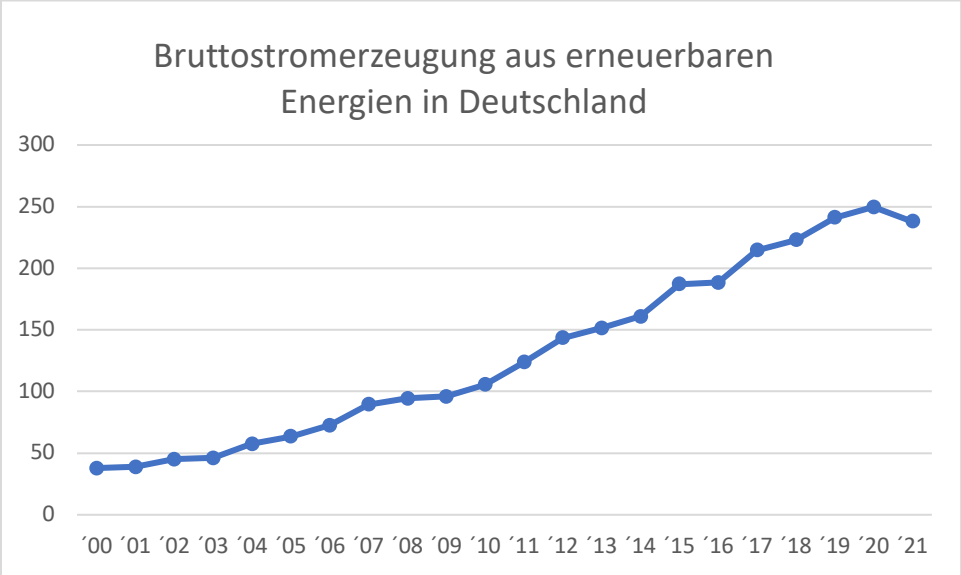

Abbildung 1 Bruttostromerzeugung aus erneuerbaren Energien in Deutschland[2]

Obige Abbildung zeigt die Stromproduktion aus erneuerbaren Energien in TWh (Terawattstunden) für die Jahre 2000 bis 2021. Es zeigt sich ein deutliches Wachstum für die Nutzung von erneuerbaren Energien. Um diese stetig steigende Stromproduktion effizient zu nutzen, müssen die Stromnetze schneller ausgebaut werden.[3] Um dem gerecht zu werden, hat die Bundesregierung im Energiekonzept 2050 Investitionen in Milliardenhöhe für eine bessere Infrastruktur beschlossen.[4]

---

[1] vgl. **Presse- und Informationsamt der Bundesregierung (2017):** *Von Kohle hin zur Zukunft*, URL: https://www.bundesregierung.de/breg-de/themen/klimaschutz/kohleausstieg-1664496

[2] vgl. Eigene Darstellung in Anlehnung an statista (2022), Bruttostromerzeugung aus Erneuerbaren Energien in Deutschland in den Jahren 1990 bis 2021

[3] vgl. ebd.

[4] vgl. ebd.

Durch die Weiterentwicklung dieser Stromnetze ist heute von intelligenten Stromnetzen die Rede. Aufgabe dieser sogenannten Smart Grids ist die Optimierung der gesamten Prozesskette beginnend bei der Produktion, über Transport und Lagerung bis hin zum Verbrauch.

Um die Stromversorgung intelligent auszulegen, werden viele technische Komponenten benötigt. Sie verknüpfen alles in einem Stromnetzwerk für die bestmögliche Nutzung und verwenden dabei auch neue Technologien wie z.B. KI (Künstliche Intelligenz).

Smart Grids sorgen für eine hohe Effizienz, werden aber auch durch die Vernetzung der Stromnetze und der generellen Abhängigkeit dem Strom gegenüber mit erheblichen Herausforderungen konfrontiert. An erster Stelle sind Cyberrisiken zu nennen, die erhebliche Schäden anrichten, was nachfolgende Grafik verdeutlicht.

