Beiträge zu einer Referenzarchitektur für ein föderales Cybersicherheitsmanagement

Dissertation

zur Erlangung des akademischen Grades

Doktor-Ingenieur (Dr.-Ing.)

der Fakultät für Informatik und Elektrotechnik
der Universität Rostock

eingereicht von:

Thomas Rehbohm M.Sc., Dipl.-Ing. (FH)
geb. am 28.01.1969 in Perleberg
Bremen, den 18.04.2025

https://doi.org/10.18453/rosdok_id00005543

Gutachter 1: Univ.- Prof. Dr.-Ing. **Kurt Sandkuhl**, Inhaber des Lehrstuhls für Wirtschaftsinformatik an der Universität Rostock

Gutachter 2: Univ.- Prof. Dr. rer. nat. **Clemens H. Cap**, Inhaber des Lehrstuhls für Informations- und Kommunikationsdienste an der Universität Rostock

Gutachter 3: PD Dr. **Karsten Sohr**, Senior Researcher in der Arbeitsgruppe Digitale Medien am Technologie-Zentrum Informatik und Informationstechnik an der Universität Bremen

Die öffentliche Verteidigung fand am 02.09.2025 an der Universität Rostock - Fakultät für Informatik und Elektrotechnik, Albert-Einstein-Straße 26, 18059 Rostock - statt.

Kurzfassung

Die Informationstechnik des neuen Jahrtausends ist geprägt von sich verändernden Rahmenbedingungen für Staat, Wirtschaft und Gesellschaft. Insbesondere die Globalisierung von Produktionsabläufen, die flexiblere Arbeitsplatzgestaltung von Beschäftigten in Ort und Zeit, die grundsätzlichen Technologieveränderungen hin zum Cloud-Computing, die zunehmende Digitalisierung und die Nutzung von Künstlichen Intelligenz (KI) Systemen haben auf die tradierte Sicht auf die Informations- und Kommunikationssysteme nachhaltige Auswirkungen. Die Abhängigkeit von der Lieferantenkette ist eklatant, gleichzeitig ist die Erwartungshaltung zu einer unterbrechungsfreien Verfügbarkeit von IKT-Systemen offenkundig. Unternehmen wie auch staatliche Institutionen müssen sich diesen Herausforderungen stellen, um zum einen den kollektiven Schutz vor Bedrohungen angemessen zu begegnen und zum anderen die Wirtschaft und Gesellschaft in dieser Ordnung zu schützen. Informationssicherheit ist für alle Organisationen daher wichtig und unentbehrlich. Dem Staat kommt dabei eine koordinierende Funktion zu.

Eingedenk der Chancen und der breitgefächerten Forschung im Umfeld der Informationssicherheit soll eine Unternehmensarchitektur – übertragen auf die Öffentliche Verwaltung – einen neuen, akzeptierten und angemessenen Beitrag leisten, um die Daseinsvorsorge fortwährend zu stärken. Es braucht Organisationsstrukturen, die adaptiert aus der Unternehmensentwicklung auf die Erfordernisse des Staates erforscht und adaptiert werden, um mit den Veränderungsprozessen der Informationstechnik standzuhalten. Mit der hier vorliegenden Forschungsarbeit im Umfeld des Enterprise Architektur Managements wurde dieses entlang des Design Science Research durchgeführt. Prinzipiell wird mit dem Ergebnis der Forschungsarbeit ein Referenzmodell im föderalen Kontext Deutschlands vorgeschlagen, welches den Herausforderungen einer sich dynamisch ändernden IT-Landschaft mit einhergehender steigender Bedrohungslage begegnet. Es handelt sich in der vorliegenden Arbeit um eine Problemlösung aus dem praktischen Umfeld der ministeriellen Landesverwaltungen Deutschlands. In iterativen Schritten wird der Forschungsprozess durchgeführt, von der Anforderungsanalyse bis zur Evaluation der Ergebnisse und deren Veröffentlichungen.

Schlagwörter: Cybersicherheit, Informationssicherheit, Unternehmensarchitektur

Abstract

The information technology of the new millennium is characterised by changing framework conditions for the state, economy and society. In particular, the globalisation of production processes, the more flexible workplace design of employees in terms of location and time, the fundamental technological changes towards cloud computing, increasing digitalisation and the use of AI systems are having a lasting impact on the traditional view of information and communication systems. The dependence on the supply chain is blatant, while at the same time the expectation of uninterrupted availability of ICT systems is often. Companies as well as state institutions must face up to these challenges in order to provide adequate collective protection against threats on the one hand and to protect the economy and society in this order on the other. Information security is therefore important and indispensable for all organisations. The state has a coordinating role to play here.

Considering the opportunities and the wide-ranging research in the field of information security, an enterprise architecture – transferred to public administration – should make an accepted and appropriate contribution to continuously strengthening services of general interest. Organisational structures are needed that are adapted from corporate development and researched and adapted to the requirements of the state in order to withstand the change processes of information technology. This research work in the field of enterprise architecture management is carried out along the lines of design science research. In principle, the result of the research work proposes a reference model in the federal context of Germany, which meets the challenges of a dynamically changing IT landscape with an increasing threat situation. This thesis applies the design science research process to propose a reference architecture. It is a problem solution from the practical environment of the ministerial state administrations in Germany. The research process is carried out in iterative steps, from the requirements analysis to the evaluation of the results and their publication.

Keywords: cybersecurity, information security, enterprise architecture

Inhaltsverzeichnis

Kurzfassung ..... **III**

Abstract ..... **IV**

Inhaltsverzeichnis ..... **V**

Abbildungsverzeichnis ..... **IX**

Tabellenverzeichnis ..... **X**

Abkürzungsverzeichnis ..... **XI**

Vorwort ..... **XIV**

1 Synopse **1**

1.1 Einleitung **2**

1.1.1 Motivation 2

1.1.2 Problemstellung 3

1.1.3 Relevanz 8

1.2 Forschungskontext **11**

1.2.1 Forschungsziel und Forschungsfragen 12

1.2.2 Forschungsmethoden 13

1.2.3 Forschungsparadigma Design Science Research 18

1.2.4 Forschungsumfeld Öffentliche Verwaltung 21

1.2.5 Forschungsvorgehen 25

1.3 Forschungsbeiträge im DSR **27**

1.3.1 Problemerkennung und Motivation 29

1.3.2 Zieldefinition und Anforderungen 31

1.3.3 Design und Entwicklung 33

1.3.4 Demonstration 34

1.3.5 Evaluation 35

1.3.6 Kommunikation 38

1.4 Schlussbetrachtung **39**

1.4.1 Zentrale Merkmale der CSA 39

1.4.2 Diskussion der Ergebnisse 42

1.4.3 Beschränkungen und künftige Arbeiten 43

1.4.4 Schlussfolgerungen 44

2 On Challenges of Cyber and Information Security Management in Federal Structures - The Example of German Public Administration 46
2.1 Introduction 46
2.2 Public sector data protection in federal structures 48
2.3 Research Methodology 51
2.4 Literature Analysis 52
2.5 Interview Study 55
2.5.1 Hypotheses 55
2.5.2 Procedure 56
2.5.3 Results 57
2.6 Conclusions 59

3 Integrated Security Management of Public and Private Sector for Critical Infrastructures – Problem Investigation 60
3.1 Introduction 60
3.2 Theoretical Background 62
3.2.1 Enterprise Architecture Management and Business/IT-Alignment 62
3.2.2 Legal framework for Critical Infrastructure Sectors 62
3.3 Research Approach 64
3.4 State of research 64
3.4.1 Literature analysis 65
3.4.2 Summary 66
3.5 Interview study 66
3.5.1 Methodological approach 66
3.5.2 Hypotheses / Theses 67
3.5.3 Interviewed companies and objectives of the interviews 68
3.6 Results 69
3.7 Conclusions and Future Work 71

4 Sicherheitsmanagement, Cybersicherheit und Daseinsvorsorge: Empirische Studie in deutschen Kommunen 73
4.1 Einleitung 73
4.2 Stand der Forschung und Literatur 74
4.3 Methodische Vorgehensweise 79
4.4 Ergebnisse 81
4.5 Diskussion und Schlussfolgerungen 83
4.6 Ausblick 85

5 Grundforderungen von Informations- und Cybersicherheit in Ländern 86
5.1 Einleitung 86
5.2 Wissenschaftliche Methode 87
5.3 Vorgehensweise und Diskussion – rechtliche Grundforderungen an die gesetzgeberische Gewalt 88
5.4 Schlussfolgerung 91

6 IT-Sicherheitsrecht der (Bundes) Länder 93

6.1 Kompetenzgefüge der IT-Sicherheit in Bund und Ländern 93
6.1.1 Öffentliche Sicherheit 93
6.1.2 IT-Sicherheit als staatsverwaltende und gefahrenabwehrrechtliche Forderung 95
6.1.3 Sicherung staatlicher Strukturen 97
6.1.4 Sicherung der Zivilgesellschaft (Daseinsvorsorge) 97
6.2 Spezifische landesgesetzliche Regelungen 101
6.2.1 Grundlegende Strukturen und Probleme 101
6.2.2 Grundelemente der IT-Sicherheit der Länder 104

7 Herausforderungen der föderalen Cybersicherheit vs. Änderung in der Bund-Länder Gewaltenteilung 108
7.1 Einleitung 108
7.2 Stand der Forschung 109
7.3 Rechtskonstrukt 110
7.4 Föderale Gefahrenabwehr 115
7.5 Schlussfolgerungen und Ausblick 116

8 Federal Cybersecurity Architecture and Information Security Management - Adoption and Diffusion of the NIS-2 Requirements 117
8.1 Introduction 117
8.2 State of the art 119
8.3 Methodology 119
8.4 Federal Cyber Security Architecture 121
8.5 NIS 2 Directive 123
8.6 CISIS12 125
8.7 Summary, Conclusions and Outlook 128

9 Entwicklung eines modularen ISMS und DSMS, Datenschutz und Datensicherheit 130
9.1 Einleitung 130
9.2 Unterschiede und Gemeinsamkeiten ISO 27701 vs. DSGVO 131
9.3 SDM 3.0 als Ergänzung zu einen ISMS 133
9.4 Vorgehensmodell CISIS12 135
9.5 Informationssicherheit und Datenschutz als Teil einer Cybersicherheitsarchitektur 138
9.6 Zusammenfassung 139

10 Referenzarchitektur Cybersicherheit im Föderalsystem Deutschlands ... 140
10.1 Einleitung 140
10.2 Grundlagen und bisherige Arbeiten 142
10.2.1 Notwendigkeit und Bedarf an Cybersicherheitsforschung in föderalem Umfeld 142
10.2.2 Unternehmensarchitekturen 142
10.2.3 Vorfeldstudien 143
10.3 Forschungsansatz 145
10.4 Anforderungen und Lösungsansatz der Referenzarchitektur 146

10.4.1 Anforderungen an eine föderale Architektur 146
10.4.2 Lösungsansatz 147
10.5 Unternehmensarchitektur 148
10.5.1 Strategische und Motivatorische Betrachtung der CSA Land 148
10.5.2 Erörterung der Business-/Application Ebenen 149
10.5.2.1 WIS 150
10.5.2.2 MISP 150
10.5.2.3 SR 151
10.5.2.4 MIRT 152
10.5.2.5 Rechtliche Betrachtung 152
10.6 Evaluierung der Architektur 152
10.6.1 Evaluation der Anforderungen an die Architektur 152
10.6.2 Evaluationsstrategie 153
10.7 Schlussfolgerungen und zukünftige Arbeit 154

11 Cybersicherheitsevaluation einer Referenzarchitektur für Land, Kommune und systemrelevante Infrastruktur 155
11.1 Einleitung 155
11.2 Forschungsmethodik 157
11.3 Stand der Forschung 158
11.4 Föderale Cybersicherheitsarchitektur 159
11.4.1 Anforderungen an die Architektur 159
11.4.2 Architektur 160
11.4.3 Evaluierungsstrategie und Grundsätze ordnungsgemäßer Modellierung 162
11.4.4 Evaluierungsepisode Kommunen 163
11.5 Schlussbetrachtung 165
11.6 Anlagen 165

12 Evaluation einer föderalen Referenzarchitektur für Cybersicherheit 167
12.1 Einleitung 167
12.2 Forschungsmethodik 169
12.3 Stand der Forschung 170
12.4 Föderale Cybersicherheitsarchitektur 171
12.4.1 Anforderungen an die Architektur 171
12.4.2 Architektur 173
12.4.3 Evaluierungsstrategie und Grundsätze ordnungsgemäßer Modellierung 175
12.4.4 Evaluierungsepisode Länder 176
12.5 Schlussbetrachtung 183

Anhang: 184
A.1 Deklaration der Forschungsbeiträge 184
A.2 Cybersicherheitsarchitektur 189

Literaturverzeichnis 193

Erklärung 218

Abbildungsverzeichnis

Abbildung 1 Informationssicherheit (eigene Darstellung) 5
Abbildung 2 Cybersicherheit (eigene Darstellung) 7
Abbildung 3 DSR Cycles (A. Hevner & Chatterjee, 2010, S. 16) 19
Abbildung 4 DSRM Prozess Modell ((Peffers et al., 2007, S. 54) 21
Abbildung 5 Forschungsvorgehen (eigene Darstellung) 25
Abbildung 6 DSR-Prozess in Anlehnung an Peffers (eigene Darstellung) 27
Abbildung 7 FEDS-Evaluationsepisoden 36
Abbildung 8 Critical infrastructure sectors in Germany 50
Abbildung 9 Cybersecurity Cube (Architecture, Goals, and Processes) 123
Abbildung 10 Cyber Security Architecture with ISMS 125
Abbildung 11 SDM 3.0 Würfel (Rost, 2022) 134
Abbildung 12 CISIS12-Vorgehensmodell 135
Abbildung 13 SDM Würfel – abgewandelte Darstellung 136
Abbildung 14 Kombination des ISMS-Vorgehensmodells mit dem SDM-Würfel 137
Abbildung 15 Cybersicherheitsarchitektur als Ergänzung zum ISMS und SDM 139
Abbildung 16 Akteure 147
Abbildung 17 Cybersicherheitsarchitektur Land 148
Abbildung 18 CSA-Land-Strategie 149
Abbildung 19 MISP 151
Abbildung 20 "Auszug der vorgeschlagenen föderalen Cybersicherheitsarchitektur: Prozesse" 165
Abbildung 21 "Strategy and Motivation" 166
Abbildung 22 Cybersicherheitsarchitektur 189
Abbildung 23 Strategy and Motivation 189
Abbildung 24 Identification and Compliance 190
Abbildung 25 Malware Information Sharing Platform 190
Abbildung 26 Mobile Incident Response Team 191
Abbildung 27 Warn and Information Service 191
Abbildung 28 Situation Report 192

Tabellenverzeichnis

Tabelle 1 Forschungsbeiträge im DSR-Prozess 29
Tabelle 2 database search 65
Tabelle 3 Literaturrecherche 79
Tabelle 4 Landesgesetze mit Bezug zu IT-Sicherheit 102
Tabelle 5 Research activities performed in DSR phases and their results 121
Tabelle 6 Gemeinsamkeiten der ISO 27701 und der DSGVO 133
Tabelle 7 „Forschungsarbeiten im DSR Prozess und ihre Ergebnisse“ 158
Tabelle 8 Ergebniszusammenfassung 183
Tabelle 9 Akzeptanz der Forschungsbeiträge 188

Abkürzungsverzeichnis

ACS ..... *Allianz für Cybersicherheit*
ADR..... *Action Design Research*
APT ..... *Advanced Persistents Threats*
B3S..... *branchenspezifische Sicherheitsstandards*
BAMAD..... *Bundesamt für den Militärischen Abschirmdienst*
BCM..... *business continuity management*
BfV..... *Bundesverfassungsschutz*
BGB..... *Bürgerliches Gesetzbuch*
BGH ..... *Bundesgerichtshof*
BGHSt ..... *Entscheidungen des Bundesgerichtshofs in Strafsachen*
BKA ..... *Bundeskriminalamt*
BMI..... *Bundesministerium des Innern und für Heimat*
BNetzA..... *Bundesnetzagentur*
BSI..... *Bundesamt für Sicherheit in der Informationstechnik*
BVerfG ..... *Bundesverfassungsgericht*
BVerfGE ..... *Entscheidungen des Bundesverfassungsgerichts*
CERT ..... *Computer Emergency Response Team*
CIA ..... *Confidentiality, Integrity und Availability*
CIR ..... *Cyber- und Informationsraums*
CISIS12..... *Compliance-Informations-Sicherheits-Management-System*
CISO ..... *Chief Information Security Officer*
CoE ..... *Council of Europe*
CSA ..... *Cybersicherheitsarchitektur*
CSIRT..... *Computer Security Incident Response Team*
CVE ..... *Common Vulnerabilities and Exposures*
Cyber-AZ..... *Nationalem Cyber-Abwehrzentrum*
DAkkS ..... *Deutsche Akkreditierungsstelle*
DLT ..... *Deutscher Landkreistag*
DSMS..... *Datenschutzmanagementsystem*
DSR..... *Design Science Research*
DSRM..... *Design Science Research Methodology*
DST ..... *Deutscher Städtetag*
DStGB ..... *Deutscher Städte- und Gemeindebund*
EA ..... *Enterprise Architecture*
ENISA..... *European Union Agency for Cybersecurity*
EU ..... *Europäische Union*
EU-DSGVO..... *Europäischen Datenschutzgrundverordnung*

EuGH ..... *Gerichtshof der Europäischen Union*
FEDS ..... *Framework for Evaluation in DSR*
GG ..... *Grundgesetzes, Grundgesetz*
Hessen3C ..... *Cyber-Competence-Center in Hessen*
HR ..... *Human Resources*
IKT ..... *Informations- und Kommunikationstechnologien*
IMK ..... *Innenministerkonferenz*
IoT ..... *Internet of Things*
ISMS ..... *Informationssicherheitsmanagementsystem*
IT-PLR ..... *IT-Planungsrat*
IT-SiG ..... *Gesetze zur Erhöhung der Sicherheit informationstechnischer Systeme*
IuK ..... *Informations- und Kommunikationsdienste*
KI ..... *Künstliche Intelligenz*
KMU ..... *kleine und mittlere Unternehmen*
KRITIS ..... *Kritische Infrastrukturen*
LfV ..... *Landesverfassungsschutzes*
LLM ..... *Large Language Model*
LSI ..... *Landesamt für Sicherheit in der Informationstechnik*
MIRT ..... *Mobile Incident Response Team*
MISP ..... *Malware Information Sharing Platform*
NCSR ..... *Nationale Cyber-Sicherheitsrat*
NIS ..... *Netzwerk- und Informationssicherheit*
NIS-2-Richtlinie ..... *europäische Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union*
NIS2UmsuCG ..... *NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz*
NJW ..... *Neue Juristische Wochenschrift*
NVwZ ..... *Neue Zeitschrift für Verwaltungsrecht*
OT ..... *Operative Technologie*
PDSG ..... *Patientendaten-Schutz-Gesetz*
SDM ..... *Standard-Datenschutzmodell*
SGB ..... *Sozialgesetzbücher*
SGI ..... *services of general interest*
SR ..... *Situation Report*
TOGAF ..... *The Open Group Architecture Framework*
TTDSG ..... *Telekommunikations-Telemedien-Datenschutz-Gesetz*
UAM ..... *Unternehmensarchitekturmodell*
VCV ..... *Verwaltungs-CERT-Verbund*
VwVfG ..... *Verwaltungsverfahrensgesetz*
WIN ..... *Wirtschaftsinformatik*

WIS ..... Warn und Information Service
ZITiS ..... Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Vorwort

Eine wissenschaftliche Forschungsarbeit zu erstellen, erfolgt regelmäßig im Anschluss an ein grundständiges Studium. Die Intention dieser Arbeit ist jedoch das Ergebnis einer jahrelangen beruflichen Tätigkeit in der Informationstechnik und der aus diesen Erfahrungen gewonnen Bedarfe an weiterführenden Forschungen im spezifischen Arbeitsumfeld. Meine Tätigkeit als Chief Information Security Officer (CISO) der Freien Hansestadt Bremen hat mir gezeigt, dass Forschungslücken bestehen, welche durch mich und in meiner hauptberuflichen Tätigkeit besonders zielführend adressiert werden können. Von einer wissenschaftlichen Betrachtung her liegen intrinsische Motive vor und es werden Ziele zur Verbesserung der Arbeitsorganisation in der hauptberuflichen Tätigkeit verfolgt. Meine Funktion als CISO (Landesbeauftragter für Informationssicherheit) hat mich dazu bewogen, die unklaren Aufgaben und Handlungserfordernisse in einen wissenschaftlichen Diskurs zu überführen.

Das grundsätzliche Zusammenwirken von Lehre und Forschung – wie es auch in der von Wilhelm von Humboldt Grundidee zur Einheit eben dieser postuliert wurde – standen weder im Fokus, noch wird diese regelmäßig erreicht. Vielmehr ist die vorliegende Arbeit im Lichte der angewandten Forschung im beruflichen Kontext zu verorten, um den aktuellen Herausforderungen und Problemen der dynamischen Informationstechnik angemessen begegnen zu können. Die Lehre ist dabei nicht Teil dieses wissenschaftlichen Vorhabens, sondern ein ergänzendes Handlungsfeld, welches ich unabhängig von der forschenden Tätigkeit wahrnehme. Dessen ungeachtet fließen die Erkenntnisse dieser Forschungstätigkeit in meine Dozententätigkeiten ein, welche ich in den vergangenen Jahren an der Universität Bremen, der Hochschule Bremen und der Hochschule für die öffentliche Verwaltung wahrnehmen durfte.

Eine solche Arbeit kann nicht ohne weitere Menschen und nur in einem wohlwollenden Umfeld entstehen, insbesondere einer verständnisvollen Familie, dem kollegialen Entgegenkommen im Beruf und den Beschäftigten an den betreuenden Lehrstühlen der Universität Rostock, die mich alle und anhaltend in diesem Vorhaben bestärkt haben. Die hier eingereichte Arbeit entstand als externer Doktorand am Lehrstuhl für Wirtschaftsinformatik (WIN) und am Lehrstuhl für Informations- und Kommunikationsdienste (IuK) der Universität Rostock. Meinen besonderen Dank möchte ich Prof. Dr. Kurt Sandkuhl aussprechen. Unsere Zusammentreffen haben wesentlich dazu beigetragen, mich als Forscher zu entwickeln und zu verbessern. Auch im fortgeschrittenen Alter habe ich vieles von ihm gelernt, vor allem, wie meine Forschungstätigkeit strukturiert bleibt und die Ergebnisse dieser methodisch im wissenschaftlichen Kontext anerkannt werden. Ich bin sehr dankbar ihn als Doktorvater hatte und als Freund in meinem Leben gewinnen konnte. Darüber hinaus bin ich sehr dankbar, dass mich Prof. Dr. Clemens H. Cap als externen Promovenden am Lehrstuhl IuK angenommen und meine Betreuung am Lehrstuhl Wirtschaftsinformatik erweitert hat. Auch von ihm konnte ich in den vergangenen Jahren vieles lernen, was für einen Forscher elementar ist. Der Kontakt zur Universität

Rostock sowie die bremische Vorort-Betreuung wurde durch Prof. Dr. Thomas Kemmerich von der Universität Bremen gewährleistet. Ein guter Freund und Ansprechpartner, der mich in meinem Forschungsvorhaben bestärkt und Möglichkeiten zu meiner persönlichen Entwicklung gegeben hat.

Mein besonderer Dank gilt schlussendlich meiner Frau Nicole und meinen Kindern Paul Benedikt sowie Anna Katharina, die auf viel gemeinsame Zeit in Urlauben, an Abenden und Wochenenden verzichten mussten, ohne jemals meine Absicht in Frage zu stellen. Ich kann mich immer auf Euch verlassen.

1 Synopse

Die föderale Cybersicherheit in Deutschland steht vor der Herausforderung, unterschiedliche Akteure auf Bundes-, Landes- und Kommunalebene zu koordinieren. Eine kumulative Promotion bietet die Möglichkeit, dieses komplexe Themenfeld durch mehrere wissenschaftliche Publikationen aus unterschiedlichen Perspektiven zu eruieren und anhaltende Veränderungen fortzuschreiben. Diese Dissertation setzt sich daher mit rechtlichen, organisatorischen und technischen Aspekten der föderalen Cybersicherheit schrittweise auseinander und untersucht insbesondere die Kooperationsmechanismen zwischen den zu beteiligenden Institutionen. Mit der vorliegenden kumulativen Promotion werden der Problemaufriss dargelegt, die anwendbaren Forschungsmethoden hergeleitet, die relevanten Publikationen erörtert und eine Schlussbetrachtung vorgenommen. Die Synopse gliedert sich daher in:

- der Herleitung der Problematik und Motivation, der Relevanz und Aktualität des Forschungsvorhabens sowie der Forschungslücke,
- den Forschungsfragen und –zielen, der methodischen Herangehensweise und dem Forschungsvorgehen in der relevanten Domäne,
- die Ergebnisse aus entstandenen Publikationen über den Forschungszeitraum und die Anwendung auf das spezifische Forschungsvorgehen und
- die Schlussbetrachtung und Diskussion der Ergebnisse sowie mögliche weitere Arbeiten sowie Beschränkungen dieser Arbeit.

Insgesamt sind in der vorliegenden Forschungsarbeit vierzehn Veröffentlichungen entstanden, von denen elf in den auf die Synopse folgenden Kapiteln einbezogen wurden. Die ersten Publikationen widmen sich der Analyse bestehender Strategien, Organisationen und Mechanismen der Informations- und Cybersicherheit in Ländern, Kommunen und Wirtschaftsunternehmen, um herauszukristallisieren, welche Defizite und gemeinsamen Anforderungen an eine Cybersicherheitsarchitektur aus Sicht der Akteure bestehen (siehe Kapitel 2, 3 und 4). Begleitend zu den technisch-organisatorischen Studien wurden über den gesamten Forschungszeitraum rechtliche Begleitstudien vorgenommen, die als Beiträge in die Synopse eingeflossen sind (siehe Kapitel 5, 6 und 7). Die kumulative Struktur der Promotion ermöglichte es, die aktuellen Entwicklungen zu berücksichtigen, und erlaubte es weiter, technische, rechtliche und organisatorische Fortschritte zeitnah in die Forschung einzubeziehen. Die in den Kapiteln 8 und 9 veröffentlichten Beiträge zeigen auf, wie einzelne Anforderungen, z. B. Informationssicherheitsmanagement oder Datenschutzmanagement, in die Architektur einbezogen werden können. Die Vorstellung der föderalen Cybersicherheitsarchitektur erfolgt in Kapitel 10 sowie die Evaluation eben dieser in den Kapiteln 11 und 12. Durch die sukzessiven Veröffentlichungen der Forschungsergebnisse in der Forschungsgemeinschaft wurde der Wissenstransfer in Politik, Verwaltung und Wirtschaft gefördert.

1.1 Einleitung

Die vorliegende Forschungsarbeit ist im beruflichen Kontext – zu föderalen Herausforderungen in der Organisation der Abwehr von Cybersicherheitsbedrohungen – entstanden und adressiert das hochdynamische sowie durch permanente Angriffe gekennzeichnete Umfeld der Sicherung von staatlichen IKT-Infrastrukturen. Die im ersten Kapitel beinhaltete Motivation, Problemstellung und Relevanz stellt eine spezifische Einführung in der Forschungsdomäne dar und soll die abstrakte Problematik der Aufrechterhaltung von Staats- und Regierungsfunktionen im Zusammenhang mit der Informationstechnik aufzeigen.

1.1.1 Motivation

Dass die Gesellschaft und ihre Menschen vor negativen Einflüssen geschützt werden müssen, ist eine Aufgabe, die von den jeweiligen Betroffenen individuell und regelmäßig vom Staat wahrgenommen werden. Der gesellschaftliche Gemeinsinn wird durch die aktuelle politische Lage geprägt – insbesondere durch die Auswirkungen kriegerischer Handlungen wie Sabotageversuche, Spionage und Desinformationskampagnen sowie die anhaltende Herausforderung der Flüchtlingsmigration. All dies stellt eine fortwährende Bewährungsprobe für die Stabilität unseres Zusammenlebens dar. Ein Staat muss sich durch ein gemeinschaftliches und rechtssicheres Handeln diesen hybriden Bedrohungen (Mazaraki & Goncharova, 2022, S. 115–120) entgegenstellen und erwehren, was kein selbstloses Unterfangen im Sinne von Altruismus bedeutet, sondern das allgemeine Verständnis einer Pflichtaufgabe des Staates widerspiegelt. Der Staat muss entscheiden wie er Aufgaben organisiert, d. h. delegiert oder selbst wahrnimmt, um das Miteinander zu sichern (Krautscheid, 2009, S. 22).

Auch die digitalisierte Welt birgt Bedrohungen, vor denen sich die Menschen, die Unternehmen und auch der Staat schützen müssen (Möller, 2023, S. 10), insbesondere um ihren kollektiven Zusammenhalt und das Vertrauen in den Staat zu sichern, aber auch zu entwickeln. Speziell im föderalen Deutschland sind traditionell stark verteilte Strukturen und Zuständigkeiten – in der allgemeinen Gefahrenabwehr – zwischen dem Bund und den Ländern entstanden, die es zu koordinieren gilt. Ein Teilaspekt dieser speziellen Gefahrenabwehr betrifft den Umgang mit Risiken und Bedrohungen der Informationstechnik für Staat, Wirtschaft und Gesellschaft. Eine Zusammenarbeit aller Akteure ist erforderlich (Daase, 2013, S. 145–147).

Die berufliche Tätigkeit in den wissenschaftlichen Diskurs zu heben, ist in der vorliegenden Konstellation zielführend, da eine praxisorientierte Problematik nicht zwangsläufig mit methodischen Bestandswissen einheitlich und übergreifend gelöst wird. Vielmehr bedarf es der empirischen Problem-Identifikation und Motivation, um neues Wissenspotenzial zu heben. Die Notwendigkeit, berufspraktisches Wissen mit dem Aufbau von akademischen Fähigkeiten zu kombinieren, stellt keinen Selbstzweck dar, vielmehr dient es

der Sicherstellung von Forschungsbeziehungen und dem Erkenntnisgewinnen (Durning & Jenkins, 2005, S. 407–426). Die Forschungsarbeit muss dabei wissenschaftlich interessant und praktisch relevant sein sowie einen Mehrwert liefern. Zielführend ist dabei die Überführung der Problematik in den anhaltenden öffentlichen und wissenschaftlichen Austausch, um Wissen zu generieren (Daumiller, 2018, S. 157–162). Als praxisrelevante Forschungsarbeit wird ein moderner Ansatz verfolgt, der über bekannte Lösungen hinausgeht und innovative Artefakte liefert. Die Nutzer- und Nutzungszentrierung wird im Forschungsprozess anhaltend über die Stakeholder Einbindung generiert.

1.1.2 Problemstellung

Die IKT hat in den vergangenen Jahrzehnten ihren zentralen Einfluss auf die Gesellschaft so weitgehend intensiviert, dass ein Leben ohne Informationssysteme nicht mehr vorstellbar ist. Dies gilt insbesondere vor dem Hintergrund der zunehmenden Digitalisierung aller Lebensbereiche, im Privaten und auch im Zusammenwirken von Wirtschaft und Verwaltung sowie in einer allgegenwärtigen Vernetzung. Vor diesem Hintergrund steigen die Anforderungen an eine verlässliche und sichere Informationstechnik stetig. Gleichzeitig wird die Notwendigkeit von Zertifizierungen zur Erhöhung der IT-Sicherheit für in die Europäische Union (EU) eingeführte Produkte diskutiert. Dabei wird jedoch die Wirksamkeit spezifischer Maßnahmen wie der Einfuhrkontrolle infrage gestellt. (A. Weber et al., 2020, S. 31–32). Die komplexen miteinander interagierenden Systeme sollen bestenfalls unterbrechungsfrei arbeiten. Gleichzeitig geschehen aber Ereignisse, die nicht vorhersehbar sind bzw. deren Folgewirkungen auch nicht im risikobasierten Management bedacht werden können. Es bedarf folglich konzeptioneller Maßnahmen zur Erhöhung der Resilienz (Neugebauer, 2018, S. 295–299), um auch bei außergewöhnlichen Störungen die Kontrolle bestmöglich zu behalten oder zeitnah zurückzugewinnen.

Die Funktionsfähigkeit von informationstechnischen Systemen ist ein Garant für das Funktionieren von Wirtschaft, Verwaltung und Gesellschaft. Dabei ist die *Verfügbarkeit* nicht auf einzelne IT-Anwendungen, IT-Systeme oder IT-Netze beschränkt, sondern umfasst die erwartungskonforme funktionale und autorisierte Nutzung in der Datenverarbeitung (safety). Daneben sind zwei weitere Definitionen zur *Integrität* und *Vertraulichkeit* relevant. Die Integrität bezeichnet die Unversehrtheit also Korrektheit von Daten und deren einwandfreie Verarbeitung in Systemen. Die Vertraulichkeit bezeichnet die berechtigte Kenntnisnahme und Bearbeitung von gespeicherten und übertragenen Daten. Diese drei allgemein formulierten Schutzziele sind als CIA-Triade bekannt (Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availability (Verfügbarkeit). Sofern diese Ziele den Schutz der technischen Infrastruktur adressieren, spricht man von *IT-Sicherheit (security)*.

Werden die Ziele der CIA-Triade zum Schutz von Daten verfolgt, unabhängig davon, ob es sich um personenbezogene oder weitere Daten handelt, ist regelmäßig die *Datensicherheit* im Fokus der Betrachtung. Solche Daten können im Unterschied zur IT-

Sicherheit in technischen und nichttechnischen Systemen anfallen. Das heißt, es können auch Schriftstücke betroffen sein, welche synonyme Ziele in der Datensicherheit verfolgen, wie zum Beispiel den Schutz vor Verlust, Manipulation und unberechtigten Zugriff (security) auf Daten.

Die informationelle Selbstbestimmung von Individuen wird mit dem *Datenschutz* und verbundenen rechtlichen Regelungen verfolgt. Der Datenschutz soll sicherstellen, dass personenbezogene oder personenbeziehbare Daten vor insbesondere unerlaubter Erhebung, Speicherung, Analyse, Verarbeitung und Weitergabe geschützt werden. Der Datenschutz umfasst organisatorische und technische Maßnahmen zur Sicherstellung von Datenschutzzielen. Neben den allgemeinen Zielen der CIA-Triade werden mit dem Datenschutz auch Ziele wie Datensparsamkeit, Zweckbindung, Revisionsfähigkeit, Authentizität, Nichtverkettbarkeit oder auch Intervenierbarkeit verfolgt (Rost, 2025, S. 93 ff). Das Datenschutzrecht ist durch die europäische Datenschutz-Grundverordnung (EU-DSGVO) und auf Ebene der Mitgliedsstaaten durch weitere Gesetze, wie das deutsche Bundesdatenschutzgesetz (BDSG), grundsätzlich geregelt. Im Föderalstaat Deutschland wird es durch Ausführungsgesetze zum Datenschutz /zur DSGVO der Länder ergänzt sowie durch spezialgesetzliche Regelungen - wie zum Beispiel im Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) oder im Patientendaten-Schutz-Gesetz (PDSG) - spezifiziert.

Die technische und nichttechnische Datenverarbeitung wird durch die IT-Sicherheit, die Datensicherheit und den Datenschutz zum einen abgegrenzt und zum anderen in der Begriffsdeutung *Informationssicherheit* inkludiert, wie in Abbildung 1 dargestellt. Technische und organisatorische Maßnahmen, die überordnete und spezifische Ziele sowie die Konformität zu gesetzlichen, vertraglichen oder auch unternehmerischen Regelungen sicherzustellen, werden als Informationssicherheit bezeichnet. Dabei sind Zielkonflikte der einzelnen Ansprüche inhärent und müssen gegeneinander abgewogen werden. Zum Beispiel werden Daten für die Abwehr von Bedrohungen für die IT-Sicherheit längerfristig Daten erhoben und gespeichert, die zur Analyse und Abwehr von zum Beispiel Advanced Persistents Threats (APT) geeignet sind und mit den Anforderungen an den Datenschutz, wie Datensparsamkeit und Zweckbindung, kollidieren. Die Abwägung und Organisation von technischen und organisatorischen Maßnahmen ist Teil eines *Informationssicherheitsmanagementsystems (ISMS)*. Definitionsgemäß trägt ein ISMS dazu bei, mit Regelungen und Prozessen innerhalb einer Organisation, die Ziele der Informationssicherheit zu definieren, dabei externe und interne Anforderungen zu bestimmen, erforderliche Prozesse und Maßnahmen einzusteuern, diese zyklisch zu kontrollieren, aufrechtzuerhalten und anhaltend zu verbessern.

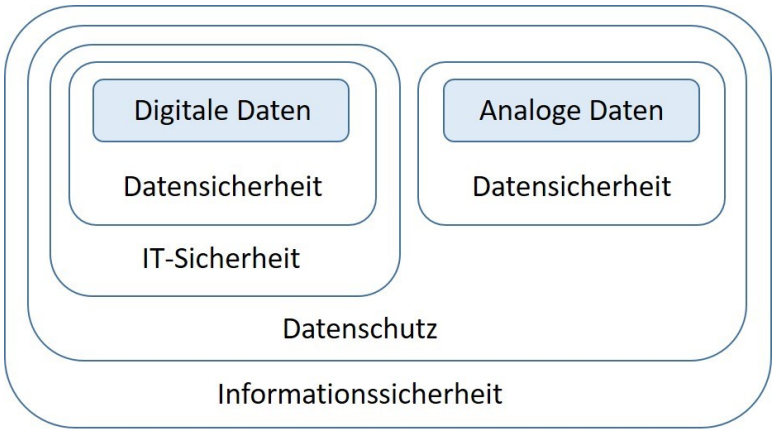

Abbildung 1 Informationssicherheit (eigene Darstellung)

Systematisierte Vorgehensweisen für die Implementierung von Informationssicherheitsmanagementsystemen existieren seit den frühen neunziger Jahren. Mit der Adaptierung des britischen Standards BS7799 „code of practise“ für Informationssicherheit wurde ein international anerkannter Standard mit der ISO/IEC 27001 veröffentlicht. Dieser Standard findet weltweit Anwendung und ist insbesondere bei Unternehmen Grundlage ggf. Bedingung von geschäftlichen Beziehungen. Für den Kontext der öffentlichen Verwaltung in Deutschland wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Quasi-Standard zuvorderst für die Bundesverwaltung entwickelt, der zwischenzeitlich auch in den Ländern und Kommunen sowie vereinzelt in Unternehmen Anwendung findet. Die beinhaltete Vorgehensweise des IT-Grundschutzes zur Etablierung eines ISMS wird anhaltend fortentwickelt und ist derzeit als BSI-Standards 200-1 bis 200-4, ergänzt um das IT-Grundschutz-Kompendium, bekannt. Um eine höhere Anerkennung des IT-Grundschutzes zu erlangen, kann eine ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz durch das BSI erfolgen. Im Unterschied zu einer akkreditierten ISO 27001 Zertifizierung handelt es sich dabei nicht um ein anerkanntes Verfahren bei der deutschen Akkreditierungsstelle (DAkkS). Gleichwohl ist die IT-Grundschutzmethodik ein wichtiger Baustein der Informationssicherheit und im Bereich der öffentlichen Verwaltung auch des Informationssicherheitsmanagementsystems.

Alle Organisationen müssen sich der Dynamik von Bedrohungslagen in der Informationstechnik erwehren. Unbestritten ist dabei, dass ein ISMS dies nachhaltig unterstützt bzw. auch als Voraussetzung verstanden wird. Dabei werden die Einführung und der Betrieb eines ISMS nach ISO27001 oder dem BSI IT-Grundschutz insbesondere für kleine und mittlere Organisationen oftmals als mit zu hohen Aufwendungen verbunden, wohingegen ein strukturierter Ansatz zur Einführung eines ISMS mit dem Compliance-Informations-Sicherheits-Management-System in zwölf Schritten (CISIS12) in allen Organisationsgrößen angemessen möglich ist (Moses & Rehbohm, 2023a, S. 14–19). Für die öffentliche Verwaltung wurde CISIS12 im IT-Planungsrat (IT-PLR) als angemessene Vorgehensweise für die Einführung eines ISMS im kommunalen Umfeld empfohlen.

Der IT-PLR wurde mit Änderung des Grundgesetzes und für die politische und technische Koordinierung der Zusammenarbeit in der Informationstechnik von Bund und Länder (Kommunen) im Jahr 2010 gegründet.

Ungeachtet dessen ist der Schutz der Informationen ein immer aufwändigeres Unterfangen, welches mit hohem Ressourceneinsatz einhergeht. Der Bereich der Cyberkriminalität nimmt dabei nicht nur den größten Anteil an Bedrohungen ein, sondern ist für die Angreifer auch der lukrativste, sofern es die kriminelle „Wertschöpfungskette“ betrifft. Es kommen unterschiedliche Vorgehensweisen zur Infiltrierung des Netzes, respektive der Opfersysteme in Frage, mit dem Ziel, eine Schadsoftware zu platzieren. Insbesondere werden mit der Einschleusung von z. B. Erpressungstrojanern vermehrt Kommunen, kleine und mittlere Unternehmen (KMU) und kritische Infrastrukturen (KRITIS) angegriffen, mit dem Ziel der Lösegelderpressung. Kritische Infrastrukturen sind all solche Einrichtungen oder Unternehmen, deren Ausfall nachhaltig das Gemeinwohl, zum Beispiel durch mangelnde Versorgung der Bevölkerung, beeinträchtigen würde. Oftmals sind solche Unternehmen in kommunaler Beteiligung oder als kommunale Betriebe tätig. Allgemeine und weitverbreitete Bedrohungen treffen aber auch die Bevölkerung oder Kleinstunternehmen. Ungezielte und auf eine breite Ebene der Betroffenheit angelegte Verteilung von Schadsoftware wird z. B. mittels *Phishings* (Passwort Fishing) ausgeliefert, unter anderem mit dem Ziel des Identitätsdiebstahls und der Intention der Abschöpfung von Daten bzw. von Kontozugängen zur Gewinnerzielung. Im Gegensatz hierzu bedrohen gezielte Angriffe die Sicherheit unserer Gesellschaft. Im Zuge der sich veränderten sicherheitspolitischen Lage werden vermehrt Aktivitäten anderer Staaten registriert, die zur Spionage und Sabotage geeignet sind und mit dem Ziel der nachhaltigen Störung der Informationstechnik oder auch der vorgelagerten elektronischen Lieferketten einhergehen. Solche Aktivitäten sind regelmäßig das Handlungsfeld eines Landesverfassungsschutzes (LfV). Im Kontext des Staatsschutzes kommen moderne Techniken der künstlichen Intelligenz, wie dem Large Language Model (LLM), zum Einsatz, um gezielt gegen die Verbreitung von Desinformationen vorzugehen und die Manipulation der Bevölkerung zu verhindern.

Eine umfassende Analyse der Bedrohungen für die Informationstechnik werden in Deutschland vom BSI jährlich in einer Veröffentlichung für das zurückliegende Jahr bewertet und publiziert. In „Die Lage der IT-Sicherheit in Deutschland 2023“ (Bundesamt für Sicherheit in der Informationstechnik, 2023) wird zusammenfassend postuliert:

„*Insgesamt zeigte sich im aktuellen Berichtszeitraum eine angespannte bis kritische Lage. Die Bedrohung im Cyberraum ist damit so hoch wie nie zuvor.*“

Entlang der Definition des BSI befasst sich die Cybersicherheit mit allen und insbesondere mit dem Internet vernetzten Systemen der Informations- und Kommunikationstechnik – der Informationsverarbeitung im Cyberraum. Dieser Ansatz ist aus Sicht des BSI und mit dem Auftrag, sich als deutsche Cybersicherheitsbehörde beim Bund für Staat,

Wirtschaft und Gesellschaft in der Informationssicherheit und Digitalisierung zu positionieren, korrekt ausgewiesen, greift aber für das hier behandelte Forschungsvorhaben zu kurz. Demgegenüber hat das Bundesministerium für Verteidigung mit seiner Definition des Cyber- und Informationsraums (CIR) einen mit Staat, Wirtschaft und Gesellschaft gleichen Adressatenkreis und stellt auch bei der Bedrohungssituation auf Institutionen, Unternehmen und Individuen ab, jedoch werden eigene Handlungserfordernisse postuliert – nämlich, dass unabhängig von politischen Konstellationen die Cybersicherheit eine gesamtstaatliche Aufgabe ist. Eine gesamtstaatliche Aufgabe ist unmissverständlich keine alleinige Aufgabe des Bundes, sondern involviert die Länder ggf. die Kommunen gleichermaßen.

Das allgemeine Verständnis über die Funktion eines Informationssicherheitsmanagements ist, es würde gezielt einer einzelnen Organisation, die sich mit technischen und organisatorischen Möglichkeiten der Abwehr von Bedrohungslagen eingegrenzt hat, dabei helfen, ihre eigene Informationssicherheit zu schützen. Die komplexe Vernetzung von Systemen, Technologien oder Diensten macht jedoch eine Abgrenzung – zum Beispiel in einem Perimeter – schwierig bis unmöglich. Die Wirksamkeit der Abwehrmaßnahmen, bezogen auf eine einzelne Organisation oder Institution, sind nicht länger gewährleistet.

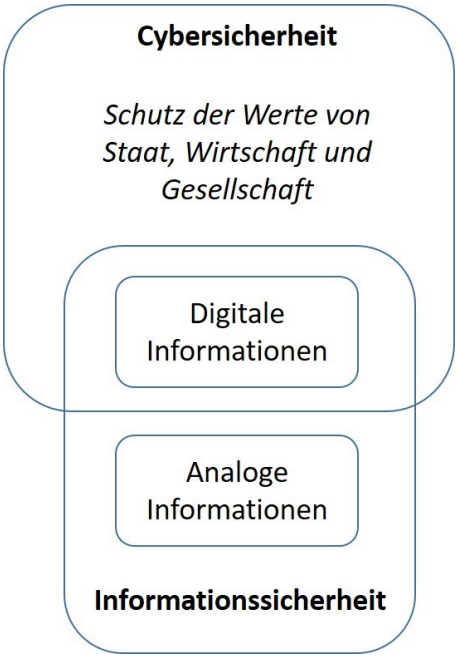

Abbildung 2 Cybersicherheit (eigene Darstellung)

Diese Forschungsarbeit zielt darauf ab, nicht die einzelne Organisation, sondern die Region bzw. ein Bundesland in Deutschland als übergreifendes Informations- und Cybersicherheitsmanagement zu problematisieren (siehe hierzu Abbildung 2 Cybersicherheit (eigene Darstellung)). Es wurde durch empirische Untersuchungen festgestellt (siehe

Kapitel On Challenges of Cyber and Information Security Management in Federal Structures - The Example of German Public Administration), dass der Bedarf an eine solche strukturell-methodischen Unterstützung gegeben ist. Das Ziel dieser Arbeit ist die Lieferung einer solchen Unterstützung, in Form einer Architekturentwicklung. Die entwickelte harmonisierte föderale Cybersicherheitsarchitektur soll nachhaltig die Cybersicherheitsresilienz des jeweiligen Landes verbessern und sich nahtlos in die deutsche und folglich auch in die europäische Cybersicherheitsarchitektur einordnen. Die methodengeleitete Forschung zur Erarbeitung einer solchen Architektur wird in diesem Beitrag thematisiert.

1.1.3 Relevanz

Diese Forschungsarbeit hat für Deutschland und seine Länder eine hohe Relevanz, da die Akteure der föderalen Cybersicherheit eine uneinheitliche Entwicklung vollzogen haben. Abhängig davon, ob für das Thema Cyber- und Informationssicherheit eine politische Aufmerksamkeit, verbunden mit der Steuerung von Ressourcen, besteht, existieren derzeit unterschiedliche qualitative Cybersicherheitsorganisationen. Eine Visualisierung der staatlichen deutschen Cybersicherheitsorganisation wird seit 2017 von der Stiftung *„Neue Verantwortung“* fortgeschrieben (Herpig & Dutke, 2023, S. 117ff). Die Autoren zielen darauf ab, mit ihrem Beitrag aufzuzeigen, dass eine strukturierte und auch politische Herangehensweise für eine effiziente und effektive Cybersicherheit erforderlich ist.

Grundsätzlich sind die Länder bei der Wahrnehmung der allgemeinen Gefahrenabwehr und Aufrechterhaltung der öffentlichen Sicherheit in Verantwortung. Das gilt insbesondere für das Polizei- und Ordnungsrecht bis hin zum Zivil- und Katastrophenschutz. Bund und Länder arbeiten zum Beispiel bei der Verfolgung von Straftaten im Polizeibereich zusammen. Es existieren aber auch Arbeitsbereiche, wie der Grenzschutz, in dem der Bund die alleinige Zuständigkeit gemäß Grundgesetz hat. Eine alleinige Zuständigkeit für die Cybersicherheit beim Bund besteht indes nicht.

Mit einer cybersicherheitspolitischen Strategie hat die Bundesregierung und mit einer Agenda das Bundesministerium des Innern und für Heimat (BMI) ein Leitbild für die digitale Sicherheit Deutschlands veröffentlicht. In Anerkennung dessen, dass Cybersicherheitsbedrohungen nicht an Landesgrenzen gebunden sind, hat der Bund verschiedene Einrichtungen in seine Cybersicherheitsorganisation eingebunden.

Das BSI als Cybersicherheitsbehörde des Bundes ist für Staat, Wirtschaft und Gesellschaft mit Leistungen für Bürgerinnen und Bürger, für die Wirtschaft unmittelbar - und für die Verwaltung zuvorderst für den Bund sowie für alle anderen öffentlichen Verwaltungen als möglicher Kooperationspartner tätig. Das Computer Emergency Response Team Bund (CERT Bund) beim BSI wurde insbesondere um den Verwaltungs-CERT-Verbund (VCV) in den Ländern erweitert. Das BSI hat jedoch nur in Bayern – mit dem Landesamt für Sicherheit in der Informationstechnik (LSI) – eine institutionalisierte Entsprechung. Die Länder haben sich überwiegend mit Zentralstellen für Cybersicherheit

organisiert, wie zum Beispiel mit dem Cyber-Competence-Center in Hessen (Hessen3C). Mit dem Bundeskriminalamt (BKA) und dem Bundesverfassungsschutz (BfV) wird zum einen Kriminalität im Bereich *Cybercrime* bekämpft und zum anderen nachrichtendienstliche Erkenntnisse zur Spionage, Sabotage oder auch zu Desinformationen ausgewertet. Für beide Bundesämter bestehen in allen Ländern entsprechende Landesämter mit bewährter Zusammenarbeit und inhaltlichem Austausch. Eine Querschnittsaufgabe im BMI nimmt die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) wahr. Diese arbeitet in Bereichen der digitalen Forensik oder Analyse in der Kryptografie für und mit allen Sicherheitsbehörden des Bundes, jedoch derzeit nicht mit den Ländern zusammen.

Neben diesen unter der Regie des BMI agierenden Behörden existieren weitere Bundeseinrichtungen aus anderen Ressorts (z. B. das Bundesamt für den Militärischen Abschirmdienst (BAMAD)), deren Zusammenarbeit im Nationalen Cyber-Abwehrzentrum (Cyber-AZ) koordiniert wird.

Grundsätzlich bestehen demnach Anknüpfungspunkte in den Ländern, welche jedoch nicht auf eine vergleichbare Landesorganisation treffen. Das BMI hat mit seiner Cybersicherheitsagenda angekündigt, das BSI zu einer zentralen Stelle für Bund und Länder ausbauen zu wollen, um die Zusammenarbeit mit den Ländern zu verbessern. Für die rechtliche Durchsetzung dieses Ansinnens und grundsätzliche Verschiebung von verfassungsrechtlichen Zuständigkeiten ist eine Änderung des Grundgesetzes (GG) erforderlich, was vom BMI angestrebt wird. Durch die europäische Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie), (Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie), 2023) sind Bund und Länder gleichermaßen verpflichtet, Vorsorge gegen Cybersicherheitsbedrohungen zu leisten. Der Bund begegnet dieser Herausforderung mit dem Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), (Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, 2024)). Der Bund schafft hiermit insbesondere Regelungen zum Informationssicherheitsmanagement in der Bundesverwaltung, erweitert den Anwendungsbereich auf Betreiber kritischer Infrastrukturen, mithin auf deren Mindestsicherheitsanforderungen und räumt dem BSI erweiterte Rechte zur Aufsichtsführung über diese Unternehmen ein. Die Länder wiederum müssen ihrerseits Rechtsnormen schaffen, um die Anforderungen der NIS-2-Richtlinie in ihrem Verantwortungsbereich sicherzustellen. Die Umsetzung erfolgt in den Ländern per Gesetz oder Verwaltungsvorschrift. Hierfür kann eine föderale Cybersicherheitsarchitektur die notwendige Organisationsstruktur schaffen, um einheitlich die gesamtdeutsche Cybersicherheitsarchitektur um die Länder zu ergänzen. Für Bund und Länder gilt gleichermaßen, dass gesellschaftliche Werte gemeinschaftlich geschützt werden müssen. Werte, die insbesondere in Familie, Arbeit, Politik oder Wissenschaft grundsätzlich im jeweiligen Kontext geregelt sind, werden angesichts der bestehenden

Cybersicherheitsbedrohungen von der Sozialforschung und hier behandelter „Technikfolgeabschätzung“ als kaum noch zu differenzieren ausgewiesen, insbesondere besteht die Gefahr, dass unsere Lebensweise bedroht ist, was wiederum den Staat als Akteur fordert (K. Weber et al., 2020, S. 12–13). Werte sind auch Daten im Kontext der Datenwirtschaft mit einhergehender Datenwertschöpfung. Die datengetriebenen Geschäftsmodelle von Wirtschaftsunternehmen verändern sich hinsichtlich des grenzkostenfreien Angebotes von Diensten. Die Überlassung von sensiblen Daten bzw. Informationen muss dabei in unternehmerischer Hinsicht die Zusicherung von Sicherheitsmaßnahmen bei den Partnern überprüfbar gewährleisten (Rohde et al., 2022, S. 139): eine koordinierende Aufgabe, die nicht der Eigenverantwortung von Unternehmen überlassen werden sollte, sofern sie der regionalen Daseinsvorsorge dient. Die staatliche Gewährleistungsverantwortung umfasst nicht nur die Digitalisierung von Verwaltungsleistungen, sondern auch die Infrastrukturen und Dienste weiterer Akteure in der Region (*Regulierung digitaler Plattformen als Infrastrukturen der Daseinsvorsorge*, 2021, S. 12). Der von *Ernst Forsthoff* geprägte Begriff der Daseinsvorsorge hat sich insofern entwickelt, dass er in der heutigen Gesellschaft die Grundversorgung mit existenziellen Gütern und mithin die Infrastrukturen einschließt (Ehrenzeller et al., 2014, S. 332–335). Die Relevanz dieser Forschungsarbeit ist daher hoch und sie wird zu einem Zeitpunkt veröffentlicht, in dem die Mitgliedstaaten der EU, aber insbesondere auch der Föderalstaat Deutschlands gefordert sind, die Akteure der Region in eine landesbezogene Cybersicherheitsorganisation einzubinden, die hier als föderale Cybersicherheitsarchitektur präsentiert wird. Die Länder haben teilweise Cybersicherheitsstrategien festgelegt, sind in der Abstimmung einer solchen oder planen diese, was für die vorgestellte Cybersicherheitsarchitektur förderlich ist. Der Bund hat in seiner Cybersicherheitsstrategie die Prüfung der aktuellen Zuständigkeits- und Aufgabenverteilung herausgehoben und stellt auf ein sinnvolles Zusammenwirken aller Akteure unter Einbeziehung der Länder ab. Das macht eine föderale Cybersicherheitsarchitektur unentbehrlich.

1.2 Forschungskontext

Forschungen im Umfeld der Cybersicherheit nehmen in der Wissenschaft zwischenzeitlich ein breites Feld von Aktivitäten ein. Der wissenschaftliche Diskurs zur Cybersicherheit ist in so unterschiedlichen Bereichen wie Rechtswissenschaften, Wirtschaftswissenschaften, Ingenieurswesen bis hin zu Sozialwissenschaften und Verwaltungswissenschaften immanent. Entlang dieser Fachbereiche sind Institute entstanden und neue Lehrstühle begründet worden. Im Fokus stehen neben der internationalen Forschung insbesondere die für diese Arbeiten relevante Europäische Union, ihre Mitgliedsstaaten und die Wirtschaft sowie für den deutschen Kontext die Kommunen. Technische Forschungsfelder befassen sich insbesondere mit der Internetsicherheit, der Erkennung und Abwehr von Bedrohungen, mit dem Schutz von Daten und elektronischen Identitäten oder auch den Chancen und Herausforderungen des Quantencomputings. In Wirtschaft und Verwaltung sind die Nutzung der KI oder die Digitalisierung von Prozessen im Fokus, um einerseits die Wertschöpfung zu verbessern bzw. die Effizienzsteigerung zu gewährleisten. In der Sozialforschung haben sich andererseits Themen wie resiliente IKT-Infrastrukturen, Daseinsvorsoge oder digitale Souveränität etabliert. Gerahmt wird das Forschungsfeld Cybersicherheit von umfangreichen rechtswissenschaftlichen Untersuchungen, insbesondere auf den Ebenen Europäische Union, Mitgliedsstaaten und Föderalstaaten. Diese nichtabschließende Aufzählung von Forschungsaktivitäten in der Cybersicherheit findet Eingang in diese Arbeit. Der disziplinäre Ansatz dieser Forschungsarbeit wird durch Erkenntnisse interdisziplinärer Forschungen anderer Bereiche angereichert. Es wurden qualitative und quantitative Forschungsmethoden angewendet, um dem identifizierten Problemaufriss (siehe Forschungsziel und Forschungsfragen) mit wissenschaftlichen Methoden (siehe Forschungsmethoden) zu begegnen. Diese Arbeit ist im Umfeld der öffentlichen Verwaltung Deutschlands, mit dem Fokus auf föderale Landesregierungen (siehe Forschungsumfeld Öffentliche Verwaltung), entstanden und entwickelt nach dem Design-Science-Research (DSR) -Forschungsansatz (siehe Forschungsparadigma Design Science Research) Artefakte, die mit Hilfe einer auf diesen Kontext der Föderalstaaten abgestellte Unternehmensarchitektur zu einem Referenzmodell weiterentwickelt werden sollen. Das allgemeine Modell stellt dabei den konzeptionellen Rahmen dar, der generell genutzt werden soll, Änderungsanforderungen umsetzen kann und grundsätzlich als zielführend anerkannt wird. Die interdisziplinäre Forschung, entlang des DSR-Prozesses (siehe Forschungsvorgehen), zeigt auf, dass die vorliegende Arbeit – in der Verwaltungsdomäne – zuvorderst das Verstehen des Problems unter zu bestimmbaren Rahmenbedingungen umfasst und das Erarbeiten und Verifizieren einer Lösung beinhaltet, welche den Anspruch an eine föderale Referenzarchitektur hat.

1.2.1 Forschungsziel und Forschungsfragen

Die Arbeit entstand mit der Intention, eine Forschungslücke in der europäischen Cybersicherheitsorganisation, insbesondere des Mitgliedstaates Deutschland, aufzuzeigen und mit dem Ziel, eine anerkannte Cybersicherheitsarchitektur in den Föderalstaaten zu entwickeln. Derzeit erarbeiten die Länder und der Bund mit den ihnen zur Verfügung stehenden Ressourcen jeweils eine Organisation, die geeignet sein soll, sich der dynamischen Herausforderungen individuell zu erwehren. Es besteht grundsätzlich die Möglichkeit, Informationen zu Schwachstellen oder auch Bedrohungslagen in Verbünden auf Ministerialebene auszutauschen. Die Involvierung der Kommunen oder auch Wirtschaftsunternehmen ist hingegen bei den Ländern auf freiwilliger Basis oder landesspezifisch rechtlich ausgestaltet. Es existieren keine ausreichenden Standards bzw. auch Kompetenzen, die eine nahtlose Verantwortung für die Funktionsfähigkeit von Staat, Wirtschaft und Gesellschaft annehmen lassen. Forschungsfragen in diesem Kontext drängen sich aufgrund der aktuellen Zeitenwende auf, um das gesamtstaatliche Handeln zu verbessern. Cybersicherheit ist eine gesamtstaatliche Aufgabe, das heißt, die Länder müssen im Rahmen ihrer rechtlichen, technischen, organisatorischen, operativen und taktischen Möglichkeiten alles dafür tun, um ihre Verantwortung in der regionalen Daseinsvorsorge wahrzunehmen. Dabei ist anzuerkennen, dass die deutschen Föderalstaaten nur eine politische Ebene verfassungsgemäß repräsentieren und bestimmte Aufgaben zwischen Bund und Länder geteilt wahrgenommen werden. Das heißt aber auch, wenn die Länder für bestimmte Aufgaben zuständig sind, beeinflussen sie auch die Art und Weise – insbesondere die Ressourcen für die Ausgestaltung – der Aufgabenwahrnehmung. Diese Prämisse vorangestellt, ergibt sich folgende Forschungsfrage:

Wie kann eine föderale Cybersicherheitsarchitektur entwickelt werden, die als harmonisierte, kooperative und komplementäre Lösung in den Ländern als Mindestforderung implementiert werden kann?

Folgende ergänzende Fragestellungen haben zudem Relevanz für die Hauptfrage:

- Was sind die Mindestanforderungen an eine Landesarchitektur und welche an die involvierten Akteure?
- Welche rechtlichen Rahmenbedingungen müssen durch die Länder gestaltet und wie sollte die verantwortliche Stelle ausgestaltet werden?
- Welche Akteure der Region und Kooperationspartner müssen identifiziert und in die Architektur einbezogen werden?
- Wie können technische Erkenntnisse aus der Angriffserkennung und präventive Informationen zu Bedrohungslagen in der Architektur sicher mit der Teilnehmergemeinschaft ausgetauscht werden?
- Wer kann in der Region in Ausnahmesituationen reaktive Maßnahmen leisten und wie kann die Kontinuität der jeweiligen Dienstleistung gewährleistet werden?

Im Kontext dieses Forschungsvorhabens entstanden entlang dieser Fragestellungen Thesen und Hypothesen, die zur Beantwortung aufgestellt und ausgewertet wurden. Im Einzelnen sind sie Teil der veröffentlichten Beiträge, welche in den Kapiteln 2-12 näher erläutert werden. Dabei kamen insbesondere Hypothesen zum Einsatz, um theoretische Annahmen über Zusammenhänge zu treffen, die eigene empirische Forschung zu initialisieren und um z. B. durch statistische Auswertungen folglich die Falsifizierbarkeit oder Verifizierbarkeit sicherzustellen. Neben der quantitativen Forschung kamen auch qualitative Explorationen, wie Experteninterviews, zur Anwendung, was im folgenden Kapitel „Forschungsmethoden“ näher erläutert wird.

1.2.2 Forschungsmethoden

In der Wissenschaft und der zugrundeliegenden Wissenschaftstheorie werden nicht zuvorderst theoretische Ansätze zu Lösungen von Problemen erarbeitet, vielmehr sollen Forschungsergebnisse veröffentlicht werden und bestenfalls in die Lehre einfließen. Diese Philosophie der Wissenschaften befasst sich mit den Grundlagen und Methoden der Forschung und unter welchen Rahmenbedingungen Wissen entsteht. Die Theorie der Wissenschaft bzw. Erkenntnistheorie hat sich in den vergangenen Jahrhunderten entwickelt und kann heute in Hauptrichtungen, also verschiedenen Ansätzen, veranschaulicht werden, die sich zum Teil ergänzen, aber auch widersprechen können (Kornmesser & Büttemeyer, 2020, S. 19–34).

Der *logische Empirismus* auch *logischer Positivismus* wird als Wissenschaft mit einer analytischen naturwissenschaftlichen Herangehensweise beschrieben, in der Aussagen auf empirischen Forschungen oder Beobachtungen beruhen sowie deduktiv hergeleitet werden können. *Carnap,* als ein Hauptvertreter dieser Wissenschaftstheorie, beschreibt in seiner Arbeit „Der logische Aufbau der Welt“ mit dem Elementarerlebnis und dem Konstitutionsprinzip die empirische Vorgehensweise aus einer philosophisch-wissenschaftlichen Perspektive (Carnap, 1998, S. 90–94). Mit dem Verifikationsprinzip wird die Richtigkeit einer Aussage zum Beispiel durch Experimente sichergestellt. Nicht überprüfbare Aussagen werden hingegen als nicht relevant gedeutet bzw. verworfen. Obwohl die Vorgehensweise logisch erscheint, wirft sie dennoch ein Problem auf; es muss auch möglich sein, dass eine Theorie als falsch bewiesen werden kann. Die in dieser Arbeit genutzte spezifische Vorgehensweise führt grundsätzlich diesen Ansatz fort, im Sinne von: Es wird ein System (Artefakt) entwickelt und empirisch evaluiert, es werden logische Argumentationen und Hypothesen genutzt, um spezielle oder allgemeingültige Aussagen zu treffen, und das Ganze wird in einem realen (Wirtschaftsinformatik-)Kontext betrachtet. Die von *Simon* in „The Sciences of the Artificial“ (H. A. Simon, 2008, S. 26–30) beschriebene Rationalität erweitert die von *Carnap* insofern, als objektive und neutrale Wissenschaftstheorie um gestalterische Perspektiven zu praktischen Lösungen führen soll.

Die Falsifikationstheorie wie sie von *Popper* vertreten wird, ergänzte bzw. ersetzte in Teilen die Verifikationstheorie. Die Falsifikation zielt darauf ab, dass keine Theorie abschließend sein kann bzw. dass aufgestellte Hypothesen etwaig auch abwegig erscheinen oder sein sollen, um sie zu widerlegen und iterativ einen vorläufigen Erkenntnisgewinn zu generieren. Grundsätzlich zielt die Theorie darauf ab, durch eine wissenschaftliche Fehlerkultur ein vorläufiges Ergebnis zu erhalten, unabhängig davon, ob eine geeignete Anzahl von z. B. Experimenten die Richtigkeit belegen könnte. Folglich wird das Prinzip der Verallgemeinerung mittels Induktion in Frage gestellt (Juhos, 1970, S. 55). Die vorliegende Arbeit enthält Beiträge zu einer möglichen Referenzarchitektur, die weder abschließend sind noch in ihren Aussagen einen absoluten und vollständigen Anspruch haben können. Vielmehr lassen sich durch weitere und veränderte empirische Fallstudien auch mit weiteren Teilnehmenden die vorliegenden Ergebnisse dieser Arbeit als falsifizierbar darstellen. Das heißt, die Ergebnisse der Studien im Kontext der Wirtschaftsinformatik müssen weiterhin hinterfragt werden, um die Schwächen möglicherweise auch alternative Lösungen zu finden. Die vorliegende konkrete Lösung gilt folglich so lange, bis sie widerlegt wird, entweder in anderen Kontexten oder durch Bildung neuer Hypothesen, neuer Theorien und deren Beweis bzw. wenn die Lösung versagt.

Die Paradigmentheorie (diachronische Wissenschaftsphilosophie) von *Kuhn* zielt darauf ab, dass Wissenschaftler in einem bestimmten Forschungsumfeld mit einer bestimmten Vorgehensweise und in einer wissenschaftlichen Gemeinschaft arbeiten, um kumulativ einen Erkenntniszuwachs und wissenschaftlichen Fortschritt zu generieren. Ein Paradigma in der Forschung wird nicht in Frage gestellt, solange keine grundlegenden krisenhaften Probleme das Paradigma selbst in Frage stellen, was bei einer Anomalie (Falsifikation) allein nicht der Fall wäre. Trägt jedoch ein Paradigma aufgrund unlösbarer Krisen nicht mehr zum kumulativen Fortschritt bei, ist eine wissenschaftliche Änderung die Folge („wissenschaftliche Revolution“) (Kuhn & Hacking, 2012, S. 106). Weitere Wissenschaftstheorien wurden postuliert, sind jedoch für dieses Forschungsvorhaben außerhalb der Betrachtung.

Eingedenk der theoretischen Ansätze des Erkenntnisgewinns in der Wissenschaft stehen die methodischen Herangehensweisen dieser Arbeit im direkten Zusammenhang zu den aufgezeigten Theorien. Das hier zur Anwendung gebrachte Forschungsvorgehen führt die Wissenschaftstheorie insofern fort, als dass die erklärende Wissenschaft um die Gestaltungswissenschaften erweitert wird, das heißt, es wird nicht die absolute Wahrheit, sondern eine funktionsfähige, nützliche und anwendbare Lösung gesucht. Für diese Forschung kamen die grundsätzlich zu unterscheidenden Methoden der *nicht-empirischen* und *empirischen* Wissenschaften zur Anwendung. Die methodischen Ansätze müssen im Zusammenhang mit dem Forschungsumfeld und der Forschungsfrage stehen sowie auf Anwendungsfähigkeit des Untersuchungsgegenstandes geprüft werden.

Für die im Fachbereich der Wirtschaftsinformatik sekundär relevanten Anteile der juristischen Begleitforschung dieser Arbeit kamen *nicht-empirische* Forschungsmethoden in Betracht. Gleichwohl kann der auf den empirischen Forschungen beruhende Grundsatz

der drei Schritte: 1. Aufstellung einer Forschungsfrage, 2. Ausbildung von Hypothesen, die geeignet sind, die Forschungsfrage zu beantworten, und die Hypothesen somit bestätigen und 3. die Diskussion der gewonnenen Erkenntnisse sinngemäß angewendet werden. Die inhaltliche Forschungsfrage und die rechtswissenschaftlichen Implikationen sollen nicht in Frage gestellt werden, jedoch ergeben sich für den zweiten Schritt Abweichungen, hinsichtlich des methodischen Ansatzes, da in der Rechtswissenschaft auch von der Argumentationswissenschaft, entlang von Auslegungsmethoden wie insbesondere systematischen oder teleologischen Auslegung, gesprochen wird. Auch in dieser Arbeit und den veröffentlichten Teilen findet dieser Grundsatz Anwendung, da Begründungen zu regulatorischen Erfordernissen entlang dem Ziel einer solchen Regelung argumentiert wurden. Es erfolgt demnach eine theoretische Erklärung bzw. Überzeugung, welche die Forschungsfrage erklären kann, ggf. auch empirisch überprüft wird und letztlich, wie in der empirischen Forschung abschließend diskutiert wird. In den Argumentationswissenschaften ist die Gültigkeit dann gegeben, wenn die Mehrzahl der Experten zur gleichen Überzeugung gelangt. Insofern sind die Beiträge dieser Arbeit unter einer normativen Wissenschaft und den beinhalteten Sollansätzen zu fassen (Lagodny, 2023, S. 52–63).

In den Fachgebieten der Sozialforschung, der Naturwissenschaften und der Ingenieurswissenschaften sind empirische Forschungsmethoden, also Erfahrungswissenschaften, von elementarer Bedeutung. Diese basieren grundsätzlich auf der systematischen Sammlung und Auswertung von erhobenen Daten der realen Welt ggf. auch aus Erfahrungen, um Hypothesen überprüfbar zu machen, Theorien zu entwickeln und einen Erkenntnisgewinn hieraus zu gewinnen sowie zu postulieren. Empirische Methoden beruhen auf Daten, wie Zahlen, Beobachtungen, Befragungen, Messungen oder auch Experimenten. Je nach wissenschaftlicher Fragestellung, kommen verschiedene oder mehrere Methoden zur Anwendung. Grundsätzlich werden quantitative und qualitative Forschungsmethoden unterschieden (Döring & Bortz, 2016, S. 182–184). Welche die geeignete Form ist, hängt vom Untersuchungsgegenstand ab; sie sind gleichermaßen anerkannt. Für die vorliegende Arbeit kam ein *Mixed-Method-Ansatz* zur Anwendung. Die Kombination von qualitativen und quantitativen Forschungsmethoden folgt einem allgemeinen Trend in der Forschung. Dabei ist der Einsatz beider Methoden abhängig von den räumlichen, sachlichen und zeitlichen Anwendungsbereichen der untersuchten Domäne, also besteht eine Abhängigkeit von der Beständigkeit des Untersuchungsumfeldes. Dort, wo stabile Strukturen das Handeln der jeweiligen Akteure bestimmen und ein hoher Kenntnisstand bei Forschenden vorhanden ist, eigenen sich quantitative Methoden vorrangig (z. B. im kommunalen Umfeld). Dort, wo die Akteure deutlich mehr Handlungsoptionen in der Ausgestaltung haben, etwaig durch Veränderung der Regeln und Strukturen, eigenen sich eher qualitative Methoden (z. B. in Ländern und Unternehmen) (Kelle, 2017, S. 58).

In *qualitativen Studien* kommen z. B. bei Interviewstudien offene Fragestellungen mit wenigen Teilnehmenden, dafür jedoch in detaillierter und teilstrukturierter Form zum Einsatz. Der Forschungsprozess soll ein allgemeines Verständnis induktiv entwickeln, mit dem Ziel, auf das das Spezielle, also deduktiv schließen zu können. Vereinfacht gesagt sollen mit der induktiven Vorgehensweise mit Beobachtungen und den Erhebungen von Daten Hypothesen und Theorien entwickelt werden. Zu unterscheiden sind dabei verschiedene explorative Befragungstechniken. Daneben können auch Diskussionen in Gruppen, Experimente, Beobachtungen oder auch Einzelfallstudien als qualitative Methoden zum Einsatz kommen. Es kommen insbesondere problemzentrierte oder narrative Methoden zum Einsatz. Problemzentrierte Interviews zeichnen sich durch eine kommunikativ und interaktive Interviewform aus. Der Gesprächsleitfaden wird über nicht vorbereitete Fragen gesteuert, die den Interviewten zur Preisgabe von Informationen im Dialog leiten soll. Wie in einem Audit werden Aussagen des Befragten aufgegriffen, um mit detaillierten Nachfragen ein subjektives Bild des Problems zu erzeugen. Das Erkenntnisziel kann aber auch durch indirekte Befragungstechniken verborgen werden. Solche Verfahren sollen dem Probanden das eigentliche Erkenntnisziel verschleiern und kamen in dieser Arbeit nicht zum Einsatz. Bei der narrativen Interviewform werden hingegen wenige Fragen zur Steuerung des Interviews vorbereitet, um den Interviewpartner die wesentlichen Inhalte berichten zu lassen. Es soll kein Dialog entstehen, vielmehr soll der Befragte relevante und gültige Informationen in Erzählform berichten (Stegreiferzählungen). Der Interviewte soll berichten, wie er zu bestimmten Ereignissen handelte. Die verbal gewonnen Daten werden verschriftlicht und mit geeigneten Verfahren ausgewertet und interpretiert. Für die Auswertung kommen grundsätzlich verschiedene Verfahren in Betracht, insbesondere Methoden für die Auswertung von Einzel- oder Gruppenverfahren sowie computergestützte Verfahren. Für alle Verfahren gilt, es dürfen keine Ausschlüsse formuliert werden (Offenheit), individuelle und abweichende Einzelergebnisse müssen Berücksichtigung finden (Individualität), wesentliche und bedeutsame Ergebnisse sollen die inhaltliche Repräsentanz der Forschungsfrage klären (Bedeutsamkeit) und eine distanzierte Haltung des Forscher gegenüber diesen retrograden Daten (Reflexibilität) muss gegeben sein (Kirchmair, 2022, S. 55–64), (Brüsemeister, 2008, S. 99ff).

Dies wurde in dieser Arbeit mit der qualitativen Inhaltsanalyse nach *Mayring* konkretisiert, mit Fragestellungen und Hypothesen durchgeführt sowie an einer bestimmten Anzahl von Teilnehmenden – als Experteninterviews – in verschiedenen Studien der Kapitel 2-12 angewendet. Interviewergebnisse wurden transkribiert und einer inhaltlich strukturierten qualitativen Inhaltsanalyse unterzogen. Die Erkenntnisgewinnung entstand deskriptiv in einem holistischen Ansatz, das heißt, die Gesamtheit des Textes bliebt unabhängig von der Kategorisierung relevant. Die Ergebnisse der Einzel- oder Gruppeninterviews wurden insbesondere dahingehend bewertet, ob grundsätzliche Inkonsistenzen die Kategorisierung erschweren, genauer gesagt, ob einzelne Aussagen bzw. Themen

eine hohe Relevanz erhalten. Die sinnstiftenden Texte werden in Hauptkategorien kodiert, weitere Textpassagen dürfen unberücksichtigt bleiben. Subkategorien werden entlang von ergänzend zu differenzierenden Merkmalen nach Erforderlichkeit gebildet. Weitere Durchläufe der Kodierungen können stärkere Ausdifferenzierungen ermöglichen, sofern eine überschaubare Anzahl von Teilnehmenden an der Studie beteiligt sind. Die Zusammenfassung der Ergebnisse kann visualisiert werden oder sofort in einem Fazit münden, welches auch die ursprüngliche Forschungsfrage thematisiert (Kuckartz, 2016, S. 99–120). Grundsätzlich wurden in der vorliegenden Arbeit zu verschiedenen Stufen des Forschungsprozesses qualitative Inhaltsanalysen durchgeführt, die zu Teilaspekten der gesamten Forschung belastbare Antworten lieferten.

In quantitativen Studien werden viele Teilnehmende meist in strukturierter Weise und regelmäßig in geschlossener Frageform untersucht sowie statistisch ausgewertet. Auch diese Methode kam in der vorliegenden Arbeit zur Anwendung und ist Teil des Forschungsdesigns geworden. Die deduktive Vorgehensweise soll von einer bestehenden Theorie und den abgeleiteten Hypothesen die Daten zur Ergebnissicherung erheben, folglich ist die allgemeine Aussagekraft von Interesse. In quantitativen Studien kommen nach Möglichkeit standardisierte Methoden zur Erhebung von Daten zum Einsatz. Auch in quantitativen Studien kommen Gütekriterien wie Objektivität, Reliabilität und Validität zur Anwendung. Weitere und für diese Arbeit auch zu beachtende Nebenkriterien sind Wirtschaftlichkeit, Vergleichbarkeit oder Nützlichkeit (Ritschl et al., 2023, S. 151–153). Bei der Bildung von Hypothesen ist grundsätzlich und auch in der vorliegenden Arbeit zu unterscheiden, dass keine deterministischen Hypothesen gebildet wurden, also keine Gesetzmäßigkeiten überprüft wurden, sondern probabilistische Hypothesen eine Wahrscheinlichkeit repräsentieren sollten. Für quantitative Verfahren kommen verschiedene Befragungsmethoden in Frage, insbesondere können auch wie in qualitativen Studien Interviewformen von wenig bis stark standardisierter Ausprägung und für Einzelpersonen oder Gruppen genutzt werden. Neben den mündlichen Interviewformen bieten sich jedoch bei quantitativen Studien vorrangig Fragebögen, bestenfalls in elektronischer Form als Survey, an. Fragebögen mit offenen oder hybriden Fragestellungen sind möglich, jedoch für die gewünschte große Anzahl von Teilnehmenden eher unrentabel hinsichtlich des Aufwandes. Geschlossene Fragestellungen, z. B. mit mehreren Antwortmöglichkeiten, ermöglichen eine bessere Auswertung hinsichtlich der Objektivität und sind für den Befragten und den Forscher gleichfalls ressourcenschonend (Raithel, 2006, S. 64–69). Für die in dieser Arbeit angewandte quantitative Studie wurde ein Multiple-Choice-Question-Set mit Ratingskala in einem Online-Survey verwendet. Für die Auswertung von erfassten Daten kommen computergestützte Verfahren wie z. B. SPSS oder Stata in Frage. Neben der Ermittlung von Mittelwerten beinhalten insbesondere Anwendungen wie SPSS-Verfahren und Methoden zur Berechnung von Regression und lassen Aussagen zu Signifikanz zu, das heißt, ob ein ermittelter Zusammenhang in den Daten zufällig ist. Die Signifikanz gibt dabei, ob das Ergebnis auf die Grundgesamtheit übertragen werden kann (Tausendpfund, 2022, S. 119–120).

Die Kombination der aufgezeigten Methoden (Mixed-Method) wurde in dieser Arbeit grundsätzlich angewendet. Die qualitative Forschung hat sich hierbei für die Analyse der Akteurs-Perspektive als geeignet gezeigt und die quantitative Forschung für strukturell getrennte Akteure als zielführend präsentiert. Gleichwohl wurden die Methoden nicht sequenziell am selben Forschungsgegenstand durchgeführt, vielmehr wurde die qualitative Forschung zur Herleitung von Hypothesen und die quantitative zur Überprüfung eben dieser genutzt. Zudem kamen die angewendeten Methoden nur teilweise in den unterschiedlichen Phasen des Forschungsprozesses (z. B. in der Phase der Problemerkennung) zum Einsatz. Eine Überprüfung der qualitativ gewonnenen Daten durch quantitative Methoden und umgekehrt ist gleichwohl gegeben (Flick, 2011, S. 79–84).

1.2.3 Forschungsparadigma Design Science Research

Design Science Research beinhaltet zusammengefasst, dass mit wissenschaftlichen Methoden Forschungsprobleme der realen Welt technologiegeleitet möglichen und zu überprüfenden Lösungen zugeführt werden, die geeignet sind, gestalterisch den Erkenntnisgewinn zu generieren. Solche Ergebnisse werden in der Designwissenschaft Artefakte genannt und sollen identifizierte Probleme im Forschungsumfeld mit formalem wissenschaftlichem Vorgehen adressieren sowie die Lösung iterativ entwickeln, evaluieren und optimieren.

Hevner postuliert, dass DSR einen Ordnungsrahmen für die Informationssystem-Forschung bietet. Dabei sind die Ausrichtung von Geschäftsstrategie und IT-Strategie sowie von Organisationsstruktur und IS-Infrastruktur erforderlich, um Design-Aktivitäten zwischen diesen Bereichen zu ermöglichen sowie an den technologischen Weiterentwicklungen zum Vorteil von geschäftlichen Bereichen partizipieren zu können. Die prozessuale Gestaltung als Tätigkeit und die Gestaltung des Artefakts als innovatives Produkt sind als *Design as Research* (Gestaltungswissenschaft) zu verstehen und ermöglichen ein besseres Verständnis der realen Probleme. Es werden verhaltenswissenschaftliche und designwissenschaftliche Paradigmen kombiniert. Die Kombination aus Verhaltenswissenschaft und Designwissenschaft ermöglicht zum einen die erklärende Forschung entlang der Bedürfnisse einer Organisation und zum anderen Forschungen entlang technischer Entwicklungen von Lösungen (Artefakten), d. h. Wahrheit und Nutzen. Bestehendes Wissen, wie z. B. Literatur, Frameworks und Theorien, bilden die Grundlage des Forschungsbeginns und mit dem angemessenen Einsatz von z. B. empirischen Forschungsmethoden wird der Anspruch an die Wissenschaftlichkeit des Design Prozesses sichergestellt. Das entstehende Artefakt zur Lösung eines Problems ist in der Forschungsdomäne zu evaluieren, um z. B. die Effektivität und Effizienz sowie die Innovation zu belegen. Nach *Hevner* muss dieser Prozess entlang von sieben Leitlinien vollzogen werden, die unter anderem Zweckmäßigkeit, Neuartigkeit und Nützlichkeit in dem Forschungsumfeld sowie die Kommunikation in der Fachwelt sicherstellen. Um diesen Beweis antreten zu können, ist eine methodengeleitete Evaluation durchzuführen, z. B.

durch eine Feldstudie und Beobachtung der Verwendung des Artefakts im realen Kontext, in Experimenten in einer überprüfbaren Umgebung oder durch Simulation. Das heißt, eine methodische Evaluation soll von laborartiger bis realer Umgebung vom Forscher selbst bis hin zum Experten durchgeführt werden (A. R. Hevner et al., 2004, S. 4–25).

In „*A Three Cycle View of Design Science Research*“ beschreibt *Hevner* weiter, dass es für die Akzeptanz des designwissenschaftlichen Forschungsparadigmas und der Anerkennung in der Forschungsgemeinschaft konsistenter Definitionen und Qualitätskriterien braucht. In Anlehnung an den von *Hevner* vorgeschlagenen DRS-Forschungsrahmen sollen zur Erreichung dieser Ziele drei Forschungszyklen (siehe Abbildung 3 DSR Cycles (A. Hevner & Chatterjee, 2010, S. 16)) in einem designwissenschaftlichen Projekt durchlaufen werden (A. R. Hevner, 2007, S. 2–5).

- Im *Relevance Cycle* steht die Innovation im Fokus und folglich die Verbesserung einer spezifischen Anwendungsdomäne, die durch Organisation, deren Menschen und verwendete Informationssysteme geprägt ist. Dieser Prozess stellt den identifizierten Problemausfriss in den Kontext der Lösung (Artefakt) und prüft deren Wirksamkeit zyklisch iterativen Schritten.
- Der *Design Cycle* befasst sich mit der Entwicklung und Verbesserung von Design-Entwürfen, deren Bewertung und den Änderungen eines finalen Entwurfs. Dieser Prozess wird im Forschungsprojekt durchlaufen, um sicherzustellen, dass das entwickelte Artefakt fortentwickelt und verbessert wird sowie innovativ ist.
- Der Rigor Cycle umfasst die Bildung oder Erweiterung bestehender Theorien unter Nutzung der Wissensbasis und technischer Methoden sowie Erfahrungen in der Anwendungsdomäne.

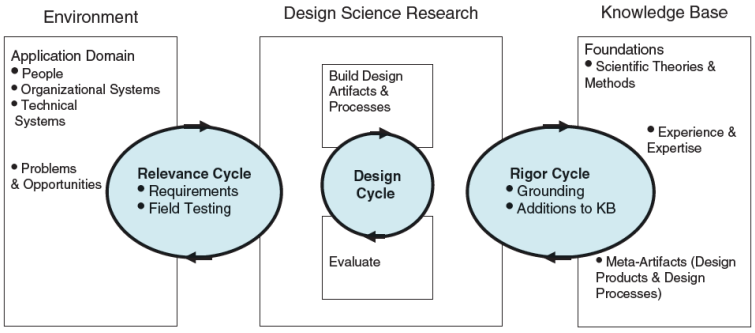

Abbildung 3 DSR Cycles (A. Hevner & Chatterjee, 2010, S. 16)

Um das DSR-Paradigma für die Forschenden zu operationalisieren, sind methodische Ansätze entwickelt worden. Eine Methode und die Notwendigkeit hierfür wurde z. B. von *Sein* mit der Arbeit *„Action Design Research“* (ADR) postuliert: In ihrer Arbeit zielen die

Forschenden darauf ab, die reale Implementierung der Artefakte und fortwährenden Interventionsmöglichkeiten der Forschungsdomäne in den Fokus des iterativen Forschungsprozesses zu legen (Sein et al., 2011, S. 38–40).

Mit der „*Design Science Research Methodology*“ (DSRM) nach *Peffers* wurde der Ansatz *Hevners* dahingehend konkretisiert, dass eine designwissenschaftliche Forschungsmethodik vorgeschlagen wird, die Prinzipien, Praktiken und Verfahren für die Umsetzung eines DSR Forschungsprojektes bereithält. Im Unterschied zu *Sein* stellt *Peffers* die Allgemeingültigkeit der entwickelten Artefakte in den Fokus und evaluiert diese in realem und laborartigem Umfeld. Das Prozessmodell umfasst die folgenden sechs Schritte (siehe Abbildung 4 DSRM Prozess Modell ((Peffers et al., 2007, S. 54)):

- *Problemerkennung und Motivation*: Der Problemaufriss ist zu beschreiben und Anforderungen zu erheben. Das Erkennen der Möglichkeit zur konzeptionellen Verbesserung, durch eine innovative Lösung, soll den Forschenden motivieren und die Forschungsgemeinschaft überzeugen. Übergeordnete Ziele tragen dazu bei, den Stellenwert und die Wichtigkeit dieser Forschung darzustellen.
- *Zieldefinition:* Basierend auf der Problemdefinition und dem aktuellen Wissensstand werden quantitative oder qualitativ Ziele definiert, um darzustellen, wie das neue Artefakt dazu beiträgt die aktuelle Situation zu verbessern.
- *Entwurf und Entwicklung*. In diesem Zyklus werden Architekturen, Methoden oder Modelle erstellt, die technischer oder informationeller Art sein können. In der Designforschung bestimmt die Funktionalität der Architektur den Forschungsbeitrag und wird zum Artefakt.
- *Demonstration:* Mit Experimenten, Simulationen oder empirischen Fallstudien wird die Wirksamkeit des Artefakts demonstriert.
- *Evaluation*: Die systematische empirische Auswertung der Sachverhalte zwischen *Zieldefinition* und *Demonstration* ermöglicht die Qualitätssicherung hinsichtlich der angestrebten Lösung. Eine erneute Aktivität im Designprozess kann als iterativer Verbesserungsprozess verstanden werden.
- *Kommunikation*. In der spezifischen Forschungsgemeinschaft muss das Artefakt diesem Fachpublikum sowie betroffenen Organisationen vorgestellt werden, um sicherzustellen, dass sowohl das Problem relevant ist als auch die Lösung einen Mehrwert liefert. Zudem ist nachzuweisen, dass die Anforderungen an das wissenschaftliche Arbeiten erfüllt wurden.

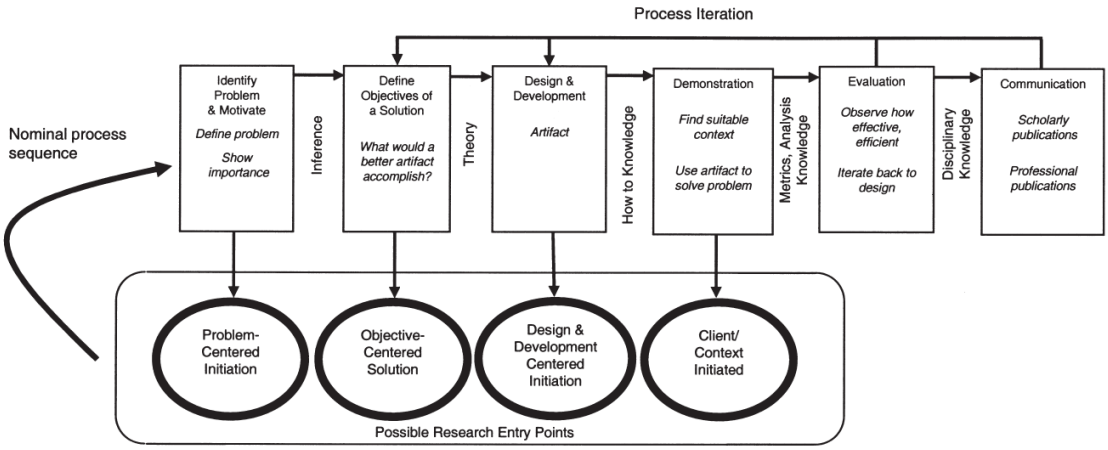

Abbildung 4 DSRM Prozess Modell ((Peffers et al., 2007, S. 54)

Grundsätzlich sind die Schritte nicht in chronologischer Reihenfolge zu durchlaufen. Je nach dem, mit welcher Intension (problemzentriert, zielorientiert, designorientiert oder kontextorientiert) man das Forschungsvorhaben startet, kann auch der Einstiegspunkt zum DSRM variieren. Zudem kann der Kommunikationsprozess als kontinuierlicher nicht explizit auszuführender Tätigkeitsbereich gestaltet sein (Peffers et al., 2007, S. 52–56).

1.2.4 Forschungsumfeld Öffentliche Verwaltung

Die in dieser Arbeit durchgeführte Forschung fand in der Domäne Öffentliche Verwaltung statt, i. e. einer föderalen Ministerialverwaltung. Bund und Länder verantworten insbesondere Aufgaben und Herausforderungen der *unmittelbaren* Staatsverwaltung. Der Staat hat als wesentliche Aufgabe die Existenzsicherung seiner Bürger wie auch des Staates selbst zu gewährleisten. Diese Aufgabe ist im Grundgesetz (GG) verankert und wird über die drei Gewalten ausgeübt (GG - Grundgesetz für die Bundesrepublik Deutschland, 1949, Article 20): die Legislative als gesetzgebende Gewalt, die Exekutive als ausführende Gewalt und die Judikative als rechtsprechende Gewalt. Die Gewalten des staatlichen Handelns haben den Auftrag, Verfassungswerte wie z. B. *Freiheit* zu schützen und Ziele der Verfassung zu fördern. Dabei stehen die Grundrechte all denjenigen Menschen zu, die dem Staat und dem staatlichen Handeln unterworfen sind (Klein, 1989, S. 1633–1640). Jeder dieser Gewalten kommen für den Schutz der Verfassungsrechte und der Umsetzung dieser Aufgabe besondere Kompetenzen zu, wobei die konkreten Gefährdungen nur zum einen relevant sind. Zum anderen muss dieser Schutz auch im Vorfeld einer möglichen unspezifischen/abstrakten Bedrohung (z. B. Cybersicherheitsbedrohungen) mit denkbarem Schadpotenzial wirksam begegnen. Hierfür muss der Staat, insbesondere auch unter föderalen Gesichtspunkten, als Gesetzgeber durch Normen regulierend einwirken.

Der allgemeinen öffentlichen Verwaltung, als Exekutive bzw. vollziehende Gewalt, kommt hingegen Entscheidungsgewalt nur in Einzelfällen zu. Grundsätzlich wird die

Exekutive nur dann tätig, wenn eine entsprechende gesetzliche Grundlage für ein Eingreifen vorhanden ist. Solche parlamentarischen Gesetzgebungen können durch Rechtsverordnungen ergänzt werden (Fleiner, 1920, S. 6, 78ff), (GG - Grundgesetz für die Bundesrepublik Deutschland, 1949, Article 80). Einher mit diesem Recht geht das staatliche Gewaltmonopol; nur der Staat darf Zwangsmittel einsetzen und ermöglicht hiermit die öffentliche Sicherheit (H.-J. Becker, 1995, S. 2077).