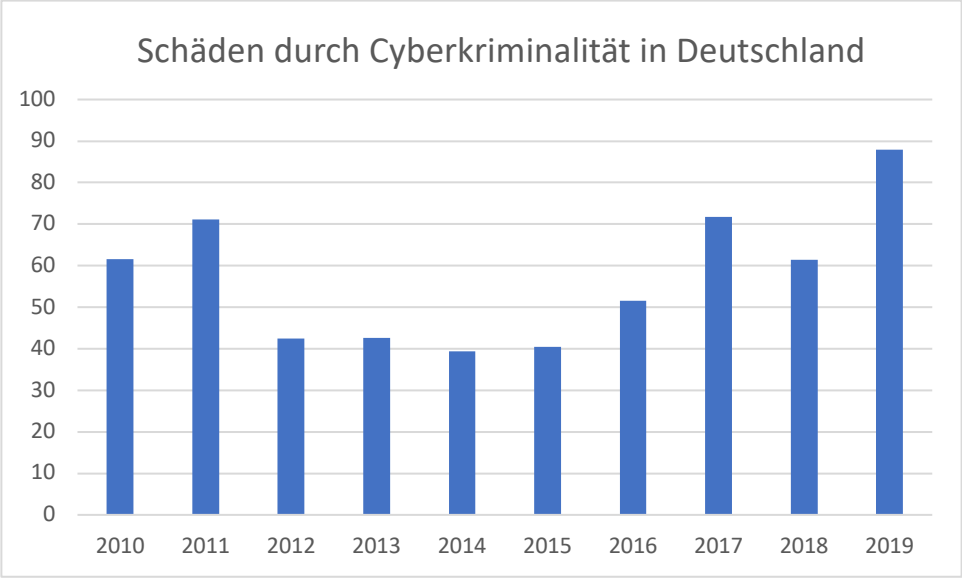

Abbildung 2 Schäden durch Cyberkriminalität in Deutschland[5]

Abbildung 2 zeigt die Schadenssummen in Millionen Euro der Jahre 2010 bis 2019. Es ist ein deutlicher Trend zu erkennen, dass Cyberrisiken immer gefährlicher werden und große Schäden anrichten. Diesen Risiken sind auch kritische Infrastrukturen, wie Smart Grids ausgesetzt.

[5] Eigene Darstellung, in Anlehnung an statista (2022), Schäden durch Cyberkriminalität in Deutschland von 2006 bis 2019

Es ergeben sich folgende Forschungsfragen:
Forschungsfrage 1: *„Welche Cyberrisiken und Sicherheitslücken bestehen für intelligente Energiesysteme“*
und
Forschungsfrage 2: *„Welche Maßnahmen gibt es, um die Cyberrisiken abzuschwächen?“*

1.2 Vorgehen

Die vorliegende Arbeit ist, in zehn Kapiteln gegliedert. Das erste Kapitel bezieht sich auf die Einleitung, sowie Forschungsfragen und Zielsetzung der Arbeit.
Im zweiten Kapitel „Theoretische Grundlagen“ werden zunächst wichtige Elemente dieser Arbeit definiert. Anschließend zeigt ein Überblick den aktuellen Stand von Smart Grid und Cyberkriminalität. Außerdem werden verschiedene Angriffsvektoren der Cyberkriminalität aufgelistet.
Im dritten Kapitel werden die Forschungsmethoden näher erklärt. Es beginnt mit der Literaturrecherche. Hierfür wird die Methode nach Webster und Watson genutzt. Nach der Literaturrecherche wird die Taxonomie erklärt. Zum Schluss wird die Clusteranalyse näher beleuchtet und das Vorgehen der Evaluation.
Das vierte Kapitel befasst sich mit der Taxonomie. Hier werden fünf Iterationen aufgezeigt. Die erste bildet sich aus der Literaturrecherche. Im Anschluss werden Cybersicherheitsunternehmen und deren Services näher analysiert.
Das fünfte Kapitel befasst sich mit der Clusteranalyse. Dazu werden die Ergebnisse aus der Taxonomie mit Hilfe von einem Programm verschiedenen Gruppen zugeordnet. Jedes Cluster bildet hier ein Archetyp.
Das sechste Kapitel dient der Evaluation. Hier werden zwei Methoden eingesetzt. Zum einen wird eine Evaluationsiteration erstellt, welche zeigen soll, ob sich die herausgefundenen Archetypen auch auf andere Cybersicherheitsunternehmen übertragen lassen. Zum anderen werden Praxispartner interviewt, welche die finale Taxonomie mit anschließender Archetypenanalyse evaluieren.
Im siebten Kapitel „Diskussion und Ergebnisse“ werden die Archetypen verglichen und die Vor- und Nachteile genauer erläutert. Außerdem werden anhand von Beispielunternehmen, welche diesen Archetypen angehören, die Wertschöpfung genauer erklärt.
Das achte Kapitel gibt Handlungsempfehlungen auf Basis der aufgedeckten Sicherheitslücken und formuliert Ansätze, wie Cybersicherheit verbessert werden kann.

Im neunten Kapitel wird der Forschungsbedarf näher beleuchtet. Es wird aufgezeigt, welche Thematiken derzeitig an ihre Grenzen stoßen.
Im Kapitel zehn geht es um die „Limitation“. Sie weist daraufhin, welche Faktoren in dieser Arbeit zu einer Verzerrung der Ergebnisse führen können. Außerdem werden weitere Forschungsfragen genannt.
Im letzten Kapitel dieser Arbeit wird die Forschungsfrage erneut aufgegriffen und wichtige Aspekte als Fazit zusammengefasst. Die Arbeit wird mit einem Ausblick abgeschlossen.

Auch der Datenschutz ist besonders in Deutschland ein sehr sensibles Thema. Daraus ergibt sich folgende Forschungsfrage:

„Wie kann der Datenschutz von Verbraucherdaten gewährleistet werden?“

Außerdem gibt es Umweltaspekte zu berücksichtigen. So gilt es z.B. im Zuge des wachsenden Ausbaus von Windkraftanlagen die Belange der Bürger*innen, wie auch der Umwelt zu berücksichtigen. Daher stellt sich hier die Frage:

*„Welche Hürden müssen die Errichter von Micro Grids bewältigen, in Bezug auf die Bürger*innen“?*

Alle Punkte der Limitation beeinflussen das Fazit und den Ausblick, was zu Veränderungen führen kann.

11. Fazit und Ausblick

Smart Grid ist ein wichtiges Thema in der heutigen Zeit und gewinnt zunehmend an Bedeutung, auch auf internationaler Ebene. Der Trend zu den erneuerbaren Energien, zeigt eindeutig, dass die stark wachsende Anzahl von Micro Grids sicher verknüpft werden müssen. Es ist festzuhalten, dass es insgesamt 4 verschiedene Archetypen für die Cybersicherheit im Smart Grid gibt. Der „All-In-One“, der „Spezialist mit Einzellösungen“ und das „Beratungsunternehmen“ sind eher den mittleren, oder großen Unternehmen zuzuordnen, wohingegen der „Netzwerkverteidiger“ seine Kundenklientel bei kleinen Unternehmen und Privatpersonen findet. Unternehmen und Privatpersonen im Smart Grid haben allerdings das Problem der zu geringen Absicherung, oder verfügen über mehrere Absicherungen für die gleiche Angriffsfläche, was eingangs zu den Forschungsfragen dieser Arbeit führte:

Forschungsfrage 1: *„Welche Cyberrisiken und Sicherheitslücken bestehen für intelligente Energiesysteme“*
und
Forschungsfrage 2: *„Welche Maßnahmen gibt es, um die Cyberrisiken abzuschwächen?“*