Neben den Organisationseinheiten des Staates, denen solche Befugnisse verfassungsrechtlich zukommen, können auch Kommunen autonom Recht setzen (GG - Grundgesetz für die Bundesrepublik Deutschland, 1949, Article 2). Entlang des Verwaltungsverfahrensgesetz (VwVfG) des Bundes existieren legitime Besonderheiten hinsichtlich gesetzlicher Ermächtigungen für die Verwaltung. Für die Ausführung von Bundesrecht dürfen zweckgebundene Ermessensentscheidungen in Einzelfällen durch selbstständige Einheiten getroffen werden (VwVfG - Verwaltungsverfahrensgesetz, 1977, Article 40). Ergänzt werden die Verwaltungsverfahrensgesetze durch spezielles Recht, wie z. B. die Sozialgesetzbücher (SGB). Beispielsweise wird im § 75c SGB V seit 2022 die *IT-Sicherheit in Krankenhäusern* rechtlich bindend geregelt (SGB 5 - Sozialgesetzbuch, 1988, Article 75).

Das Grundgesetz sieht vor, dass die staatlichen Befugnisse neben der klassischen Dreiteilung weiter differenziert werden, nämlich in Kompetenz-Zuständigkeiten für den Bund und die Länder. Obwohl der Bund im GG angeführt ist, sind die Grundkompetenzen regelmäßig bei den Ländern verortet (GG - Grundgesetz für die Bundesrepublik Deutschland, 1949, Article 30). Die Bundesverwaltung ist nach der Verfassung begrenzt durchsetzungsfähig, die Länder sind in der Regel die Ausführenden von Bundesgesetzen. Die Gemeinden nehmen ebenfalls Verwaltungsaufgaben, als ausführende Organisationseinheiten der Länder, wahr. Da diese gegenüber der Bund-Länder-Verwaltung „ausgegliedert“ sind, gelten sie als *mittelbare* Staatsverwaltung, eine Aufgabenüberwachung findet gleichwohl statt, z. B. in Form einer Kommunalaufsicht in den Ländern (Koch et al., 2023, S. 35).

Grundsätzlich ist festzustellen, dass die rechtliche Gestaltung der mittelbaren und unmittelbaren öffentlichen Verwaltung in Deutschland auf eigene Kompetenzen und autarke Aufgabenwahrnehmung ausgelegt ist, im Sinne einer starken föderalen Struktur. Die Länder haben jedoch mithin die herausgehobene Rolle des Ausführenden – im Sinne des Bundesrechts – und in der Umsetzung des Landesrechts sowie als Integrator der auf Selbstverwaltung ausgelegten kommunalen Strukturen. Einheitliche, und vor allem rechtlich durchgängige vollzugsfähige Regelungen bestehen insbesondere bei der tradierten Aufgabenwahrnehmung des Staates, jedoch nicht im Bereich der Cyber- und Informationssicherheit von Bund, Länder und Gemeinden (siehe hierzu: Publikationen ab Kapitel 2).

Trotz des ausgeprägten Föderalismus als Paradigma ist Deutschland dennoch nicht in einem gänzlich selbstverwalteten Umfeld, insbesondere nicht bei der Stärkung der Abwehrfähigkeit im Kontext der Cybersicherheit. Dort, wo die europäische Union ihre Regelungskompetenz nutzt, um verbindliche Rechtsakte für die Mitgliedsstaaten zu schaffen, wird dieses Paradigma zuweilen durchbrochen.

- Mit *Verordnungen* (Regulations) existieren europäische Rechtsakte mit allgemeiner Geltung, das heißt, sie sind in den Mitgliedstaaten verbindlich und gelten unmittelbar, unabhängig von etwaigen Föderalstaaten (z. B. die Datenschutz-Grundverordnung). Diese rechtlich bindende Entfaltung kann jedoch mit nationalen und föderalen Gesetzen weiter gestaltet werden, was in Bezug auf das Beispiel in Deutschland auch so geschehen ist, insbesondere um die Sanktionsmöglichkeiten für Datenschutzverstöße in den Ländern zu regulieren bzw. auch einzuschränken.
- Mit *Richtlinien* (Directives) werden regelmäßig Ziele der EU in einem europäischen Rechtsakt definiert, wo die Mitgliedsstaaten gefordert sind, diese in eigene Rechtsvorschriften zu angemessen umzusetzen (z. B. die EU-Richtlinien zur Netzwerk- und Informationssicherheit (NIS)). Die erste NIS-Richtlinie hatte die öffentliche Verwaltung nicht im Anwendungskreis und wurde folglich nur als Bundesgesetz für bestimmte sektorale Akteure umgesetzt. Die zweite NIS-Richtlinie adressiert hingegen weitere Akteure, welche auch in erweiterte Sektoren eingeteilt wurden, mithin auch die öffentliche Verwaltung. Folglich ist deutsche Gewaltenteilung, das Föderalsystem, umfänglich an der Umsetzung der Richtlinie in Bund und Ländern gefordert.
- Mit Beschlüssen (Decisions) werden bestimmte Mitgliedstaaten oder Unternehmen adressiert. Solche nichtlegislativen Beschlüsse wurden beispielsweise auch gegen marktbeherrschende Unternehmen gerichtet, die wiederum mit Geldbußen einhergehen können, wohingegen Beschlüsse an dedizierte Mitgliedstaaten unmittelbare, jedoch nicht sanktionsfähige Wirkung haben.

Mit dem Instrument des Vertragsverletzungsverfahrens kann die EU die Ziele und das objektive EU-Recht durchsetzen. Es kann folglich auf die vertragskonforme Herstellung eines einheitlichen Zustandes bestehen, ggf. auch unter Beachtung des Individualrechtsschutzes die Vorgaben weiterentwickeln. Sanktionen wie Zwangsgelder nach einem Klageverfahren am Gerichtshof der Europäischen Union (EuGH) sind für fehlende oder mangelhafte Umsetzung der EU-Vorgaben möglich (Borchardt, 2020, S. 258–316). Bei der Umsetzung der zweiten NIS-Richtlinie wird dieses Vertragsverletzungsverfahren zwischenzeitlich zwischen Bund und Länder offen diskutiert, insbesondere, weil die Länder in der Sache gefordert sind, eine einheitliche und angemessene Lösung zu schaffen, und die Mitgliedsstaaten – hier Deutschland – Ziel der europäischen Sanktionen sein könnten.

Mit dem Europarat (Council of Europe (CoE)) und seinen 46 Mitgliedsstaaten existiert noch eine weitere, über die EU hinausgehende Ebene der möglichen organisatorischen Einflussnahme auf die Belange der hier thematisierten Cybersicherheitsforschung in Deutschland. Es bleibt jedoch gleichwohl festzuhalten, dass beim Europarat im Vergleich zur EU keine gesetzlichen Durchsetzungsmöglichkeiten in den Mitgliedstaaten existieren und der Erfolg eines Abkommens von dem Wohlwollen der Unterzeichner und deren Willen zur gesetzlichen Ratifizierung in den jeweiligen Ländern abhängt. Beispielsweise wurde mit der Budapester-Konvention aus dem Jahr 2001 (Convention on Cybercrime) das erste internationale und völkerrechtliche Übereinkommen zur Bekämpfung von Cyberkriminalität bzw. Computerkriminalität vom Europarat initiiert, welches zwischenzeitlich von deutlich mehr als den Mitgliedsstaaten unterschrieben und ratifiziert wurde. Mit den Zusatzprototollen aus den Jahren 2003 und 2022 wurden weitere inhaltliche Ziele zur Kriminalitätsbekämpfung von Rassismus in Computernetzen und der Datenaustausch zwischen staatlichen und privatwirtschaftlichen (Providern) Akteuren geschärft. Auch die EU hat zwischenzeitlich reagiert und mit einem Beschluss die Mitgliedsstaaten zur Ratifizierung des zweiten Zusatzprotokolls, d. h. zur Intensivierung der Zusammenarbeit bei Computerkriminalität aufgefordert (*Beschluss (EU) 2023/436 des Rates vom 14. Februar 2023 zur Ermächtigung der Mitgliedstaaten, im Interesse der Europäischen Union das Zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität über eine verstärkte Zusammenarbeit und die Weitergabe elektronischen Beweismaterials zu ratifizieren*, 2023).

Das Forschungsumfeld der öffentlichen Verwaltung Deutschlands ist zuvorderst geprägt von rechtlichen Rahmenbedingungen. Dabei sind zwei Begriffe von besonderer Relevanz für Bund, Länder und Gemeinden: das Opportunitäts- und Legalitätsprinzip. Dort, wo die Verwaltung aus Opportunitätserwägungen auf das Eingreifen oder Handeln verzichten kann, ist dies unter Legalitätsaspekten z. B. einer Strafverfolgungsbehörde nicht möglich (Wehr, 2005, S. 345–348). Dies gilt im übertragenen Sinn auch für die Cybersicherheit. Die Studien dieser Arbeit haben gezeigt, dass insbesondere die kommunalen Bereiche, aber auch die Unternehmen der kritischen Infrastruktur im Allgemeinen ohne rechtlich abgesicherte Verpflichtungen – und im Speziellen ohne Ressourcensteuerung durch die Länder an die Gemeinden – nur intrinsisch motiviert sind. Es bleibt derzeit im Benehmen der jeweiligen Organisation, sich dem Thema Cybersicherheit zu stellen. Tatsächlich ist daher zu begrüßen, dass die EU zwischenzeitlich regulierend auf die Mitgliedsstaaten und in Deutschland auch auf die Länder einwirkt. Folglich bleibt es daher die Aufgabe der Länder, in Ermangelung von Regelungen für die Gemeinden, diese Strukturen und ggf. kleinere Unternehmen – außerhalb des regulatorischen Adressatenkreis der EU – dergestalt in eine funktionale, technische und rechtssichere Lage zu bringen, die eine nachhaltige Stärkung der Resilienz gegen Cybersicherheitsbedrohungen ermöglicht.

1.2.5 Forschungsvorgehen

Ziel dieser Arbeit ist es, eine innovative Lösung zu schaffen, die wissenschaftlich fundiert eine Cybersicherheitsarchitektur für die Föderalstaaten Deutschlands entwickelt und ein aktuelles Problem der Länder adressiert. In der folgenden Abbildung 5 Forschungsvorgehen (eigene Darstellung) wird der Gesamtprozess visualisiert.

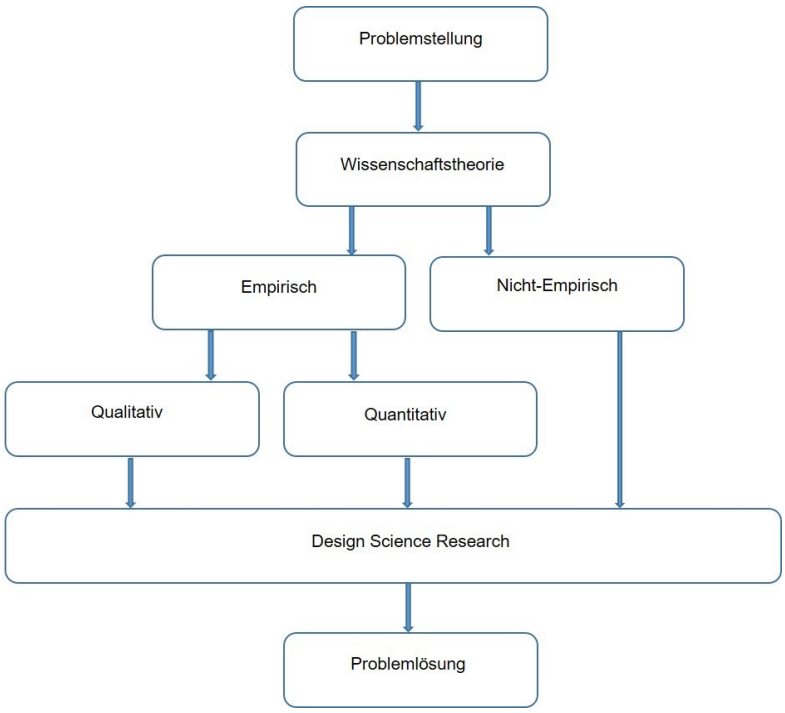

Abbildung 5 Forschungsvorgehen (eigene Darstellung)

Beginnend mit dem Problemaufriss des ministeriellen Arbeitsumfeldes eines CISO, wird aus Erfahrungswissen und der inhärenten Kenntnis der individuellen Ausgestaltung von Cyber- und Informationssicherheit in den Ländern eine Problemstellung formuliert. Im Folgenden wird eruiert, ob mit wissenschaftlichen Methoden eine Lösung des Problems grundsätzlich möglich ist, und eine prinzipielle Vorgehensweise in der Forschung fixiert. Diese umfasst in dieser Arbeit und in Anerkennung der Kapitel Einleitung und Forschungskontext nicht-empirische und empirische Studien zur Annäherung an eine mögliche Lösung. Der DSR-Prozess bietet eine anerkannte wissenschaftliche Methode zur Strukturierung des Vorhabens. Zur Problemidentifikation wurden qualitative und quantitative empirische Studien durchgeführt, die strategische, operative, technische, rechtliche und organisatorische Untersuchungen bei den Stakeholdern zum Ziel hatten. Um die Zieldefinition weiter zu verfeinern, wurden nicht-empirische Studien – insbesondere rechtswissenschaftlichen Charakters – durchgeführt. Die Lösungsentwicklung, Demonstration und Evaluation ist im DSR als Verbesserungsprozess angelegt und trug dazu bei, die vorgeschlagene Lösung entlang der Evaluationsepisoden weiter zu verbessern. Der finale Schritt stellt im DSR-Forschungsprozess die Kommunikation dar,

welcher in dieser Arbeit über Veröffentlichungen in einschlägigen Zeitschriften und Teilnahme an Konferenzen und Konferenzbeiträgen während der Forschung fortlaufend realisiert wurde (siehe hierzu Forschungsbeiträge im DSR) und final in diese Arbeit mündet. Die vorgestellte Problemlösung, eine föderale Cybersicherheitsarchitektur, stellt den Abschluss dieser Forschungsarbeit dar und kann in den Ländern implementiert und weiterentwickelt werden.

1.3 Forschungsbeiträge im DSR

Der in Abbildung 6 DSR-Prozess in Anlehnung an Peffers (eigene Darstellung) visualisierten Forschungsprozess soll grundsätzlich verdeutlichen, welche Tätigkeiten und Erwartungshaltungen an die einzelnen methodischen Schritte des DSR geknüpft sind und erforderlich waren, um einen Erkenntnisgewinn in Form von Veröffentlichungen zu generieren.

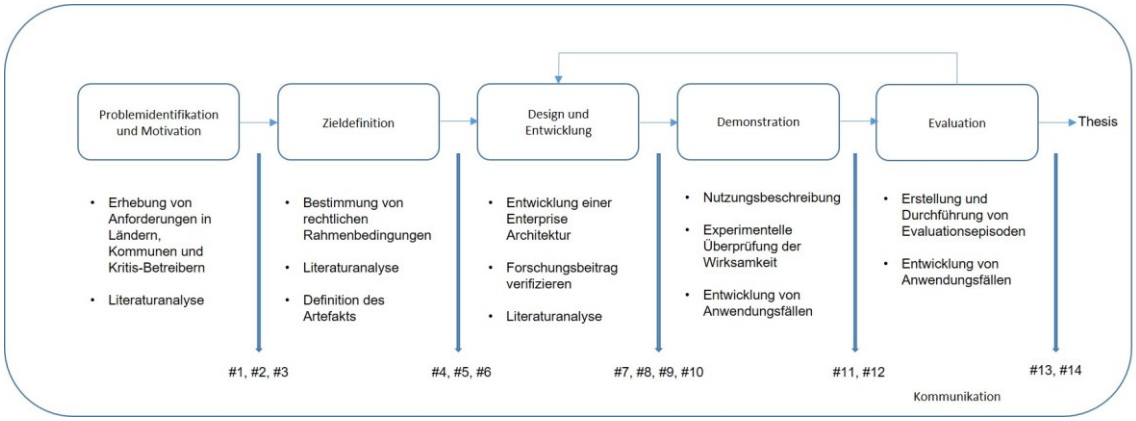

Abbildung 6 DSR-Prozess in Anlehnung an Peffers (eigene Darstellung)

Folgende Beiträge sind Teil des gesamten DSR-Forschungsprozesses und sind in dieser Arbeit berücksichtigte Veröffentlichungen, sofern sie mit Kapitel-Verlinkung versehen sind.

Nr.	Forschungsbeiträge	Kapitel
#1	Rehbohm, Thomas; Sandkuhl, Kurt; Kemmerich, Thomas, (2019); On Challenges of Cyber and Information Security Management in Federal Structures - The Example of German Public Administration, BIR 2019. (Rehbohm et al., 2019)	2
#2	Thomas Rehbohm, Kurt Sandkuhl, Clemens H. Cap, Thomas Kemmerich (2021), Integrated Security Management of Public and Private Sector for Critical Infrastructures – Problem Investigation, Business Information Systems Workshops. BIS 2021. Lecture Notes in Business Information Processing, vol 444. Springer. (Rehbohm et al., 2021)	3
#3	Thomas Rehbohm, Robin Kemmerich, Clemens H. Cap, Kurt Sandkuhl (2022), Sicherheitsmanagement, Cybersicherheit und Daseinsvorsorge: Empirische Studie in deutschen Kommunen, Datenschutz und Datensicherheit – DuD Ausgabe 7/2022, Springer. (Rehbohm et al., 2022)	4
#4	Rehbohm, Thomas; Kalmbach, Peter (2021), Grundforderungen von Informations- und Cybersicherheit in Ländern; MMR-Aktuell 2021(Multimedia und Recht), 438461, Verlag C. H. Beck. (Rehbohm & Kalmbach, 2021)	5

#5	Malek Barudi u. a. (2023) Cybersecurity. 2. Auflage. hrsg. Dennis-Kenji Kipker, Kapitel 15.3. Thomas Rehbohm, Peter Lutz Kalmbach, IT-Sicherheitsrecht der (Bundes) Länder, München: C.H. Beck. (Barudi et al., 2023)	6
#6	Thomas Rehbohm, Peter Lutz Kalmbach (2023), Herausforderungen der föderalen Cybersicherheit vs. Änderung in der Bund-Länder Gewaltenteilung – DuD Ausgabe 6/2023, Springer. (Rehbohm & Kalmbach, 2023)	7
#7	Frank Moses, Thomas Rehbohm (2022), CISIS12 – Vorgehensmodell zur Einführung eines Informationssicherheitsmanagementsystems, kes Ausgabe 1/2022, DATAKONTEXT GmbH. (Moses & Rehbohm, 2022)	-
#8	Thomas Rehbohm, Frank Moses (2023), Föderale Cybersicherheitsarchitektur und Informationssicherheitsmanagement im Kontext der NIS-2-Richtlinie, Datenschutz und Datensicherheit – DuD Ausgabe 10/2023, Springer. (Rehbohm & Moses, 2023b)	-
#9	Frank Moses, Thomas Rehbohm (2023), CISIS12-Modell – In zwölf einfachen Schritten zum ISMS, IT-Sicherheit - Management und Technik, August/September Ausgabe 4/2023, DATAKONTEXT GmbH. (Moses & Rehbohm, 2023a)	-
#10	Thomas Rehbohm, Frank Moses (2023), Federal Cybersecurity Architecture and Information Security Management, GI Edition Proceedings, Gesellschaft für Informatik e. V. (GI), Band 341 6. Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023). (Rehbohm & Moses, 2023a)	8
#11	Frank Moses, Thomas Rehbohm (2023), Entwicklung eines modularen ISMS und DSMS, Datenschutz und Datensicherheit – DuD Ausgabe 11/2023, Springer. (Moses & Rehbohm, 2023b)	9
#12	Thomas Rehbohm, Kurt Sandkuhl (2023), Referenzarchitektur Cybersicherheit im Föderalsystem Deutschlands, HMD Praxis der Wirtschaftsinformatik, Springer. (Rehbohm & Sandkuhl, 2023)	10
#13	Thomas Rehbohm, Kurt Sandkuhl (2024), Cybersicherheitsevaluation einer Referenzarchitektur für Land, Kommune und systemrelevante Infrastruktur, GI Sicherheit 2024, Fachtagung des Fachbereichs "Sicherheit - Schutz und Zuverlässigkeit" der Gesellschaft für Informatik e.V. (Rehbohm & Sandkuhl, 2024)	11
#14	Thomas Rehbohm, Kurt Sandkuhl (2025), Evaluation einer föderalen Referenzarchitektur für Cybersicherheit, Gesellschaft für Informatik e. V. (GI), Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023), in "Praxishandbuch Verwaltungsinformatik". (Pidun & Auth, 2025)	12

Tabelle 1 Forschungsbeiträge im DSR-Prozess

1.3.1 Problemerkennung und Motivation

Mit den Beiträgen aus den Kapiteln 2, 3, 4 wurden zuvorderst die drei Perspektiven, der in einer föderalen Cybersicherheitsarchitektur zu involvierenden Akteure erhoben und zugleich die Notwendigkeit einer Forschungstätigkeit in diesem Kontext nachvollzogen. Weitere und sinnstiftende Handelnde außerhalb des regionalen Bezuges (z. B. Branchenverbände oder der Deutsche Landkreistag (DLT)) werden über das Land koordiniert und berücksichtigt.

Die nachfolgend zusammengefassten Ausführungen und die zugehörige Aufzählung (#1 bis #14) stellen alle Forschungsbeiträge des Forschungsprojektes chronologisch dar und sind, wie in Tabelle 1 Forschungsbeiträge im DSR-Prozess angegeben, Teil dieser Gesamtveröffentlichung.

#1. Mit der Interviewstudie bei den CISOs der Bundesländer konnte die Bedeutung einer strukturiert-wissenschaftlichen Vorgehensweise in einem stark regulierten Umfeld bestätigt werden (**Landesperspektive**). Von einer politischen Perspektive gesehen, wird die Informationssicherheit in den Ministerien dezentral verantwortet, andererseits existieren ressortübergreifende Funktionen der inhaltlichen Steuerung im jeweiligen Land. Die Risikoabwälzung erfolgt regelmäßig auf wenige IT-Landesdienstleister, was auch die Mandate der CISOs beschnitten hat. Funktionsfähige Managementsysteme, welche die Wirksamkeit messen und verbessern helfen, sind nur vereinzelt funktionsfähig in den Ministerien implementiert. Die Zuständigkeit für Cybersicherheit ist weniger häufig bei den CISOs angegliedert, sofern sie nicht in den Innenministerien verortet sind. Zum Zeitpunkt der Studie waren die Kommunen aufgrund der verfassungsrechtlich abgesicherten Selbstverwaltung nicht in die Prozesse des Informationssicherheitsmanagements bzw. auch nicht im Cybersicherheitsmanagement der Länder eingebunden. Innovative Techniken halten gegenüber anderen Anforderungen (z. B. „digitaler Souveränität“) nur sehr langsam Einzug in die öffentliche Verwaltung, was auch für das Thema Angriffserkennung zur Behandlung von Bedrohungslagen nachweisbar war. Des Weiteren konnte der Bedarf an regulatorischen Maßnahmen nachgewiesen werden, da rechtliche Voraussetzungen erst den Einsatz von „Stand der Technik“ Informationstechnik zur Angriffserkennung gestatten.

#2. Eine weitere Perspektive konnte mit einer folgenden Interviewstudie bei Betreibern kritischer Infrastrukturen des Landes Bremen erhoben werden, um die Bedarfe und Defizite an einem einheitlichen und über die Grenzen des jeweiligen Unternehmens hinausgehendes Informationssicherheitsmanagement zu bewerten (**Unternehmensperspektive**). Eine wesentliche Erkenntnis der Befragung

war, dass die eigentliche Betroffenheit als kritische Infrastruktur auf einer reinen Selbsteinschätzung beruht und bei Nicht-Meldung keine Sanktionen zu befürchten seien. Das Identifizierungskonzept und die einhergehenden Schwellwerte zur Betroffenheit eines Unternehmens sind zwischenzeitlich durch europäische Richtlinien deutlich enger und nachprüfbarer gefasst, was grundsätzlich auch eine Identifizierung von Seiten der Verwaltung ermöglicht. Die Unternehmensphilosophie, dass die eigene Dienstleistung zur Daseinsvorsoge zählt, war unterdurchschnittlich entwickelt. Zudem wurde vereinzelt angesprochen, dass die föderale oder deutsche Verwaltung überhaupt einen Einfluss auf die Cybersicherheitsorganisation eines europaweit tätigen Unternehmens nehmen sollte. Vereinzelt bestanden zu verschiedenen Akteuren der öffentlichen Verwaltung (wie Strafverfolgungsbehörden, Aufsichtsbehörden oder weiteren Regulierungsbehörden) Kontakte, im Sinne eines kontextübergreifenden Austausches. Die IT-Ausstattung, deren Betrieb und das Management sind stark von den Unternehmensgrößen abhängig und sind grundsätzlich als tradiert zu bewerten. Dies gilt insbesondere auch für das Verständnis von Trennung der operativen und Office-IT. Der ohnehin schon hohe regulatorische Rahmen für deutsche Unternehmen wurde kritisiert, gleichwohl wurde gefordert, dass die Behörden Vorgaben erlassen - aber gleichzeitig auf Freiwilligkeit abstellen sollten. Kooperationsmöglichkeiten mit anderen Unternehmen der gleichen Branche bestehen grundsätzlich, jedoch waren die Befragten aufgrund von Ressourcenproblematiken höchst unterschiedlich mit diesen vernetzt. Das Verständnis und das Erfordernis für ein Kontinuitätsmanagement – im Sinne von Resilienz – war den Befragten unterentwickelt ausgeprägt.

#3. Die dritte Studie zur Erhebung der Problematik fand in einer bundesweiten Umfrage bei kommunalen Organisationen statt (**Kommunalperspektive**). Die Kernbotschaft aus der Umfrage war, Kommunen beurteilen grundsätzlich ihre eigene Dienstleistung nicht als kritische Infrastruktur, allenfalls sind sie indirekt an Kritis-Betreibern beteiligt und selten sind sie Betreiber einer solchen Unternehmung. Aber auch für die selbst- oder im Auftrag betriebene IT-Infrastruktur wird nur ein Mindestmaß an Vorsorge getroffen. Es fehlte grundsätzlich an einem innerhalb der Organisation erwartungskonform zu etablierenden ISMS, Ressourcen und dem Bewusstsein, für die Kritikalität von IKT, selbst wenn die Kommunalverwaltungen größer (100 Beschäftigte) waren. Sofern die Länder ihren Kommunen Vorgaben gemacht haben, sind diese nicht verpflichtend einzuhalten, werden grundsätzlich nicht überwacht und sind insofern auch sanktionslos. Vorgaben, die in manchen Ländern über Anschlussbedingungen an das jeweilige Landesnetz erzwungen werden sollen, steht die Verfassungsgarantie der kommunalen Selbstverwaltung im Wege. Auch hat die Umfrage in den Kommunen ergeben, dass eine Verantwortung für die IKT und die verbundenen Dienstleistungen auch nicht beim jeweiligen Land liegen würden, allenfalls Kooperationsmöglichkeiten.

Die gewonnenen Erkenntnisse aus den drei Perspektiven werden in die Ziele und Anforderungen des nächsten DSR-Prozesses überführt und dienen folglich als deklaratorischer Teil. Zusammenfassend kann in diesem Schritt festgestellt werden, die Aspekte der befragten Akteure weisen darauf hin, dass anforderungsgerechte, auf die Domäne angepasste ISMS nicht etabliert sind. Der politischen Leitungsebene bzw. den Geschäftsführenden ist das Thema Daseinsvorsorge und kritische Infrastrukturen bekannt und sie sieht auch Verantwortung in der eigenen Rolle, gleichzeitig sind jedoch nur rudimentär delegierende Maßnahmen der Verantwortungszuweisung in der eigenen Organisation gesteuert worden. Für alle Akteure gilt, dass ohne Vorgaben eine opportunistische Haltung anzunehmen ist.

1.3.2 Zieldefinition und Anforderungen

Die Anforderungen an eine ebenenübergreifende Cybersicherheitsarchitektur werden zuvorderst bestimmt durch die Erkenntnisse aus der Befragung der Akteure, ergänzt um die im Betrachtungszeitraum fortgeschriebene rechtliche Perspektive, hinsichtlich europäischer, deutscher und föderaler Bestimmungen. Hierfür wurden ergänzend folgende Studien Teil dieser Definition:

#4. Die Quintessenz der ersten rechtlichen Studie ist, dass der Staat steuernd eingreifen muss, wenn er Gefahren für die Bevölkerung erkennt. Unabhängig davon, ob der Staat, die Kommunen oder Unternehmen Dienstleistungen für große Teile der Bevölkerung anbieten, ist dies der Daseinsfürsorge zuzuordnen. Die Bevölkerung hat einen Anspruch auf das Funktionieren der Träger der Daseinsvorsorge. Die Zuweisung der gestalterischen Rolle ist dabei eindeutig, hinsichtlich der Zuständigkeit in den Ländern und in Teilen auch beim Bund. Der Staat muss nach seinem Ermessen ggf. auch gesetzgeberisch handeln, wenn es notwendig ist und dazu beiträgt, die öffentliche Verwaltung in einen handlungsfähigen Zustand zu versetzen. Dies kann präventive Maßnahmen umfassen und muss erfolgen, sofern sich eine Gefahr konkretisiert z. B. in einem gegenwärtigen Angriff. Die regionale Cybersicherheit ist bei der allgemeinen Gefahrenabwehr einzubeziehen und kann folglich in das Ordnungsrecht eingeordnet werden. Im Ordnungsrecht können die erforderlichen Ermächtigungen vorgehalten werden, um einen wirksamen Schutz der Bevölkerung zu etablieren, wie es beispielsweise auch im Katastrophenschutz, der Polizei oder der zivilen Alarmplanung etabliert ist.

#5. Der zweite rechtliche Beitrag befasste sich mit der Umsetzung der Anforderungen an Kodifizierungen in den Bundesländern, wobei insbesondere die Herausforderungen in der praktischen Anwendung, die Unterschiede in den landesspezifischen Regelungen sowie mögliche Harmonisierungsmöglichkeiten thematisiert wurden. Grundsätzlich konnte festgestellt werden, dass die Möglichkeiten der Länder – zielführend regulierend einzugreifen – nicht ausgeschöpft worden

sind. Dabei zielt die IT-Sicherheit bzw. Cybersicherheit generell auf die Sicherung der staatlichen Strukturen und mithin auf die Zivilgesellschaft ab. Die Sicherstellung der Funktionsfähigkeit des Staates bzw. seiner Institutionen ist grundsätzlich geregelt und Voraussetzung zur Gestaltung der regionalen Sicherheit. Insbesondere haben die Länder bei der Betrachtung der Cybersicherheitsrisiken zuvorderst ihre eigenen Landesnetze in Betracht gezogen und nicht die Daseinsvorsorgeträger, unabhängig davon, ob sie staatlich oder privatrechtlich organisiert sind. Neben den vom Bund etablierten quantitativen Bestimmungen von Daseinsvorsorgeträgern haben die Länder keine qualitativen Identifizierungsprozesse zur Bestimmung von ergänzenden Trägern der Daseinsvorsorge etabliert. Zudem haben die Länder bislang auch nicht die kommunalen Strukturen angemessen in den möglichen Regelungsrahmen einbezogen.

#6. Bezogen auf die Veröffentlichungen des Bundes, die Cybersicherheit in eigenen Strukturen für Gesamtdeutschland sicherstellen zu wollen, mithin Daseinsvorsorgeträger des gesamten Bundesgebietes zur Registrierung zu verpflichten, entstand ein dritter Beitrag zur Gewaltenteilung zwischen Bund und Länder. Dieser umfasste insbesondere das Spannungsfeld der Ausgestaltung des staatlichen Handelns. Es betrifft letztlich den Schutz von Verfassungswerten (Rechtsgütern) im Kontext einer verwaltungsrechtlichen Gefahrenabwehr, einer ureigenen Aufgabe der Länder. Einher geht der Wunsch oder das Angebot des Bundes, in den Ländern, d. h. in Landesnetzen Schadsoftware bzw. Angriffe detektieren zu wollen. Generell ist das BSI Teil der föderalen Cybersicherheitsarchitektur, Wissensträger und als Kooperationspartner unerlässlich für die Resilienz Deutschlands. Gleichwohl wird aber deutlich, dass mit den Angeboten und Möglichkeiten des BSI keine unmittelbare regionale Cybersicherheit gestärkt wird, sondern der Erkenntnisgewinn beim Bund entsteht. Mit der Registrierungspflicht von unternehmerisch tätigen Daseinsvorsorgeträgern sind diese Unternehmen in der Beweispflicht, dass sie dem Thema Cyber- und Informationssicherheit angemessen begegnen. Gleichzeitig wird aber deutlich, dass hiermit keine Rechte verbunden werden, insbesondere zum Informationsaustausch oder zur Hilfeleistung in Ausnahmesituationen. Dies ist Bestandteil der föderalen Architektur. Auch sind im Erfassungsbereich des Bundes die kommunalen Strukturen (verfassungsrechtlich) ausgeblendet, da sie grundsätzlich den Ländern zuzuordnen sind. Letztlich wirft das Angebot des Bundes, in Landesnetzen Angriffe zu detektieren, mehr rechtliche Fragen auf, als Lösungen damit einhergehen. Die technischen Systeme der Länder können mit Informationen des Bundes angereichert werden, um gleiche Leistungsfähigkeit aller Akteure zu gewährleisten. Die Ausführungen in diesem Beitrag machen deutlich, dass der Bund in Teilen hilfreich und wirkungsvoll ist, die Gefahrenabwehr jedoch vor Ort stattfinden muss.

Folgende ableitbaren Ziele und Anforderungen an das Artefakt sollen abgebildet werden. Die Architektur muss die regionalen Bezüge umfänglich berücksichtigen. Die Akteure der Region brauchen anwendbare Vorgehensweisen und Standards zu Etablierung von IT-Service, Risiko- und IT-Sicherheitsmanagementsystemen. Es müssen Fähigkeiten und Unterstützungen im Kontext der Threat Intelligence aufgebaut werden. Es muss Teilhabe generiert werden, um den Kenntnisstand bei den Mitwirkenden zu erhöhen und ein regionales Lagebild zu erzeugen. Die Involvierung von staatlichen und privatrechtlichen Organisationen muss ergänzend zum quantitativen Vorgehen des Bundes um qualitative Kriterien erweitert werden. Es muss ein Rechtsrahmen entstehen und fortgeschrieben werden, der alle Daseinsvorsorgeträger regional zur Mitwirkung und Compliance verpflichtet, eine Aufsicht und eine Steuerungsorganisation etabliert und konkrete Hilfe leisten kann.

1.3.3 Design und Entwicklung

Im folgenden Prozessschritt wurde die föderale Cybersicherheitsarchitektur mit Toolnutzung und als Enterprise Architektur entlang der Anforderungen und Ziele entwickelt sowie in mehreren Versionen kontinuierlich verbessert. Die veröffentlichten Beiträge dieses Abschnittes sollten dabei dokumentieren, wie die Anforderungen adressatengerecht erfüllt werden können.

#7. Mit der CSA sollen die Akteure in die Lage versetzt werden, erkannte Defizite des Informationssicherheitsmanagements zu kompensieren und diesen Vorgang gegenüber der Aufsichtsbehörde zu präsentieren. Diese geforderte Fähigkeit muss bei den Akteuren der Cybersicherheitsarchitektur interoperabel angelegt und in verschiedenen Organisationsgrößen praktikabel anwendbar sein. Hierfür wurde ein auf kleinere und mittlere Organisationen zugeschnittenes ISMS nach dem Vorgehensmodell CISIS12 – ohne dabei relevante Projekt-Vorerfahrungen vorzuhalten, um ein Sicherheitsmanagement zu etablieren und zu betreiben – im Zusammenwirken der CSA nachvollzogen. Insbesondere ist hier auch relevant, dass dieses Vorgehensmodell sowohl tradierte Standards der Informationssicherheit als auch „branchenspezifische Sicherheitsstandards“ (B3S) vereinigen kann. Vor dem Hintergrund der Involvierung verschiedenster Daseinsvorsorgeträger und deren B3S sowie der Notwendigkeit der Überwachung der Einhaltung der Konformität ist dies zielführend.

#8. In Anbetracht der Erneuerung der EU-Richtlinie zur Netzwerk- und Informationssicherheit sollte in diesem Beitrag verifiziert werden, ob das Vorgehensmodell zur Etablierung eines ISMS zu den Zielen der CSA passt und mit den Anforderungen der NIS-2-Richtlinie harmoniert. Mit der föderalen Architektur werden die Kernprozesse Compliance, Risikomanagement, Betrieb, Kontrolle und Verbesserung und Sicherheits-Standards definiert, welche die Ziele Rechtssicherheit, Anwendbarkeit, Resilienz, Nachhaltigkeit und Kooperation verfolgen. Die NIS-2-

Richtlinie fordert von den Mitgliedstaaten und in Föderalstaaten auch von den Ländern insgesamt 14 Maßnahmen ein. Das Vorgehensmodell CISIS12, zusammen mit CSA, erfüllt die Vorgaben, Maßnahmen und damit verbundenen Anforderungen dieser Richtlinie.

#9. Mit diesem Beitrag wurde die CSA dahingehend fortgeschrieben, dass die Fortentwicklung von weiteren Sicherheitsstandards, wie dem BSI-Kommunalprofil, Berücksichtigung findet und im Kontext einer anhaltenden Etablierung eines ISMS verifiziert werden kann. Insbesondere wurde in den Fokus gerückt, dass die Cybersicherheit von kritischen Infrastrukturen mit den verschiedenen Compliance Anforderungen an die kleinen und mittleren Unternehmen sowie der öffentlichen Verwaltung zusammenwirken. Am Beispiel des Vorgehensmodells CISIS12 konnte dies überprüft werden.

#10. Mit der Veröffentlichung bei einer der wichtigsten Tagungen im Bereich Cybersicherheit der Gesellschaft für Informatik sollte die die föderale Cybersicherheitsarchitektur eines EU-Mitgliedsstaates wie Deutschland vorgestellt werden. Insbesondere muss sich die CSA in den deutschen und europäischen Kontext einfügen. Das theoretische Modell des Zusammenwirkens wurde um die Vorgehensweisen zur Implementierung von Informationssicherheitsmanagementsystemen ergänzt. Im Ergebnis ist eine umfassende Cybersicherheitsarchitektur, die auch externe Anforderungen erfüllt, möglich. Durch die Verzahnung der CSA und des CISIS12 kann jeder Ansatz unabhängig vom anderen initialisiert werden. Informationen können über technische und organisatorische Schnittstellen ausgetauscht werden.

Grundsätzlich ist in dieser Phase des DSR-Prozesses die Entwicklung und Anpassung der Architektur, d. h. des Artefakts, vorgenommen worden, die von parallelen Literaturrecherchen begleitet wurde. Das Design und der Entwicklungsprozess enden jedoch nicht, vielmehr wird dieser Prozess – nach Auswertung der Ergebnisse aus Demonstration und Evaluation – erneut aufgegriffen, um veränderten Anforderungen angemessen Rechnung zu tragen. Vorschläge aus der Evaluation (z. B. Datenschutz), welche in der Demonstration ohne vorherige Evaluation thematisiert wurden, haben an dieser Stelle keinen Eingang in die Architektur gefunden.

1.3.4 Demonstration

Dieser Abschnitt soll zuvorderst die Gesamtarchitektur der wissenschaftlichen Gemeinde in einem Forschungsbeitrag prominent präsentieren. Der Prozess startet mit einem Vorschlag zur Modularisierung der Architektur und dem darunterliegenden Vorgehensmodell.

#11. Ziel dieses Beitrags war es zu verifizieren, ob die CSA derart modularisiert fortentwickelt werden kann, um Anforderungen weiterer Stakeholder zu bedienen. Da das Vorgehensmodell zur Implementierung von verschiedenen ISMS-Standards geeignet ist, sollte herausgestellt werden, dass auch verwandte Standards die CSA ergänzen können. Der hier exemplarisch und theoretisch angewendeten Standards ISO 27701 (Datenschutz) und die Datenschutz-Grundverordnung der EU besitzen hohe Übereinstimmungen und werden daher um Aspekte des deutschen Standard-Datenschutzmodells (SDM) ergänzt. Es wird somit eine Verknüpfung eines ISMS und eines Datenschutzmanagementsystems (DSMS) in der CSA vorgenommen. Es bedarf der Definition, welche Informationen der übergeordneten föderalen Cybersicherheitsarchitektur zur Verfügung stehen muss, um den Aufsichtspflichten innerhalb der CSA nachkommen zu können. Folglich kann das entstandene gemeinsame Managementsystem aus ISMS und DSMS um die übergeordneten Strategieelemente der CSA ergänzt werden.

#12. Dieser Beitrag stellt zum ersten Mal die Gesamtarchitektur zur Verzahnung der systemrelevanten Akteure der regionalen und föderalen Cybersicherheit vor. Gemeinsame Aktivitäten sowie technische Vernetzungen der betroffenen Organisationseinheiten des jeweiligen Landes, der Kommunen und der Unternehmen werden in inter-organisationalen Prozessen und einer Cybersicherheitsorganisation eingebunden. Die Darstellung der vorgeschlagenen Cybersicherheitsorganisation erfolgt in einem Unternehmensarchitekturmodell. Prozess-, Organisations-, Informations- und Technologieebene sind in der Architektur entwickelt. Der Anspruch an eine Referenzarchitektur für Bundesländer wird postuliert.

Das zu evaluierende Artefakt ist entstanden, die verfolgten Ziele sind benannt, die Architektur ist entwickelt und der Einsatz sowie die Funktionsfähigkeit grundsätzlich und laborartig verifiziert worden. Es wurde veranschaulicht, wie dieses Artefakt dazu beitragen kann, die Herausforderung einer resilienten Region zu begegnen.

1.3.5 Evaluation

Die Evaluation stellte in diesem Prozessschritt sicher, dass das entwickelte Artefakt effektiv, effizient und relevant für die gestellte Problematik ist und eine mögliche und innovative Lösung darstellt. Die Eignung und der Mehrwert des entwickelten Artefakts wurden bewertet. Die Evaluation fand in realen Umgebungen und nach Fertigstellung des Artefakts statt, um den Nutzen in der Praxis zu bewerten. Die Ergebnisse der Evaluation sollen darstellen, dass die Relevanz des wissenschaftlichen Beitrags gegeben ist. Auch haben die Evaluationen dazu beigetragen, den Entwicklungsprozess zu hinterfragen, auch um eine Fort- und Weiterentwicklung zu ermöglichen.

Für die Bewertung des Design-Artefakts wurde das “*Framework for Evaluation in DSR*” (FEDS) (Venable et al., 2016, S. 77–89) *verwendet*. Das Framework unterscheidet zwischen zwei orthogonalen Dimensionen der Evaluation. Erstens kann eine Evaluation im

Hinblick auf ihren funktionalen Zweck formativ oder summativ sein, d. h. auf das Verbesserungspotenzial von Vorversionen abzielen oder die Endversion eines Artefakts evaluieren. Zweitens identifiziert der Rahmen das zugrundeliegende Paradigma einer Evaluation als artifiziell oder naturalistisch, d. h. in einer Laborumgebung oder in der realen Welt. Nach *Venable* geht eine gründliche DSR-Evaluation von einem Zustand formativer und artifizieller Evaluationsmethoden zu einem vollständigeren und realistischeren Evaluations-Szenario über, das summative und naturalistische Methoden verwendet.

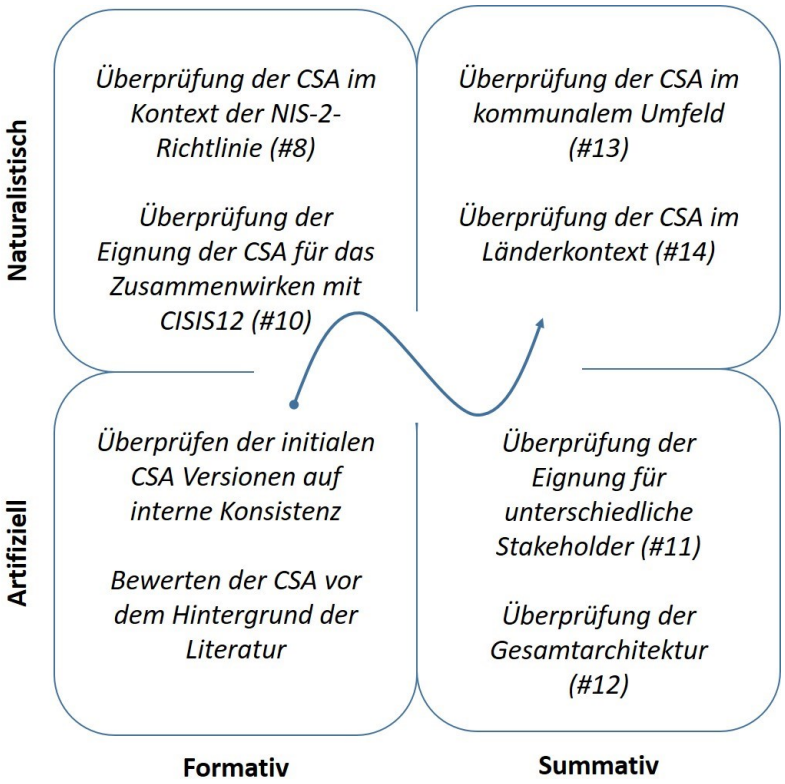

Abbildung 7 FEDS-Evaluationsepisoden

In unserem Fall wurde das Design-Artefakt bereits während der Entwicklung (s. 1.3.3) und der Demonstration (s. 1.3.4) einer formativen Evaluation in einem artifiziellen und naturalistischen Kontext unterzogen. *Venable* et al. schlagen die Durchführung von Evaluationsepisoden vor, die für diese Arbeit in Abbildung 7 FEDS-Evaluationsepisoden zusammengefasst sind. Hier sind auch die Episoden zur formativen Evaluation enthalten.

Das Ziel der Evaluationsphase war es, durch die Anwendung des Design-Artefakts in einer realen Umgebung (naturalistische Umgebung) die finale Version (summative Evaluation) zu bewerten. Das Hauptziel dieser Evaluationsepisoden war es, die Effektivität und Übertragbarkeit des Ansatzes zu evaluieren, d. h., dass er in einer realen Situation anwendbar ist und auf verschiedene Kontexte übertragbar ist. Diese Episoden sind in #13 und #14 enthalten.

#13. Die Evaluation im realen Umfeld fand in einem ausgewählten kommunalen Umfeld statt. Bei der Auswahl geeigneter Interviewpartner kamen zum Zeitpunkt der Interviews Städte in Frage, die eine Einwohnerzahl von mindestens 100.000 aufwiesen. Ungeachtet der möglichen und unmittelbaren Betroffenheit großer Kommunen durch die NIS-2-Richtlinie ist die Architektur für alle kommunalen Größen anwendbar. Grundsätzlich werden die Architekturentwicklung im DSR-Prozess und die Ergebnisse von den Befragten als zielführend bewertet. Die schon in vorherigen Studien geforderte Rechtssicherheit ist auch in dieser Evaluationsepisode als grundlegende Forderung der Interviewpartner ausgemacht worden. Daneben sind die erheblichen Ressourcenbedarfe und Forderungen gekoppelt an Verpflichtungen, die Bund und Länder den Kommunen auferlegen wollen. Es besteht kein Zweifel daran, dass die geforderten Prozesse der Enterprise Architecture (EA) erfüllt werden sollen und auch müssen, jedoch fehlt es anhaltend an der Kommunikation durch die Länder und deren Erwartungshaltung. Daneben müssen die rechtlichen Aspekte und auch die Ressourcenproblematik angemessen adressiert werden. Grundsätzlich muss eine politische Willensbildung zuerst erfolgen und eine regulatorische Verpflichtung für die Kommunen entstehen. Die Cybersicherheitsarchitektur selbst stellt eine umsetzbare Vorgehensweise dar und kann von den Kommunen bewältigt werden.

#14. Die zweite Evaluation wurde in Organisationen des Cyber- und Informationssicherheitsmanagements ausgewählter Länder durchgeführt. Die Evaluierungsepisode fand in Ländern unterschiedlicher Größe, finanzieller Ausstattung und überwiegend abgeschlossener politischen Willensbildung statt. Die Architektur wurde in den Experteninterviews zum einen als korrekt dargestellt bewertet, um den Herausforderungen der Cybersicherheitsbedrohungen begegnen zu können, und zum anderen aus verschiedenen Perspektiven auf die sukzessive Erweiterbarkeit hin geprüft. Insbesondere kamen von einzelnen Forderungen, die EA um Themenkomplexe wie dem Katastrophenschutz, dem Kontinuitätsmanagement, dem Datenschutz oder auch um technisch-kooperative KI-Systeme zu erweitern. Dass regulatorische Vorgaben von den Ländern vorzugeben sind, wurde zwar bestätigt, jedoch waren die Interviewpartner einheitlich in den Aussagen, dass die rechtlichen Rahmenbedingungen auf den jeweiligen Kontext – der Region – abgestellt werden müssen und keine Harmonisierung anzustreben ist. Die Cybersicherheitsarchitektur wird als zielführend in den Ländern bewertet.

In diesen Evaluationsepisoden konnte die Qualität und Relevanz des entworfenen Design-Artefakts sichergestellt werden. Die Funktionalität konnte sowohl verifiziert als auch Möglichkeiten zur Weiterentwicklung durch Experteninterviews identifiziert werden. Die Rückmeldungen fanden in *„Design und Entwicklung“* iterativ Eingang und wurden hinsichtlich des Mehrwerts bzw. der Erhöhung der Komplexität geprüft. Die EA konnte durch die Evaluation Akzeptanz bei relevanten Stakeholdern der Forschungsdomäne generieren, trägt zum Erkenntnisgewinn bei und wird als wissenschaftlich valide bewertet.

1.3.6 Kommunikation

Die Kommunikation – als elementarer Teil des DSR-Prozesses – fand entlang aller veröffentlichten Beiträge in der Forschungsgemeinschaft statt, um die Reflexion dieser wissenschaftlichen Arbeit in der relevanten Gruppe sicherzustellen. Die Vernetzung mit den einschlägigen Forschern trug dazu bei, Kollaborationen mit Partnern und anderen Forschern zu ermöglichen, den Wissenstransfer zu generieren und den Praxisbezug anhaltend zu überwachen. Daneben konnte Problemaufriss und die mögliche Lösung mit den interessierten Parteien (Stakeholdern) ausgetauscht werden, auch um die Einschränkungen der Arbeit zu erfassen. Durch den interdisziplinären Ansatz dieser Forschungsleistung konnte das Fundament für erste regulatorische Maßnahmen in Ländern beobachtet und bewertet werden. Beispielsweise wurden in der Freien Hansestadt Bremen die Cybersicherheitsstrategie und die Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen (VV NIS2Ums FHB) verabschiedet – als Teil der europäischen Notifizierung – sowie gesetzliche Regelungen zur Cybersicherheit als Referentenentwurf vorgeschlagen.

Mit der Veröffentlichung dieser Arbeit ist der gesamte DSR-Prozess, angefangen von der Problemdefinition bis zur Ergebnisvalidierung, dargestellt.

1.4 Schlussbetrachtung

In diesem Beitrag und den im Zusammenhang stehenden veröffentlichten Publikationen wurde die Möglichkeit einer Verbindung von praxisbezogenen Problemen, zusammen mit einer wissenschaftlichen Lösungsannäherung, zur Abwehr von Cybersicherheitsbedrohungen in föderalen Strukturen anwendungsbezogen erarbeitet. Die Beantwortung von Forschungsfragen konnte im Kontext dieser Arbeit dazu beitragen, die relevanten Akteure der regionalen Gemeinschaft zu beteiligen, um diese angemessen in der Lösung zu berücksichtigen. Die folgenden Abschnitte fassen die erreichten Ergebnisse und die Anwendbarkeit der entstandenen Lösung zusammen, legen die Begrenztheit der vorliegenden Arbeit hinsichtlich der zusätzlich zu involvierenden Thematiken dar und soll einen Ausblick für künftige Forschungsfelder ermöglichen.

1.4.1 Zentrale Merkmale der CSA

Die zentralen Bausteine der CSA stellen ein zu etablierendes System von minimal darzustellenden Funktionalitäten dar. Der kontinuierlich anzulegende Prozess der *„Identification und Compliance“* ist insbesondere bei den Ländern von elementarerer Wichtigkeit. Das jeweilige Land muss unabhängig von den europäischen NIS-2-Richtlinie und der verbundenen Pflicht der Unternehmen zur Aufsichts- und Meldepflicht beim BSI erfahren, welche kritischen Infrastruktur-Betreiber in der Region tätig sind. Folglich muss die Erwartungshaltung der Länder gegenüber dem Bund nachhaltig aufrechterhalten werden, dass diese Unternehmen den Ländern unverzüglich zur Kenntnis gegebenen werden. Daneben ist es erforderlich, dass die Länder die darüberhinausgehenden Betreiber selbst und in der jeweiligen Region erfassen, da viele Betreiber nicht dem europäischen Regelungsrahmen unterfallen, entweder aufgrund ihrer Größe oder weil diese Betreiber Teil der öffentlichen Verwaltung sind bzw. auch weil sie keinem Sektor zuzuordnen sind.

Alle Akteure müssen ein Risikomanagement (*Risk & Performance*) aufbauen und ihre Tätigkeiten in einer abgestimmten Bewertungsmetrik anhaltend messen: eine Forderung, die mit einem ISMS und zwischenzeitlich mit der NIS-2-Richtlinie einhergeht und unter vereinheitlichten Bedingungen der Region erfolgen kann.

Die Steuerung des Gesamtsystems erfolgt über den Prozess *„Authority & Sanctioning“* der „Aufsichtsbehörde“. Hier sind alle Akteure bekannt zu machen, zu vernetzen, deren Dienstleistung im Kontext der regionalen Daseinsvorsorge zu bewerten und die Hilfe bzw. Hilfe zur Selbsthilfe zu steuern. Teilaspekte sind durch die NIS-2-Richtlinie zwischenzeitlich in den Ländern zwingend erforderlich und werden mit der Verpflichtung zur Einrichtung eines Computer Security Incident Response Team (CSIRT) erfüllt. Gleichwohl ist festzustellen, dass einige Länder die CSIRT-Funktionalität auf Landes-IT-Dienstleister ausgliedern wollen oder auch schon haben, was einer Prüfung unterzogen

werden sollte. Grundsätzlich sind die Aufgaben der Aufsichtsbehörde in der CSA deutlich weiter gefasst und stellen einen Mehrwert für die Region dar und wurde durch die Evaluation bestätigt.

Der Unterstützungsprozess „*Cooperation & Communication*“ ist der Aufsichtsbehörde zuzuordnen. Unabhängig von der individuellen Gestaltung und des Reifegrades der Informationssicherheit bei den Akteuren, hat nur die Aufsichtsbehörde in einem Land das Recht, Unterstützungsleistungen beim BSI einzufordern. Sofern Kooperationsverträge mit dem BSI bestehen, was überwiegend in den Ländern der Fall ist, können weitere Zusammenarbeitsbereiche genutzt werden. Im Fall einer aktuellen Bedrohungslage können jedoch nur beratende Funktionen vom BSI gewährleistet werden und sollen grundsätzlich den gesamtstaatlichen Erkenntnisgewinn in Deutschland erhöhen. Folglich haben die Länder darüber hinaus operativ zu gewährleisten, dass sie selbst Expertise vorhalten oder spezialisierte Unternehmen des „Incident Response“ für die Region vertraglich binden und für die Bewältigung einer akuten Cybersicherheitsbedrohung eines Akteures oder der Region zum Einsatz gebracht werden. Abhängig von den Ressourcen sind verschiedene dieser Varianten in den Ländern zwischenzeitlich etabliert worden.

Der operative Prozess „*Operation & Support*“ der CSA wird ebenfalls von der Aufsichtsbehörde inhaltlich gesteuert. In der CSA sind die vier Kernaufgaben der operativen Unterstützung zusammengefasst, welche die Länder anerkannt jedoch derzeit in höchst unterschiedlicher Qualität ausgeprägt haben.

- Insbesondere wird der „*Warn und Information Service“* (WIS) nur vereinzelt in Ländern allen Akteuren der Region angeboten. Technische Systeme sind hierfür verfügbar, jedoch mit erheblichen finanziellen Ressourcen verbunden, insbesondere, weil die allgemein verfügbaren Informationen (Common Vulnerabilities and Exposures (CVE)) mit externen und teilweise vertraulichen Quellen angereichert werden. Die vollständige Umsetzung dieser Funktionalität wurde in der Evaluation bestätigt.
- Das technische System „*Malware Information Sharing Platform*“ (MISP) zum Austausch und zur Erfassung und Bewertung von Angriffsvektoren ist derzeit überwiegend in Ministerien – im Verbund des Bundes und der Länder – in Betrieb, zuvorderst bei den Landes-IT-Dienstleistern. Einzelne Länder involvieren ihre Kommunen, jedoch niemand die Wirtschaftsunternehmen der Region unmittelbar. Die CSA sieht hier jedoch vor, dass die Teilhabe bei allen Akteuren im Kollaborationsverbund zu gewährleisten ist und die Länder für die angemessene und pseudonymisierte Interaktion sorgen muss. Insbesondere werden Bund und Länder darüber entscheiden, welche Unternehmen von den gesamtstaatlichen Erkenntnissen aufgrund von wirtschaftspolitischen Interessen ausgeschlossen werden müssen. Die Konzeption zur gemeinsamen Erkennung und Abwehr von IT-Angriffen liegt zwischenzeitlich als Mindeststandard zur Detektion, Information und Abwehr vor und soll vom IT-PLR verabschiedet werden.

- Der nicht durch IT unterstützte Prozess des „*Mobile Incident Response Team“* (MIRT) beruht auf Kooperationsverträgen oder auf eigene Expertise im Land. Unstrittig ist in der Evaluation der CSA, dass solche Funktionen aus dem Land heraus zu generieren sind. Die Ausprägung reicht derzeit von Remoteunterstützung bis hin zur Vorortunterstützung in den Ländern und bei den Kommunen. Auch hier werden die Unternehmen derzeit nur unzureichend bzw. nicht involviert. Ursächlich ist die mangelnde Kenntnis von Unternehmen, welche einer bundesstaatlichen Aufsicht unterfallen in den Ländern. Die Unternehmen können derzeit an Beratungen durch die jeweiligen Landesverfassungsschutzbehörden (hier der Wirtschaftsschutz) und den Landekriminalämtern partizipieren.
- Der derzeit nicht durch IT unterstützte Prozess „*Situation Report“* (SR) umfasst die Erstellung eines regionalen Sicherheitslagebildes und wird den MISP-Prozess perspektivisch involvieren. Die Evaluation hat gezeigt, dass sowohl ein regionales Lagebild aller Akteure bei der verantwortlichen Stelle erforderlich ist als auch dieses zur Anreicherung des Bundes- und europäischen Lagebild genutzt werden kann. Das derzeitige Lagebild beim Bund entsteht aus Erkenntnissen des BSI, wird ausschließlich durch vereinzelte Meldungen der Länder angereichert und beruht auf einem nichttechnischen Formular, einem quasi Meldestandard.

Die auf Erhöhung der Informations- und Cybersicherheit beruhenden Standards der IT müssen nach Evaluation fortwährend überprüft werden, um die Zusammenarbeit und Aufsichtsführung zu gewährleisten. Der *„Cyber Security Standard“* Prozess sieht vor, dass die anwendbaren und praktikablen Standards, die zur Akzeptanz bei der Aufsichtsbehörde in der Region führen, überwacht und fortgeschrieben werden bzw. die Partizipation gewährleistet wird. Welcher Standard angemessen ist, hängt von der Dynamik der Bedrohungslage ab und kann deshalb nicht auf langfristige Sicht angemessen sein. Weiterhin sind Innovationsfähigkeit, Wettbewerbsvorteile, ökonomische Aspekte oder auch Nachhaltigkeitsaspekte für die Zusammenarbeit erforderlich. Die Evaluation hat gezeigt, dass z. B. CISIS12 oder das verwandte BSI-Kommunalprofil für Kommunen verschiedener Größen einsetzbar sind. Eine Verbindlichkeit kann hierfür über den IT-PLR gesteuert werden. Für die BSI-Standards sind wiederum nur Länder bei der Fortschreibung beteiligt, insofern ist die Rolle der Aufsichtsbehörde bei der Ausgestaltung erforderlich. Wirtschaftsunternehmen haben oft branchenspezifische Sicherheitsstandards, die von Branchenverbänden befördert werden. Die Anerkennung dieser B3S erfolgt derzeit ausschließlich beim BSI und muss mit Anforderungen der Länder harmonieren.

Der Prozess zur Gesetzgebung „*Regulation & Legislation & Obligation*“ wird uneingeschränkt von der jeweiligen Aufsichtsbehörde, den Parlamenten und Ressorts der Länder gestaltet. Die Länder haben hier verschiedene und teilweise vorläufige Vorgehensweisen gewählt. Insbesondere werden im Rahmen der europäischen Cybersicherheits-Regulierung in vielen Ländern vorerst Verwaltungsvorschriften erlassen, um zuvorderst die Konformität herzustellen. Dort, wo Gesetze ergänzend erlassen werden, sind die

Ressorts der Länder – nach zwischen dem Bund und den Ländern abgestimmten Identifikationskonzept – im Anwendungskreis. Das heißt, Unternehmen werden überwiegend nicht und Kommunen nur mittelbar in den Fokus gerückt. Dieser Prozess ist folglich vorerst in keinem Land umfänglich und auf alle Akteure der CSA wirksam. Gleichwohl hat die Evaluation gezeigt, dass die Erforderlichkeit gesehen wird, jedoch ressourcentechnische und politische Hinderungsgründe dies noch verhindern.

1.4.2 Diskussion der Ergebnisse

Das Forschungsvorhaben konnte aufzeigen, dass eine grundsätzlich auf Unternehmen ausgerichtete Forschung zur Entwicklung von Enterprise Architekturen auch auf die öffentliche Verwaltung anwendbar ist. Insbesondere konnte nachgewiesen werden, dass der Bedarf dergestalt gegeben ist, dass Anforderungen aus dem Umfeld der Cybersicherheit zu strukturieren sind, um vergleichbar, effektiv, effizient und bestenfalls einheitlich sich diesen Herausforderungen zu stellen.

Durch Literaturrecherchen im gesamten DSR-Prozess wurde deutlich, dass insbesondere das Forschungsfeld Cybersicherheit in föderalen Strukturen Deutschlands zu wenig in den wissenschaftlichen Fokus gerückt wurde. Dabei ist der Staat mit seinen föderalen Strukturen für die Aufrechterhaltung von Sicherheit und Ordnung verantwortlich und ist folglich der Garant für das Gemeinwohl. Es besteht demnach eine hohe Relevanz für die Forschung in der spezifischen Domäne und greift dabei eine Forschungslücke auf, die mit der vorgeschlagenen föderalen Cybersicherheitsarchitektur gelöst werden kann. Das Architekturmodell ist das wesentliche Artefakt dieses DSR-Prozesses und beinhaltet die abstrakte Repräsentation von Systemen und Prozessen. Dieses Modell konnte im natürlichen und im laborartigen Umfeld evaluiert werden und schließt die spezifische Forschungslücke. Dabei konnten empirische und nicht-empirische wissenschaftliche Forschungsmethoden aus der bestehenden Wissensbasis eingesetzt werden, um das Artefakt wissenschaftlich zu fundieren und gleichzeitig die Praxisrelevanz sicherzustellen. Die Strukturierung des Forschungsprozesses mit einhergehender Entwicklung neuen Wissens macht das DSR zu einer Vorgehensweise, die ein gemeinsames Verständnis schafft und die Komplexität des Artefakts reduzieren hilft. Dieser Anspruch ist aufgrund der verschiedenen politischen und unternehmerischen Akteure der Architektur ein wesentlicher Aspekt, dem Rechnung getragen wurde.

Unabhängig davon, ob die Akteure dem öffentlichen Bereich oder den privatrechtlich handelnden Unternehmen zuzuordnen sind, wird durchgehend anerkannt, dass nur ein gemeinsames Interagieren die regionale Versorgungssicherheit befördern kann. „Strategisch und motivatorische Elemente“ der CSA sind für alle Beteiligten nachvollziehbar und korrekt dargestellt. Für alle Beteiligten ist deutlich geworden, Forderungen und Vorgaben der Landesregierung, um spezifische Defizite des IT-Servicemanagements, des Informationssicherheitsmanagements und der aktiven Bedrohungsanalyse zu kompensieren, müssen bei der jeweiligen Organisation angemessen und unter ökonomischen

Gesichtspunkten realistisch sein. Gleichzeitig ist es unzweideutig, dass weder die Kommunen noch die Unternehmen ohne eine entsprechende rechtliche Vorgabe bzw. Anreizsystemen die identifizierten Defizite in einem einheitlichen Rahmen adressieren würden. Vielmehr wird im eigenen Ermessen und in Übereinstimmung mit den interessierten Parteien gehandelt, das heißt, nur das Notwendigste. Insbesondere in Wirtschaftsunternehmen richtet sich das Handeln zuvorderst an wirtschaftlichen Gegebenheiten und im kommunalen Umfeld an den politisch aktuellen Themen aus. Folglich sind das Risikobewusstsein und das Risikomanagement unterentwickelt. Die Länder haben durchweg den Umstand erkannt, dass sie in der regionalen und digitalen Daseinsvorsorge politisch und zwischenzeitlich auch durch europäische Vorgaben gefordert sind. Entsprechend widmen die Länder mehr Aufmerksamkeit auf diese Herausforderungen aus. Gleichwohl nutzen nicht alle Länder die Chance der zielführenden Gesetzgebung, wobei auch in den Ländern Defizite existieren, die es zu kompensieren gilt. Die vorgeschlagene Architektur mit seinen Prozessen kann bei flächendeckender Anerkennung dazu beitragen, sich den Herausforderungen systematisch anzunähern.

Durch die Intention des Autors wurde in der Freien Hansestadt Bremen mit einer Senatsvorlage (Kabinettsvorlage) die grundsätzliche Zuständigkeit für das Thema Cybersicherheit zwischenzeitlich beim Senator für Inneres – als Teil des Ordnungsrechts – verortet und ist folglich nicht mehr alleinig Teil der CISO-Organisation. Diese Entwicklung ist zwischenzeitlich auch in weiteren Ländern zu beobachten, in denen die CISOs nicht den Innenministerien zugeordnet sind. Alle Länder mussten nunmehr die europäischen Vorgaben der NIS-2-Richtlinie durch eine jeweilige Cybersicherheitsstrategie und Regulation notifizieren. Sowohl die Cybersicherheitsstrategie als auch die einschlägige Verwaltungsvorschrift entstanden unter der Mitwirkung des Autors. Das von mir und einem juristischen Kollegen vorgeschlagene vollumfängliche bremische Cybersicherheitsgesetz liegt als Referentenentwurf vor und wurde mit den relevanten Ressorts abgestimmt. Das Cybersicherheitsreferat beim Innensenator hat diesen Referentenentwurf vorerst zugunsten eines bremischen Cybersicherheitsbasisgesetzes zurückgestellt. Diese Gesetzgebung soll zuvorderst die IKT der Ministerialverwaltung regulieren, greift aber für die vollumfängliche Cybersicherheit zu kurz, was gleichwohl bekannt ist. Die von mir vorgeschlagene vollumfängliche Cybersicherheitsgesetzgebung soll schrittweise erfolgen.

1.4.3 Beschränkungen und künftige Arbeiten

Die Architektur wird in der vorgelegten Arbeit als Ausgangspunkt einer weiterzuentwickelnden Arbeit betrachtet. Die Evaluation hat gezeigt, dass der Support-Prozess *„Human Resources“ (HR)*, als Ergebnis der Befragungen, nicht in den Fokus der CSA gerückt werden sollte. Potenzial für die Erweiterung der Architektur wird gleichwohl gesehen. Insbesondere wurde mit den Interviewpartnern herausgearbeitet, ob es zum jetzi-

gen Zeitpunkt sinnstiftend ist, Themen wie den Katastrophenschutz, das Kontinuitätsmanagement oder den Datenschutz in die Architektur einzubauen. Die Interviewpartner kamen jedoch zum Ergebnis, dass die derzeitigen Bausteine und Prozesse wesentliche Elemente zur Erhöhung der Resilienz liefern und weitere Aspekte die Komplexität unnötig erhöhen würden. Daher ist die CSA in den folgenden Forschungen und Entwicklungen weiterhin relevant. Das Forschungsumfeld der Verwaltungsdomäne ist breit gefächert und geprägt von Selbstbestimmung in der jeweiligen hierarchischen Ebene, das heißt, föderale Strukturen in jeder Verwaltungsebene. Dies gilt insbesondere auch für die Informationstechnik, obgleich dies als wesentlicher Hinderungsgrund für eine erfolgreiche Digitalisierung zu sehen ist. Zudem lässt sich aus der aktuellen Bedrohungslage bestätigen, dass Cybersicherheit in der EU, den Mitgliedstaaten, den Föderalstaaten, den Kommunen, den Unternehmen oder der Gesellschaft nicht isoliert betrachtet werden kann. Vielmehr sind Forschungen und Entwicklungen für ein übergreifendes Cybersicherheitsmanagement zu forcieren und den aktuellen Entwicklungen anzupassen. Deutlich ist auch geworden, dass viele Akteure keine umfängliche Cybersicherheitsabwehr leisten können und sich daher auf Partner im Betrieb, den jeweiligen Branchenverbänden und der öffentlichen Verwaltung verlassen müssen. Kommunen brauchen abhängig von ihrer Größe – mithin der verfügbaren Ressourcen – oftmals Unterstützung und müssen ggf. die IT-Infrastrukturen konsolidieren, um sich auf den Stand der Technik einlassen zu können. Die Unternehmen sind Teil der regionalen CSA und müssen dergestalt auch angemessen involviert werden. Die CSA ist nach abgeschlossener und vereinbarter Meldung von Unternehmen durch das BSI an die Länder – betroffene Akteure wie der NIS-2-Richtlinie– dahingehend zu prüfen, wie diese quantitativ und weitere durch die Länder identifizierte Unternehmen qualitativ erfassten kritischen Infrastrukturbetreiber erfolgreich zusammenarbeiten können. Dieser Bereich bleibt für zukünftige Arbeiten und zur erneuten Evaluierung als Forschungsfeld bestehen. Gleichfalls müssen die regulatorischen Anforderungen widerspruchsfrei zur bundesdeutschen Regulierung und bestenfalls im Benehmen der Länder weiterentwickelt werden: ein weiteres interdisziplinäres Forschungsfeld, was nicht im Fokus dieser Arbeit stand.

1.4.4 Schlussfolgerungen

Die CSA kann als eine wirksame harmonisierte Architektur in den Ländern eingesetzt und grundsätzlich in den föderalen Gremien als Standard deklariert werden, um den Herausforderungen der Cybersicherheitsbedrohungen angemessen zu begegnen. Durch die jüngste Entwicklung in Deutschland und anderen Mitgliedstaaten wird deutlich, dass es einer vereinheitlichten Vorgehensweise insbesondere im föderalen Deutschland bedarf, da die EU ein Vertragsverletzungsverfahren wegen der mangelnden Umsetzung der NIS-2-Richtlinie eröffnet hat. Dabei stellt gerade die CSA wesentliche organisatorische, technische und regulatorische Prozesse bereit, die auch von der EU gefordert werden. Die Umsetzung der CSA in den Ländern hätte demnach die Chance die Compliance zu EU-Forderungen zu erfüllen. Für die Länder kommt erschwerend hinzu, dass der

Bund nach eigener Aussage die vorgeworfenen Defizite ausschließlich in der Länderumsetzung sieht und in Aussicht stellt, vom Lastentragungsgesetz (LastG - Gesetz zur Lastentragung im Bund-Länder-Verhältnis bei Verletzung von supranationalen oder völkerrechtlichen Verpflichtungen, 2006) Gebrauch zu machen. Sanktionen der EU würden folglich vornehmlich die Länder treffen: ein Umstand, der durch den Einsatz der CSA abgemildert werden kann.

2 On Challenges of Cyber and Information Security Management in Federal Structures - The Example of German Public Administration[1]

Abstract: Security management in organizations is a complex task requiring defined organizational structures and processes. Established standards and recommendations provide methodological guidance for establishing and managing security. However, it has been observed that governmental or public bodies show different challenges in security management than industrial organizations due to their often densely regulated settings. In this context, in particular federal multi-layered structures have been pointed out as hard to manage. The main contributions of this paper are the results of an interview study among the chief information and security officers (CISOs) of the federal states of Germany. The results shed light on current challenges in cybersecurity management. The results are meant to establish the relevance of research work in this area and to be the starting point of developing artefacts or instruments supporting cybersecurity management at the interface of federal states and municipalities in particular.

Keywords: Reference model, cyber security, public administration.

2.1 Introduction

Security management in organizations is a complex task requiring defined organizational structures and processes and encompassing various aspects, such as technology, culture, competency, documentation, etc. (von Solms & van Niekerk, 2013, S. 97–102). Established standards and recommendations, as for example ISO 27001 (Disterer, 2013), SABSA (Burkett, 2012, S. 47–54) or IT Grundschutz (German Federal Office for Information Security, 2019), provide methodological guidance for establishing and managing security. However, it has been observed that governmental or public bodies show different challenges in security management than industrial organizations due to their often densely regulated settings. In this context, in particular federal multi-layered structures have been pointed out as hard to manage. This paper aims at contributing to a better understanding of the organizational and policy-related challenges of implementing cybersecurity management in federal states based on the example of Germany.

[1] Der Inhalt dieses Kapitels ist bereits wie folgt veröffentlicht worden: Thomas Rehbohm, Kurt Sandkuhl und Thomas Kemmerich, (2019) On Challenges of Cyber and Information Security Management in Federal Structures - The Example of German Public Administration, in BIR Workshops. 18th International Conference on Perspectives in Business Informatics Research

Taking the relationship between the federation, federal states and municipalities as focus area, the paper investigates the perceived challenges of policy implementation on executive level in the states from a governance perspective. More concrete, the study investigates the view of the CISO within an interview study.

Although our work investigates challenges for management of cyber and information security in German public administration only, there are indications of previous work that similar challenges are also visible in other federal structures. For example, (Shackelford et al., 2016) analysed and compared practices in cybersecurity implementation in the US, Germany and China, and concluded the need for detailed analysis work.

The information and cyber security of the public administration at federal, state and local level is determined by many factors. Germany's federal system is subject to dependencies comparable to those of Europe in relation to its member states. All public administrations face the same challenges as citizens and businesses. Information and cyber security is threatened and can only be ensured with increased use of technical and human resources. In addition, the political will must exist and legal conformity must be established. The technical infrastructures of the administrations are an essential basis for government services for citizens and society. Therefore, the resilience of companies providing services of general interest - including the public sector - in the administrative structure must be ensured. Information security of the public administration therefore has to include all relevant aspects of cyber security.

Cyber and information security is not a question of national or federal administrative structures. The legislation and the associated rights and obligations must be determined by uniform possibilities of action against highly dynamic - also criminal - actors on the Internet. This problem is to be investigated in an interview study as part of this work. The specific aspects of IT management in the administrations and their internal structure in Europe, the German Federal Government, the Federal States and local authorities will be identified and approaches to solutions will be developed. Possibilities for the collection of data arise in the federal states' working committees of the Conference of the Interior Ministers and the IT Planning Council.

Despite certain coordination attempts by the German IT Planning Council, the digitisation of the administration also takes place according to the strategy of the federal state and local authority. Due to this form of digitisation in Germany in general and in the administrations in particular, the efforts of comparable and uniform information security management at all levels of government in Germany will be given lower priority. In comparison to the private economy, the administrations have no overriding requirements for the implementation of information technology content objectives, an inherent problem of the system. The public administrations are not only responsible for their own IT and the digitalisation of administrative services, but also for the critical infrastructure. With the federal legal requirements on critical infrastructures, the federal states have at least moved into the focus of IT situations in the area of existence prediction. In the meantime, it has

also become apparent that purely arithmetically recorded companies of general interest do not cover the target group of major cities and regions.

From a political perspective, the federal government, the separate governments of the federal states and the various municipality councils are in charge of implementing EU laws and regulations or transposing into national law or directives. From an executive perspective, i.e. implementation of the political will manifested in the legislation, the federal states and their organization structures play an important role, as they are in charge of guiding, directing and supervising the subordinate agencies or administrations in their federal state. In this context, the CISOs of the federal states are the central roles (cf. section 2 and 4).

The main contributions of this paper are the results of an interview study among the CISOs of the federal states of Germany. The results shed light on current challenges in cybersecurity management. They are meant to establish the relevance of research work in this area and to be the starting point of developing artefacts or instruments supporting cybersecurity management at the interface of federal states and municipalities in particular.

The remaining part of the paper is structured as follows: Section 2 introduces background information on public sector data protection in federal structures. Section 3 introduces the research methodology applied in the paper. Section 4 summarizes the results of a literature study. Section 5 presents design and results of the interview study performed among the CISOs. Section 6 summarizes the findings and implications for future work.

2.2 Public sector data protection in federal structures

The information and cyber security of the federal, state and municipal public administrations is determined by many factors. Germany's federal system is subject to dependencies comparable to those of Europe in relation to its member states. Public administrations commonly face the same challenges in cyber security as citizens and businesses. Information and cyber security is threatened and can only be ensured with increased use of technical and human resources. In addition, the according political will must exist and legal conformity must be established.

The technical infrastructures of administrations are an essential basis for government services for citizens and society. Therefore, the resilience of companies providing services of general interest – including the public sector – must be ensured in the administrative division of Germany. The information security of the public administration is to be extended thus by the aspects of the cyber security.

In the literature, the topic of technology and “data protection impact assessment” of the critical infrastructure "public administration" and its information technology with regard to

ensuring information and cyber security has not yet been dealt with in a structural approach. Only partial aspects of the respective responsibilities of the ministries at federal and state level are subject to closer scientific examination.

The Committee for Education, Research and Technology Assessment in the Bundestag, for example, dealt with the "endangerment and vulnerability of modern societies - using the example of a large-scale and long-lasting power failure" and its effects on society's telecommunications and information technology (Deutscher Bundestag, 2011).

"The impact analyses have shown that after only a few days it is no longer possible to ensure the nationwide supply of the population with (vital) necessary goods and services in the affected area. Public security is at risk, and the state can no longer meet the constitutional obligation to protect the life and limb of its citizens. In doing so, it would also lose one of its most important resources - the trust of its citizens". (Deutscher Bundestag, 2011)

This result does not go far enough for the consideration envisaged in this paper, but shows that even a power failure with a low probability of occurrence – across state borders – would be tantamount to a national catastrophe.

As a result of such investigations, the federal government has renewed the implementation plans for critical infrastructures and the federal government. The sectors (Abbildung 8 Critical infrastructure sectors in Germany) energy, food, finance and insurance, health, information technology and telecommunications, media and culture, transport and traffic as well as water are addressed via the UP Critis, the state and administration via the UP Bund. The Federal Office for Civil Protection and Disaster Relief is responsible together with the Federal Office for Information Security and pursues the following objectives:

- Promotion of the robustness of ICT components in critical processes
- Exchange on current incidents
- Joint assessment and evaluation of the cyber security situation
- Development of common documents and positions
- Establishment and expansion of crisis management structures
- Coordinated crisis response and management
- Conducting emergency and crisis exercises
- Joint action vis-à-vis third parties

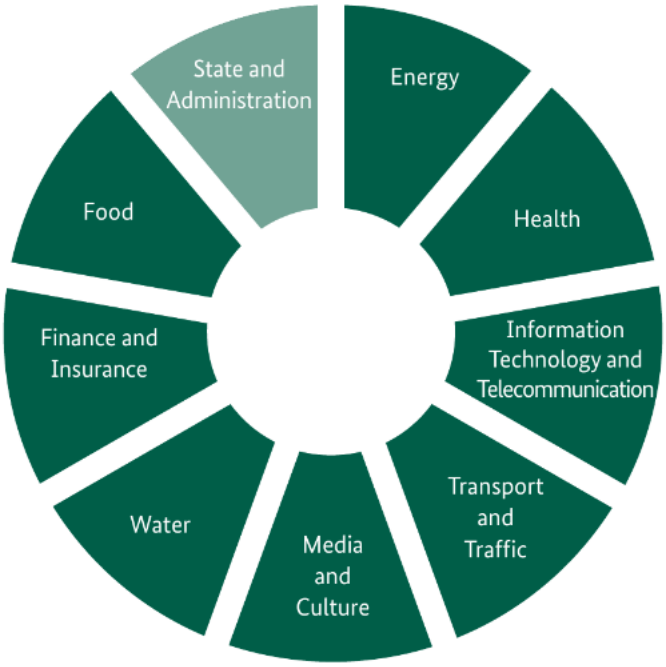

Abbildung 8 Critical infrastructure sectors in Germany

Within the framework of the legislative competence of the federal government, these objectives are supported at several legal levels. The Act to Increase the Security of Information Technology Systems (IT Security Act) – as an Article Act – applies to most of the aforementioned sectors and obliges operators of such infrastructures to take special measures, coordinated with the Federal Office for Information Security (BSI), to increase resilience to cyberattacks.

The "state and administration" sector is only indirectly affected by federal regulations, as the sector cannot be legally addressed due to federal responsibilities and is provided for in the UP Bund. This scientific work should start with the effects.

The federal government and the federal states have set up various working groups for the topics of information security and cyber security with conditionally coordinated work contents. Different departments for reasons of competence also staff them:

- A working group chaired by the Conference of Interior Ministers (IMK) is dealing with the issue of cyber security. A scientific discussion under a holistic approach is to take place - governed by the National Cyber Security Council (NCSR) – the permanent working group of the IMK has been established as the working level of the NCSR. The NCSR is composed of political leaders and business representatives, bundles the activities for cyber security between state and business and is coordinated by the Federal Government Commissioner for Information Technology.
- The information security concerns of the Federal Government and the federal states are coordinated in a permanent working group of the IT Planning Council

(IT State Treaty on the Establishment of the IT Planning Council). Representatives from various departments are delegated to this working group.

In 2009, the Federalism Commission II created the basis for binding IT coordination between the federal and state governments with Article 91c of the Basic Law, i.e. constitution of the Federal Republic of Germany.

At European level, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security of network and information systems in the Union (NIS Directive) was adopted. As in the IT Security Act, the scope of "State and Administration" was not dealt with here either. The Act to Implement the Directive (EU) 2016/1148 of the European Parliament and the Council, the IT Security Act and the BSI Act with corresponding BSI Critis Ordinances are merely the national legal implementations of the EU Directive and can therefore not close this gap.

2.3 Research Methodology

The main research methodologies used in this paper are literature research and interview study. The literature search (presented in section 4) aims at analysing relevant related work in the scientific body of knowledge. One conclusion from this research is the lack of knowledge about the view of the federal states regarding the challenges of cybersecurity implementation. Thus, it was decided to perform an interview study among the CISO and analyse interview contents based on qualitative content analysis. The research question for the study performed is: *On the executive level of the federal states of Germany, what are the perceived status and expressed challenges of cybersecurity management?* "Executive level" in this context means that we include only the CISOs of the federal state in the study.

The research question is then further defined with an analysis of the content – the determination of the relevance of the topic - and the theoretical introduction into the research field.

A study in the form of guideline-supported interviews was carried out in order to define the topic area. Participants were the IT security officers of the federal states. The colleagues, also known as CISOs, described the challenges, opportunities and risks of their activities in an interview with defined questions. The interview guideline is the result of preliminary considerations, theoretical studies and maturity models developed in the past. The results obtained and written on were subjected to a qualitative content analysis according to *Phillip Mayring* (Mayring, 1983). This method serves the purpose of empirical data evaluation and includes recommendations for a systematic and verifiable text analysis.

Mayring's approach (Mey & Mruck, 2010) includes 6 steps: Step 1 is to decide what material to analyse, which consists in our case of the notes taken during the interviews.

The interviewed CISOs all are experienced in the field of cybersecurity and qualified for their positions, which makes them suitable sources and experts for the research question. Step 2 is to make explicit how the data collection (i.e. in our case the interviews) was arranged and prepared. The purpose of this step is to make all factors transparent which could be relevant for interpreting the data. The CISOs were selected based on their position and from existing contacts of the researchers involved. As preparation for the interviews, the hypotheses and interview guidelines were arranged. The interviewees received information about the purpose of the interview. The interviews with the CISOs were between 28 and 56 minutes long.

Step 3 is to make explicit, how the transcription of the material had to be done. The material was analysed step by step following rules of procedure devising the material into content analytical units. The rules included what IDs to use for the units of different interviews, how to tag content related to the interviewer and content from the interviewees, how to mark comments, etc. Step 4 concerns the subject-reference of the analysis, i.e. that the connection to the concrete subject of the analysis is made sure. Subject-reference was implemented by (a) defining the research question and corresponding sub-questions in the interview guidelines and (b) using the subjects of these sub-questions as categories during the analysis.

Step 5 recommends theory-guided analysis of the data, which is supposed to balance vagueness of qualitative analysis with theoretical stringency. For theory guidance, we took the state-of-the-art into account during both, formulation of the sub-questions and analysis of the material. Step 6 defines the analysis technique, which in our case was content summary. This attempts to reduce the material in such a way as to preserve the essential content and by abstraction to create a manageable corpus which still reflects the original material.

All in all, the qualitative research focuses on the understanding of interrelationships, which is done here by means of interviews. This means, an inductive approach, which is concluded from empirical individual observations on the general. Quantitative research, on the other hand, is usually based on a questionnaire structure, with closed questions and given answer possibilities, as in the preliminary studies collected by the maturity models. Contexts are worked out and hypotheses tested. A deductive approach means, from the general to the specific. In a further step of the research, the questionnaires are to be carried out with a more extensive group of addressees.

2.4 Literature Analysis

Relevant literature for the topic under consideration was identified by using Google Scholar as the main search tool. Due to the nature of the topic, it quickly became obvious that many of the relevant sources were publications in German. The available literature on this topic includes essential articles from the field of government and administration,

which are mainly published in the context of German administrations. In addition, there are current developments from European research activities.

The article "Cyber security in critical infrastructures, European and German regulation - an overview" (Dürig & Fischer, 2018, S. 209–213) deals with the connections between European and national regulation. In particular, the cooperation of the member states and the operators of infrastructures of general interest and their obligation to exchange information (reporting obligations) via central contact points. The federal states have established their own federal state CERTs (Computer Emergency Response Teams) for this purpose. Operators of critical infrastructures can also set them up, but are only obliged to have a single point of contact for receiving information and for reporting incidents. The joint exercises will also be conducted in the European area, which will now also play an important role at the national level.

Analogous to the Lükex (state and interdepartmental crisis management exercise) - controlled by the Federal Office for Civil Protection and Disaster Relief - states such as Hessen design special IT crisis management exercises (KRITEX) to deepen interdepartmental cooperation in the event of critical cyber events.

In the article "Security-Management-as-a-Service" (Pfeiffer & Seiffert, 2019), a problem is addressed which found in the meantime be identified in the entire German administrative structure, the lack of skilled workers. Another aspect is the fundamental affinity of IT employees with regard to awareness of cyber security risks, but there is a lack of holistic control of the security management process and a commitment to responsibility:

“Our investigations and in-depth interviews in several authorities throughout Germany gave a detailed but heterogeneous picture of the infrastructure used, the knowledge and motivation of the employees in the areas of IT security and security management, as well as the available personnel and financial resources.“ (Stefan Pfeiffer, 1/2019)

The administrations in Germany are structured in such a way that – as in the past decades – they can only recruit skilled workers with salaries and collectively agreed wages in areas that are specific to vocational training (traditionally according to vocational or academic qualifications). Unless rapid civil service is identified as a unique selling point of the administration, the administration must face up to the competition from commercial enterprises. Where administrations can overcome the proven systems of employee recruitment, a co-appointment between administrations of federal, state and local authorities (cannibalisation) is additionally created. A new way of recruiting employees and retaining them in the company, as well as employer branding, can only be expected in the future.

In the article "IT security - a law-free space" (Hackenjos et al., 2018), the authors discuss the need to create further regulations; analogous to the basic data protection regulation, a basic IT security regulation should be created. This is based on the idea that IT security is a basic prerequisite for digital sovereignty. Digital sovereignty is understood to be mul-

tidimensional, to develop key technologies itself and to exercise control and self-determination over actions in the digital space. The evaluation from the interviews of this work resulted in a similar assessment. The Karlsruhe Institute of Technology, the FZI Research Center for Computer Science and the Fraunhofer Institute for Optronics, Systems Engineering and Image Evaluation (Beyerer et al., 2018) investigated the complexity of the ideas about digital sovereignty in Europe. Important definitions of the understanding of digital sovereignty were also developed for this research.

"Infrastructure sovereignty refers to the ability to establish or verify the trustworthiness of technical infrastructures and to operate them in such a way that services offered thereon can be trusted. Data sovereignty refers to the ability to inform and decide for oneself how and by whom information about one's own person or institution, one's own actions or products is collected, processed and passed on. Decision sovereignty refers to the possibility of tracing the origins and justifications for decisions and recommendations for action of autonomous systems and assistants and, if necessary, influencing them by human intervention. Platform sovereignty arises when the market power of major players in a platform economy is limited to a degree where fair competition remains possible through regulation and conscious customer decisions." (Beyerer et al., 2018)

The above mentioned definitions are used in this work. The Karlsruhe Theses themselves and open research questions establish a motivation to investigate the topic of this work.

In "Systematization of IT Security Law" (Raabe et al., 2018) the authors see an discrepant, incomprehensible and thus inconsistent IT legislation. The review begins with the 1990s; the first BSI laws, the data protection law, the signature law and the liability law. It is shown that since then the IT legislation has strongly diversified and in the following years, more than 60 legally effective regulations in the IT security environment arose at the federal government alone. From the area of critical infrastructures, special legal regulations were added, such as from the areas of energy, nuclear industry or telecommunications, which were last adapted in 2016 with the Article Law on IT Security (IT-SiG). Furthermore, shortcomings in the timely implementation of European legislation into German law are pointed out.

The European Parliament, the Council and the European Commission have reached political agreement on the legal act on cyber security at the end of 2018. It strengthens the mandate of the European Union Agency for Network and Information Security (ENISA). Resources will be pooled at ENISA to better help Member States deal with cyber security threats and attacks. A common cyber security certification will also be introduced. European Parliament passed the Cybersecurity Act in March 2019.

The "Case study-based analyses of IT security in critical infrastructures" (Dännart et al., o. J.) are an illustrative practical example. Particular attention was paid to critical infra-

structures only after the Stuxnet incident (malware for Supervisory Control and Data Acquisition). However, the infiltration of industrial control systems was only the beginning. Private households, public administration or even hospitals are attacked in a targeted and non-targeted manner.

The case studies were based on guided expert interviews. A qualitative content analysis according to Mayring evaluated the data according to their significance. Codes, such as the assessment and measurement of IT security, the enhancement of IT security, the simplicity of the measure or the cost efficiency of the measure, were formed and subjected to a cross case analysis in order to filter out similarities and differences. The study serves the understanding of the complex connections of IT security projects and is suitable for the development of new research questions.

2.5 Interview Study

Based on the results of the literature study, it can be concluded that the existing publications cover the general situation in cybersecurity regulation in Germany and between Germany and the EU, but there is a lack of information about the political, strategic and technical challenges arising from managing cybersecurity on the federal state level. Thus, we decided to conduct an interview study involving the top executive level in the federal states. Section 5.1 describes the hypotheses underlying our work, section 5.2 discusses the procedures applied for performing the interview study and section 5.3 summarizes the results.

2.5.1 Hypotheses

Based on the literature work in sections 2 and 4, we define two hypotheses which are subject to investigation in the interview study.

Hypothesis 1: The management of information security and cyber security is carried out in a fragmented structure of responsibilities at federal and state level. The Federal Government mainly maps the links to Europe. The states are not established and in demand as designers of information and cyber security management.

Hypothesis 2: Although it is their intended role in the federation, the federal states do not act as driving forces shaping the cyber security of their municipalities – partly because of the municipal right of self-determination. This is aggravated by the obligation of the federal states to be connected (the relationship between the federal states and the municipalities is a legal principle that establishes legally enforceable claims by the municipalities against the federal states if they enact laws that have financial consequences for their municipalities). Only the central municipal associations can be identified here as further possible participants and co-designers. The Deutscher Landkreistag (DLT) has a coordinating function for the Deutscher Städtetag (DST) and the Deutscher Städte- und Gemeindebund (DStGB). Accordingly, the associations in the respective federal states are listed below.

Coordinating information and cyber security is a challenge given in the abovementioned federal structures, inconsistent responsibilities and financial dependencies. This work will be the subject of a scientific study on the resilient structures of cooperation.

2.5.2 Procedure

The guideline-based interviews conducted in this study were based on the premise that information and cyber security are subject to political, strategic, technical and legal dependencies. In all cases, the interview partners were the CISOs of the federal states of Germany. The role of the information security officer of a federal state has been established as a functional office (Role of Information Security Management System (ISMS)), which is usually located in the hierarchy of a ministry. Due to the special importance of the topic of information security, all CISOs have a direct right to speak to the head of the authority, the state secretary or the minister, and have also arranged regular meetings. As a rule, CISOs are career civil official or employees who, depending on their position in the respective ministry, also possess a corresponding qualification such as, jurists, engineers, natural scientists or corresponding qualification in the fields of law.

Two examples of questions from each of the four areas are given below for the lead question-supported interviews.

Political: How do you see the digital sovereignty of your federal state in the future?

What competencies and mandates does your ISMS and the CISO have?

Strategical: How "broad" is the scope of responsibility of the “information security management system” organization in your federal state (cyber vs. Information security)?

Why do they (not) see IT as a strategic tool or would they also give up competences?

Technical: How do they view virtualisation on the internet and its use by their federal states (cloud)?

Which systems are used for active attack detection?

Legal: Where do you see regulatory deficiencies in your federal state?

How do they ensure compliance requirements for cloud usage variants?

In the course of the guideline-based interviews, the questions did not have to be used chronologically or entirely. Rather, in the course of the discussion it emerged that the contents desired by this work were addressed in full by the interviewees themselves.

2.5.3 Results

After evaluating the transcripts of the interviews, identical answers or identical tendencies were assigned to the statements of a group and were thus taken into account. Similarities, contradictions and differences were identified. Strongly differing statements were not taken into account for reasons of resilience or were suitable for elimination, especially tendentious statements. The official or personal circumstances of each interviewee were taken into account.

The results of the interviews are that both hypotheses were confirmed. The core results can be aggregated as follows:

a) Political perspective:

The concerns of the CISOs can be addressed on an adequate hierarchic level in the management (ministerial level) and are in part also regulated by law; this also applies beyond relevant safety incidents that are effective for the public.