Unklar ist jedoch was mit den Schnittstellenproblemen im Smart Grid passiert. Die momentan größten Sicherheitslücken sind zum einen die fehlenden sicheren Hardwarekomponenten zum Schutz der Smart Meter, oder den Gatways, und zum anderen die SCADA-Netze, welche immer noch sehr anfällig für Cyberangriffe sind. Hierzu wurde die Entwicklung von Hardware-Sicherheitsmodulen vorgeschlagen und die Errichtung einer Micro Firewall. So ausgestattet werden Angriffe auf die SCADA-Netze frühzeitig erkannt. Außerdem müssen die Plattformen natürlich auch „betreibersicher“ sein, was bedeutet, dass sensible Daten allein verschlüsselt, transferiert und gesichert werden, und im Zuge der weiteren Bearbeitung spezielle Vorkehrungen auf der Plattform zu treffen sind, um eine unzulässige Informationsweitergabe zu verhindern (Data Leakage Prevention). Erforderlich ist ebenfalls ein Security Level Management, welches die Planung, Umsetzung und Überwachung der Sicherheitseigenschaften unterstützt. In Anlehnung an das Software-as-a-Service-Paradigma (SaaS) können allgemeine Sicherheits-eigenschaften und -funktionen als Dienste im Sinne von „Security as a Service“ bereitgestellt werden. Außerdem ist der Datenschutz ein wichtiger Aspekt, der keinesfalls vernachlässigt werden darf.
In der Recherche ist weiterhin aufgefallen, dass Unternehmen und Mitarbeiter stärker für die Gefahren von Cyberangriffen sensibilisiert werden müssen und Rollen, sowie Domänen aufzubauen sind. Für eine transparentere Marktübersicht können Level Systeme eingeführt werden, welche sich an die rechtlichen Rahmenbedingungen orientieren und es so ermöglicht den Schutzgrad verschiedener Produkte zu vergleichen. Zum Thema Datenschutz gibt es besondere Herausforderungen. Hier wird der Ansatz einer Anonymisierung verfolgt, sodass bei einem Cyberangriff nicht zurückverfolgt werden kann, zu welcher Person die jeweiligen Daten gehören. Es besteht jedoch die Möglichkeit, dass der Kunde seine Daten gegen spezielle Benefits preisgibt. Die Cyberrisiken und Sicherheitslücken sind sehr schnelllebig. Daher ist eine kontinuierliche Risiko-Analyse in bestimmten Zeitabständen Voraussetzung für ein funktionierendes und sicheres Smart Grid. Somit werden neue Risiken frühzeitig erkannt und behoben. Hilfreich ist auch eine steigende Anzahl von Unternehmen, welche sich auf die Cyberabwehr von Smart Grid spezialisieren. So wird die Innovationskraft auf diesem Gebiet verstärkt und innovative Produkte sorgen für mehr Sicherheit, z.B. auch bei den Smart Metern, oder SCADA-Netzen.

Zukünftig ist Smart ein sehr bedeutendes Thema, welches immer weiter ausgebaut wird. Momentan gibt es allerdings neben der Cybersicherheit auch viele weitere Bereiche, die für das Smart Grid enorme Herausforderungen sind. Hierzu zählen beispielsweise die erheblichen Kosten des Netzausbaus und somit der Finanzierung, die technische Umsetzung, und die rechtlichen Aspekte bei grenzüberschreitenden

Tätigkeiten. Zu bedenken ist auch, dass die Cyberrisken mit Hilfe der Handlungsempfehlungen zwar abgeschwächt werden können, aber nie ganz eliminiert werden. Ein Restrisiko bleibt bestehen. Allerdings sind Smart Grids aufgrund ihrer erheblichen Einsparpotenziale ein enormer Wachstumsmarkt, was zu einer steigenden Anzahl von Unternehmen in diesem Marktsegment führen wird, mit der positiven Folge, dass die Innovationskraft der Branche gestärkt und damit das Smart Grid sicherer wird.