The resources of information security management are predominantly acquired centrally and are responsible decentral (departmental sovereignty). To date, no federal state has been able to establish a system of indicators for the effectiveness or improvement process of security management. "Key Performance Indicators" are defined by the federal states as a Request and are to be included in the annual reports.

Conformity with the respective national budget regulations is given, but no proof of a "return on investment" can be offered.

The respondents have different interpretations of the topic of digital sovereignty. As shown in the literature research, the CISOs want scope for action for different aspects of sovereignty (infrastructures, data, decisions or platforms). The concentration on a few central and "state-owned service providers" was the main focus of all respondents.

In the federal structures of the federal states in internal relations, no special mandates or competences were transferred to the CISOs or the central security management - over and above the rights in coping with emergency situations. The procedures are based on guidelines of the respective administration that are capable of compromise or consensus.

b) Strategic perspective

All central security management systems are consistently linked to ministerial authorities, if necessary with the Chief Information Officer (CIO) or the Chief Digital Officer (CDO) of the respective federal state. As a rule, the responsibility for cyber security does not lie within the information security management; in the classical structure of administrations, this topic can be found with civil protection/crisis management or with the state criminal investigation offices of the interior departments. Consequently, responsibility for commercial enterprises (critical infrastructures) is not linked to information security management either. The same applies to classic data protection, which is provided for by law

and set up in independent authorities of its own. An exchange of content takes place via the working levels. Apart from the conflicting goals of information security and data protection (value protection vs. Data protection), however, a common risk process has been formulated as a requirement.

IT and information security management is seen as a strategic means of achieving efficiency gains, i.e. the modernisation of administration and digitisation. Decision-making authority over IT and IT security is becoming a monopoly of power.

The municipalities are currently only rudimentarily involved in the IT (security) management processes. Local self-government has so far been little involved in the strategic planning of the federal states, although the special role of the municipalities as initiators of digitisation is clear.

c) Technical perspective

Technically, IT of public administration is far behind the state of the art. The existing classical systems and infrastructures have been developed along the requirements of the past decades. Newer technologies, for example for active attack detection, are only occasionally tested because they require a legal basis. The first federal states have made improvements here. Although respondents were aware of the enormous importance of cloud computing or artificial intelligence (AI) applications, there is only a limited willingness to exploit this potential. In very few federal states, there is a resilient strategy for use of cloud services; in addition, respondents see too many parties involved in the procedure, so that they are not prepared to do anything in advance.

d) Legal perspective

In many federal states there are legally binding regulations on information security in addition to data protection and the respondents mainly see implementation deficits here. Cyber security aspects have so far not been addressed, nor have municipal aspects. In all federal states, there is a need to clear the backlog, starting with the critical infrastructures of the community (state and economy) up to municipal suppliers and the municipalities themselves.

There are sporadic legal bases in the federal states for the intervention in telecommunications secrecy, which is necessary for resilience against cyber-attacks, in particular for breaking encrypted communication connections. The interviewees in the federal states consider national legislation in the federal government to be effective, whereas European legislation is too vague and federal state legislation creates inconsistencies. There is no legal basis for the use of cloud services; rather, the federal states rely on traditional mechanisms of audits along frameworks or federal guidelines, such as the BSI's Cloud Computing Compliance Controls Catalogue (C5).

2.6 Conclusions

The survey on information security carried out identified challenges and perspectives on the level of CISO and contributes to scoping future research in the field. No study before had access to the view of the CISOs of federal states of Germany which makes the study and its results unique. In particular, the evaluation using the maturity model showed that only the federal states are in a position to achieve above-average results, in which strategic and political intentions – explained via the change process in IT management – and measures were taken, which in turn have technical and legal consequences. Resource management in the respective institutions is of decisive importance. Both financial resources made available and availability of skilled personnel represent influences to be taken into account in all the dependencies considered.

The core result of our study is that there is a need for more specific instruments in coordinating the federation and the federal state level. Such instruments should exceed the support level offered by policies or guidelines and rather offer normative or best practice recommendations. In particular, we believe that a reference model covering organizational, application and information, and technology oriented aspects and at the same time showing how existing legislation is implemented, could be of significant value to the CISOs. Thus, future work will investigate both pertinence and feasibility of reference models and their development.

The presented study refines or condenses the result in such a way that further aspects of federal cooperation must be examined more closely. In addition, there is an extended focus on cyber security. Information security – maturity model – must be considered together with cyber security. Furthermore, an additional study is to determine which companies in the counties – and which measures – need to be supported by the federal states. Such dependencies should also be examined for the "state and administration" sector.

In research, IT has played a subordinate role in government and administration. The functioning of public infrastructures is of enormous importance for services of general interest. Interdependencies with other critical sectors were – if at all – insufficiently considered.

The further research will investigate the conflicts and deficits identified here, create a model a reference and evaluate the context in the federal, state and local governments. The results of this preliminary study must be taken into account.

The reference model must do justice to the dynamic challenges of digitisation (transformation process) but at the same time remain sufficiently scalable, so that in particular the topics of information and cyber security, digital sovereignty, technology and willingness to innovate, critical infrastructure and continuity management are addressed more closely in the administrative structure of Germany.

3 Integrated Security Management of Public and Private Sector for Critical Infrastructures – Problem Investigation[2]

Abstract: The interaction between security management in public and private organisations includes complex challenges. Especially cross-organisational structures and processes have to be defined. In particular in critical infrastructure sectors, there is a need for instruments that enable the holistic and overarching management of private and public providers. Here, regulated framework conditions of the federal government exist. Unfortunately, the existing technical and organisational measures fall short for federal states. However, the federal states were not sufficiently involved in the design of the first IT Security Act. Correspondingly the federal states will only be involved in a rudimentary way in the second edition. Federal state structures are beyond the scope of the legislative procedure of federal level. Furthermore, has the federal law a detrimental effect to the Metropolitan Region Northwest, in this context.

This study shall promote the development of an "Enterprise Architecture Framework" for the state, its municipalities and their enterprises in critical infrastructure sectors. The main contributions of this paper will be derived from the results of an interview study. The interview partners are representatives of the enterprises and public bodies covered by the federal IT security regulations. In particular, the results are very important in that, they highlight and show the current challenges for services of general interest and how to increase the resilience of public service providers. In particular, cybersecurity management in the context of public institutions is examined.

Keywords: Cybersecurity, security management, services of general interest.

3.1 Introduction

Cyber- and information security has become even more important in pandemic times. The current crisis impressively shows how systemically relevant the availability of digital services and information and communication technology (ICT) infrastructures are, even for countries or federal states such as Germany's Free Hanseatic City of Bremen, which serves as motivating case and subject of investigation in this paper. Despite this all-German case, the challenge of cooperation between governmental structures (in our case in a federal state) and private companies being part of critical infrastructure sectors is a challenge in many democratic countries.

[2] Der Inhalt dieses Kapitels ist bereits wie folgt veröffentlicht: Thomas Rehbohm, Kurt Sandkuhl, Thomas Kemmerich und Clemens H. Cap, (2021) 'Integrated Security Management of Public and Private Sector for Critical Infrastructures – Problem Investigation, in Business and IT Alignment, BITA

Not only is much more data being processed – including sensitive data – but digital services and secure data networks are the backbone of society in the age of contactless working. Information security and data protection must meet these increased demands. Therefore, the basic values of information security, such as availability, integrity and confidentiality, are becoming increasingly important.

Using the example of the Free Hanseatic City of Bremen, the research work presented here aims to gain a better understanding of organisational structures and processes relevant to services of general interest, which particularly concerns the interface between organisations responsible in the public sector and private operators of critical infrastructures. For the Bremen federal state administration, not only its own infrastructures are of elementary importance, but rather also the functioning of the ICT infrastructures that enable a common life in the whole region. This includes in particular the "system-relevant" providers of services in the municipal environment. Such service providers were partially reached in Germany by the Act to Increase the Security of Information Technology Systems (cf. (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 2015)). The IT Security Act amended the BSI Act, among other things. With the following BSI Kritis Ordinance, the companies that are classified as critical infrastructure sectors and ensure a certain size of population supply were obliged to implement requirements for the security of the processing of information technology systems (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2021a).

However, there is no established procedure, best practice, public body, organisational structure or other instrument to support implementation of cyber-security for critical infrastructures when it comes to the cooperation between federal state, municipality and private sector companies. This gap has been addressed by research on Business and IT-alignment (BITA) (Seigerroth, 2011, S. 14–36), for example in (Rehbohm et al., 2019, S. 1–13), but is not fully covered yet. BITA is a continuous process aiming at aligning strategic and operational objectives and ways to implement them between the business divisions of an organization and the organization’s information technology division. The concrete contribution of the research work is an empirical study among the operators of critical infrastructures in the Free Hanseatic City of Bremen in order to collect information on the security management of infrastructures relevant to the provision of public services that has been difficult to access for research to date. After a brief description of the theoretical background (section 2), research methodology (section 3) and state of research (section 4), the hypothesis-driven survey is described in section 5 and analysed in section 6. Section 7 summarizes conclusions.

3.2 Theoretical Background

3.2.1 Enterprise Architecture Management and Business/IT-Alignment

In general, an enterprise architecture (EA) captures and structures all relevant components for describing an enterprise, including the processes used for development of the EA as such (Ahlemann et al., 2012). Research activities in EAM are manifold. The literature analysis included in (Wißotzki & Sandkuhl, 2015, S. 82–96) shows that elements of EAM (Buckl et al., 2010, S. 17–46), process and principles (Glissmann & Sanz, 2011), and implementation drivers and strategies (Szilagyi, 2018) are among the frequently researched subjects. Furthermore there is work on architecture analysis (Johnson et al., 2007, S. 163–180), decision making based on architectures (Johnson et al., 2004) and IT governance (Simonsson et al., 2010, S. 10–24). However, there is no specific focus on EAM use in the German public sector.

The existing research on EAM and IT governance for the public sector to a large extent is specific to certain countries. This is obviously caused by the strong influence on national regulations and laws on governing structures, decision and implementation procedures, and policies. Much work for the public sector has been done in the USA (see, for example, (Pang, 2014, S. 274–285)) which is due to the fact that the Clinger-Cohen act already in 1996 made it mandatory for public agencies to show how planned investments in information technology would improve efficiency and effectiveness. Similar regulations and related research can be observed in Australia (see (Ali & Green, 2007, S. 41–63)). Examples for EA in public administration in Europe can be found in Denmark, the Netherlands (Janssen & Hjort-Madsen, 2007) and Finland (Valtonen, 2017, S. 267–282). However, due to the specifics of the German governmental system with its federal structure and a combination of state-level and federation-level regulations, the work from other European countries is not easily applicable in Germany.

Business and IT-alignment (BITA) in general is a continuous process aiming at aligning strategic and operational objectives and ways to implement them between the business divisions of an organization and the organization's information technology division (Seigerroth, 2011, S. 16–34). Many challenges are linked to BITA since the business environment continuously changes and so does the IT in an enterprise, but the pace of change and the time frame needed to implement changes are different. Cybersecurity management is considered as major driver of changes in both, business environment and IT. As a consequence; BITA is of high relevance in implementation of cybersecurity. In this context, the integration of security management in public and private sector can serve as contributions to structuring the BITA.

3.2.2 Legal framework for Critical Infrastructure Sectors

With the Article Law on Increasing the Security of Information Technology Systems (IT Security Law) (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

(IT-Sicherheitsgesetz), 2015) Germany goes much further in the scope of application than the European regulations envisaged (cf. (Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, 2016)). The legal framework is based on the findings and experiences from Germany's cyber security strategy from 2011, which was first published in 2016 and is currently being revised and updated. Due to the federal structures in Germany, the federal legislation for the federal state is only partially possible, as there is only limited regulatory competence for this.

For different sectors of critical infrastructure (critis) the Federal Government defined requirements for companies of general interest. The Federal Office for Information Security (BSI) was assigned the mandate to supervise the fulfilment of the requirements of the companies affected by the IT Security Act. The BSI provides for rights and obligations, in particular obligations to provide evidence, of the operators. Public administration in the federal states and municipalities are also belongs to the critical infrastructures, but could not be addressed by the federal legislator for legal reasons of the federal state structure.

The companies identified in the Free Hanseatic City of Bremen are active in various Critis sectors. Thereby, the number of companies is significantly smaller than the identified Critis company parts. For instance, municipal water treatment and disposal are bundled in one company, whereas water distribution, due to regulation by the Federal Network Agency (BNetzA), is located in other companies. For the Free Hanseatic City of Bremen, there are currently less than 10 identified companies of general interest that fall under the federal law. This approach, based on self-disclosure, is not expedient for a federal state and falls short of increasing the resilience of critical infrastructure operators in the Free Hanseatic City of Bremen. The federal government and also the federal states must decide how systemically important companies are identified and addressed. Qualifying characteristics for federal states are preferable to a purely quantitative assessment.

There are currently no regulations with regard to the actual and verifiable affectedness of the reported company or part of the company, which would oblige a company, which from the point of view of the Free Hanseatic City of Bremen should be affected, but which have not reported, which, from the perspective of the Northwest Metropolitan Region, are important for society, but which, due to their size, will not fall within the focus of the federal regulations in the future.

For operators of critical infrastructures, the BSI negotiates individual verification obligations with the respective company (for instance, introduction of management in accordance with ISO27001) or facilitates a sector-specific security standard (B3S) of the respective sector working group of a critical sector. The federal regulation of IT security for operators of critical infrastructures (cf. (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2021a), which is now in force and is currently being revised, has identified

challenges in the federal states and municipalities that were not conclusively and purposefully regulated by the law itself.

3.3 Research Approach

The work presented in this paper is part of a research project aimed at method and tool support for cross-organizational structures and processes between the public and the private sector supporting systematic implementation of cybersecurity management in critical infrastructure sectors. The core of the method and tool support is expected to be an EA-based reference model for how to organize the cooperation between the different levels of public administration (i.e., federal state, municipality) and the private sector (i.e., enterprise in the critical infrastructure sector). The overall research project follows the paradigm of design science research (Johannesson & Perjons, 2014). This study concerns a step to-wards the explication of problems and elicitation of requirements for the envisioned design artefact: EA based reference model for integrated cybersecurity management. The work presented in this paper started from the following research question:

RQ: *In the context of cybersecurity in critical infrastructure sectors, what challenges are visible in the cooperation of public administration and private sector and what problems have to be addressed in method support?*

The research method used for working on this research question is a combination of literature study, expert interview and argumentative-deductive work. Based on the research question, we started identifying research areas with relevant work for this question and analysed the literature in these areas. The purpose of the analysis was to find existing approaches or theories supporting cybersecurity integration in public/private sectors allowing us to study the problem relevance in detail. Since the literature study showed a lack of established approaches (see section 4), we decided to focus on an expert interview in a real-world case for investigating the problem (see section 5). The case is used to explore the existence and shape of the challenge of public/private sector integration.

3.4 State of research

For a few years now, the number of research papers in the field of cyber and information security has been growing steadily. Due to the transposition of the Directive of the European Parliament and of the Council on measures to ensure a high common level of security of network and information systems in the (Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, 2016) into national law, this topic is of high interest in the member states. In the context of the digitalisation of public administration and society, the results of the colloquium "Do we need a new art of statecraft" -challenges for state and admin-

istrative action due to digital development- are processed in a socio-political, state-theoretical, constitutional and administrative discourse (Lühr et al., 2019). A comprehensive presentation of IT security law and its current technical basis is provided in the legal handbook "Cybersecurity" (Kipker & Barudi, 2020). In particular, it shows how responsible corporate management and supervision (corporate governance) and compliance with laws and regulations (corporate compliance) are to be interpreted in this context. IT governance comprises management and organisational models, which are supplemented by the aspects of conformity with rules on processes and law. The intended research of this thesis is to close the gap that arises in the federal design of the ambitious digitisation projects from the perspective of the federal state administration.

3.4.1 Literature analysis

In addition to the book publications mentioned above, a consideration of conference and journal publications is also necessary to analyse the state of research. To this end, a literature analysis was conducted in relevant German and English-language literature databases. Specifically, SSOAR (administrative sciences), EconLit and WISO (public service, business administration) as well as Scopus (various disciplines, mainly English) were selected. The following table (Tabelle 2 database search) shows the search terms, database and number of hits. The search was conducted in the title, abstract and keywords of the publication. The search was conducted at the End of January 2021.

Such Term	Datenbank	Treffer	Relevant
Daseinsvorsorge UND Cybersicherheit	Scopus	0	0
services for the public AND cybersecurity		0	0
Public services AND cybersecurity		12	0
Public services AND IT-securtiy		3	0
Public services AND information securtiy		43	0
Daseinsvorsorge UND (Cybersicherheit ODER IT-Sicherheit ODER Informationssicherheit ODER IT-Sicherheitsmanagement)	EBSCO EconLit	0	0
(Kommune ODER Bundesland) UND (Cybersicherheit ODER IT-Sicherheit ODER Informationssicherheit ODER IT-Sicherheitsmanagement)		0	0
Daseinsvorsorge	SSOAR	59	0
Daseinsvorsorge UND Sicherheit	WISO	2	0

Tabelle 2 database search

The 12 hits in Scopus on public services and cybersecurity concerned military aspects of cybersecurity or case studies in emerging countries. The 3 and 43 hits on IT security or information security in the public sector were also not relevant to our work, as they dealt with studies on the state of affairs in specific countries (e.g. Indonesia, Cameroon,

Nigeria), specific aspects of IT security (e.g. access control or continuity), or aspects of continuing education or e-learning. None of the 59 hits in SSOAR for the search term services of general interest dealt with a topic in the context of IT security. The two articles in WISO focused only on security in healthcare.

Overall, no publication on cyber security or IT security and services of general interest could be found through the literature search.

3.4.2 Summary

Current cybersecurity research is very wide-ranging, dealing in particular with technologies, digital sovereignty and liability issues in the context of the European Union, regulation and national implementation. Cybersecurity research cannot be defined to a specific field.

In contrast, the critical infrastructure "public administration", together with the responsibility for municipal services of general interest, is little researched. Organisational structures should be researched, should be the focus of further development, in order to ensure the interaction of federal state government, municipalities and companies for the common good. It is about the interaction between law and information technology.

3.5 Interview study

3.5.1 Methodological approach

For the research in the field of cyber security, a study was conducted in the form of a guideline-based interview. The participants were identified through the notification of the BSI, to the coordinating bodies of the federal state (single point of contact), in this case the Free Hanseatic City of Bremen.

The head offices for IT, the management and also the CISOs (Chief Information Security Officers) of the companies concerned were interviewed with defined and open questions. A total of nine interviews were conducted with the organisations concerned in a period of between one and four hours. The obtained and transcribed results were subjected to a qualitative content analysis according to (Mayring, 2008). The same text passages of identical main categories were summarised and refined by forming subcategories. The formation of subcategories corresponds to the induction process. In addition to the category-based evaluation, individual case interpretations were created along the main categories.

The central research question is further defined by the interview study. Organisational structures or organisational architectures, as well as the accompanying legal de-sign, should promote cooperation between the public administration and the business community in such a way that an exchange of content is made possible and legitimised,

obligations are created where necessary and joint IT security status reports can be created.

3.5.2 Hypotheses / Theses

In order to be able to examine the central research question of this thesis in the interview study, theses were first developed which served as a basis for the definition of interview questions. The following 9 statements form an important input for the qualitative content analysis of the interviews.

1. "The companies have not been informed that they are affected!" The BSI Critis Regulation did not lead to the automatic identification of the addressed companies according to coverage. The more time passed, the more companies found out in their compliance management that they were affected rather by chance.
2. „The companies do not consider themselves to be part of the municipal utilities and are therefore not willing to recognise the potential impact of services of general interest!” Affected companies do not see their own service as elementary for the common good. Distribution effects in the region can compensate for any shortfalls at any time.
3. "The municipality is not seen as a stakeholder by business enterprises!" The federal state government or the municipality is not seen as an institution to be involved with business enterprises, rather it is seen as a disruptive factor. The more regulations are created, the more dependent business decisions are.
4. "Companies are of the opinion that IT is part of the normal core business that can be afforded by the company itself, this also applies to IT security (networking idea underdeveloped)!” IT infrastructures and services are part of the company's own value chain and must be located within the company. IT and information security can be managed within the company. The more complex the requirements become, the more there is a willingness to outsource.
5. "The development and transfer (stabilisation) of know-how can be achieved without outsourcing partners!” If there are requirements that force a qualification of employees, this is granted within the company. External consultations are only helpful to a limited extent.
6. “The risk in networking office IT and OT is underestimated by companies!" Networking (connecting) operational and office IT has more benefits for the organisation. Cybersecurity risks can be managed. In particular, the focus here is on the "creeping" networking of systems of operational IT, office IT and possibly further IoT systems.
7. “The choice of information security and data protection frameworks are inconsistent and influenced by several factors!" If there are external requirements, for instance from the Basic Data Protection Regulation, management systems are

introduced. Implementing management systems voluntarily are only cost factors and have no added value. Are the classic functions of planning, organisation, personnel, management and control available in a form that is conducive to cyber security?

8. „Interdependencies were not taken into account!" The own service is not dependent on other service providers. A failure of suppliers or providers of ICT services is unacceptable and has a fundamental impact on value creation.
9. „The companies do not see the public authorities as partners, but as a source of information. They do not see any regulatory deficits on the part of the legislator!" The more regulatory requirements there are, the less advantageous this is for service provision. Non-binding networking with public administration institutions, including the exchange of current threat situations, can be beneficial.

The prepared 16 questions, which were to be used to investigate the hypotheses, were asked of all participants in the course of the discussion - but not chronologically. The results were written down during the interviews.

3.5.3 Interviewed companies and objectives of the interviews

The operators of the critical infrastructures located in the Free Hanseatic City of Bremen, which were identified by the Federal IT Security Act, are not yet dependent on or even obliged to cooperate with the federal states and municipalities in terms of content due to the existing legal regulations. Operators of a critical infrastructure within the meaning of the law must, in particular, name a contact point to the BSI within six months of the BSI KritisV coming into force, via which they can be reached at any time. However, in the view of the federal state government, this circumstance is not to be considered appropriate, since the federal states were not informed or were only partially informed about the addressed companies. In order to better understand the needs of the operators and also of the federal state government or the supervisory authorities in municipalities within the administration, structured interviews were conducted with the entrepreneurs currently notified. These companies reported to the state are critical infrastructures that did not fall under existing special legal regulations. In particular, companies that fall under the Energy Industry Act, the Telecommunications Act or the Telemedia Act were not among the interviewees.

The companies surveyed are operators in Bremen and Bremerhaven that provide services in the following facility categories:

Wastewater disposal, facilities for ordering, distribution and sale of food and raw materials, oil and product storage, water distribution network, control facilities, sewerage, wastewater treatment plants, logistics centres and hospitals.

These companies in the Free Hanseatic City of Bremen belong to the Kritis sectors: sewage treatment plants, food supply, fuel and heating oil supply, drinking water sup-

ply, sewerage, passenger and goods transport and stationary medical care. These twelve notified operators belong to fewer than 8 companies in the Free Hanseatic City of Bremen. In addition, there are operators who fall under the IT Security Act and are to be designated as municipal.

Telephone appointments were arranged with all operators identified in the Free Hanseatic City of Bremen and face-to-face appointments with individual operators. The telephone interview partners were, depending on the organisation and size of the respective company, the managing director, the IT security officer and/or the IT manager. The crisis/emergency management officer, the information security officer, the head of network operations and a member of the management were present at the face-to-face appointment. The survey was conducted in 2020.

Questions such as "Which regulatory authorities (local, state or federal state) do you have?", or "Are there established processes and reporting channels?" helped to understand the context of the organisation. Questions that approached the topic of critical infrastructure on a technical level (especially the operation of ICT systems) were intended to reveal whether the respective company operates particularly high-risk infrastructures (e.g. "Are operational information technology and office IT separate in your company?").

The aim of the interviews was to find out where comparable challenges exist among the operators, how the operators can imagine cooperation with the supervisory authorities in terms of content, and what regulatory deficits, training needs or further training requirements exist. From the perspective of the central information security management of the Free Hanseatic City of Bremen, the consideration of interdependencies in the context of service provision is also of elementary importance.

3.6 Results

The 9 hypotheses/theses are evaluated in detail below:

H1 The examination of whether the company is affected by the IT Security Act was carried out exclusively internally; in the broadest sense, compliance management is in place at larger companies. It can be assumed that many companies in the general interest are not yet aware of this. Extensive laws, regulations and controls are common in other subject areas (environment [water and emission protection], trade supervision). More extensive regulations are not advocated by any company. For instance, one interviewee replied: "It is not clear to us how the threshold values were arrived at. Although we are not a big supplier, in our company the annual production thresholds are reached on a weekly basis."

H2 The own understanding of service provision – in the context of services of general interest – is not very well developed. Only once was a comprehensive emergency management system found that also addressed cyber security risks. Although the ongoing pandemic did not begin until after the interviews, one company also had concepts for the

operation of systems separated in terms of personnel and space. For instance, one interviewee replied meaningfully: "Our Company is a global player that does not operate according to rules in Germany."

H3 Companies that perform public tasks in the broadest sense (e.g. water supply) have a much better understanding of cooperation with municipal public authorities and the relevance for services of general interest. Other sectors are only committed to their original business objective and do not see their service in the context of services of general interest. For instance, one interviewee replied: "We are in contact with Bremerhaven's municipal authorities and the federal state Criminal Police Office regarding threatening situations.

H4 Depending on the size of the company, the IT equipment and the associated IT security are developed very differently. Large companies rely on partners in the IT environment and have awareness-raising concepts for their employees. Networking with industry associations is well developed. Centralised (corporate) IT was also cited in one company to make it clear that necessary decisions are not made in Germany. Smaller companies are not very networked, operate traditional IT environments and see themselves as committed to data protection goals at most. For instance, one interviewee replied: "The combination of regional and central partners is effective. A Security Operation Centre (SOC) is at the corporate level already established."

H5 Few companies had a training concept or tracked their training in a management system. When training is provided, it tends to be on an annual basis and often as an electronic and optional learning opportunity. On-, off- and change boarding processes for employees are established in the companies' HR management. For instance, one interviewee replied: "We have a network of internal and external partners, we are a global player! But it also varies from country to country. We have a global safety policy, as well as e-learning offers."

H6 The separation of operational and office IT varies greatly; the smaller the company and the resources available for IT, the higher the degree of networking and thus the risk appetite. In larger companies, complete separation of the IT systems can be found, up to and including regulated technical transitions. The danger of networking these two segments is perceived as a high risk. For instance, one interviewee replied: "Production software is integrated, but subject to special regulations with high technical requirements" or "There is only one IT, not connected in a separable way."

H7 There are few industry-specific security standards (B3S) published at the time of the interview. The BSI has often recognised ISO 27001 (native) as a framework, as evidence for the BSI KritisV (Guidance on evidence). Data protection management, on the other hand, is consistently established. For instance, meaningfully, one interviewee replied, "It is well known that you can participate or contribute to industry or thematic working groups. It's a resource issue."

H8 Public authorities are expected to provide a framework. No further explicit requirements or obligations are expected. Rather, voluntary cooperation is advocated. In the meantime, the Bremen federal state Criminal Police Office has contacted the operators affected by the IT Security Act and offered to exchange information. For instance, one interviewee replied: "Further regulations are not really desired. Companies like these, are active in all federal states (of Germany), networking would be overregulated. Too many contact persons."

H9 Very few companies have taken precautions to make themselves less dependent on supplier services in the ICT environment. Nor are most entrepreneurs aware of whom they are dependent on for performance (internet and infrastructures) in the first place. One single company (as mentioned above) is aware of almost all aspects of business continuity management (BCM), thanks to its well-developed emergency and dis-aster recovery management. Contractual arrangements have also been concluded with replacement service suppliers in this example. For instance, one interviewee replied: "There is complete dependency on ICT. A technical failure in Africa meant that we were no longer able to operate there for a week. ICT can only survive without partners at the head office in Denmark."

3.7 Conclusions and Future Work

The validity of the analysis is generally given by the use of several evaluators and multiple qualitative content analysis of the interview transcripts (data). For the existing data sets of the nine interviewed companies, this seems unnecessary, as further surveys, especially supra-regional-municipal studies, will follow, which should also verify the present result. The transferability and possibility of generalisation already exists in the author's view, although there is the possibility that the answers of the interview partners were not always correctly understood or depended significantly on the interview partner and his "role" in the company. The very heterogeneous structure of the interviewed companies (local company to part of a group) shows that there are no uniform or comparable approaches or architectures in the organisation of the companies to adequately counter cyber security risks.

Technically and organisationally, the measures taken are mostly not effective. The larger and more decentralised the IT, the more agile and also sensitive the companies are with regard to the required cyber security. Smaller companies can be said to have an underdeveloped understanding of resilience issues. Companies currently affected by the IT Security Act are not fully covered, as the IT Security Act aims at "self-disclosure". The BSI has not reported several large companies in Bremen known to the public administration to the Senator for the Interior. A deficiency that can only be countered by identifying system-relevant undertakings oneself. The required screening of critical infrastructures must map such enterprises of the region or the federal state Dependent services (interdependencies) must be fully worked through.

It should be noted that Bremen, like the other federal states, has not yet been able to create any binding structures to promote cooperation between the relevant stakeholders in the common good. The evaluation also shows that most of the Bremen companies reported so far do not have well-developed resilience structures. A common organisational architecture must be developed. Other federal states (such as Saarland, Lower Saxony and Saxony) have adopted legal foundations for information security in the federal state administration. In this context, cooperation with the public welfare organisations can only be targeted on a voluntary basis.

Future work: Based on the present study, supplemented by further municipal and country-specific studies, an enterprise architecture model is to be developed, which can be integrated into the existing management systems. The architecture must consider the following aspects: The public administration is to network the providers of services of general interest identified based on qualitative characteristics in, for instance, a "country-based alliance for cyber security". Rights and obligations of the participants are defined; in particular, the automated exchange of information, e.g. on cyber security risks and current threat situations must be made possible. The establishment of a cybersecurity control centre, modelled on a Computer Emergency Response Team, should be established between stakeholders. At the same time, legal foundations must be created to oblige the providers of services of general interest in the federal state, especially because the tasks of disaster control, crisis management and hazard prevention are the original responsibility of a federal state.

4 Sicherheitsmanagement, Cybersicherheit und Daseinsvorsorge: Empirische Studie in deutschen Kommunen[3]

Zusammenfassung: Die angespannte Cybersicherheitslage, die anhaltende Pandemielage sowie die Digitalisierung der Gesellschaft verdeutlichen, dass sich die gesamte föderale Verwaltung Deutschlands den Herausforderungen eines kontinuierlichen Betriebs der digitalen Infrastruktur stellen muss. Gleichzeitig trägt die Verwaltung nicht nur für ihre eigenen Dienstleistungen Sorge, sondern auch dafür, dass Unternehmen der Daseinsvorsorge unterbrechungsfreien Betrieb sicherstellen. Die kritischen Infrastrukturen der Öffentliche Verwaltung und der Daseinsvorsorgeträger müssen gemeinsam agieren, um die Daten von Bürgern, Wirtschaft oder auch Kunden angemessen zu schützen, und um somit die Versorgungssicherheit mit kritischen Dienstleistungen sicherstellen zu können.

Die vorliegende Studie soll aus den jeweils individuellen Perspektiven verschiedener kommunaler Organisationen aufzeigen, wie mit den Herausforderungen der Informations- und Cybersicherheit für selbst verantwortete informationstechnische Systeme umgegangen wird und inwieweit sich dieser Anwendungsbereich auf die systemrelevanten Infrastrukturen der jeweiligen Region erstreckt. Insbesondere soll herausgearbeitet werden, ob eine organisationsübergreifende Sicherheitsorganisation existiert, die auch die Belange der Daseinsvorsorge adressiert.

4.1 Einleitung

Die Gewährleistung der Cyber- und Informationssicherheit in öffentlichen Verwaltungsstrukturen allgemein und insbesondere in kommunalen Verwaltungsstrukturen, erfordern einen ganzheitlichen Ansatz zur Erhöhung der Resilienz. Die Cybersicherheit erweitert die Informationssicherheit einzelner Organisationen insofern, dass unsere gesellschaftlichen Werte bedroht und betroffen sind, insbesondere durch die Störung der kritischen Infrastrukturen. Solche erhöhten Anforderungen an öffentliche Stellen erfordern die Übernahme von Verantwortung durch diese Stellen, auch für die ansässigen Daseinsvorsorgeträger der jeweiligen Region.

Mit der neuen Cybersicherheitsstrategie der EU und damit verbundenen neuen Vorschriften zur Erhöhung der Widerstandsfähigkeit kritischer Einrichtungen werden weitere Sektoren der kritischen Infrastrukturen definiert sowie die öffentliche Verwaltung im Zusammenhang mit der Erfordernis von Wissenschaft und Forschung adressiert (Europäische Kommission, 2020b, S. 4). Die einhergehende Novellierung der EU-Richtlinie zur

[3] Der Inhalt dieses Kapitels ist bereits wie folgt veröffentlicht worden: Thomas Rehbohm, Robin Kemmerich, Clemens H. Cap, Kurt Sandkuhl (2022), Datenschutz und Datensicherheit - DuD

Netz- und Informationssicherheit (NIS-2-Richtlinie) (Europäische Kommission, 2020a) greift dabei die föderalen Strukturen Deutschlands allerdings nur in Teilen auf.

Regionale Strukturen und Strategien müssen folglich von den Ländern im Föderalsystems Deutschlands und den Kommunen entwickelt werden. Kritische Infrastrukturen sind in Deutschland zunächst im Bundesgesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 2015) definiert worden. In seiner neuesten Fassung ergänzt das IT Sicherheitsgesetz unter anderem auch mit der Definition „Unternehmen im besonderen öffentlichen Interesse (UBI)“ den Betroffenenbereich solcher Infrastrukturen (Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, 2021). Auf Länderebene haben bereits einige eigene Gesetze verabschiedet (z. B. Baden-Württemberg, Niedersachsen) oder planen diese (z. B. Hessen, Bremen).

„In Deutschland werden Organisationen und Einrichtungen aus den Bereichen Energieversorgung, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur zu den Kritischen Infrastrukturen gezählt“ (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2021b).

Obwohl Staat und Verwaltung als ein eigener Sektor der Kritischen Infrastruktur erfasst wurde, kommen diesen eine von weiteren Sektoren zu unterscheidende Funktion zu, die im Rahmen der weiteren Forschungsarbeiten herausgearbeitet werden soll. Der Schwerpunkt dieses Artikels liegt auf dem derzeitigen Stand der Cybersicherheitsarchitektur in kommunalen Strukturen. Dabei ist die Kollaboration des Landes, seiner Kommunen und Unternehmen der systemrelevanten Infrastrukturen von besonderem Interesse. Konkret wurde eine Online-Umfrage unter kommunalen Organisationen in Deutschland durchgeführt, die die Themen Sicherheitsorganisation, Informationssicherheitsmanagement und Daseinsvorsorge im Kontext der digitalen Infrastruktur adressiert. Nach der Analyse des Stands der Forschung (Abschnitt 2) und der Beschreibung der methodischen Vorgehensweise (Abschnitt 3) erfolgt die Darstellung der Ergebnisse der Umfrage (Abschnitt 4) und deren Diskussion (Abschnitt 5). Der abschließende Ausblick (Abschnitt 6) zeigt die Potentiale der Nutzung von Unternehmensarchitekturen im Bereich Cybersicherheit für kommunale Organisationen auf.

4.2 Stand der Forschung und Literatur

Forschungsbeiträge betreffend Dienstleistungen von allgemeinem Interesse (services of general interest (SGI)) bzw. Daseinsvorsorgeträger behandeln insbesondere dezidierte Themen der Versorgungssicherheit einzelner Sektoren. Das Forschungsfeld von staatlichen Akteuren als Daseinsvorsorgeträger ist für die Föderalstruktur Deutschlands im Kontext des Onlinezugangsgesetzes und der Digitalisierung im Fokus von wissenschaftlichen Arbeiten (*Bostelmann*), (Seckelmann & Brunzel, 2021, S. 165). Die Interaktion

und Kollaboration in einer gemeinsamen Cybersicherheitsarchitektur bleibt hingegen offen.

Die aktuelle Cybersicherheitsstrategie des Bundes ist auf strategische Zusammenarbeit von Bund und Ländern ausgerichtet, ist aber hinsichtlich der Zusammenarbeit mit den Kommunen und Wirtschaftsunternehmen der Daseinsvorsorge zu wenig konkret (Bundesministerium des Innern, für Bau und Heimat, 2021a, S. 90). Rechtlich wurde für die Umsetzung der Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz und Informationssystemen (NIS) in der Union ein nationaler Regelungsrahmen der Mitgliedstaaten geschaffen (Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, 2016). Im Gesetz zur Umsetzung der NIS Richtlinie wurde dies in Deutschland adressiert (Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, 2017). Die EU definiert in der NIS-Richtlinie:

> *„Dienstleistungen von allgemeinem Interesse sind Dienste, die Behörden der EU-Länder als solche einstufen und die daher mit bestimmten gemeinwirtschaftlichen Verpflichtungen verbunden sind. Sie können entweder vom Staat oder von der privaten Wirtschaft bereitgestellt werden“* (Europäische Kommission, 2021).

Im Kontext der europäischen Vorgaben und Strategien sind Dienstleistungen von allgemeinem bzw. wirtschaftlichen Interesse mit Themen, wie dem Binnenmarktrecht, Wettbewerbsrecht und dem öffentliche Auftragsvergaberecht, wissenschaftlich aufgearbeitet worden. Zum Beispiel führt Krajewski an, dass im Vertrag von Lissabon unter anderem die Mitgliedstaaten (nationale, regionale und lokale Behörden) der Europäischen Union, die allgemeine Zuständigkeit für die „Bereitstellung, Beauftragung und Organisation“ von Dienstleistungen von allgemeinem Interesse haben (Krajewski, 2015, S. 237). Hieraus lässt sich eine direkte Zuständigkeit von z. B. kommunalen Strukturen für Dienstleistungen von allgemeinem Interesse auch im Kontext der Cybersicherheit begründen.

Das Spannungsverhältnis von Marktregelungen und Eingriffen des Staates ist anhand von Fallbeispielen aus verschiedenen Sektoren in der Literatur untersucht worden. In der Europäischen Regulierung wird der Begriff der Dienstleistungen von allgemeinen Interesse bzw. SGI als eine Entsprechung zu staatlichen Aufgaben aufgefasst. Die Auslegung, was im allgemeinen Interesse der Gesellschaft steht, muss demnach auch die jeweilige Gesellschaft definieren (Zhu, 2020, S. 31). Ein politischer Prozess zur Definition von SGI ist in den Mitgliedsstaaten notwendig, berichtet Zhu weiter, um eine Bestimmung von Werten, Werturteilen und die Abwägung der verschiedenen Interessen in einen demokratischen Prozess zu führen. Das Vorhandensein einer solchen Definition

kann im Mitgliedsstaat Deutschland durch die einschlägige Bundesgesetzgebung unterstellt werden. Auf den föderalen Ebenen muss ein solcher Prozess jedoch noch ausgestaltet werden.

Die vorliegenden Erkenntnisse in Deutschland ergeben sich hauptsächlich aus Erfahrungen des Bundes, insbesondere aus dem Umsetzungsplan Kritis (UP Kritis). Im Kapitel „Grenzen und Möglichkeiten der öffentlich-privaten Zusammenarbeit zum Schutz Kritischer IT-Infrastrukturen am Beispiel des Umsetzungsplan KRITIS“ zeigt Freiberg auf, dass nach wie vor unterschiedliche Interessensschwerpunkte existieren. Aus Sicht des privaten Sektors sind die komplexen Beziehungen zwischen Bundes- und Landesbehörden (auch Kommunen) schwer zu erfassen. Aus Sicht des öffentlichen Sektors ist das Bewusstsein für eine IT-Krisensituation im privaten Sektor schwer herzustellen (Lange & Bötticher, 2015, S. 110). Die gesamtstaatliche Verantwortung muss ihre Ausprägung in der föderalen Struktur Deutschlands finden und kann nicht ausschließlich beim Bund verortet werden.

Außerhalb Europas und in föderalen Strukturen der Vereinigten Staaten bestehen dieselben Herausforderungen wie im deutschen System. Im Kapitel 5 „The Cybersecurity Policy Challenge, The Tyranny of Geography” arbeitet *Kamarck* das Thema der Streuung der Verantwortung zwischen staatlichen Organisationen auf und kommt zu folgender Schlussfolgerung:

> *“Die Regierung ist seit Jahrhunderten nach geografischen Gesichtspunkten organisiert aber die Cyber-Bedrohung ist grenzenlos und fordert die innere und die nationalen Sicherheitsseiten der Regierung, eine nahtlose Architektur der Architektur der Zusammenarbeit zu schaffen“* (Andreasson, 2012, S. 124).

Zu einer vergleichbaren Aussage kommen auch *Harknet* und *Stever* mit ihrem Beitrag zur Cybersicherheit in vernetzten Systemen. Dort haben die Regierungsinstitutionen der Vereinigten Staaten erkannt, welche Bedeutung die Cybersicherheit für die wirtschaftlichen, sozialen und politischen Aktivitäten der Gesellschaft ausmacht.

> *„Das Problem der Cybersicherheit passt nicht in herkömmliche oder traditionelle Sicherheitskategorien, die auf der Verantwortung des Einzelnen für die Sicherheit, auf wirtschaftlichen oder unternehmerischen Sicherheitsfragen, auf militärischen Sicherheitsproblemen sowie auf nationalen oder internationalen Problemen basieren.“*
> (Harknett & Stever, 2011, S. 455)

Die Entwicklung einer kohärenten Cybersicherheitspolitik ist erforderlich. Auch in den USA wird ein Cybersicherheitsframework gefordert, welches auch die Unternehmen kritischer Infrastrukturen einbezieht. Gleichwohl haben diese Unternehmen Sorge, Informationen mit Aufsichtsbehörden zu teilen, insbesondere über bestehende Sicherheitsmängel oder auch aus Haftungsgründen. Wie in Deutschland, verfügen insbesondere die staatlichen Stellen der USA über Informationen zu Cybersicherheitsbedrohungen und potenziellen Zielen. Eine bilaterale Kooperationsverweigerung würde zumindest in

den USA zu Konsequenzen hinsichtlich zukünftiger Beschaffungsentscheidungen führen (Rodin, 2015, S. 519).

Bund und Länder in Deutschland versuchen sich strategisch zu organisieren, gleichwohl haben die Länder vergleichbare Herausforderungen im Zusammenwirken mit ihren Kommunen und den Wirtschaftsunternehmen der Daseinsvorsorge der Region, die nicht vom Bund adressiert werden.

Die schnelle und angemessene Zusammenarbeit bei Bedrohungslagen, besser noch der synchrone Informationsaustausch von Bund, Ländern, den behördlichen Strukturen und Unternehmen ist erforderlich, sodass Maßnahmen einheitlich und zielgerichtet erfolgen können (Bretschneider et al., 2020, S. 53).

In einer aktuellen Studie der European Union Agency for Cybersecurity (ENISA), der zuständigen europäischen Behörde für ein hohes gemeinsames Niveau der Cybersicherheit, ist die aktuelle Umsetzung der NIS-Richtlinie, inkl. relevanter Investitionen, Sicherheitsvorfälle etc. in den Mitgliedsstaaten erhoben und ausgewertet worden.

„Schätzungen zufolge werden bis 2025 40 % der Vorstände einen speziellen Ausschuss für Cybersicherheit haben, während es heute weniger als 10 % sind“ (European Union Agency for Cybersecurity, 2021, S. 65).

Gleichzeitig wird auch in der Studie der anhaltende Fachkräftemangel in der Informationssicherheit behandelt: Insbesondere im Zusammenhang mit Fähigkeiten im Bereich des Risikomanagements ergeben sich aktuell Defizite, die auch in dieser Studie nachvollzogen werden können.

Der Stand der Forschung im Bereich der öffentlichen Verwaltung ist zuvorderst geprägt von den Digitalisierungsbemühungen und der gewünschten Zurückgewinnung der Digitalen Souveränität. Beispielweise schreibt *Bizer* im Kapitel 1 „Digitale Souveränität – wer steuert, organisiert und kontrolliert die digitale Verwaltung?“:

„Eine funktionsfähige IT für die Verwaltung zu gewährleisten, wird damit zur Staatsaufgabe“ (H. Becker, 2019, S. 27).

Obwohl eine staatliche Aufgabe identifiziert wird, greift die digitale Souveränität der öffentlichen Verwaltung zu kurz. Die beschriebene Sicherheit von Unternehmens- und Verwaltungsdaten, der Schutz von Urheber- und Markenrechten oder auch Patenten ist für das gesellschaftliche Zusammenleben nur als ein Beitrag zu sehen, jedoch liefert es keinen ganzheitlichen Ansatz.

Vom rein bundesrechtlich betrachteten Standpunkt aus, stellen die Autoren des Beitrages „Cybersicherheit in Kritischen Infrastrukturen“ fest:

„In der Gesamtschau hat sich der Ansatz einer kooperativen Zusammenarbeit gerade im Bereich Cybersicherheit bewährt, weil hier eine erfolgreiche Reaktion auf die aktu-

elle und zukünftig zu erwartende Cyberbedrohungslage maßgeblich von der vertrauensvollen Kooperation zwischen Staat und Wirtschaft in einer „shared mission" abhängt" (Dürig & Fischer, 2018, S. 209–213).

Aus Sicht dieser Autoren ist das eine nachvollziehbare Aussage, weil sie aus dem Blickwinkel des europäischen und bundesdeutschen Rechts die Wirtschaft adressiert. Eine erforderliche und weitergehende Analyse der weiteren Verwaltungsebenen ist jedoch erforderlich.

Auch *Schünemann* erkennt die besondere Relevanz der Cybersicherheit im Kontext der Digitalisierung an und sieht Staat und Verwaltung in einer gestalterischen Verpflichtung, als Garant für das Funktionieren der eigenen und der besonders schützenswerten IT-Systeme (Klenk et al., 2020, Teil 3). Weiter führt er aus, dass Staat und Verwaltung aktiv an der Entwicklung und Zertifizierung von IT-Sicherheitsrahmenwerken teilhaben, als Aufgabe des Gemeinwohls. Die Entwicklung von Rahmenwerken der Informationssicherheit kann aber nur ein Baustein der zukünftigen Cybersicherheit sein. Insbesondere in der IT-Sicherheitsforschung ergeben sich laut *Eckert* Herausforderungen, die unter dem Begriff „kognitive Sicherheit" etabliert wurden. Es wird an automatisierten Analyse- und Erkennungsverfahren geforscht, die Angriffe und Angriffsversuche erkennen oder vorhersagen können (Bode et al., 2017, Teil 1).

Neben formalen Strukturen, gesetzlichen oder untergesetzlichen Regelungen, ist einer der wichtigsten Faktoren im Leitfaden zur Etablierung eines resilienten Sicherheits-Ökosystems benannt worden:

„Gute und wertschätzende Kommunikation: der Dreh- und Angelpunkt für nachhaltige Veränderung" (Maier & Aengenheyster, 2020).

Die Autoren zielen hier auf die Schärfung des Bewusstseins für Risiken im Umgang mit Informationstechnik ab. Eine Kommunikationsherausforderung, die bei Beschäftigten, in der Führung und in den politischen Gremien bewältigt werden muss.

Ergänzend zu den oben genannten Veröffentlichungen wurde eine Suche nach wesentlichen Konferenz- und Zeitschriftenpublikationen durchgeführt, um den Stand der Forschung zu verifizieren. Eine Literaturanalyse in relevanten deutsch- und englischsprachigen Literaturdatenbanken wurde bei Scopus (übergreifende Disziplinen, vorwiegend englischsprachig), IEEE (Berufsverband von Ingenieuren), EBSCO (Wissenschaftsdienst), SSOAR (Verwaltungswissenschaften) und WISO (Öffentlicher Dienst, Betriebswirtschaft) im Mai 2021 durchgeführt. Folgende Tabelle 3 Literaturrecherche zeigt die entsprechenden Treffer in den Datenbänken auf.

Suche	Literatur	Treffer
services of general interest	Scopus	147
Services of general interest UND Federal		5
Daseinsvorsorge		37
services of general interest	IEEE	1
services of general interest	EBSCO	13
services of general interest	SSOAR	18

services of general interest	WISO	198
Services of general interest UND Federal		26
Daseinsvorsorge UND Cybersicherheit		33

Tabelle 3 Literaturrecherche

Die Treffer in Scopus beziehen sich überwiegend auf die aktuellen Herausforderungen bei den bestehenden Sozial-, Versorgungsund Gesundheitssystemen, im Zusammenhang mit der Thematik der schrumpfenden Bevölkerung in ländlichen Regionen und setzen sich mit der Versorgung von Gütern der Daseinsvorsorge oder staatlicher Leistungen (Bildung, Bibliotheken) auseinander. Im engeren Sinne wird Sozioökonomie in Verbindung mit Demographie untersucht sowie im weiteren Sinne mit Raumordnung und Territorialplanung verbunden. Weitere Treffer beziehen sich auf die Regelungskompetenz der Europäischen Union und ihrer Mitgliedsstaaten, insbesondere werden die Auswirkungen auf die Binnenmarkt- und Wettbewerbsregeln thematisiert. In diesem Zusammenhang existiert ein wissenschaftlicher Diskurs zur EU-Kohäsions- und Strukturpolitik, der den wirtschaftlichen, sozialen und territorialen Zusammenhalt in der Union sichern soll. Dabei wird auch das Subsidiaritätsprinzip der Union im Kontext der Daseinsvorsorge betrachtet. Weiterhin werden Aspekte von Rekommunalisierung und Deregulierung von Daseinsvorsorgeträgern aufgearbeitet. Im weiteren Verlauf der Untersuchung aufgezeigter Quellen konnten keine wesentlichen Veröffentlichungen gefunden werden, die im Kontext dieser Untersuchung stehen.

Die aktuelle Cybersicherheitsforschung ist nicht fest definiert bzw. schwer abgrenzbar und kann dementsprechend sehr weit gefasst werden. Eine in der Literatur angebotene Definition lautet:

„Cybersicherheit ist nicht nur IT-Sicherheit. IT-Sicherheit ist Teil der Cybersicherheit, aber die Cybersicherheit ist viel komplexer und schließt neben den technischen auch nicht-technische Aspekte wie organisatorische, physische und personelle Aspekte ein“
(Bartsch & Frey, 2017, Teil 1).

Der von dieser Forschungsarbeit gesuchte Zusammenhang von Cybersicherheitsarchitekturen regionaler Daseinsvorsorgeträger, in Verbindung mit regulierenden staatlichen Stellen auf Landesund Kommunaleben, konnte in der vorgenommenen Literaturrecherche nicht aufgefunden werden.

4.3 Methodische Vorgehensweise

Im zweiten und dritten Quartal des Jahres 2020 wurde eine Online-Umfrage bei kommunalen Organisationen (Landkreise, Städte und Gemeinden) durchgeführt. Als Vorbereitung der Umfrage wurde Ende 2019 eine Interviewstudie (Rehbohm et al., 2021) durchgeführt, deren Ergebnisse nicht nur die Vermutung zulassen, dass deutlicher Verbesserungsbedarf in kommunalen Einrichtungen hinsichtlich Sicherheitsorganisation, Informationssicherheitsmanagement und Daseinsvorsorge besteht, sondern auch, dass die

Sichtweise auf den Verbesserungsbedarf von der Größe der Organisation und der zuständigen Person abhängt. Für die Online-Umfrage wurden daraus Hypothesen hergeleitet, die mit der Umfrage untersucht werden sollen:

- Leithypothese H0 „Abhängig davon, wer die Frage beantwortet, ist die Informationstechnik (auch das Informationssicherheitsmanagement) etwaig nicht im Fokus der Organisation und kann delegiert werden."
- Hypothese H1 „Je kleiner die Organisation, desto weniger Aufmerksamkeit wird der eigenen Informationstechnik und dem Thema „Digitalen Souveränität" gewidmet."
- Hypothese H2 „Je kleiner die Organisation, desto weniger ist man in der Lage die eigene Institution auch für die Informationssicherheit/Cybersicherheit und Daseinsvorsorge aufzustellen (Sicherheitsorganisation)."
- Hypothese H3 „Je größer die Organisation, desto wichtiger wird die Informationstechnik der eigenen- und fremden (Unternehmen) Organisation bewertet."
- Hypothese H4 „Desto weniger die Rollen des Compliance-Managements (IT Sicherheit und IT Recht) im Unternehmen verortet wurden, je weniger Aufmerksamkeit besteht für die Daseinsvorsorge."

Um die genannten Hypothesen überprüfen und anschließend Schlussfolgerungen zu ermöglichen, wurde ein quantitativer Forschungsansatz auf Basis einer Umfrage gewählt. Die Online Umfrage wurde bei den deutschen Spitzenverbänden im Bund, wie dem Deutschen Landkreistag (DLT) durchgeführt und beim Deutschen Städtetag (DST) und Deutschen Städte und Gemeindebund (DStGB) beworben.

198 Personen haben den Fragebogen ausgefüllt. Zwei Personen wurden von der Analyse ausgeschlossen, da sie lediglich die beiden Eingangsfragen beantwortet haben. Die restlichen 196 Fragebögen wurden für die Auswertung genutzt.

Die Auswertung erfolgte mit IBM SPSS Version 26. Die Befragung der Teilnehmenden erfolgte auf Basis von 14 kategorischen Fragestellungen mit drei bis fünf Antwortmöglichkeiten. Zunächst werden die Verteilungen der Variablen deskriptiv dargestellt. Multinomiale logistische Regression wurde durchgeführt, um den Einfluss verschiedener Faktoren auf jeweils verschiedene Variablen zu untersuchen. So wurde zuerst untersucht, ob die Anzahl der Mitarbeitenden der jeweiligen Kommune einen Einfluss darauf haben, ob für die Kommunen Landesvorgaben für IT-Sicherheitsmanagement existieren, ob es innerhalb der Kommunen solche Vorgaben existieren, ob die Kommune selbst Betreiber von KRITIS ist und ob es Konzepte zur Bewältigung von IT-Notfällen existieren.

Im nächsten Block werden die Einflüsse der beruflichen Position der Antwortenden und die Anzahl der Beschäftigten der jeweiligen Kommune untersucht. Die abhängigen Variablen hier beinhalten, ob IT als eine auslagerbare Leistung angesehen wird, ob die

eigene erbrachte kommunale Dienstleistung als eine kritische Infrastruktur (KRITIS) angesehen wird, ob die Betreiber der regionalen kritischen Infrastruktur den Antwortenden bekannt sind, ob ein inhaltlicher Austausch mit diesen Betreibern existiert sowie welche Aufgaben- und Verantwortungsverteilung zwischen Land und Kommune im Bereich Cybersicherheit bekannt sind. Da insgesamt zehn statistische Auswertungen erfolgen wird das Signifikanzlevel im Sinne der Bonferroni-Korrektur auf $p < 0{,}005$ gesetzt.

4.4 Ergebnisse

Von den insgesamt 196 Teilnehmenden waren 25,5% (n = 50) in der IT-Leitung mit operativen Aufgaben, 26,5% (n = 52) in der IT-Leitung mit strategischen Aufgaben, 36,7% (n = 72) im IT-Sicherheitsmanagement und 11,2% (n = 22) in generellen Leitungsaufgaben tätig.

Von den 72 im IT-Sicherheitsmanagement tätigen Personen in der Stichprobe sind 40,3% (n = 29) mit ihrer vollen Arbeitszeit, 31,9% (n = 23) mit weniger als 50% ihrer Arbeitszeit, 5,6% (n = 4) mit weniger als 10% der Arbeitszeit und 22,2% (n = 16) ohne festen Stundenanteil für die Institution tätig.

Die Anzahl der Beschäftigten der jeweiligen Kommune wurde von 8,7% (n = 17) der Teilnehmenden mit bis zu 100, von 30,1% (n = 59) mit bis zu 500, von 25% (n = 49) bis zu 1000, von 31,6% (n = 62) mehr als 1.000 und von 4,6% (n = 9) mit mehr als 10.000 Angestellten angegeben. Für die Verwendung in den späteren Regressionsmodellen wurden die letzten beiden Kategorien zusammen zu mehr als 1000 vereint.

Von den Befragten teilten 94,9% (n = 186) die Ansicht, Informationstechnik sei das Rückgrat der kommunalen Dienstleistungserbringung. Weitere 5,1% (n = 10) gaben an, maximal wenige Stunden bis Tage auf IT verzichten zu können. Niemand gab an, Tage bis Wochen oder generell auf IT für die eigene Aufgabenerledigung verzichten zu können.

Folgend wird die Anzahl der Beschäftigten der jeweiligen Kommune als unabhängige Variable in logistischen Regressionsanalysen verwendet. Hinsichtlich möglicher Vorgaben der Länder zum IT-Betrieb oder IT-Sicherheitsmanagement gaben 60,7% (n = 119) der Befragten an, dass solche Vorgaben existieren. Bei 26% (n = 51) existieren solche Vorgaben nicht, 13,3% (n = 26) wissen es nicht. Die Existenz einer Landesvorgabe ist nicht signifikant von der Größe der jeweiligen Kommune abhängig ($\chi^2(6) = 9{,}506$; $p = 0{,}147$).

In den meisten Kommunen selbst existieren hingegen Vorgaben hinsichtlich eines Informationssicherheitsmanagements. So gaben 51% (n = 100) der Stichprobe an, vollständige Vorgaben inklusive eines Sicherheitsbeauftragten zu haben, für weitere 39,3% (n = 77) existieren solche zumindest teilweise. Nur 8,2% (n = 16) haben keine kommunalen Vorgaben zum Informationssicherheitsmanagement, drei der Befragten (1,5%) wussten es nicht. Das Vorhandensein solcher Vorgaben hängt signifikant von der Größe der Kommune ab ($\chi^2(9) = 30{,}434$; $p < 0{,}001$).

Die Mehrheit der Kommunen ist nicht selbst Betreiber einer kritischen Infrastruktur im Sinne der KRITIS. So gaben 63,3% (n = 124) der Befragten an, dass ihre Kommune keine solche betreibt. Nur 31,6% (n = 62) arbeiten in einer Kommune, die selbst eine solche Infrastruktur betreibt. Der Rest der Teilnehmenden hatte diese Information nicht.

Ob die Kommune selbst eine Kritische Infrastruktur betreibt, hängt nicht von der Größe der Kommune ab ($\chi^2(6) = 5{,}864$; $p = 0{,}439$). Hinsichtlich der Existenz von Konzepten zur Bewältigung von IT-Sicherheitsvorfällen gaben 32,6% (n = 64) an, dass ein solches aktuell nicht vorliegt oder sich noch in der Planung befindet. Bei 66,4% (n = 130) liegt ein solches Konzept mindestens teilweise vor, weitere zwei Personen (1%) wussten hierzu keine Antwort. Zwar existieren in größeren Kommunen tendenziell eher solche Konzepte, diese Abhängigkeit ist allerdings nicht signifikant ($\chi^2(6) = 5{,}257$; $p = 0{,}511$).

Die Frage, ob die Informationstechnik der Kommune eine Leistung ist, die ausgelagert werden kann, wird nicht von diesen Prädiktoren erklärt ($\chi^2(18) = 16{,}815$; $p = 0{,}536$).

Die eigene Position und die Größe der Kommune haben einen signifikanten Einfluss auf die Einschätzung, ob die eigene kommunale Dienstleistung als kritische Infrastruktur gesehen wird ($\chi^2(18) = 37{,}629$; $p = 0{,}004$), wobei die Größe der Kommune einen höheren Einfluss hat. Ob die Betreiber regionaler KRITIS bekannt sind, ist nicht abhängig von den hier betrachteten Faktoren ($\chi^2(18) = 22{,}17$; $p = 0{,}225$).

Weiterhin ist knapp nicht signifikant, ob ein inhaltlicher Austausch mit diesen Betreibern der KRITIS existiert ($\chi^2(18) = 28{,}294$; $p = 0{,}058$), wobei hier die berufliche Position des Antwortenden einen deutlich höheren Einfluss hat.

Auch die Frage, welche Aufgaben- und Verantwortungsverteilung zwischen Land und Kommune im Bereich Cybersicherheit bekannt ist, hat einen nur knapp nicht signifikanten Einfluss der Position der Befragten und der Größe der Kommune ($\chi^2(12) = 22{,}648$; $p = 0{,}031$). Interessanterweise ist niemandem in der Stichprobe eine Landesverantwortung bekannt. Insgesamt 53,1% (n = 104) geben an, nur kommunale Selbstverwaltung zu kennen, bei 19,4% (n = 38) herrscht eine Kooperation zwischen Land und Kommune. Die restlichen 27,6% (n = 54) kennen die Verantwortungsverteilung nicht.

Zuletzt geht es darum, ob den Teilnehmenden der Befragung Prozesse der Zusammenarbeit zwischen Land und Kommune im Bereich Cybersicherheit bekannt sind. Knapp einem Drittel (32,1%, n = 63) sind keine der genannten Prozesse bzw. generell keine Prozesse bekannt. 30,1% (n = 59) der Befragten kennen CERT (Computer Emergency Response Team) als Prozess, 28,1% (n = 55) kennen einen Notfallmanagement Prozess (z. B. nach dem BSI Grundschutz). Den restlichen 9,7% (n = 19) sind Behörden und Organisationen mit Sicherheitsaufgaben (BOS) bekannt. Die Kenntnis über solche Prozesse ist nicht von den hier betrachteten Faktoren abhängig ($\chi^2(24) = 28{,}143$; $p = 0{,}254$), wobei die Position der Teilnehmenden mehr Einfluss hat als die Größe der Kommune.

4.5 Diskussion und Schlussfolgerungen

Die Ergebnisse der Umfrage (s. Abschnitt 4) zeigen, dass nicht alle Hypothesen, die im Bezug zur Leithypothese entwickelt wurden, bestätigt werden konnten. Hinsichtlich der Sichtweise unterschiedlicher Personengruppen (Rolle in der Organisation) ergeben sich beispielsweise unterschiedliche Eindrücke. Es lässt sich eindeutig ableiten, dass keiner der Antwortenden einer Institution willens ist, auf Informationstechnik über mehr als Stunden bis wenige Tage verzichten zu können. Obwohl dies eine eindeutige Aussage hinsichtlich der Informationstechnik verschiedener Funktionsträger der Organisation ist, kann festgestellt werden, dass Prozesse des Informationssicherheitsmanagements unterdurchschnittlich entwickelt sind. Zum Beispiel wird die Rolle des Informationssicherheitsbeauftragten überwiegend mit weniger als einem halben Vollzeitäquivalent bzw. ohne feste Personalressourcen wahrgenommen. Gleichzeitig ist die Organisationsgröße überwiegend mit mehr als 100 Beschäftigten angegeben worden. Dies ist ein Hinweis darauf, dass Informationssicherheitsmanagementprozesse nicht durchgehend etabliert wurden, obwohl für kleine und mittlere Organisationen benannter Größe Empfehlungen seitens des IT-Planungsrates (Bundesministerium der Justiz, 2019) und der kommunalen Spitzenorganisationen bestehen.

Unabhängig von der Größe der Organisation gaben die Befragten an, Vorgaben der jeweiligen Länder zu kennen. Gleichwohl kann festgestellt werden, dass diese Vorgaben nicht verpflichtend eingehalten werden müssen bzw. vom Land auch nicht überwacht werden. Vielmehr ist dies ein Beleg dafür, dass die Verfassungsgarantie zur kommunalen Selbstverwaltung gewahrt wird und sich in diesem Kontext inhaltlich negativ auf das Informationssicherheitsmanagement auswirkt. Die aus dem Konnexitätsprinzip entstehenden finanziellen Verpflichtungen der Länder gegenüber seinen Kommunen sind hierfür ursächlich. Ob und wie sich eine Institution selbst Vorgaben zum Informationssicherheitsmanagement macht, hängt hingegen signifikant von der Größe der Organisation ab, d. h. die Hypothese H3 wird klar unterstützt. Insofern wäre es zielführend, dass sich kleinere kommunale Organisationen zu größeren Organisationen zusammenschließen oder einer größeren Kommune anschließen, um die Sicherheit der Informationstechnik zu institutionalisieren.

Die kommunale Dienstleistungserbringung der befragten Organisationen selbst wird nicht als kritische Infrastruktur wahrgenommen. Ein Teil der Befragten gab jedoch an, für kritische Infrastrukturen verantwortlich zu sein, bzw. solche zu betreiben. Auch hatte ein nicht zu vernachlässigender Teil der Antworten angegeben, keine Kenntnisse zu kritischen Infrastrukturen zu besitzen. Die Bearbeitung der Aufgaben Notfallmanagement bzw. Business Continuity Management (Bundesamt für Sicherheit in der Informationstechnik, 2022a) ist nur rudimentär ausgeprägt und wird folglich der Verantwortung für systemrelevante Infrastrukturen der Kommunen nicht gerecht. Insbesondere ist festzustellen, dass es an einem Regulativ zwischen den Ländern, seinen Kommunen und den möglichen systemrelevanten Wirtschaftsunternehmen fehlt. Sofern in den Kommunen keine rechtlichen Verpflichtungen zur Anwendung gekommen sind, können die Länder

dennoch entsprechende Strukturen schaffen, die eine über Freiwilligkeit hinausgehende Kooperation ermöglicht.

Ob die kommunale Informationstechnik eine auslagerbare Leistung ist, hängt signifikant von der Größe der Organisation und der wahrgenommenen Aufgabe (aus Frage 1) des antwortenden Teilnehmers ab. Hier wird die Leithypothese H0 gestärkt, dass auf Leitungsebene eher die Bereitschaft besteht, sich vom Betrieb der kritischen IT-gestützten Geschäftsprozesse zu lösen. Auch ist der Zusammenhang zur Kenntnis von Betreibern von weiteren kritischen Infrastrukturen eher auf Leitungsebene gegeben, da nur hier ein gewisser Grad der Vernetzung zu unterstellen ist, welcher hingegen auf operativer Ebene nicht nachgewiesen werden kann.

Im Zusammenhang mit weitgehend fehlenden Informationssicherheitsmanagementsystemen in kleineren Organisationen, kann hier abgeleitet werden, dass der Zusammenschluss von kleineren kommunalen Einheiten primär auf Leitungsebene verfolgt werden muss, um Aufgaben der eigenen Informationssicherheit und der Verantwortung für kritische Infrastrukturen wahrnehmen zu können. Die inhärente Skepsis gegenüber einem Outsourcing bei einem organisationsfremden Dienstleister könnte somit umgangen werden. Das „Einer für Alle/Viele“ Prinzip (Bundesministerium des Innern, für Bau und Heimat, 2021c), welches aus der Digitalisierung öffentlicher Dienstleistungen bekannt ist, müsste auch bei kommunalen IT-Infrastrukturen Einzug halten. Die beiden Hypothesen H1 und H2, welche eine Aussage zu kleineren Organisationen postulieren, sind mit der Auswertung bestätigt.

Ein inhaltlicher- oder auf Strukturen basierender Austausch zwischen Ländern und Kommunen bzw. auch weiteren Betreibern kritischer oder systemrelevanter Infrastrukturen ist nicht bzw. unzureichend entwickelt. Auch ist bei keinem der Befragten bekannt, dass eine etwaige Verantwortung für systemrelevante Infrastrukturen in der jeweiligen Landesverwaltung bestehen würde. Aus den Befragungsergebnissen kann abgeleitet werden, dass die kommunale Selbstverwaltung umfassend interpretiert wird. Operative Zusammenarbeit auf Basis eines CERT Verbundes kann bei ca. einem Drittel der Befragten bestätigt werden. Ein umfassendes Engagement aller Beteiligten ist jedoch unumgänglich, um die Resilienz der kritischen Infrastrukturen zu erhöhen. Die Hypothese H4 lässt sich nicht bestätigen.

In Bezug auf die Hypothesen ist zusammenfassend festzustellen, dass für die Informations- und Cybersicherheit keine institutionalisierte oder verpflichtende Zusammenarbeit zwischen Kommunen, Betreibern kritischer bzw. systemrelevanter Infrastrukturen und den Ländern besteht. Kenntnisse über die integrierende Rolle einer kommunalen IT-Verwaltung, der Verantwortung für die Daseinsvorsorge und der Bereitschaft zu Änderungen in der IT Architektur bzw. auch Sicherheitsorganisation herbeizuführen, bestehen bei strategischen Leitungsfunktionen (Leithypothese H0). Weiterhin lässt sich erkennen, dass auf strategischen Leitungsebenen eher eine Konzentration der Informationstechnik auf einer nächst höheren Verwaltungsebene (Outsourcing) möglich erscheint.

Defizite in der Sicherheitsorganisation kommunaler Strukturen sind unabhängig von ihrer Größe festzustellen. Insbesondere sind die Rollen einer solchen Organisation nicht durchgängig und in zu geringen personellen Ressourcen besetzt. Eine Verantwortung im jeweiligen Land wird nicht gesehen.

Es fehlt an einheitlich abgestimmten und verbindlichen Vorgaben, Kontrollen und Mechanismen zur strategischen und taktisch operativen Zusammenarbeit.

4.6 Ausblick

Vor dem Hintergrund der Umfrageergebnisse erscheint es für die nachhaltige Entwicklung einer Cybersicherheitsorganisation sinnvoll, konkretere Empfehlungen für kommunale Organisationen zu entwickeln, wie Sicherheitsorganisation, Informationssicherheitsmanagement und Kooperation mit Daseinsvorsorgeträgern realisiert werden können. Solche Empfehlungen dürfen sich dann nicht nur auf organisatorische, strukturelle oder technische Aspekte begrenzen, sondern müssen alle relevanten Aspekte gleichermaßen abdecken. Da Ansätze aus dem Gebiet der Unternehmensarchitekturen in diesem Kontext vielversprechende Ergebnisse gebracht haben, wie beispielsweise bei der Definition von Referenzrahmen zur Umsetzung von Regulation (Sandkuhl et al., 2018, S. 16–22), sollen in weiterführenden Arbeiten in einer solchen Unternehmensarchitektur alle relevanten Komponenten erfasst und strukturiert sowie die beteiligten Prozesse modelliert werden (Ahlemann et al., 2012). Die bestehende Forschung zu Unternehmensarchitekturen und IT-Governance für den öffentlichen Sektor ist weitgehend länderspezifisch, da die Regelungskompetenz für die Gefahrenabwehr und den Wirtschaftsschutz in den Ländern liegt.

Ein solches Unternehmensarchitekturmodell (UAM) würde speziell im Kontext der föderalen Strukturen in Deutschland entworfen werden, hätte zunächst den Fokus auf die Geschäftsarchitektur und würde auch die Kollaboration zwischen Daseinsvorsorgeträgern abdecken. Die hier erhobenen und ausgewerteten Daten sowie die abgeleiteten Schlussfolgerungen werden in die Entwicklung dieser Architektur einfließen. Insbesondere sollen die Informationssicherheitsmanagementsysteme der einzelnen Organisationen im Land, seinen Kommunen und den landesspezifischen kritischen Daseinsvorsorgeträgern ineinandergreifen, um eine übergreifende Cybersicherheitsarchitektur aufzubauen.

Beginnend mit der Motivationsebene sollen mindestens die Technologie-, Anwendungs- und Geschäftsebenen modelliert werden. Weitere Erkenntnisse aus in diesem Kontext entstandenen Studien, insbesondere auf Ebene der Länder, von Kritischen Infrastrukturen und einer in diesem Zusammenhang stehenden Rechtsstudie werden ebenfalls in die Entwicklung einfließen. Die Erwartungshaltungen der interessierten Parteien müssen erhoben- und landesspezifische systemrelevante Infrastrukturen identifiziert werden, um eine an Anforderungen basierende Architektur zu modellieren.

5 Grundforderungen von Informations- und Cybersicherheit in Ländern[4]

Thomas Rehbohm, M.Sc., ist Mitarbeiter der Freien Hansestadt Bremen, Institute of Computer Science der Universität Rostock. Dr. Peter Lutz Kalmbach, M.A., ist Mitarbeiter der Freien Hansestadt Bremen und Lehrbeauftragter am Fachbereich Rechtswissenschaften der Universität Bremen.

Zusammenfassung: Eingedenk der Gesetzgebung der EU und Deutschlands (Bund) im Umfeld von Netz-, Cyber- und Informationssicherheit und der einhergehenden Definition von Kritischen Infrastrukturen für die Daseinsvorsorge, stellt sich die Frage, ob Regelungsdefizite in den Ländern bestehen. Forschungsschwerpunkte sind in diesem Umfeld bislang unzureichend gesetzt worden. Alle Länder stehen vor der Herausforderung, rechtliche und organisatorische Maßnahmen zu initiieren, die ein Zusammenwirken mit den Gemeinwohlträgern einer Region erwirken.

Der Beitrag basiert auf Erkenntnissen von Interview- und Umfragestudien. Insbesondere wurde in Interviews erhoben, wie sich einzelne Bundesländer den Themen Cybersicherheit und Informationssicherheit bei rechtlichen, technischen und organisatorischen Bedingungen zuwenden. Des Weiteren erfolgte eine Interviewstudie mit Betreibern Kritischer Infrastrukturen in der Freien Hansestadt Bremen sowie eine deutschlandweite kommunale Umfrage. Die Erkenntnisse dieser Forschungsarbeiten werden hier genutzt, um die Schließung vermuteter rechtlicher Regelungslücken anzuregen.

5.1 Einleitung

Die Gewährleistung der Cyber- und Informationssicherheit ist für staatliche Institutionen und wirtschaftlich ausgerichtete Organisationen (Unternehmen), aber auch in der Gesellschaft eine besondere Herausforderung. Cyberangriffe sind zwischenzeitlich allgegenwertig, werden qualitativ immer ausgereifter und stellen für alle Betroffenen ein enormes Risiko dar. Solche Risiken bestehen insbesondere darin, dass Produktionsabläufe gestört werden, die Kommunikation unterbunden wird, Pflegeleistungen vor allem in Krankenhäusern nicht zur Verfügung stehen oder auch öffentliche Verwaltungsleistungen nicht erbracht werden können. Die IT-Infrastrukturen aller Organisationen sind hochvernetzt, involvieren durch das Internet of Things (IoT) die Telematik z. B. für die Haustechnik und verbinden teilweise die Produktions-IT (Operative IT) in einem Gesamtnetz. Durch die Nutzung von Diensten und Infrastrukturen außerhalb der eigenen Organisation (Outsourcing) wird die Komplexität maßgeblich gesteigert. Die klassische IT-Administration wird mit quantitativen und qualitativen Anforderungen konfrontiert, die in den vergangenen Jahrzehnten so nicht bestanden. Für die IT-Verantwortlichen stellt der

[4] Der Inhalt dieses Kapitels ist bereits wie folgt veröffentlicht worden: Thomas Rehbohm und Dr. Peter Lutz Kalmbach (2021), Multimedia und Recht, MMR

hohe Integrationsgrad enorme Chancen dar, welche jedoch mit (gesteigerten) Herausforderungen und Risiken einhergehen.

Im Hinblick auf die zunehmende Digitalisierung aller Lebensbereiche sind alle Institutionen auf funktionierende informationstechnische Systeme angewiesen. Diese digitale Transformation muss sich in Prozessen niederschlagen, welche die Sicherheit der informationstechnischen Systeme im eigenen Verantwortungsbereich, insbesondere die Informations- und Kommunikationstechnik (IKT), die Operative Informationstechnik (OT) und sämtliche Interdependenzen (abhängige Zulieferleistungen) adressieren. Organisationen, unabhängig davon, ob staatlich oder als Wirtschaftsunternehmen tätig, prüfen ihre Abhängigkeit von bestimmten IT-Infrastrukturen, Anwendungen oder Diensten. Digitale Souveränität wird zunehmend eine Herausforderung in Europa und den hier tätigen Institutionen. Hersteller- bzw. Anbieterbewertungen und Notfälle (Rückfallebenen) müssen in diesem Kontext betrachtet werden. Rechtliche Anforderungen des Gesetzgebers, insbesondere in den Bereichen des Datenschutzes, der Informationssicherheit und weiterer regulatorischer Anforderungen, müssen genau wie vertragliche Regelungen mit Partnern im Fokus einer jeden Organisationen sein.

Anforderungen an eigene Arbeitsplätze haben sich, nicht erst durch die Pandemielage, wesentlich verändert. Beschäftigte aller Organisationen wollen ein hohes Maß an Flexibilität an Ort und Zeit ihrer Tätigkeit, neben den finanziellen Aspekten, um somit Gestaltungsmöglichkeiten auszuüben. Entsprechend ist die Nutzung von bestimmten technischen Ausstattungen zunehmend ein Thema für Beschäftigungsverhältnisse. Dementsprechend nehmen die Sicherheit und Verfügbarkeit von Informationstechnologie einen gewichtigen Stellenwert ein, um einen verlässlichen Gebrauch durchgehend möglich zu machen. Für ein Mindestmaß an Sicherheit muss sich in vielfacher Hinsicht der Staat in der Verantwortung sehen. Hinsichtlich der laufenden Digitalisierung aller Lebensbereiche des privaten, wirtschaftlichen und staatlichen Handelns, muss er Leitplanken aufzeigen können, auch um z. B. Cyberbedrohungen in Wirtschaftsbereichen wie Spionage und Sabotage angemessen begegnen zu können. Damit ist nicht allein gemeint, dass es selbstverständliche Aufgabe sein muss, die IT-Infrastrukturen der öffentlichen Gewalt, also des Bundes, der Länder und der Kommunen, gegen Angriffe abzusichern. Auch privatwirtschaftliche Bereiche sind von dieser staatlichen Verantwortung betroffen. Für eine kooperative Zusammenarbeit aller identifizierten Akteure müssen zudem Verwaltungs- und Unternehmensarchitekturen erforscht und entwickelt werden, die dies ermöglichen.

5.2 Wissenschaftliche Methode

Die aus der statistischen Analyse einer Kommunalumfrage beim Deutschen Landkreistag und nach qualitativer Inhaltsanalyse von Interviewstudien gewonnen empirischen Daten sollen in einem Enterprise Architecture Model (EAM) weiterverarbeitet werden. Bei den Interviewstudien wurden zum einen Infrastrukturbetreiber Bremens befragt, die

vom IT-Sicherheitsgesetz betroffen sind und zum anderen die Landesbeauftragt*innen für Informationssicherheit in den Ländern. Das EAM soll die Kollaboration einzelner Partner im Land, in Kommunen und systemrelevanten Wirtschaftsunternehmen ermöglichen. Eine Verprobung ist in der Freien Hansestadt Bremen angezeigt, da hier die entsprechenden Infrastrukturen zeitnah zu identifizieren sind. Zudem ist die Konstellation aus Landverwaltung und einer weiteren Kommune prototypisch für Flächenländer.

Die Motivation für die Erstellung eines Architekturmodells liegt in der besonderen Verantwortung des Landesgesetzgebers für die in der Region tätigen Unternehmen, den Kommunen und deren Bevölkerung. Die Ziele der systemrelevanten Unternehmen sollen dabei nicht in Widerspruch zu Anforderungen des Staates und der Daseinsvorsorge stehen. Der Vorschlag, gesetzliche Regelungen für Länder zu schaffen, erfüllt einen Teil des Induktionsprozesses für die Allgemeine Theorie.

5.3 Vorgehensweise und Diskussion – rechtliche Grundforderungen an die gesetzgeberische Gewalt

Eine effektive Cyber- und Informationssicherheit ist nur in einem Zusammenwirken von Staat, Wirtschaft und Gesellschaft denkbar. Dies liegt zum einen darin begründet, dass allein der Staat die Ressourcen – und die mitunter erforderlichen Zwangsmittel – aufbringen kann. Zum anderen ist zu beachten, dass es zu seinen Kernaufgaben gehört, für notwendigen Schutz zu sorgen – dies ist nicht zuletzt die Kehrseite seines Gewaltmonopols (H.-J. Becker, 1995, S. 2077).

Bereits das IT-Sicherheitsgesetz des Bundes (banz, 2015, S. 1324) – bzw. das BSI-Gesetz (banz, 2009, S. 2821) im Verbund mit der aus ihr hervorgegangenen Kritis-Verordnung (BSI-KritisV) nimmt Einfluss auf privatwirtschaftliche Sektoren. Dergestalt werden bestimmte Industrien und Versorgungsbereiche (sog. Kritische Infrastrukturen/KRITIS) zur Einhaltung von Standards der IT-Sicherheit verpflichtet. Der einbezogene Kreis ist jedoch auf Einrichtungen begrenzt, die für die Gesamtbevölkerung der Bundesrepublik von erheblicher Bedeutung sind. Nur indirekt sind über den überschaubaren Kreis hinaus noch Unternehmen einbezogen, die wiederum relevante Dienstleistungen für die eigentlichen Kritischen Infrastrukturen erbringen, um deren Funktionieren zu gewährleisten (Lurz et al., 2015, S. 2755). Zahlreiche Unternehmungen, die zwar ebenfalls von besonderer Relevanz für Bevölkerungsgruppen, (Metropol-)Regionen oder die staatliche Infrastruktur von Ländern und Kommunen sind, aber nicht vom BSI-Gesetz erfasst werden, bleiben außen vor. Zudem werden Interdependenzen, also Teildienstleistungen, die für eine Unternehmung von wesentlicher Bedeutung sind, nicht adressiert.

Diese Rechtslage muss gesetzgeberisch ausgebaut werden. Die hinreichende Sicherheit von IT-Systemen ist keine beliebige Angelegenheit der betreffenden Wirtschaftsakteure und es existieren bereits zahlreiche Rechtsvorschriften, die insoweit Standards in anderen Kontexten setzen. Nehmen wir als Beispiel einen Hackerangriff, der sich – egal

ob zielgerichtet oder nicht – gegen ein Unternehmen richtet: Selbstredend sind die dahinterstehenden Personen für die eintretenden Folgen verantwortlich und müssen (so man ihrer habhaft werden kann) für eingetretene Schäden haften; aber: auch die betroffene Organisation kann in der Pflicht stehen! Wer Dienste und Waren für andere anbietet, ist regelmäßig Rechtspflichten unterworfen. Er muss sich als zuverlässig erweisen und ganz allgemein so verhalten, dass andere nicht in Mitleidenschaft gezogen werden. Dies ist zivilrechtlich über Schadensersatzvorschriften abgesichert, insbesondere über solche des Vertrags- (z. B. §§ 241, 280 BGB), aber auch des Deliktsrechts (z. B. § 823 Abs. 1 BGB). Hier können Verhaltensweisen in Rede stehen, die anhand von Fahrlässigkeitsmaßstäben zu bewerten sind (vgl. § 276 Abs. 1, 2 BGB) – auch durch Formen des Unterlassens gebotener Handlungen (BGHNJW 1953, 700).

Außerdem wirken gesetzlich gefasste Berufspflichten ein. Insoweit ist bei diesem Gesichtspunkt bereits der Übergang zum Verwaltungsrecht vorhanden, welches gleich mehrere Kernbereiche bereithält, die Bezug zur IT-Sicherheit haben. Beispielhaft sei angeführt: Der fahrlässige Umgang mit sensiblen Daten kann gewerberechtliche oder datenschutzrechtliche Konsequenzen haben. Mitunter können Bußgeldtatbestände betroffen sein. Der fahrlässige Umgang mit IT-Infrastrukturen muss jedoch im Verwaltungsrecht stärker verankert werden. Ausgangspunkt ist dabei nicht zuletzt die Frage, inwieweit Akteure, die Vorteile der Digitalisierung nutzen, durch Nachlässigkeiten Gefahren für Dritte hervorrufen. Dergestalt sind die bisherigen Regelungen auszubauen und zu erweitern, um bestmöglichen Schutz für die Bevölkerung zu gewährleisten.

Ein Blick auf grundlegende verfassungs- und staatsrechtliche Bestimmungen unterstreicht diese Forderungen: Art. 1 GG legt das Grundverständnis des bundesrepublikanischen Staates wie auch des Miteinanders in der Gesellschaft fest – und damit auch die rechtliche Grundordnung. Demnach steht der (einzelne) Mensch im Zentrum der staatlichen Aufgaben (vgl. BVerfGE 61, 82 (100)). Fasst man diesen Auftrag weiter, dann ist es die Aufgabe des Staatswesens, das Gemeinwohl zu fördern (Axer et al., 2007, S. 4–79). Anders ausgedrückt, gewährleistet es Schutz – und zwar der Grundrechte wie auch der Gemeinschaftsrechtsgüter (Degenhart, 2007, S. 3–131); (Birkenmaier & Butzer, 2018, Nummer 140 ff.). Im Fokus staatlicher Fürsorge stehen entsprechend Werte, wie das Recht auf Leben, auf körperliche Unversehrtheit (auch: individuelle Gesundheit), die Volksgesundheit, Funktionsfähigkeit von Verwaltung und Rechtspflege, das Zusammenleben im Gemeinwesen schlechthin usw.

Der Staat darf entsprechend drohenden Gefahren nicht schlichtweg abwartend gegenüberstehen, sondern muss aktiv werden, um Schlimmstes zu verhindern – dies entspricht dem sog. Untermaßverbot, dass einem Zuwenig an staatlichen Bemühungen entgegenwirkt (vgl. BVerfGE 88, 203 (254); vgl. BVerfG NVwZ 2009, 1489 (1490); (Sodan, 2009, S. 545)). Gleichwohl darf seine Reaktion nicht etwa zu heftig, also unverhältnismäßig, ausfallen, was als Verbot des Übermaßes umschrieben werden kann (vgl. BVer-

fGE 8, 71 (80); 20, 351 (361)). Der wichtigste Schritt ist dabei die Schaffung von gesetzlichen Regeln, denn ohne Rechtsgrundlagen kann die Exekutive nicht tätig werden (vgl. BVerfGE 40, 237 (248 f.); 49, 89 (126)).

Die zu regelnden Sachverhalte sind als Teil des allgemeinen Gefahrenabwehrrechts zu deuten, welches grundsätzlich in die Kompetenz der Länder fällt (vgl. Art. 30 und Art. 70 ff. GG). Es gilt also, die bestehenden Regeln des Bundesrechts, also des BSI-Gesetzes/der KritisV zu ergänzen, um den staatlichen Schutzauftrag auch hinsichtlich des Bundesstaatsprinzips (Art. 20 Abs. 1 GG) zu vollenden.

Um dieses Ziel zu erreichen, reicht es nicht aus, allein öffentliche Einrichtungen – deren Funktionsfähigkeit übrigens ein kollektives Rechtsgut ist – einer gesetzlich festgelegten adäquaten IT-Sicherheitsstrategie zu unterwerfen. Auch jene Teile der Privatwirtschaft, deren Dienstleistungen eine elementare Grundversorgung der Menschen sicherstellen und dergestalt besonderes Vertrauen in Anspruch nehmen, müssen einheitlich in die Pflicht genommen werden.

Nehmen wir ein einfaches Beispiel:

> Es sei erinnert, dass im November 2018 ca. 450 PCs des Klinikums Fürstenbruck/Bayern unbenutzbar wurden, nachdem ein mit Schadsoftware infizierter E-Mail-Anhang geöffnet worden war (vgl. Bundeskriminalamt, Bundeslagebild Cybercrime, 2019, S. 21); im Klinikum Düsseldorf starb eine Patientin, nachdem Erpresser die örtlichen IT-Systeme ausgeschaltet hatten (vgl. Hackerangriff auf Krankenhaus, Süddeutsche Zeitung v. 18.9.2020, S. 10).

*Ein Krankenhaus mit einer Kapazität von 500 Betten wird durch einen Hackerangriff lahmgelegt. In kurzer Zeit ist der Zugriff auf Daten ebenso unmöglich wie der Gebrauch sämtlicher Kommunikationsmittel, die über IT-Infrastrukturen genutzt werden. Kurzum: Bis auf Einzelfälle, die mit den manuellen Fähigkeiten von Mediziner*innen erledigt werden können, sind die technikunterstützten ärztlichen Dienstleistungen weitgehend unmöglich geworden. In der Folge müssen Operationen verschoben werden, Handlungsspielräume sind verengt, weil der Zugriff auf digitalisierte Akten unmöglich ist usw.*

Es liegt auf der Hand, dass Menschen zu Schaden kommen und Gesundheitsbeeinträchtigungen eintreten werden. Es handelt sich insofern stets um Körperverletzungen. Wenn darüber hinaus operative Eingriffe, Transplantationen oder Notfallbehandlungen undurchführbar gemacht, erschwert oder verzögert werden, dann sind auch Lebensgefahren und tödliche Verläufe wahrscheinlich.

Zwar kann man die zweifelsohne vorhandene Schuld bei jenen suchen, die als Hacker verantwortlich für dieses Szenario sind. Aber dies kann nur auf den ersten Blick rechtlich zufriedenstellen. Gestützt wird dieser Gedanke durch die im deutschen Recht geltende Bedingungstheorie. Danach gilt, dass sich jeder Schaden zurechnen lassen muss, wenn man selbst eine Bedingung für deren Eintritt gesetzt hat (vgl. BGHSt 1, 332 (333); 2, 20

(24)). Dies gilt auch für Zusammenwirken mehrerer Ursachen (Ambos & Radtke, 2017, S. 342).

Es drängt sich zudem die Frage auf, ob dies mittels naheliegender Maßnahmen durch die betroffenen Unternehmen zu verhindern gewesen wäre. D. h. auch die Dienstleister tragen Mitverantwortung für jene Verbraucher*innen und Nutzer*innen, die abhängig von der Versorgung sind. Es muss entsprechend ein akzeptabler Schutz vorgehalten werden, denn: Wer die Vorteile der Digitalisierung für die Profitmaximierung nutzt, muss andererseits mit Bedrohungen durch Schadsoftware rechnen. Zwar kann man hier auf bereits vorhandene Rechtsregeln verweisen und z. B. Schadensersatzmöglichkeiten benennen. In drastischen Fällen wäre sogar ein Verweis auf das Strafrecht möglich, sollte sich herausstellen, dass jemand – oder hier im o.g. Beispiel möglicherweise der Krankenhausträger – seine Informationstechnik unzureichend gesichert hat: Es könnte möglicherweise ein Fall des strafbaren Unterlassens vorliegen (vgl. § 13 Abs. 1 StGB), der auch durch unabsichtliches, sprich fahrlässiges (vgl. § 15 StGB), Verhalten eintreten kann. Diese strenge Geltung liegt darin begründet, dass manche Personen als sog. Garanten für andere – etwa ihre Kund*innen, Patient*innen, sonstig Anvertraute – eine besondere Fürsorge (z. B. weil sie Verträge geschlossen haben) übernehmen, sodass sie jedenfalls keinen abwendbaren Schaden erleiden (vgl. BGHSt 19, 286 (289) (291); 38, 388 (390); BGH NJW 1961, 2068).

Der Staat, also der Bund oder ein einzelnes Land, darf jedoch nicht abwarten, ob im äußersten Fall ein strafbewehrter Sachverhalt vorliegt. Hier muss das Verwaltungsrecht greifen (in der Form des sog. Ordnungsrechts) und das Gefüge des Rechtssystems durch präventive Regelungen absichern. Es gilt mithin, in den Ländern ausreichende und effektive gesetzliche Vorschiften zu schaffen, die es möglich machen, jedenfalls vorhersehbaren Gefahren frühzeitig zu begegnen und nötigenfalls privatwirtschaftlich agierende Akteure zu einem Mindestmaß an Schutz zu verpflichten. Die Polizeigesetze reichen dafür nicht aus. Demnach erfordert nicht nur der regelmäßige erhebliche wirtschaftliche Schaden (Es sei allgemein darauf verwiesen, dass durch Schadsoftware im Zeitraum 2015-16 in Deutschland Schäden in Höhe von ca. 100 Milliarden Euro verursacht worden sind, (Brisch & Rexin, 2019, S. 606–616)) ein strukturiertes und wirksames Eingreifen, sondern auch die darüberhinausgehenden erwartbaren extremen Schäden an höchsten Verfassungsrechtsgütern, die Menschen und Gesellschaft zustehen. Das Ordnungsrecht – zu dem man auch das Ordnungswidrigkeitenrecht zählen kann – soll konkrete Gefahren (also die verdichtete Wahrscheinlichkeit eines Schadenseintritts) und sogar abstrakte Gefahren (die „nur“ hinreichende Wahrscheinlichkeit, dass Schäden eintreten) abwehren.

5.4 Schlussfolgerung

Entsprechend sind jene, die Dienstleistungen oder Waren anbieten, welche elementar wichtig für große Teile der Bevölkerung, aber vielleicht auch nur für einzelne Menschen,

sind, also die Träger der Daseinsfürsorge, als maßgebliche Akteure per Gesetz und nötigenfalls per Verwaltungsakt zu identifizieren und in die Pflicht zu nehmen.

Wie im Einzelnen Verpflichtungen für private Träger der Daseinsvorsorge und die staatlichen Organe formuliert sein sollten, wie weit Ermächtigungen zur Kontrolle und zum Ergreifen von Maßnahmen – oder auch Sanktionen – gehen sollen, ist eine Frage des gesetzgeberischen Ermessens (Kalmbach, 2018, S. 386–388). Aber: dieses Ermessen ist nicht grenzenlos, sondern an Notwendigkeiten gebunden (vgl. zum Folgenden BVerfGE 39, 2 (42); 88, 203 (354)). Daher müssen die Maßnahmen unbedingt effektiv sein. Die Verwaltung muss ausreichend handlungsfähig gemacht werden, um den Schutz im besten Fall dort wirken zu lassen, bevor eine Gefahr auch nur konkret wird; er muss aber spätestens dann wirken, wenn sich die Gefahr in einem gegenwärtigen Angriff zeigt und sich als gemeine Gefahr darstellt. Die Bürger*innen haben einen Anspruch auf das Funktionieren einer ausreichenden Daseinsfürsorge und auf umfangreichen Schutz vor vermeidbaren Schäden durch mangelnde IT-Sicherheit.

Idealerweise fügen sich die Regelungen zur IT-Sicherheit an die bisher bestehenden anverwandten Bereiche des Ordnungsrechts an, um einen lückenlosen Grundrechtsschutz zu gewährleisten. Dergestalt würde selbst im Falle einer durch Hacks oder allzu sorglosen Umgang mit Spam-E-Mails ausgelösten erheblichen Cyber-Gefahrenlage, die sich vielleicht sogar zu einer epidemischen Lage steigert, dass Ordnungsrecht alle Ermächtigungen vorhalten, die erforderlich sind. Dann ist IT-Sicherheitsrecht eine sinnvolle Ergänzung von Polizei-, Feuerwehr-, Gewerbe- und sogar Katastrophenschutzrecht. Eine in sich stimmige Sicherheitsarchitektur sollte zudem ihren präventiven Charakter stärken, indem digitalisierte Unternehmensprozesse nachhaltig befördert werden. Dies kann über den Betrieb von Wissensplattformen geschehen oder auch durch Arbeitsgruppen, die ihre Mitglieder ertüchtigen, um einen guten Stand der IT-Sicherheitstechnik zu gewährleisten.

6 IT-Sicherheitsrecht der (Bundes) Länder[5]

IT-Sicherheit ist ein umfassendes und – vor allem mittlerweile – rechtliches Themenfeld mit immenser Wirkung auf Staat, Wirtschaft und Gesellschaft. Die Nützlichkeit und Unverzichtbarkeit von moderner Informationstechnologie geht einher mit ihrer Verwundbarkeit. Daher sind die IT-Systeme insbesondere in ihrer Verfügbarkeit und Datensicherheit in der Art zu gestalten, dass sie als Teil der Wertschöpfungskette durchgehend erhalten bleiben.

Diese Aufgabe ist insbesondere im Kontext verfassungsrechtlicher Grundforderungen zu sehen. Hier werden Vorteile zukunftsweisender Technologien gepaart mit Pflichten, die in erster Linie durch den Staat umgesetzt und – jedenfalls in Teilen – regelrecht garantiert werden müssen, denn er ist verantwortlich für elementare Versorgungsleistungen sowie für die Gewährleistung eines ausreichenden Maßes an Sicherheit für die Allgemeinheit wie auch für einzelne Grundrechtsträger

Die dazu notwendigen gesetzgeberischen Anstrengungen erschöpfen sich weder durch Erlass von Verordnungen und Richtlinien auf europäischer Ebene noch durch entsprechendes Tätigwerden des Bundestages (und durch Rechtsverordnungen auf ministerieller Stufe). Die (Bundes-)Länder und die Kommunen sind ebenso Teil dieser geforderten Sicherheitsarchitektur.

Es muss konstatiert werden, dass der bislang stattgefundene Kodifizierungsprozess nicht ausreichend ist, um erforderliche Architekturen vorzuhalten, die der Exekutive diejenigen Handlungsoptionen bereitstellen, um diesen Schutz vor Gefahren gegen die Funktionsfähigkeit von IT-Systemen, die der öffentlichen Gewalt sowie der Grundversorgung der Bevölkerung dienen, zu garantieren: Nicht alle Länder haben bisher zielführende Gesetze erlassen, und diese wiederum haben zuvorderst die Sicherheit der eigenen Landesnetze und damit die Sicherheit der Landesbehörden adressiert. Insbesondere die Inpflichtnahme von Trägern der Daseinsvorsorge (hier vor allem jene, die halbstaatlich oder privatrechtlich organisiert sind) und von kommunalen Strukturen hat nur unzureichend Eingang in diesen Regelungsbereich gefunden.

6.1 Kompetenzgefüge der IT-Sicherheit in Bund und Ländern

6.1.1 Öffentliche Sicherheit

Funktionell verstanden ist IT-Sicherheit ein technischer Aspekt. Versteht man sie jedoch umfassend und bezieht sie auf die Lebens- und Rechtsrealität, dann ist sie notwendige Voraussetzung für eine erfolgreiche Digitalisierung (Lühr, 2020, S. 46) – und fügt sich entsprechend in den verfassungsmäßigen Rahmen ein.

[5] Der Inhalt dieses Kapitels ist bereits wie folgt veröffentlicht worden: Thomas Rehbohm und Dr. Peter Lutz Kalmbach (2020), Buchkapitel 15 C in Cybersecurity Kipker/Barudi

„Die Digitalisierung schlechthin ist wegen ihrer allumfassenden Einwirkung auf Gesellschaft und Wirtschaft eine Angelegenheit aller staatlichen Ebenen, von Gesetzgebung über Verwaltung zu Rechtsprechung (Schliesky, 2016, S. 12)*.“*

IT-Sicherheit ist insoweit rechtlich geboten und Bestandteil der öffentlichen Sicherheit. Außerdem ist sie maßgebliche Voraussetzung für die Funktionsfähigkeit der staatlichen Organisationen.

Die Gestaltung, Aufrechterhaltung und Durchsetzung der öffentlichen Sicherheit ist eine (gesamt-) staatliche Aufgabe (vgl. zum Folgenden BVerfGE 49, 24 (56 f.). Dies wird vor allem durch Gesetze sowie deren Vollzug mittels Behörden gewährleistet.

Diese weit gefasste Definition von IT-Sicherheit liegt in der allumfassenden Wirkung des Verfassungsrechts begründet: Die im Grundgesetz explizit genannten oder aus ihm heraus gedeuteten Wertvorstellungen bilden die höchsten Prinzipien der bundesdeutschen Rechtsordnung (Benda et al., 2012, S. 127). Sie werden damit auch Teil der Staatsziele (Schladebach, 2018, S. 118).

Der Schutzauftrag des Staates wird aus mehreren Grundüberlegungen gespeist: Vor allem werden über Art. 1 Abs. 1 S. 2 GG der Mensch und seine schutzwürdigen Bedürfnisse in den Mittelpunkt staatlichen Handelns gerückt. Hieraus zieht der Staat überhaupt erst seine Existenzberechtigung (vgl. BVerfGE 61, 82 (100)). Art. 1 Abs. 3 GG verpflichtet den Staat insoweit, die Grundrechte der Menschen zu bewahren. Sie sind folglich mit staatlicher Macht zu schützen (Birkenmaier & Butzer, 2018, Nummer 140). Dies wird auch durch Art. 20 Abs. 3 GG betont, indem die staatlichen Institutionen – angefangen bei der Gesetzgebung – die Rechtsordnung, insbesondere die verfassungsmäßig garantierten Bürger- und Menschenrechte, zu wahren haben.

Hier spielt auch das Gewaltmonopol des Staates hinein: Allein der Staat ist befugt, Zwangs- oder gar Gewaltmaßnahmen einzusetzen, um dem Recht Geltung zu verschaffen (H.-J. Becker, 1995, S. 2077). Auch insoweit ist er verpflichtet, die öffentliche Sicherheit zu garantieren. Dies ist zumal dadurch zu gewährleisten, dass der Staat aktiv werden muss; ein Abwarten oder gar Aussitzen wäre nicht verfassungskonform (Sodan, 2009, S. 545). Ein Nichtstun oder auch nur ein Zuwenig an zu erwartender Initiative des Staates würde dem Ignorieren verfassungsmäßiger Gebote gleichkommen und so einen Verstoß gegen das vom BVerfG festgelegte Untermaßverbot bedeuten (vgl. BVerfGE 88, 203 (254); BVerfG NVwZ 2009, 1489 (1490)). Insoweit zu befürchtenden Schäden für Rechte und Rechtsgüter wäre nicht erst bei einer gegenwärtigen Gefahr zu begegnen (vgl. zum Folgenden BVerfGE 56, 54 (74 ff.); BVerwG NVwZ 2012, 757 (759)). Stattdessen hat der Staat als fürsorgende Instanz Risiken in einem weitläufigen Sinne zu erkennen und diese aktiv anzugehen. Eine effektive Gefahrenabwehr ist demnach Richtschnur staatlichen Handelns (vgl. BVerfGE 46, 160 (164 f.)).

Ausfluss aus dieser Verantwortung ist eine Pflichtenstellung, die je nach Betroffenheit des jeweiligen Rechts, Rechtsguts oder der jeweiligen gesetzlichen Regelung zu einer sog. „Garantenstellung“ führt, die im schlimmsten Fall in § 13 StGB ein Einschreiten

staatlicher Institutionen zur strafbewehrten Notwendigkeit macht (Fischer et al., 2021, Nummer 29).

6.1.2 IT-Sicherheit als staatsverwaltende und gefahrenabwehrrechtliche Forderung

Cyberangriffe auf die IT-Sicherheit von beliebigen Entitäten sind gerichtet oder ungerichtet und adressieren Staat, Wirtschaft und Gesellschaft gleichermaßen. Die Regelungen zur IT-Sicherheit allein der Europäischen Union oder dem Bund zu überlassen greift zu kurz. Im Föderalsystem Deutschlands steht den Ländern ein Gestaltungsauftrag zu.

Die Deutungshoheit des Erfassungsbereichs staatlicher Strukturen auf Landes- und Kommunalebene, die im weitesten Sinne eine Daseinsvorsorge für Bürger leisten, liegt auch bei den Ländern. Die Verwaltungsgliederung in Deutschland und insbesondere in den Ländern darf für die Erhöhung der IT-Resilienz kein Hinderungsgrund sein. Aus Sicht der Länder ist dabei unerheblich, ob an einem wirtschaftlich ausgerichteten Unternehmen eine Majorität, Minorität oder keine Beteiligung eines Landes oder einer Kommune – zum Beispiel an Versorgungsdienstleistern in der Region –besteht. Die Länder müssen Rahmenbedingungen schaffen, die eine technische, politische und strategisch/operative Kollaboration ermöglichen. Rechtlich belastbare und für die betroffenen Versorger Klarheit bietende Bedingungen sind für diese Zusammenarbeit förderlich. Es handelt sich um eine gesellschaftspolitische Aufgabe aller staatlichen Organisationen in EU und Bund, vor allem aber auch in den Ländern und den kommunalen Strukturen. Eine ausschließliche Regelungskompetenz des Bundes in Bezug auf kritische Infrastrukturen ist weder haltbar noch in der Sache zielführend.

Die von den Ländern eingeforderte stärkere Beteiligung bei der Ausgestaltung des IT-Sicherheitsgesetzes wurde vom Bund nur unzureichend berücksichtigt (Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, 2021). Nicht nur der zeitliche Rahmen der Länderbeteiligung war zu kurz bemessen, sondern wurden auch die inhaltlichen Änderungswünsche nur rudimentär berücksichtigt.

Die Länder haben z. B. beim Thema Informationspflichten durch den Bund, abgestimmte Anträge eingebracht, welche in der Länderoffenen Arbeitsgruppe Cybersichersicherheit (LAG CS) erarbeitet wurden. Die LAG CS ist bei der Innenministerkonferenz etabliert worden und wird vom Hessischen Ministerium des Innern und für Sport geleitet.

Keine Berücksichtigung fand z. B. die Forderung nach Unterrichtungspflichten der Länder, bei Vorfällen in Kritischen Infrastrukturen, welche vom IT-Sicherheitsgesetz betroffen sind. Gefahrenabwehrmaßnahmen, Risikobewertungen oder vorbereitende Handlungen sind somit ungleich schwerer in der betroffenen Region (dem Land) zu koordinieren.

Ein anschauliches Beispiel ist in diesem Zusammenhang die Trinkwasserversorgung. Vom IT-Sicherheitsgesetz betroffen sind aufgrund ihrer Größe weniger als ein Prozent

der anbietenden Unternehmen. Auch wenn Schwellenwerte in einer Neufassung der BSI-KritisV (BSI-KritisV Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz, 2016) nach unten korrigiert oder weit flexibler gehandhabt werden könnten, ist nicht von einer umfänglichen Resilienz auszugehen, die die Versorgung ganzheitlich sicherstellt. Eine quantitative Vorgehensweise bei der Identifikation Kritischer Infrastrukturen hinterlässt Lücken in der Sicherheitsarchitektur. Vielmehr müssen hier die Länder und Kommunen zusammen mit ihren Daseinsvorsorgeträgern interagieren, ggf. auf freiwilliger oder vorzugsweise auf rechtlicher Basis.

Für die konkrete Verortung der IT-Sicherheit auf nationaler Ebene muss beachtet werden, dass Deutschland dem föderalistischen Prinzip folgt. Der Gesamtstaat besteht folglich auch aus den Ländern als Gliedstaaten (vertikale Gewaltenteilung, vgl. BVerfGE 13, 54 (77)). Die staatlichen Kernaufgaben (zuvorderst: Schutz der Grundrechte (Sodan, 2009, S. 545)) jedoch sind nicht teilbar (vgl. etwa BVerfGE 13, 54 (76 f.)). Die Aufgliederung in Bund und Länder wie auch in Legislative, Exekutive und Judikative (horizontale Gewaltenteilung) sind lediglich einer ausgleichenden und mäßigenden Machtverteilung geschuldet (Jarass et al., 2020), sie dürfen aber nicht einer nachlässigen Wahrnehmung staatlicher Aufgaben Vorschub leisten.

Die föderalen Prinzipien werden seitens des Bundes bei der IT-Sicherheit im Portalverbund aufgrund der Regelungen „im Benehmen mit dem IT-Planungsrat durch Rechtsverordnung ohne Zustimmung des Bundesrates“ im Onlinezugangsgesetzes (OZG) durchbrochen.

Mit dem vorliegenden Entwurf einer Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten (IT-Sicherheitsverordnung Portalverbund) – PVV, zum §5 des OZG, wird die Interpretation genutzter IT-Infrastrukturen in der gesamten Verwaltungsgliederung in die Deutungshoheit des Bundes gegeben.

Länder und Kommunen werden zu umfänglichen Maßnahmen einer nicht abschließend bestimmbaren Anzahl von Infrastrukturkomponenten verpflichtet. Solche Komponenten sind im weitesten Sinne mit dem Internet verbunden und leisten einen Beitrag zu Onlinediensten. Dies betrifft Fachanwendungen, IT-Komponenten oder auch IT-Dienstleister gleichfalls und verpflichtet diese zum BSI-Grundschutz. Allgemeine Kernkomponenten des Portalverbundes wie Servicekonten, Elektronische Identitäten und Vertrauensdienste sind hingegen bestimmbar.

IT-Sicherheit ist damit eine Anforderung, die der Staat auf allen Ebenen wahrnehmen muss. Grds. wird diese Aufgabenwahrnehmung nicht durch die vorgesehenen unterschiedlichen Staatsebenen durchbrochen. Ob IT-Sicherheit eine zuvorderst bundesstaatliche Aufgabe oder Angelegenheit der Länder ist, steht daher nicht im Vordergrund. Durch die Aufteilung der Gesetzgebungskompetenz wird jedoch in erster Linie eine Verantwortung der Länder begründet.

IT-Sicherheit zielt rechtlich betrachtet auf zwei Bereiche ab: Erstens auf die Sicherung des staatlichen Sektors und zweitens auf jene der Zivilgesellschaft. Ersteres ist eine ureigene staatliche Aufgabe, da es um die Funktionsfähigkeit des Staates bzw. seiner Institutionen geht (vgl. BVerfGE 30, 1 (18); 100, 24 (54)). Die Umsetzung dieses Schutzauftrages ist nach dem Prinzip der Bundesstaatlichkeit anzugehen. Das IT-Sicherheitsgesetz des Bundes ist demnach ein relevanter Ausgangspunkt und die dortigen Regelungen sind ein gewichtiger Teil der gesamtstaatlichen IT-Sicherheitsinfrastruktur. Jedoch kann sich die Reichweite bundesgesetzlicher Regelungen nur auf Einrichtungen der öffentlichen Gewalt des Bundes beziehen.

Die Länder müssen demnach für die Sicherung ihrer Gewalten selbst aufkommen und können hierfür entsprechend Landesgesetze erlassen. Der zweite Bereich – die Sicherung von Grundrechten mit Mitteln der Eingriffsverwaltung – ist als besonderer Teil der öffentlichen Sicherheit (hier: Gefahrenabwehr) eine Angelegenheit, die in erster Linie Sache der Länder ist, da es sich um eine iwS polizeiliche Aufgabe handelt.

6.1.3 Sicherung staatlicher Strukturen

Soweit staatliche Pflichten betroffen sind, handelt es sich zuvorderst um den Schutz kollektiver Rechtsgüter, insbesondere geht es um die Funktionsfähigkeit des Staates schlechthin. Darüber hinaus werden damit zusammenhängende grundrechtliche Belange gewahrt, insb. das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 iVm Art 1 Abs. 1 GG, vgl. zu diesem neuen Grundrecht BVerfGE 120, 274 (302)), zudem liegt insoweit ein Schwerpunkt auf der Gewährleistung des Telekommunikationsgeheimnisses (Art. 10 Abs. 1 GG, vgl. BVerfGE 106, 28 (35-37). Zusammengefasst ist insoweit der umfangreiche Schutz von Daten der Bürgerinnen und Bürger, die mit staatlichen Stellen kommunizieren oder von ihrer Datenverarbeitung erfasst sind, zu garantieren. Dabei geht es nicht um die typische Ausrichtung der Grundrechte im Sinne einer Abwehrfunktion gegenüber dem Staat, sondern um die Aufgabe des Staates, auch Schutz vor An- und Zugriffen durch Dritte zu gewährleisten.

6.1.4 Sicherung der Zivilgesellschaft (Daseinsvorsorge)

Bei der Bewahrung privatrechtlicher Belange der IT-Sicherheit ist Ausgangspunkt, dass Beeinträchtigungen nicht immer als singulärer Schaden eintreten, denn häufig können auch weitere Personen in Mitleidenschaft gezogen werden. Nicht zuletzt ist hier auch ein direkter Bezug zu strafbaren Handlungen zu berücksichtigen.

IT-sicherheitsrechtliche Pflichten müssen demnach auch in die Zivilgesellschaft hinein Berücksichtigung finden, vor allem dann, wenn es um unternehmerische Leistungen geht, die derart für die Grundversorgung bedeutsam sind, dass die entsprechenden Unternehmen als Träger der Daseinsvorsorge zu begreifen sind (um eine Abgrenzung zu den Regelungen auf Bundesebene vorzunehmen, wird hier der Begriff der Kritischen

Infrastruktur vermieden, da dieser durch quantitative Maßstäbe geprägt ist.) Die hier vorgenommene Erweiterung der gesetzgeberischen Handlungspflicht fußt auf der Überzeugung, dass die Wahl eines qualitativen Ansatzes zielführend und notwendig ist. Dergestalt kann es bei solchen Leistungen nicht darauf ankommen, wie viele Menschen von potenziellen Gefährdungen der IT-Sicherheit betroffen sein können, sondern wie intensiv der zu befürchtende Schaden ist.

Vorsätzliche Beeinträchtigungen der IT-Sicherheit stellen häufig zugleich Straftaten („Cybercrime“) dar: Davon umfasst sind Handlungen, die sich entweder gegen Datennetze sowie informationstechnische Systeme richten oder bei denen Straftaten mittels der Informationstechnik oder des Internets begangen werden (Wernert, 2021, S. 34).

Das Strafrecht greift dort, wo elementarste Grundforderungen durch den Staat mit äußersten Mitteln gewährleistet werden müssen, also auch durch Kriminalstrafen (vgl. Sachs Art. 74, Rn. 11; BVerfGE 39, 1 (46 f.); 120, 224 (240)). Das Strafrecht ist gem. Art. 74 Abs. 1 Nr. 1 GG als Teil der konkurrierenden Gesetzgebung weitgehend Bundesmaterie. Die Bekämpfung von Straftaten wiederum ist eine gesamtstaatliche Angelegenheit. Gemeint sind insoweit die Verfolgung von Straftaten, was zuvorderst eine rein polizeilich-staatsanwaltschaftliche wie auch gerichtliche Tätigkeit umfasst, aber auch vorbeugendes (präventives) Handeln. Tendenziell ist letzteres noch entscheidender und im Wesentlichen eine behördliche Angelegenheit, insbesondere der Ordnungs- bzw. Eingriffsverwaltung. Allerdings liegt der Schwerpunkt der Kompetenz, Straftaten zu verhüten, bei den Ländern (vgl. BVerfGE 113, 348 (368); BVerwG NVwZ 2012, 757 (759)). Hier sind im Rahmen präventiver Gegenmaßnahmen sowohl verwaltungsrechtliche Eingriffskompetenzen auf gesetzlicher Ebene bereitzuhalten wie auch entsprechende Gefahrenabwehrbehörden vorzuhalten. IT-Sicherheit sollte dergestalt als Untergliederung des Ordnungsrechts verstanden und somit als Teil der Sicherheitsarchitektur gesehen werden, die angefangen beim Polizeirecht zahlreiche weitere Kodifikationen bereithält, um umfassende Sicherheit für Bürger zu garantieren (vgl. die Polizeigesetze der Länder, aber auch beispw. das Gewerberecht, die gesetzlichen Grundlagen der Berufsgenossenschaften oder auch das Recht anderer Aufsichtsbehörden, wie etwa für Krankenhäuser, Apotheken etc. Im Gegensatz zur Leistungs- und Abgabenverwaltung sind für die Ordnungsverwaltung die Verwaltungsverfahrensgesetze der Länder maßgeblich, um das eigene Handeln auch formellrechtlich abzusichern.). Sinnvollerweise schließen die entsprechenden landesgesetzlichen Regelungen an jene an, die durch den Bund – insbesondere über das IT-Sicherheitsgesetz – vorgehalten werden, um auch im Rahmen der vertikalen Gewaltenteilung nahtlosen Schutz zu ermöglichen.

Die strafrechtliche Relevanz von IT-Sicherheit geht über die typischen Cyber-Straftaten hinaus – wie etwa Spionage, Urheberrechtsverletzungen oder Mobbing: Entscheidend ist vielmehr die Frage der Ursache bzw. der Kausalität von Fehlverhalten (vgl. BGHSt 1, 332 (333); 2, 20 (24)). Wer beispielsweise durch einen Angriff eine IT-gestützte Infrastruktur lahmlegt – möglicherweise nur aus dem Motiv heraus, sein technisches Können unter Beweis zu stellen – ist für die weiteren Folgen verantwortlich, soweit diese (auch

nur abstrakt) absehbar sind. Erleiden dementsprechend Patienten eines Krankenhauses einen Gesundheitsschaden oder kommt es gar zum Tode von Patienten, nachdem die für Behandlungen relevante Technik manipuliert wurde, ist der Täter für ein Tötungsdelikt verantwortlich. Im Angesicht der Tatsache, dass für jeden verständigen Menschen die Wirkungen seines Tuns abschätzbar sind, dürfte dabei häufig sogar vorsätzliches Handeln anzunehmen sein (Vorsatz liegt etwa vor, wenn jemand sicher voraussieht, dass sein Handeln einen bestimmten Schaden verursachen wird. Ob dieser als unangenehm empfunden wird, ist insoweit unerheblich, vgl. RGSt 5, 314 (317)).

Es geht bei der Daseinsvorsorge somit explizit nicht um die Verhinderung jeder möglichen Cyber-Straftat, sondern um die Gewährleistung eines wirksamen Schutzes vor schwersten Folgen für Einzelne sowie um absehbare Gefahren für die Gesamtbevölkerung oder jedenfalls für erhebliche Teile der Bevölkerung. Im Fokus der Entwicklung stehen die systemrelevanten – in den Ländern auch „Sub-Kritis“ genannten – Träger der Daseinsvorsorge. Damit sind jene Dienstleister gemeint, die in erheblicher Weise durch staatlichen Auftrag (Berg, 2021, S. 699) oder im Sinne einer gewinnorientierten und vertragsbasierten Leistung für die Grundversorgung der Bürger einstehen. Das bedeutet: Wer gegen Entgelt lebensnotwendige Dienste oder Sachleistungen erbringt (etwa Versorgung mit Trinkwasser, Strom, Medikamenten usw., aber auch die Möglichkeit der Unterbringung von Kranken, die Aufrechterhaltung des Transport- und Flugverkehrs etc.), muss im Sinne eines erträglichen und nachvollziehbaren Mindestschutzes auch dafür Sorge tragen, dass die Versorgung nicht durch vermeidbare Schäden an der eigenen IT-Infrastruktur ausbleibt.

Eine solche Anforderung sollte Einzug in die IT-Sicherheitsgesetzgebung aller Länder finden, da die bisherige Rechtslage diese Eindeutigkeit missen lässt. Dabei wäre eine solche Anforderung weder eine revolutionäre Neuerung noch eine Verschärfung der bisherigen Rechtslage: Sie würde sich letztlich an den ohnehin bestehenden Sorgfaltspflichten orientieren, die bereits jetzt im Sinne von Straf-, Schadensersatz- oder auch berufsrechtlichen Vorschriften bestünden und sich auf der Ebene von Vorsatz- und Fahrlässigkeitsmaßstäben widerspiegeln.

Dem immensen Schadenspotenzial, das Gefahren für die IT-Sicherheit innewohnt und spiegelbildlich die Verletzung von einschlägigen Straftatbeständen bedeuten kann, ist durch Eingriffsbefugnisse entgegenzuwirken, die den zuständigen Exekutivorganen entsprechend Handlungsfähigkeit geben. Nötigenfalls kann dies bereits jetzt umfangreich über polizeiliche Generalklauseln erfolgen – ist dann aber auf jene Behörden beschränkt, die durch diese Gesetze legitimiert sind. Rechtlich schwieriger, aber durchaus möglich wäre zudem die Handhabe nach Notstandsrechten: Insbes. das StGB hält sog. Rechtfertigungstatbestände vor, die es erlauben, bei Angriffen gegen Grundrechte oder Gefahren für Grundrechte und Kollektivrechtsgüter notwendige Abwehrmaßnahmen zu ergreifen. Hier ist v. a. auf § 34 StGB abzustellen, aber ggf. auch auf § 32 StGB (hier: Nothilfe bei Angriffen gegen Dritte). Problematisch ist jedoch, dass solche Sonderrechte tendenziell für Bürger vorgehalten sind, die diese nutzen dürfen, wenn staatliche Hilfe

nicht erreichbar ist. Im Kontext des staatlichen Schutz- und Fürsorgeauftrags ist es im Einzelfall auch Staatsdienern erlaubt, auf sie zurückzugreifen (vgl. BGHSt 31, 304, 307; auch 27, 260, 263; Fischer, § 34, Rn. 34). Das praktische Problem liegt eben darin begründet, dass es sich um einen Notbehelf handelt, bei dem die Akteure in den entscheidenden Situationen sich voraussichtlich auch nicht stets sicher sein werden, ob sie sich darauf berufen dürfen.

Es sollte aber bedacht werden, dass solche gefahrenabwehrrechtlichen Handlungen aus Gründen der Rechtssicherheit (Der sog. Vorbehalt des Gesetzes verpflichtet die Exekutive dazu, ihr Handeln mit Außenwirkung ausschließlich auf gesetzliche Grundlagen zu stützen, vgl. BVerfGE 40, 237 (248 f.); 49, 89 (126)) und auch der Rechtsstaatlichkeit sowie Bestimmtheit in eigenen Gesetzen als Standardmaßnahmen normiert sein sollten. In Bremen ist dies als Landesgesetz zur IT-Sicherheit geplant. Im BayEGovG ist ein Ansatz zur Einbeziehung von relevanten Versorgern der Bevölkerung zwar angedacht, aber nur in einem unterstützenden Sinne und daher ohne Eingriffsrechte (vgl. Art. 10 Abs. 2 BayEGovG. Im niedersächsischen IT-Sicherheitsgesetz – NDIG – ist in § 16 eine Generalklausel vorgehalten, die bei gegenwärtigen Gefahren dem IT-Sicherheitsbeauftragten die Ermächtigung gibt, Sofortmaßnahmen zu ergreifen. Die Vorschrift wirkt jedoch nur in die Verwaltung hinein (ressortübergreifend) und hat keine Außenwirkung gegenüber Bürgern.). Es ist daran zu denken, dass Verwaltungs- bzw. Dienstvorschriften nur intern wirken und da ihnen jeder Rechtscharakter fehlt, nicht gegenüber Dritten anwendbar sind. Der durch sie beabsichtigte Schutz ist in seiner Außenwirkung daher nur mittelbar vorhanden und entsprechend begrenzt. Es ist an dieser Stelle Aufgabe der Länder, gesetzgeberisch weiter tätig zu werden, um im Spannungsfeld einer Rechtsfriktion ergänzenden Schutz zu schaffen, der die bestehenden Regelungen bis auf das notwendige Maß ausdehnt, um einerseits jenen Schutz zu gewährleisten, der verfassungsrechtlich geboten ist und andererseits der handelnden Exekutive ausreichend Rechtssicherheit zu geben (Rehbohm & Kalmbach, 2021).

Bei solchen notwendigen Eingriffen mit Außenwirkung gegenüber Bürgern ist freilich zu beachten, dass Rechtsbehelfe vorhanden (vgl. Art. 19 Abs. 4 GG) und daher auch Informationspflichten seitens des Staates gegeben sein müssen, sollten die Betroffenen identifiziert werden. Entsprechend bleiben die Rechte nach den Datenschutzbestimmungen unbenommen (→ Kap. 7).

Ob der jeweilige Eingriff einen Charakter als Real- oder Verwaltungsakt hat, ist vom Einzelfall abhängig. Ersteres dürfte va bei rein technischen Maßnahmen der Fall sein, wie der Angriffs- oder Anomalie-Erkennung in IT-Systemen oder Informationsverbünden. Diese präventive Suche nach potenziellen Bedrohungen in Netzwerken und IT-Umgebungen wird als „Threat Hunting“ (mittels „Threat Intelligence“) bezeichnet. Solche Methoden sind neben den klassisch reaktiven und auf retrograden Daten basierenden Ansätzen zeitgemäß, erfassen und verarbeiten jedoch ungleich höhere Datenmengen. Die zweite Option – eine behördliche Einzelfallentscheidung – hingegen gilt insbeson-

dere bei Maßnahmen, die auf einer Einzelfallentscheidung basieren, z. B. einer Anordnung gegenüber einem Unternehmen, bestimmte Maßnahmen zur Eigensicherung zu ergreifen. Es können insbesondere die Einführung eines Informationssicherheitsmanagementsystems, der Einsatz von Maßnahmen gem. „Stand der Technik“ und umfängliche Kontrollrechte beaufschlagt werden.

6.2 Spezifische landesgesetzliche Regelungen

6.2.1 Grundlegende Strukturen und Probleme

Im Vordergrund landesgesetzlicher Regelungen zur IT-Sicherheit steht die Sicherheit informationstechnischer Systeme ihrer staatlichen Stellen. Insbesondere werden hier die Landesverwaltungsnetze adressiert. Gesetze, die sich reinweg auf diesen Aspekt beziehen, bilden die Mehrheit.

Bundesland	**Gesetze**
Baden-Württemberg	Gesetz zur Förderung der elektronischen Verwaltung des Landes Baden-Württemberg (E-Government-Gesetz Baden-Württemberg - EGovG BW) Gesetz zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften
Bayern	Gesetz über die elektronische Verwaltung in Bayern (Bayerisches E-Government-Gesetz – BayEGovG), Gesetz zur Errichtung des Landesamts für Sicherheit in der Informationstechnik
Berlin	Gesetz zur Förderung des E-Government (E-Government-Gesetz Berlin - EGovG Bln)
Brandenburg	Gesetz über die elektronische Verwaltung im Land Brandenburg (Brandenburgisches E-Government-Gesetz - BbgEGovG)
Bremen	Gesetz zur Förderung der elektronischen Verwaltung in Bremen
Hamburg (kein Gesetz)	Compliance Rahmen-Richtlinie
Hessen	Hessisches Gesetz zur Förderung der elektronischen Verwaltung (Hessisches E-Government-Gesetz - HEGovG)
Mecklenburg-Vorpommern	Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern (E-Government-Gesetz Mecklenburg-Vorpommern - EGovG M-V)
Niedersachsen	Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (NDIG)
Nordrhein-Westfalen	Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen (E-Government-Gesetz Nordrhein-Westfalen - EGovG NRW)
Rheinland-Pfalz	Landesgesetz zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz (E-Government-Gesetz Rheinland-Pfalz - EGovGRP)
Saarland	Gesetz zur Förderung der elektronischen Verwaltung im Saarland (E-Government-Gesetz Saarland - E-GovG SL)

	Gesetz zur Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes (Informationssicherheitsgesetz Saarland - IT-SiG SL)
Sachsen	Sächsisches E-Government-Gesetz Sächsisches Informationssicherheitsgesetz
Sachsen-Anhalt	Gesetz zur Förderung der elektronischen Verwaltung im Land Sachsen-Anhalt (E-Government-Gesetz Sachsen-Anhalt - EGovG LSA)
Schleswig-Holstein	Gesetz zur elektronischen Verwaltung für Schleswig-Holstein (E-Government-Gesetz - EGovG)
Thüringen	Thüringer Gesetz zur Förderung der elektronischen Verwaltung (Thüringer E-Government-Gesetz - ThürEGovG -)

Tabelle 4 Landesgesetze mit Bezug zu IT-Sicherheit

Nicht immer sind zum Schutze der Verwaltungs-IT IT-Sicherheitsgesetze geschaffen worden, überwiegend handelt es sich auch um Vorgaben, die in E-Government-Gesetze (Damit sind gesetzliche Regelungen gemeint, die – als Ergänzung zu den Verfahrensgesetzen – staatliche Arbeitsprozesse (im Sinne von Regieren und Verwalten) unter Verwendung elektronischer Medien regeln.) integriert wurden. Eine Verortung in staatsorganisationsrechtlichen Vorschriftenzusammenhängen mindert jedoch nicht den ordnungsrechtlichen Stellenwert, da es nach wie vor um Gefahrenabwehr geht. Jedoch ist die Abwehr erheblich reduziert, da sie sich in erster Linie auf Schnittstellen zwischen dem Landesverwaltungsnetz und anderen Netzen bezieht. Weitere Sicherheitsaspekte beziehen sich auf die Innenstruktur der Verwaltungs-IT und haben somit keine Außenwirkung. In den Ländern, die bislang keine speziellen gesetzlichen Regelungen zur IT-Sicherheit geschaffen haben, ist ein teilweiser Schutz der landeseigenen Netze durch Rückgriff auf datenschutzrechtliche Regelungen möglich. Zudem können Verwaltungsvorschriften greifen.

Beispielsweise sind in der Freien und Hansestadt Hamburg (FHH) keine spezialgesetzlichen Regelungen zur IT-Sicherheit oder zum E-Government getroffen worden. Hier wird auf Basis von Compliance Rahmenrichtlinien u. a. die IT-Sicherheit, der Daten- und Geheimnisschutz und der Umgang mit vertraulichen Informationen adressiert. Beinhaltete Verweise auf die Informationssicherheitsleitlinie der FHH oder dem Rahmensicherheitskonzept der FHH definieren keine expliziten Maßnahmen, wie z. B. die Speicherdauer oder die Verarbeitung von Protokolldaten, vielmehr wird auf die Standards des BSI-Grundschutzes referenziert, welche die nicht ausdifferenzierten Maßnahmen grundsätzlich ermöglichen. In der Freien Hansestadt Bremen existiert ein E-Government-Gesetz, die Belange der IT-Sicherheit referenzieren hier auf die Beschlüsse des IT-Planungsrates zu IT-Sicherheitsstandards, wie z. B. dem BSI-Grundschutz.

Anders verhält es sich hingegen in Brandenburg. Hier werden im E-Governmentgesetz die Mandate des Landes-CERT beim brandenburgischen IT-Dienstleister definiert. Insb. handelt es sich dabei um die Erhebung von anfallenden Protokolldaten im Betrieb und

an Schnittstellen von Kommunikationstechnik, welche bis zu drei Monaten pseudonymisiert gespeichert und ausschließlich automatisiert ausgewertet werden dürfen. Dies dient der Abwehr von Angriffen auf die Informationstechnik des Landes oder zum Erkennen und Beseitigen technischer Störungen. Eine über die automatisierte Auswertung von Protokolldaten hinausgehende Verwendung wird z. B. für die Gefahrenabwehr wird ebenfalls legitimiert. Gleiche Regelungen existieren im E-Government-Gesetz von Berlin.

Baden-Württemberg hat ein E-Government-Gesetz, adressiert jedoch das Thema Informationssicherheit in einem expliziten Cybersicherheitsgesetz. Neben den Möglichkeiten der Protokolldatenauswertung wird hier insb. die Cybersicherheitsagentur legitimiert und der Wirkungsradius dieser Agentur über die Landesverwaltung hinaus definiert. U.a. werden Daseinsvorsorgeträger als natürliche oder juristische Personen des Privatrechts adressiert. Die Cybersicherheitsagentur kann auf Ersuchen unterstützend tätig werden. Eine vergleichbare gesetzliche Regelung ist in Bayern mit dem Landesamt für Sicherheit in der Informationstechnik geschaffen worden.

Durchweg wurden die Kommunen (einschließlich weiterer Verwaltungsebenen) und deren Informationssicherheit (inkl. IT-Sicherheit) bisher nicht in die Landesregelungen zur IT-Sicherheit involviert (Beispielsweise wird das Bayerische Landesamt für Sicherheit in der Informationstechnik nur auf Ersuchen durch Kommunen tätig – und dies auch lediglich beratend und unterstützend, vgl. Art. 10 Abs. 2 BayEGovG.). Es ist zu unterstellen, dass verfassungsrechtliche Bedenken bis hin zu Folgewirkung der Konnexität – insbes. Finanzierungsdefizite – ursächlich sind.

Eine in wenigen Ländern, etwa in Bayern, genutzte indirekte, jedoch weit weniger wirksame Maßnahme ist die jeweilige Erfüllung der Anschlussbedingungen an die Landesnetze einzufordern, die den kommunalen Strukturen direkt Auflagen zur Informationssicherheit aufzwingt. Dieser Mechanismus ist bereits aus den Anschlussbedingungen an das Bund-Länder-Verbindungsnetz bekannt und entfaltete bedauerlicherweise nur geringe positive sicherheitstechnische Folgewirkungen in den angeschlossenen Teilnehmernetzen. Kommunalnetze können direkt oder auch indirekt über Kommunalverbünde bzw. IT-Dienstleister an Landesnetze angeschlossen werden, um insbes. ebenenübergreifende Fachverfahren (z. B. Kfz-Zulassung) von Bund und Ländern nutzbar zu machen. An solchen dedizierten Übergängen zum Bund–Länder-Verbindungsnetz ist der BSI-IT-Grundschutz einzuhalten.

In einzelnen Ländern existieren zudem Förderprogramme auf Landesebene, die eine Einführung von Informationssicherheitsmanagementsystemen wie ISIS12 (CISIS12 (Compliance-Informations-Sicherheits-Management-System in 12 Schritten (Weiterentwicklung ISIS12))) oder ISO27001 auf kommunaler Ebene begünstigen, jedoch hierzu nicht verpflichten.

Informationssicherheitsmanagementsysteme (ISMS) sind wichtig für die öffentliche Verwaltung, damit insbes. Gefahren erkannt und mitigiert werden können – und damit eine

Verantwortungsübernahme des Managements gewährleistet wird. Die Informationssicherheit zu systematisieren ist kein Selbstzweck, sie dient dem gemeinsamen Ziel der Erhöhung der Abwehrfähigkeit gegen Cybersicherheitsrisiken und wird zudem als Anforderung der DS-GVO verstanden. In Art. 32 Abs. 1 lit. d wird:

„ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“

gefordert, dass wiederum ein ISMS impliziert. Wie einzelne Länder mit den Anforderungen an die Etablierung eines ISMS umgegangen sind, wurde in der Studie „On Challenges of Cyber and Information Security Management in Federal Structures – The Example of German Public Administration“ (Rehbohm et al., 2019) erhoben. Die in dieser Studie vorgenommenen leitfadengestützten Interviews beruhten auf der Prämisse, dass Informations- und Cybersicherheit politischen, strategischen, technischen und rechtlichen Abhängigkeiten unterliegen. Die Interviewpartner waren in diesen Fällen die CISOs der Länder.

6.2.2 Grundelemente der IT-Sicherheit der Länder

Die gesetzlichen Bestimmungen der IT-Sicherheit in den Ländern, insbesondere iSv Voraussetzungen zur Ermächtigung von Sicherheitsmaßnahmen, basieren vor allem auf einigen Grundfestlegungen, die an dieser Stelle skizziert werden.

Wesentlich ist die Ausrichtung auf das vom BVerfGE aus der Zusammenschau der Art. 2 Abs. 1 und Art. 1. Abs. 1 GG entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (vgl. BVerfGE 120, 274 (302 f.)). Die wortwörtliche Übernahme eines Grundrechts in viele der (landes-)gesetzlichen Regelungen ist tendenziell ungewöhnlich, zeigt aber dessen herausragende Bedeutung für die Gegenwart. Umgesetzt wird in diesem Kontext vor allem ein umfangreicher Schutz der Daten und sonstiger Belange der Bürger.

Aufgeführt in den Gesetzen sind zudem Sicherheitsereignisse und -vorfälle, die sich als drohende Gefahr für informationstechnische Systeme zeigen. Diese drücken sich vor allem in der Form von Schadprogrammen aus.

Als informationstechnische Systeme werden alle technischen Einrichtungen verstanden, die der Erfassung, Speicherung, Verarbeitung oder Übermittlung von Informationen und Daten dienen. Institutionalisierte Zusammenarbeit auf Basis eines Computer Emergency Response Team (CERT)-Verbundes ist dabei zwischen allen Ländern und dem Bund im teilnehmergeschlossenen Verwaltungs-CERT-Verbund (VCV) gegeben. Jedoch haben die wenigsten Länder Regelungen geschaffen, die eine kommunale Zusammenarbeit mit dem jeweiligen Land erzwingen. Somit kann die Informationskette zu aktuellen Bedrohungen, insbesondere von öffentlichen Verwaltungen, abreißen.

Kommunen oder Kommunalverbünde können CERTs und kommunale CERT-Verbünde unterhalten und sich somit untereinander vernetzen, ein über das föderale System hinweg funktionierender Informationsaustausch ist hingegen nicht durchgängig geregelt. Es existiert allerdings kein Anschlusszwang der Kommunen an Landes-CERTs.

Organisationen der Daseinsvorsorge, ieS Wirtschaftsunternehmen und auch die öffentliche Verwaltung, können sich in weiteren CERT-Verbünden engagieren, z. B. in der Allianz für Cybersicherheit (ACS) oder dem Deutschen CERT-Verbund.

Dem CERT-Bund des BSI steht eine integrierende Rolle in allen CERT-Verbünden zu, um auch den europäischen – zum Beispiel der ENISA – und weltweiten Informationsaustausch zu garantieren. Die Länder haben sich mit dem IT-Planungsratsbeschluss zur Informationssicherheitsleitlinie verpflichtet, am Verwaltungs-CERT-Verbund teilzunehmen.

Kern der gesetzlichen Bestimmungen bilden Ermächtigungsgrundlagen und die Festlegung von zuständigen Stellen. Es ist von elementarer Wichtigkeit, dass auch die öffentlichen Verwaltungen in den Ländern in die Lage versetzt werden, IT-Systeme zum Einsatz zu bringen, die dem Stand der Technik entsprechen. Hierfür bedarf es einer rechtlichen Würdigung in der Form, dass moderne Angriffserkennungssysteme, die technische Daten zur Anomalie-Erkennung sammeln, zum Einsatz gebracht werden müssen. Konsequenterweise sind die Landesgesetze so zu gestalten, dass Daten aus Informations- und Kommunikationssystemen über einen längeren Zeitraum erfasst, verarbeitet und ausgewertet werden können. Eingedenk der hohen Integration von Kommunikations- und Informationstechnik ist dabei nicht auszuschließen, dass es sich neben Verwaltungsdaten auch um solche von Bürgerinnen und Bürgern auf allen Kommunikationsebenen handeln wird. Auch kann es ggf. erforderlich sein, verschlüsselte Verbindungen, mithin die meistgenutzte Darreichungsform von Internetseiten, aufzubrechen. Nur wenige Länder haben für sich und ihre Kommunen solche Regelungen ausreichend gewürdigt und gesetzlich verankert. In den Ländern Baden-Württemberg, Bayern, Berlin, Brandenburg, Niedersachsen, Rheinland-Pfalz, Saarland, Sachsen und Thüringen sind in den oben benannten gesetzlichen Regelungen die automatisierte und pseudonymisierte Auswertung von Protokolldaten mit einer Mindestspeicherdauer von drei Monaten möglich. Die Ermächtigungen reichen von der Pflicht allgemeine Sicherheitsvorkehrungen zu treffen über technische Abwehrmittel bis hin zu Einzelmaßnahmen, die von Fall zu Fall angeordnet werden müssen. Solche Einzelmaßnahmen werden insbes. unter Einschränkung von Grundrechten, wie dem Fernmeldegeheimnis, im Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (NDIG) in den §§19-24 subsummiert.

Verantwortliche Stellen sind im Regelfall die Landesbeauftragten für die Informationssicherheit. Vorteilhaft wirkt sich hier die Verortung dieser Beauftragten in Innenministerien aus, da der Zugang zu wesentlichen Beteiligten der Gefahrenabwehr gegeben ist. Über-

all dort, wo dies nicht gewährleistet ist, entstehen in der Praxis erhöhte Abstimmungsaufwände und folglich Reibungsverluste, die die Effektivität und Effizienz getroffener Maßnahmen mindern. Die Informationssicherheitsbeauftragten der Länder brauchen einen effizienten Austausch mit Strafverfolgungsbehörden und dem Verfassungsschutz, da hier etablierte Meldewege bestehen und die Zusammenarbeit auf erprobten Mechanismen beruht. Insbesondere ist dies im Kontext des Gemeinwohls von großer Wichtigkeit. Die Länder sind auf die Beteiligung aller relevanten Daseinsvorsorgeträger in einer gemeinsamen Cybersicherheitsarchitektur angewiesen, dazu gehören auch die Ordnungsbehörden.

Einzelne Länder stellen sich dieser Herausforderung in der Begründung von Agenturen oder Kompetenzzentren, die eine Zusammenarbeit von Wirtschaft und Verwaltung sichern sollen (in Bayern und Baden-Württemberg ist dies gesetzlich geregelt). An dieser Stelle seien beispielhaft das „Hessen Cyber Competence Center (H3C)“, das Landesamt für Sicherheit in der Informationstechnik (Bayern) oder auch die Cybersicherheitsagentur in Baden-Württemberg genannt.

Insbesondere bei der Begründung solcher Agenturen oder Kompetenzzentren sind die flächen- und bevölkerungsreichen Länder deutlich weiter in der Entwicklung als kleinere Länder. Die Agenturen sind rechtlich abgesichert und finanziert, der Teilnehmerkreis bleibt jedoch offen und unverbindlich in Richtung Unternehmen. Rechtliche Verpflichtungen wurden durchweg nicht vorgesehen. Die institutionalisierten Organisationen können Notfallteams vorhalten, haben diese zum Teil etabliert und ergänzen die Tätigkeiten des Bundes, sind insofern auf die Bedürfnisse in einem Land zugeschnitten. Dies wird allgemein als komplementäre Zusammenarbeit im Kontext einer gemeinsamen föderalen Cybersicherheitsarchitektur von Bund und Länder verstanden.

Daseinsvorsorgeträger, die nicht unter das IT-SiG fallen, sind (bisher) nicht verpflichtet, mit staatlichen Stellen zu kooperieren. Hilfestellungen kommen nur auf Ersuchen Betroffener Akteure zustande. Eine Herausforderung in den Ländern und Kommunen verbleibt inhaltlich, die systemrelevanten Daseinsvorsorgeträger (Sub-KRITIS) im eigenen Verantwortungsbereich und zusätzlich zu den vom IT-Sicherheitsgesetz identifizierten KRITIS-Unternehmungen in einen fortwährenden Austauschprozess eintreten zu lassen und mit den staatlichen Akteuren verbunden zu werden.

Unternehmen der Daseinsvorsorge der Region müssen qualitativ identifiziert werden, da der quantitative Ansatz des Bundes für die Länder nicht zielführend ist. Die Untersuchung der Betroffenheit eines spezifischen Unternehmens kann nicht allein im Kontext der Gesetzgebung und vom Unternehmen selbst vorgenommen werden. Das Compliance-Management der öffentlichen Verwaltung muss folglich in seiner Perspektive erweitert werden. Die Interdependenzen der betroffenen Unternehmen müssen fortwährend beobachtet werden. Die territorialen, insbesondere länderübergreifenden Zuständigkeiten sind zu betrachten. Auch müssen die Länder über aktuelle Veränderungen der

Sicherheitslage bei den vom Bundes-IT-Sicherheitsgesetz betroffenen Unternehmen unverzüglich und angemessen unterrichtet werden, um die aktuelle Sicherheitslage im Land beurteilen und ggf. Maßnahmen zur Gefahrenabwehr steuern zu können. Im Kontext der aktuellen IT-Sicherheitsgesetzgebung des Bundes wurden durch die Länder solche umfänglichen Informationspflichten eingefordert. Bei den in Austausch tretenden Institutionen werden technische und organisatorische Daten in einem beachtlichen Umfang entstehen und ausgewertet werden müssen. Diese vertraulichen, auch personenbezogenen Daten werden gemäß den geltenden rechtlichen Bestimmungen aus EU, Bund und Länder verarbeitet – insbes. im Kontext der DSGVO.

7 Herausforderungen der föderalen Cybersicherheit vs. Änderung in der Bund-Länder Gewaltenteilung[6]

Zusammenfassung: Bund, Länder und Kommunen wollen die Digitalisierung von Staat, Wirtschaft und Gesellschaft vorantreiben und müssen sich gleichzeitig den Herausforderungen einer hybriden Bedrohungslage stellen. Teile dieser dynamischen Bedrohungslage sind verbunden mit Angriffen auf die IT-Infrastrukturen und Dienste der öffentlichen Verwaltung und weiterer Träger der Daseinsvorsorge. Die Motivationslagen solcher Angriffe sind dabei im höchsten Maße unterschiedlich; jedoch egal ob Spionage, Sabotage oder kriminelle Aktivitäten, die gesamte Verwaltungsorganisation Deutschlands muss sich im Kampf gegen Cybersicherheitsbedrohungen behaupten.

Dort, wo Menschen leben, verlassen sich diese darauf, dass die öffentliche Verwaltung – als Garant – das Gemeinwohl der Region sichert und systemrelevante Infrastrukturen sowie die Menschen als Individuum schützt. Den Ländern steht demnach in Fragen der allgemeinen und speziellen Gefahrenabwehr nicht nur eine herausgehobene Rolle zu, vielmehr sind sie alleinig für die öffentliche Sicherheit und die öffentliche Ordnung – zusammen mit den Kommunen – zuständig. Das Bundesministerium des Innern und für Heimat sieht inzwischen Anlass dazu, an dieser Aufgabenstellung einen Wandel über eine Grundgesetzänderung herbeizuführen. Sollten Funktionen der föderalen Sicherheitsarchitektur tatsächlich durch grundgesetzliche Änderungen in Richtung des Bundes – hier Bundesamt für Sicherheit in der Informationstechnik (BSI) – verlagert werden, ergeben sich Änderungen an der föderalen Cybersicherheitsarchitektur.

7.1 Einleitung

Für Staat, Wirtschaft und Gesellschaft ist die Frage nach der Verfügbarkeit von bedeutenden Verbrauchsgütern und Infrastrukturen so wichtig und aktuell wie schon seit Jahrzehnten nicht mehr. Die Cybersicherheitsbedrohungslage hat sich mit Beginn der Kriegshandlungen in der Ukraine weiter verändert. Europa, Deutschland und die Länder mussten feststellen, wie fragil unsere Gesellschaft und welchen externen Einflüssen unser Gemeinwohl ausgesetzt ist. Der wirtschaftliche und soziale Zusammenhalt ist in einem hohen Maß von Informationstechnik abhängig.

Die Cybersicherheitsarchitektur Deutschlands ist auch aufgrund von erfolgreichen Angriffen auf z. B. kommunale IT-Infrastrukturen oder auf IT-Systeme von Krankenhäusern in der jüngeren Vergangenheit mehrfach hinterfragt worden (Ernst, 2020). Dabei ist die gesamte Sicherheitsarchitektur das Produkt unserer Föderalstruktur und grundsätzlich als solche beabsichtigt. Die Gründer des modernen Deutschlands wollten eine verteilte Machtstruktur in Bund und Ländern. Dennoch ist die Verlagerung von Kompetenzen im

[6] Der Inhalt dieses Kapitels ist bereits wie folgt veröffentlicht worden: Thomas Rehbohm und Dr. Peter Lutz Kalmbach, Datenschutz und Datensicherheit, DuD 5/2023

Bereich der Cyber- und Informationssicherheit zugunsten des Bundes in der Diskussion. Nach Aussagen der Bundesinnenministerin Nancy Faeser zur Cybersicherheitsstrategie (Bundesministerium des Innern und für Heimat, 2022), soll mit dem BSI eine dritte Sicherheitssäule nach dem Vorbild des Bundeskriminalamtes (BKA) und des Bundesamtes für Verfassungsschutzes (BfV) entstehen. Eine vergleichbare Struktur wie beim BKA oder dem BfV träfe derzeit auf keine organisatorische Entsprechung in den Ländern, diese Erwartungshaltung wird seitens des Bundes jedoch auch nicht geäußert. Vielmehr steht im Vordergrund, dass eine konstruktive Zusammenarbeit nur mit einer Grundgesetzänderung möglich sei. Diese Aussage wird in den Ländern unterschiedlich bewertet, grundsätzlich weisen die Länder zwar keine behördliche Entsprechung aus, gleichzeitig trifft die gewünschte „kooperative und komplementäre“ Zusammenarbeit in den Ländern nicht auf ein Vakuum. Vielmehr haben sich die Länder über die Zusammenarbeit in speziellen Arbeitsgruppen im IT-Planungsrat und der Innenministerkonferenz konstituiert und arbeiten seit Jahren erfolgreich mit dem Bund zusammen.

Die Aussage der Bundesinnenministerin, dass man dem Bund mehr Kompetenzen zuweisen will, da die Gefahrenabwehr mithin die Cybersicherheit bei den Ländern liegt, zeigt das Dilemma auf. Das Europäische Parlament und der Rat der Europäischen Union haben mit der sogenannten NIS-2-Richtlinie (Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie), 2023) die Herausforderung eloquent adressiert. Wenn das Paradigma zuträfe, die Kommunen sollten im Rahmen der kommunalen Selbstverwaltung dennoch den Vorgaben der Länder in Angelegenheiten der Informationssicherheit folgen, und die Länder den Vorgaben des Bundes durch Grundgesetzänderung hinsichtlich der Kompetenzverschiebung, dann muss die Ausgestaltung der NIS-2-Richtlinie in den Ländern stärker hinterfragt werden. Denn im Grunde haben die Länder, genau wie der Bund, vergleichbare Herausforderungen angesichts dieser EU-Richtlinie. Eine Entlastung der Länder durch den Bund scheint in dieser Hinsicht als wenig wahrscheinlich. Anforderungen dieser Richtlinie müssen im Bund und in den Ländern binnen 21 Monaten nach Veröffentlichung umgesetzt werden. Dies betrifft insbesondere eigene Cybersicherheitsstrategien, eigene Gesetzgebungsverfahren und die Identifizierung von wichtigen und wesentlichen Organisationen des Landes. Die technische und organisatorische Vernetzung aller wesentlichen Akteure der Daseinsvorsorge wird die Arbeit bis zum Ablauf der Frist in den Ländern bestimmen. Folglich braucht es eine föderale Cybersicherheitsarchitektur, welche den Anforderungen der Richtlinie angemessen Rechnung tragen kann.

7.2 Stand der Forschung

Forschungsbeiträge zu Cybersicherheit und das Cybersicherheitsrecht sind in den vergangenen Jahren angewachsen. Die öffentlichen Verwaltungen – zusammen mit weiteren Trägern der Daseinsvorsorge – sind jedoch unterrepräsentiert, insbesondere in Föderalsystemen. Viele europäische Beiträge im Umfeld der Daseinsvorsorge befassen

sich mit dem Binnenmarktrecht, dem Wettbewerbsrecht und im Kontext von strukturellem und demografischem Wandel mit Sozial-, Versorgungs- und Gesundheitssystemen. Wenige Artikel befassen sich hingegen mit den Dienstleistungen im allgemeinen Interesse oder „services of general interest“ (SGI) im Zusammenhang mit Cybersicherheitsstrukturen. Staatliche Akteure und Daseinsvorsorgeträger sind in Verbindung mit dem Onlinezugangsgesetz und der Digitalisierung durch *Bostelmann* im „Handbuch Onlinezugangsgesetz“ (Seckelmann & Brunzel, 2021, S. 165) adressiert worden. Eine eingehende Literaturrecherche ist Teil des Beitrages „Sicherheitsmanagement, Cybersicherheit und Daseinsvorsorge: Empirische Studie in deutschen Kommunen“ (Rehbohm et al., 2022). Folgende Beispiele sind hieraus extrahiert und sollen das Thema exemplarisch illustrieren.

Mit dem Föderalsystem der Vereinigten Staaten ist eine Vergleichbarkeit zu Deutschland gegeben. In „The Cybersecurity Policy Challenge – The Tyranny of Geography” empfiehlt *Kamarck*, dass eine nahtlose Architektur der Zusammenarbeit entstehen muss, da Cybersicherheitsbedrohungen – anders als Regierungen – grenzenlos sind (Andreasson, 2012, S. 124).

Auf europäischer Ebene wird in „Services of general interest beyond the single market“ von Krajweski ausgeführt, dass im Vertrag von Lissabon (EUVtr Liss Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft, 2009) unter anderem die Mitgliedstaaten (nationale, regionale und lokale Behörden) der Europäischen Union die allgemeine Zuständigkeit für die „Bereitstellung, Beauftragung und Organisation“ von Dienstleistungen von allgemeinem Interesse haben (Krajewski, 2015, S. 237).

Auf nationaler Ebene wird in „Cybersicherheit in Kritischen Infrastrukturen“ von den Autoren ausgeführt, dass sich der kooperative Ansatz im Bereich Cybersicherheit bewährt hat, insbesondere, weil eine vertrauensvolle Kooperation zwischen Staat und Wirtschaft eine „shared mission“ ist (Dürig & Fischer, 2018, S. 209).

Warum rechtliche Rahmenbedingungen in den Ländern entstehen müssen, um eine kooperative Zusammenarbeit aller identifizierten Akteure zu ermöglichen, ist im Artikel „Grundforderungen von Informations- und Cybersicherheit in Ländern“ (Rehbohm & Kalmbach, 2021) aufgearbeitet worden. Wie Informationssicherheitsmanagementsysteme unabhängig vom Framework implementiert werden können, wird im Artikel „CISIS12 – Vorgehensmodell zur Einführung eines Informationssicherheitsmanagementsystems“ (Moses & Rehbohm, 2022) beschrieben. Diese strukturierte Möglichkeit kann hinsichtlich einer übergreifenden Cybersicherheitsorganisation nutzbar gemacht werden.

7.3 Rechtskonstrukt

Zu den politisch-strategischen Erwägungen ist der Rechtsrahmen zu beschreiben, denn Kompetenzen sind letztlich erst dann wirksam, wenn sie mit Rechtsmacht versehen sind.

Diese wiederum ist abhängig von der Bereitstellung konkreter Ermächtigungsgrundlagen, die ein Handeln gegenüber Bürgern oder sonstigen Personen wie auch Unternehmen – also gegenüber Grundrechtsträgern – verfassungsrechtlich möglich machen (vgl. die sog. „Gesetzmäßigkeit der Verwaltung“ BVerfGE 40, 237, 248f; 107, 59,102).

Während dies eine rechtsstaatlich gebotene Einhegung staatlicher Funktionen ist, fordert die Verfassung jedoch auch zu einem Handeln durch staatliche Institutionen auf: Demnach ist der Staat Bundesrepublik (mit seinen Ländern) verpflichtet, menschliche Bedürfnisse in den Mittelpunkt seiner Tätigkeiten zu stellen (vgl. BVerfGE 61, 82 (100)). Entsprechend sind Grundrechte der Menschen sowie Verfassungswerte, die der Gesamtheit der Bevölkerung dienen sollen (sog. Kollektivrechtsgüter), zu fördern und zu schützen ((Birkenmaier & Butzer, 2018, S. 140), (Sodan, 2009, S. 545), (Kindhäuser et al., 2023, Nummer 126 ff. und 138), BVerfGE 58, 1, 26).

Genau in diesem – mitunter ambivalenten – Spannungsfeld ist auch die Cybersicherheit zu verorten; ebenso wie alle Überlegungen ihrer Ausgestaltung, der Verortung von Kompetenzen und auch der Schaffung von Organisationen, die ihr dienen. Dabei haben die politischen Akteure einen Spielraum, dessen Grenzen nicht immer völlig klar erkennbar sind. Jedoch gibt es relevante Aspekte, die als Rahmenbedingungen zu verstehen sind und bei den Überlegungen einer föderalen Cyber-Sicherheitsarchitektur berücksichtigt werden sollten.

Das staatliche Handlungsfeld spielt sich dergestalt zwischen der Pflicht, etwas zum Schutze des Gemeinwohls zu tun (Verbot des Zuwenig/sog. „Untermaßverbot“) und dem Gebot der Maßhaltung (Verbot des Zuviel/sog. „Übermaßverbot“) ab. (vgl. BVerfGE 20, 351 (361); 88, 203 (254); BVerfG NVwZ 2009, 1489). Sinnhaft verknüpft mit dem Übermaßverbot ist zudem die Aufteilung staatlicher Kompetenzen in horizontaler („Gewaltenteilung“) und vertikaler Hinsicht (föderaler Bundesstaat) (Vogel, 1996, S. 1505–1511).

Letztlich wird durch die Gesamtheit des Rechts gewährleistet, dass Verfassungswerte (Rechtsgüter) bewahrt werden. Der Rechtsgüterschutz findet aber im Kontext verwaltungsrechtlicher Gefahrenabwehr statt (vgl. BVerfG, Urteil vom 2.03.2010, Az. 1 BvR 256/08, 1 BvR 263/08, 1 BvR). Dies wiederum ist in erster Linie eine Angelegenheit der Länder (vgl. BVerfGE 125, 260 (346)), wie überhaupt dort die innere Sicherheit in der Hauptsache gewährleistet werden soll (Isensee & Kirchhof, 2003, S. S 3 (S. 118)).

Natürlich kann man Cybersicherheit nicht eins zu eins gleichsetzen mit althergebrachten Bereichen des Ordnungsrechts, so etwa dem Polizeirecht. Jedoch hat es ebendort, im Ordnungsrecht, einen klaren Standort und muss sich insoweit in die bestehende Rechtssystematik einordnen (lassen). Es hat von dort aus Bezüge zu anderen gewichtigen Rechtsfächern, die sich vom Zivilrecht (hier insbes. Deliktsrecht) bis zum Strafrecht erstrecken. Insbesondere Letzteres ist von ausgesprochener Wirkungsmacht, da es der Sicherung des Rechtsfriedens schlechthin dient und seine Durchsetzung zum Kern staatlicher Aufgaben gehört (vgl. BVerfGE 107, 104, 118).

Natürlich ist zu bedenken, dass solche staatlichen Pflichten keiner Teilung im eigentlichen Sinne unterfallen (Vogel, 1996, S. 1506). Entsprechend ist es Aufgabe der gesamten öffentlichen Gewalt, Sicherheit zu gewährleisten und Straftaten zu bekämpfen. Andererseits sind aber Grundmuster vorhanden, die dafür Sorge tragen sollen, dass es keine Konzentration von Macht gibt. Dergestalt sind bestimmte Aufgaben unverrückbar einer Kernverwaltung zuzuordnen (vgl. BVerfGE 107, 59 (93)). Demnach will die Verfassung sicherstellen, dass grundlegende staatliche Funktionseinheiten Aufgaben wahrnehmen, die ihnen eine grundgesetzkonforme originäre Verantwortung belassen (Vogel, 1996, S. 1505 ff.).

Dies betrifft auch die föderale Aufgabenverteilung im Bund. So ist im Kontext der Gefahrenabwehr schon allgemein eine Zuständigkeit der Länder gegeben – die aber noch dadurch verstärkt wird, dass zu dieser Aufgabe auch die Gefahrenvorsorge (als Vorfeld der eigentlichen Gefahrenabwehr) zu zählen ist (vgl. zum Folgenden BVerwG NVwZ 2012, 757 (759)). Sie richtet sich zumal gegen die Begehung von Straftaten und soll bereits dann wirken, wenn abstrakte Gefahrensituationen gegeben sind. Da Cyberangriffe regelmäßig mit der Begehung von Straftaten einhergehen bzw. auf deren Begehung abzielen, ist also hier eine tendenziell strikte Kompetenz der Länder gegeben. Auch sollte in diesem Zusammenhang bedacht werden, dass durch ebendiesen Bezug die Cybersicherheit im Wesentlichen durchaus gleichwertige Aufgaben umfasst wie das Polizeirecht. Die schwerpunktmäßige Verortung polizeilicher Macht bei den Ländern ist nicht nur Teil der Verfassung selbst, sondern auch ihrer Entstehung: Die westlichen Alliierten sahen in einer überstarken Polizeiorganisation auf Bundesebene ein unerwünschtes Risiko, welches die Mahnung an die Auswüchse des Dritten Reiches und seiner Gewaltpolitik negieren könnte, sodass sie auf eine wesentliche Verortung des Polizeiwesens bei den Ländern drangen (vgl. BVerfGE 110, 33 (51 f.)). Diesem Verlangen entspricht auch die langjährige Form der Präsenz von Polizei und Nachrichtendiensten auf Landes- und Bundesebene. An diesem Gefüge sollte sich auch die Stellung einer Organstruktur der Cybersicherheits-Ämter messen.

Veranschaulichen lässt sich diese Problematik anhand der Annahme, das BSI bekäme die zentrale Aufgabe zur Erkennung von Schadprogrammen in den Landesnetzen. Die Länder müssten hierfür den gesamten Netzwerkverkehr zum Bund umfänglich ausleiten. Mithin beträfe das regelmäßig die Kommunikation der Landesregierungen. Grundsätzlich profitieren dabei die Länder vom Know-how des BSI, gleichzeitig besteht die hypothetische Gefahr, dass auf die politische Willensbildung im Föderalsystem Einfluss genommen werden könnte. Und noch mehr Verzwicktes steckt in dieser Herangehensweise: Abgesehen vom Rechtsgüterschutz dient die Cybersicherheit zwar selbstredend auch der staatlichen Infrastruktur (Hornung, 2015, S. 3334–3340). Da die Verwaltungsnetze der Länder aber logischerweise in deren eigene Verantwortung fallen, muss ihnen insoweit eine gewichtige Organverantwortung zufallen, um ihrer Rolle im Bundesgefüge gerecht zu werden.

Ein weiterer Aspekt ist die Schaffung von Rechtsgrundlagen, die der Cybersicherheit dienen. Bereits aus den obigen Ausführungen ergibt sich, dass den Ländern hier eine starke Kompetenz zukommen muss. Auch ist an die Komplexität des Themenbereichs zu denken, der in vielfältiger Weise die Bürger berührt. Dabei geht es nicht nur um die Verlässlichkeit der staatlichen Infrastruktur, sondern auch um die Grundrechtssphären: Nachlässigkeiten und Versäumnisse in der IT-Sicherheit bei privaten Akteuren können ausgesprochen vielgestaltige rechtliche Folgen auslösen. Es sei allein darauf verwiesen, dass gegebenenfalls bestehende Pflichten als verletzt anzusehen sind, die zivilrechtliche Haftungen auslösen. Zudem hat sich gezeigt, dass die Verortung von gesetzlichen Kompetenzen zur Erhaltung der öffentlichen Sicherheit auf allen staatlichen Ebenen, die zur Rechtsetzung befugt sind, zu einem dichten Netz kollektiver Sicherheit geführt hat. So können ordnungsrechtliche Normierungen sogar durch Satzungsrecht – also beispielsweise durch Kommunen – erfolgen. Dazu kann nicht zuletzt auf das Ordnungswidrigkeitenrecht zurückgegriffen werden (vgl. BVerfG NJW 1972, 860 (861 f.)).

Im Hinblick auf bestehende Landesgesetze, die die unmittelbare wie auch die mittelbare Staatsverwaltung umrahmen, sollte überlegt werden, ob Ausweitungen auf privatwirtschaftliche Bereiche angezeigt sind, sodass dem ausreichenden Schutz von Rechtsgütern, die Individual- und Gemeinwohlinteressen in erheblicher Weise dienen, Genüge getan wird.

Dies zeigt, dass Gefahrenabwehr auch regional oder sachspezifisch wahrzunehmen ist. Mag die Cybersicherheit von Entgrenzung gekennzeichnet sein – die Folgen können und haben individuellen und örtlichen Bezug. Hier also soll(te) eine starke Verankerung stattfinden, die zudem hilft, der Dynamik von Bedrohungslagen effektiver entgegentreten zu können. Regelungen, die durch eine etwaige Grundgesetzänderung die Länder träfen, sind nicht grundsätzlich auf die Kommunen übertragbar und folglich nicht ortsbezogen wirksam. Vielmehr sind die Länder – auch durch die NIS-2-Richtlinie – aufgefordert, die föderale Cybersicherheit angemessen auch rechtlich zu regeln. Die sich aus einer Zentralstelle im BSI ergebenden Rechte, Pflichten oder auch nur Möglichkeiten für Kommunen sind derzeit unklar, sodass eine grundgesetzliche Regelung zuvorderst die Ministerialverwaltungen der Länder adressiert. Der örtliche Bezug kann daher nur durch die Länder selbst sichergestellt werden.

Und noch ein weiterer Aspekt ist bei der Rechtssetzung, die über mehrere Hierarchieebenen verteilt stattfindet und greift, zu beachten: Der Schutz in gesetzlicher Form findet auch durch Reichweite und Bestimmtheit der jeweiligen Regelungen seine Eignung.

Auf Bundesebene sind bereits Regelungen vorhanden, die ein hohes Maß an Cybersicherheit gewährleisten. Jedoch stellt sich die Frage, ob es angesichts der fundamentalen Bedeutung des Themas und der Vielschichtigkeit des Problems ratsam ist, die Regelungen insbesondere durch (formelle) Gesetze und Rechtsverordnungen auf Bundesebene weiter zu formen – was mit einer verstärkten Verlagerung von Kompetenzen dorthin noch an Gewicht zunehmen wird.

Hier spielen nicht nur Bedarfe hinein, die sich eventuell erst auf abgestuften politischen Ebenen ergeben, sondern auch der Umstand, dass Gesetze für jedermann verständlich und die Folgen – auch für die Rechtsanwender – abschätzbar sein müssen. Es ist nicht damit getan, dass Akteure mit Spezialkenntnissen verstehen, was notwendigerweise für eine funktionsfähige Cybersicherheit getan werden muss.

Es stellt sich die Frage, ob angesichts der vollständigen Verschränkung der Cybersicherheit mit dem Schutz zahlreicher Rechtsgüter und ebenso einer Vielzahl von Rechtsgebieten überhaupt eine zentrale Verortung auf Bundesebene zielführend bei der Bestimmung eines grundlegenden Verständnisses zu Kritischen Infrastrukturen ist. Kritische Infrastrukturen nach Definition des Bundes sind ungleich systemrelevanter als Infrastrukturen einer Region oder eines Föderalstaates. Abgesehen von der näheren Bestimmung kann es unterschiedliche Herangehensweisen an die Beseitigung von Gefahrenpotenzial geben, etwa angesichts der Frage, ob vorhandene Rechtsnormen eine gebundene Folge vorsehen oder einen Ermessensspielraum gewähren.

Dergestalt können gravierende Probleme entstehen, weil die Normierungen nicht für alle Bürger und die zahlreichen Amtswalter, die mit Cybersicherheit direkt oder indirekt zu tun haben, auch nachvollziehbar sind. Soweit staatliche Maßnahmen mit Grundrechtseingriffen einhergehen, sind nach Art und Intensität sowohl die Verständlichkeit wie auch die Verhältnismäßigkeit von steigender Bedeutung (vgl. zum Folgenden BVerfG NJW 2008, 1505 (1507)). Dies gewinnt noch mehr an Gewicht, wenn es um Eingriffe geht, die praktisch jeden treffen können.

Sowohl für die Geeignetheit der staatlichen Maßnahmen wie auch für die Betroffenheit von Bürgern kann es etwa davon abhängen, ob eine Gefahr quantitativ oder qualitativ bemessen wird. Hier sollte bedacht werden, dass die gesetzgeberischen Kompetenzebenen berechtigterweise mit zunächst unterschiedlichen Niveaus an das Problem herangehen (Einschätzungsprärogative). Manches muss eben auch widerstreitend erarbeitet und ermöglicht werden, um mit späterem Erfahrungswissen eine verfassungskonforme Herangehensweise auszutarieren. Hier mag gelten, dass wer näher dran ist (personell, sachlich, örtlich) auch haltbarere Expertisen und Meinungen einbringt – und gegebenenfalls dann auch für nachhaltigere rechtliche Rechtsnormen sorgt. Es kann also die Frage schlechthin sein, ob nun Bund oder Länder hilfreiche oder entbehrliche Ansätze bieten. Nach dem Ausgeführten und gem. Art. 30 GG liegt hier die Verantwortung vor allem bei den Ländern. Es mag insoweit also auch im Verantwortungsbereich der Länder liegen, erst einmal Strukturen zu schaffen, die dann tatsächlich spiegelbildlich auf Bundesebene ihre Entsprechung finden (Polizei, Nachrichtendienst und Cybersicherheit). Es muss dabei keine einseitige Herangehensweise von unten nach oben sein, sondern kann von beiden Seiten herangegangen werden. Jedoch sollten die Kompetenzen auf Landes- und kommunaler Ebene ebenfalls voll ausgeschöpft werden. Idealerweise greifen gesetzliche Vorkehrungen dann derart ineinander, dass sich in Zweifelsfällen mehrere Organisationen für verpflichtet halten, einzugreifen, sodass Cyberangriffe auf ein lückenloses Schutzsystem stoßen. Nicht zuletzt wird darin der Gedanke eines

zum Rechtsgüterschutz entschlossenen Staatsgefüges und jener der Bundestreue verwirklicht.

7.4 Föderale Gefahrenabwehr

Die obigen Ausführungen machen deutlich, dass es der Verfassung entspricht, wenn wichtige Aspekte des Rechtsgüterschutzes „vor Ort“ umgesetzt werden. Die Gefahrenabwehr muss kurzerhand und in Präsenz stattfinden. Es muss Handlungsmöglichkeiten – auch gesetzliche – geben, die selbst regionale oder administrative Besonderheiten widerspiegeln und damit die Effektivität von Gegenmaßnahmen erhöhen. Dazu gehört natürlich auch die Vernetzung von Akteuren jenseits der Zentralinstanzen.

Aber nicht nur Gesetze und Verfügungen werden die Cybersicherheit um- und durchsetzen, sondern auch weitere Handlungen staatlichen Charakters. Viele Bundesländer in Deutschland sind den Herausforderungen von Cybersicherheitsbedrohungen begegnet, haben ihrerseits entsprechende Cybersicherheitsstrategien entwickelt und diese auch rechtlich abgesichert. Dies wird in Zukunft jedoch keine optionale Möglichkeit sein, sondern wird durch die Anforderungen und Regelungen der EU an die Mitgliedstaaten verbindlich geregelt, konsequenterweise auch in Föderalstaaten und somit in den Bundesländern hierzulande. Eine Kompetenz-Konzentration auf den Bund ist vor diesem Hintergrund nunmehr zu hinterfragen, da die Erwartungshaltung der EU auf Institutionalisierung und vollständige Umsetzung in den Föderalstaaten abzielt.

Welche Möglichkeiten der Ausbau des BSI zu einer Zentralstelle mit sich bringt, ist derzeit unklar, womöglich verpflichtet es den Bund nicht zu konkreten Hilfeleistungen in Ländern und Kommunen. Dies erscheint auf den ersten Blick angemessen, da allein die Beschäftigenanzahl der öffentlichen Verwaltung von Ländern und Kommunen annähernd zehnmal größer ist als die des Bundes. Hinzu käme die derzeit unbestimmte Anzahl von weiteren Akteuren in den Ländern und Metropolregionen.

Weitere Themenfelder einer möglichen Zentralstelle sind schon heute Teil der etablierten Zusammenarbeit. Insbesondere der Austausch von Angriffsvektoren, Informationen zu Bedrohungslagen bzw. Schwachstellen, gemeinsame IT-Notfall-Übungen sowie Aus- und Fortbildungsmaßnahmen bedürfen demnach keiner nachträglichen Verfassungsänderung. Konkretisierende Zusammenarbeitsbereiche der Länder mit dem BSI sind über dedizierte Kooperationsverträge gewährleistet.

Die notwendige internationale und europäische Zusammenarbeit, konzentriert auf das BSI, muss nicht zwingend als Insellösung erfolgen. Genau wie die Zusammenarbeit im Forschungsumfeld sind die Netzwerke aller Akteure gefragt und wertvoll und können durchaus einen Beitrag zur gemeinsamen Cybersicherheit leisten. Eine Ausgestaltung in den Ländern sollte nicht unmöglich sein. Weitere mögliche Handlungsfelder, wie zum Beispiel Beratungen im Umfeld von RZ-Sicherheit und Hochverfügbarkeit, können ebenso durch die Länder erfolgen, da auch hier die Kompetenzen unbestritten vorhanden sind.

7.5 Schlussfolgerungen und Ausblick

Grundsätzlich kann festgestellt werden: Cybersicherheit ist vor Ort zu realisieren und muss sich in das Gefahrenabwehr- bzw. Ordnungsrecht des Föderalstaates einfügen. Der Kontakt zu den wesentlichen und wichtigen Trägern des Gemeinwohls ist in der Region herzustellen. Eine vertrauensvolle organisatorische und technische Zusammenarbeit kann von Kooperationspartnern, wie dem BSI, der Agentur der Europäischen Union für Cybersicherheit (ENISA), internationalen Partnern oder auch angrenzenden Ländern wertvoll unterstützt werden. Eine Teilhabe am Informationsaustausch zu Schwachstellen und Bedrohungslagen sowie konkretere Hilfestellungen müssen durch die öffentliche Hand und bei den zu identifizierenden Akteuren generiert werden. Eine föderale Cybersicherheitsarchitektur muss sich in die des Bundes und in die europäische nahtlos einfügen. Forschungen und die Zusammenarbeit mit Forschungseinrichtungen müssen intensiviert werden, insbesondere in technischer, organisatorischer und rechtlicher Hinsicht.

Erkenntnisgewinne in Deutschland zu generieren wird nicht daran scheitern, dass dies nur mit einer Verfassungsänderung möglich wird. Die Cybersicherheitsarchitektur Deutschlands muss – wie der Staat selbst – föderal gestaltet werden. Eine koordinierende Rolle beim Bund ist möglich und sinnvoll, darf aber nicht zu unterschiedlichen Kenntnisständen in den Ländern führen. Gleichberechtigte Partner sind anzustreben.

Die Länder müssen zuvorderst und mit Weitblick prüfen, welche Kompetenzen sie in einer komplementären Architektur abgeben wollen und welchen nachhaltigen Beitrag zur deutschen Cybersicherheitsarchitektur eine solch einhergehende „Machtverschiebung“ in den Ländern mit sich bringen würde. Jedenfalls sollten Änderungen der von der Verfassung dezentral verstandenen Gefahrenabwehr mit Bedacht gewählt werden. Und es dürfen die Vorteile der abgestuften, aber mitunter ausgeprägt sachbezogenen und örtlich notwendigen Staatsorganisation nicht außer Acht gelassen werden.

8 Federal Cybersecurity Architecture and Information Security Management - Adoption and Diffusion of the NIS-2 Requirements[7]

Abstract: Europe, the federal government, the federal states, municipalities, and their business enterprises are facing the challenges of a hybrid threat situation. At a time when information technology is growing faster than ever before, information cyber security and security management system (ISMS) assessment have become one of the most important aspects of most public sector organisations. The dependency on technology for almost every single process in public sector organisations has put ISMS at the top of the corporate agenda. For public organisations in particular, the NIS 2 Directive describes abstract requirements for the development of an ISMS. At the same time, minimum requirements should be defined that help municipal administration set up an information security management system quickly and easily. This paper summarizes the different requirements and generates a foundation for a rough procedural model, for implementing the upcoming requirements of the NIS-2-Directive quickly and easily in local governments. In particular, the current discussion focuses on securing ICT infrastructures and services of all providers of services of general interest. European and national regulations provide the framework for an appropriate response to this threat to the common good. The federal cybersecurity architecture of a member state such as Germany, presented here, must fit into the European context. Procedures for the implementation of information security management systems complement this theoretical model. This thesis presents a federal cybersecurity model.

Keywords: Security Architecture, Federal Government Institutions

8.1 Introduction

For a federal state in Germany, the respective member state and the European Union, the availability of important consumer goods and infrastructures is part of public services. The public administration is responsible as a guarantor at all levels of the protection of the state, economy, and society (Riek et al., 2016, S. 26), (Watson & Webster, 2020, S. 710). State institutions must act, since the Federal Republic of Germany and its states are obliged to place human needs, including economic ones, at the centre of their activities (Bundesverfassungsgericht, 1982, S. 82–118).

[7] Der Inhalt dieses Kapitels ist bereits wie folgt veröffentlicht worden: Thomas Rehbohm und Frank Moses (2023), Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023), GI Edition Proceedings Band 341

The current threat situation leaves no room for discretion here, information security is endangered and thus higher than ever (Bundesamt für Sicherheit in der Informationstechnik, 2022b). In particular, due to successful attacks on e.g., municipal IT infrastructures or on the IT systems of hospitals, Germany is also called upon to do more for the cooperation of all actors and for a common approach to strengthen resilience.

A functionally effective and federal cybersecurity architecture must be underpinned by the information security management systems of the respective actors. In this context, the strategy and motivation of the state, business and society as well as municipalities are fundamentally comparable, although it is recognized that commercial enterprises serve other stakeholders.

The architectural superstructure is to be produced in consultation with all the federal states and, at best, should be seamlessly embedded in European architecture. According to statements by the Federal Minister of the Interior on the expansion of the German BSI into a central office for cyber security matters, (Bundesministerium des Innern und für Heimat, 2022) a third security pillar is to be created along the lines of the Federal Criminal Police Office (BKA) and the Federal Office for the Protection of the Constitution (BfV). The transfer of competencies in the field of cyber security of the states, in favour of the federal government, may require adjustments but are not the focus of this work.

The research object of this thesis relates to an effective interaction of a federal cybersecurity architecture, which is substantiated with information security management systems – regardless of the framework included – according to the CISIS12 process model and adequately takes into account the requirements of the NIS 2 Directive (Moses & Rehbohm, 2022), (Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie), 2023).

In chapter 2 we give an overview of the state of the art. This is followed by chapter “3 Methodology" that describes the phases of the Design Science approach, which are progressed through step by step. Chapter "4 Federal Cybersecurity Architecture” describes the development of the cybersecurity architecture, considering the requirements of the NIS 2 Directive (chapter 5). These results were structured in a further step in order to develop and describe a rough process model based on them. The results will be used to realize an implementation in practice with the help of the CISIS12 process model (section 6). This process model has already been successfully tested in an artificial environment. Currently, the procedure model is being tested in a real environment with different test subjects. The section 7 briefly summarises the result.

The goal of our research is to identify the specifics of public sector organisations and develop a Cyber Security Architecture and ISMS Approach tailored to their demands. The current requirements of the NIS-2 Directive (Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie), 2023) should be considered.

8.2 State of the art

Research contributions in the context of cyber and information security, combined with topics such as information security management systems, cybersecurity law and cybersecurity architectures, have continued to grow due to the current threat situation and topicality.

European contributions in the field of services of general interest are mainly concerned with internal market law, competition law and, in the context of structural and demographic change, with social, care and health systems. In principle, these are contributions that concern the common good but do not represent the services of general interest related to the ICT structures of a region. State interaction between actors in services of general interest is currently not a research focus; rather, contributions to cybersecurity law are in current discussions (Kipker & Barudi, 2020) or civil security (Gusy et al., 2017) in the context of services of general interest. An in-depth literature review is part of the article "Security Management, Cyber Security and Services of General Interest: Empirical Study in German Municipalities" (Rehbohm et al., 2022). The following examples are extracted from this and are intended to illustrate the topic as examples.

The federal system of the United States is comparable to Germany. In "The Cybersecurity Policy Challenge – The Tyranny of Geography," *Kamarck* recommends that a seamless architecture of collaboration must emerge because, unlike governments, cybersecurity threats are borderless (Andreasson, 2012).

At the European level, *Krajweski's* "Services of general interest beyond the single market" states that in the Treaty of Lisbon, the Member States (national, regional and local authorities) of the European Union, among others, have general responsibility for the "provision, commissioning and organisation" of services of general interest (Krajewski, 2015).

At the national level, the authors of "Cyber Security in Critical Infrastructures" state that the cooperative approach in the field of cyber security has proven its worth, especially because trusting cooperation between the state and business is a "shared mission" (Dürig & Fischer, 2018).

8.3 Methodology

This work is part of a research project aiming at methodical and technological support for cybersecurity architecture and information security management in public sector organisation units. The project follows the paradigm of design science research (DSR) (Johannesson & Perjons, 2014). DSR is a research paradigm aiming at problem-solving in organizational settings with a focus on developing valid and reliable knowledge for designing the required solutions. DSR research projects typically consist of several phases and require the use of different research methods depending on the DSR phase and intended design solution.

This paper concerns the phase requirements definition and design and development of the design solution, i.e., the core artefact. Tabelle 5 Research activities performed in DSR phases and their results provides an overview of the research activities performed in the different phases of the DSR process, the research methods used for these activities, the results achieved and the sections of this paper providing information about the results.

According to the DSR paradigm, the problem investigation must investigate two aspects: the knowledge base and the business relevance. The knowledge base consists in general of the published scientific work in the area under investigation. Using a literature analysis, we identified relevant existing work. The results presented in section 1 confirm that there is no tailored approach in science for a Cyber Security Architecture in the federal context. The business relevance has to show that the research challenge is not only relevant for a small number of organizations, i.e., an isolated “local” problem to solve but has substantial relevance in organizational practice and deserves research. In addition to previous studies confirming the general relevance of a Cyber Security Architecture implementation, a survey among Public Sector Organisations also confirms the existence of inhibiting factors. The phase of requirements definition in DSR addresses the initial definition of the core artefact that is supposed to address the identified problems, and the identification of requirements that the artefact must meet. The artefact in our context is a procedural approach tailored to the needs of Public Sector Organisations on how to introduce ISMS and the Cyber Security Architecture. The needs of Public Sector Organisations are expressed by the requirements which in turn are derived from the inhibiting factors in combination with identified success factors. Design and development of the artefact in DSR is an iterative process accompanied by demonstration or evaluation. As the artefact in its current form is documented in a handbook (already published (Moses & Sandkuhl, 2022)). Demonstration means exposing the first applicable version of the artefact to a real-world application case or experts from the field. Evaluation can use different strategies, like initial evaluation in a lab setting or evaluation in real-world cases. As the artefact already is used by many Public Sector Organisations, we chose a combination of real-world evaluation and evaluation based on the features of the artefact.

DSR Phase	Research activity	Result	Section /Literature
Problem Investigation	Literature analysis to determine the state of research	Inhibiting factors and critical success factors visible in the literature	section 1 (Moses et al., 2022b)
	A survey to determine business relevance	Inhibiting factors visible in the practice of Public Sector Organizations	section 2.2 (Moses et al., 2022a)
Define Requirements	Argumentative-deductive work to derive requirements from results of problem investigation	Summary of inhibiting and success factors List of requirements	section 4

Design and develop Artefact	Conceptual-deductive work to design procedural model based on requirements	ISM procedural model and handbook	summary of this paper section 4 (Moses & Sandkuhl, 2022); (Moses & Rehbohm, 2023a)
Demonstrate	Application of Cyber Security Architecture	Not covered in this work	
Evaluate artefact	Evaluation	Not covered in this work	

Tabelle 5 Research activities performed in DSR phases and their results

First, we have primarily considered the requirements of the NIS-2 Directive in this document. At the same time, we have identified further important requirements through a literature review. We merged both lists of requirements to create an overarching list of requirements as a foundation for the development of a rough procedural model.

8.4 Federal Cyber Security Architecture

Cyber Security architectures should be an elementary component of digital services of general interest in Germany's federal system. (Schallbruch, 2018) Essential actors of a regional structure must be actively connected in such a way that joint interaction can take place before, during and after cybersecurity events. The architectures, which are as harmonious as possible between the federal states, together with the federal government, represent the level of overall security that meets the requirements of European regulation. Initially, the core processes and support processes as well as the processes for the strategy of an enterprise architecture are modelled in the architecture. The inter-organizational process design of the cybersecurity organization is documented as an enterprise architecture that is to be further developed into a reference architecture. The modelling of the reference architecture was done in the modelling language ArchiMate and is shown as an example in Figure 1 on the top. In addition to research, enterprise architecture management has also evolved to provide practical support for decision-support functions in organizations such as administration (D. Simon et al., 2014).

The research presented here aims to determine the interlocking of a federal architecture with the information security management systems of the systemically important actors. Within the framework of a study and expert interviews, various requirements and goals for a federal Cyber Security Architecture were derived (Rehbohm & Kalmbach, 2021), (Rehbohm et al., 2022), (Rehbohm et al., 2021) and (Rehbohm et al., 2019).

The foundation of such an architecture is formed by the support processes, namely **legislative processes**. Furthermore, **communication and cooperation**.

The pillars of the actual Cyber Security Architecture are built on this foundation.

- Compliance
- Risk management
- Operation
- Control and improvement
- Safety standards

On top of these supporting pillars lies the level of strategy and motivation as an umbrella.

Legislative processes: This is an essential support process that includes the obligation of the federal states to initiate legislation and regulations in line with external and internal requirements and to adapt them to the changed European regulations.

Communication and cooperation include all necessary actors and tasks to detect and defend against cybersecurity threats.

Within the framework of the core processes (pillars of the architecture), the following tasks are focused on:

Compliance: Initial and recurring identification of essential legal frameworks.

Risk Management: Monitoring the change in threats to the federal infrastructure and related threats to it and related processes.

Operation: All tasks that guarantee the operation of the cybersecurity architecture.

Control and improvement: Steering committee for assessing resilience and deriving concrete measures to maintain or improve it.

Security standards: All tools, measures and procedures that promote operations on the one hand and the resilience of the cybersecurity architecture on the other, especially in information security.

This cybersecurity architecture aims to achieve the following objectives: legal certainty, applicability, resilience, sustainability, and cooperation. Strategy and motivation are the umbrella process that is mapped in the architecture and visualizes the expectations of the stakeholders.

In addition to these two dimensions of "**strategy, core and support processes" and "goals"**, the cybersecurity architecture consists of another dimension. These are processes that can be individually designed by the users to the respective context. The figure below summarizes these three dimensions (Abbildung 9 Cybersecurity Cube (Architecture, Goals, and Processes)).

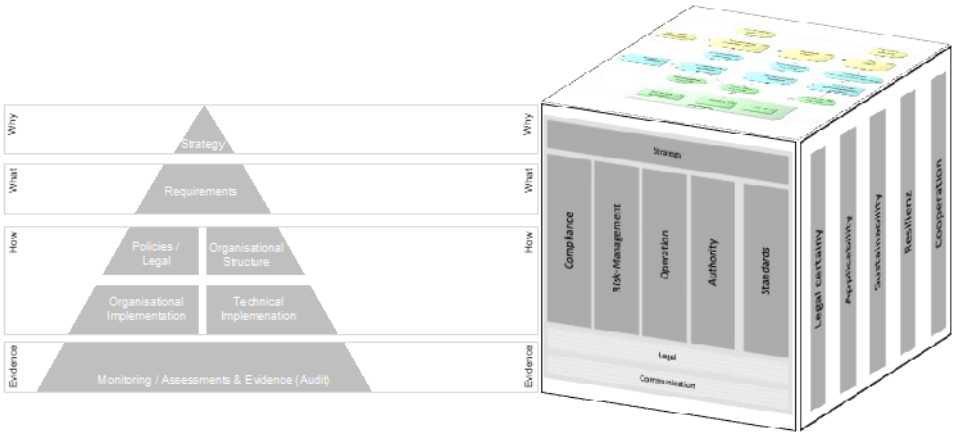

Abbildung 9 Cybersecurity Cube (Architecture, Goals, and Processes)

8.5 NIS 2 Directive

The Network and Information Systems Directive 2 (NIS-2) (Weissmann, 2023) is a European directive that aims to improve cybersecurity in critical infrastructures and digital services. It significantly expands the scope and obligations of the previous Directive and thus provides for various measures to achieve the objective of improved resilience, including:

- **Mandatory security requirements:** Operators of critical infrastructure and digital services must implement appropriate safeguards to identify and prevent threats.
- **Security incident reporting:** Operators must report security incidents to national authorities and share information about these incidents to improve response capability.
- **Establishment of CSIRTs:** National authorities must establish Computer Security Incident Response Teams (CSIRTs) to respond to security incidents.
- **Regular security audits:** Operators must conduct regular security audits and review their security measures to ensure they are adequate and in line with current threats.
- **Cooperation between Member States:** Member States need to work together and share information to join Cybersecurity Cube (Architecture, Goals, and Processes) to combat threats and improve cybersecurity in Europe.

These measures are intended to ensure that critical infrastructures and digital services in Europe, including Germany, are safe and secure, and that they can respond to threats and prevent attacks. In practice, the development and sustainable establishment of an information security management system (ISMS) form an essential foundation for the implementation of the NIS 2 Directive, as an ISMS helps to ensure the security of critical infrastructures and digital services and to respond quickly and effectively to threats (Eckhardt & Kotovskaia, 2023). In Art. 21 of the NIS 2 Directive, four core requirements are formulated that must be met by an ISMS (Weissmann, 2023). These include:

- **Policies:** Risk & Information Security Policies
- **Incident Management:** Prevention, detection, and management of cyber incidents
- **Business Continuity:** Business Continuity Management, Crisis Management
- **Supply Chain Management:** Security in the supply chain — up to secure development at suppliers
- **Procurement:** Security in the procurement of IT and network systems
- **Effectiveness:** Requirements for measuring cyber and risk measures
- **Training:** and Cyber Security Hygiene
- **Cryptography:** Specifications for cryptography and, where possible, encryption
- **Personal:** Human Resources Security
- **Physical access control**
- **Asset Management** (ISMS)
- **Authentication:** Use of multifactor authentication (MFA) and single sign-on (SSO)
- **Communication:** Use of secure voice, video, and text communication
- **Emergency communication:** Use of secure emergency communication systems

At this point, the cyber security architecture described above provides a frame of reference. First and foremost, a strategy must be formulated by the deploying organisation to define the why in the implementation of the cyber security architecture. This is followed by the definition of requirements for the respective context. The organizational and technical implementation of the requirements is coordinated by an appropriate organizational structure and flanked by appropriate guidelines. Corresponding evidence must be generated, for example, by audits, which can then also be used as proof of guarantee against third parties.

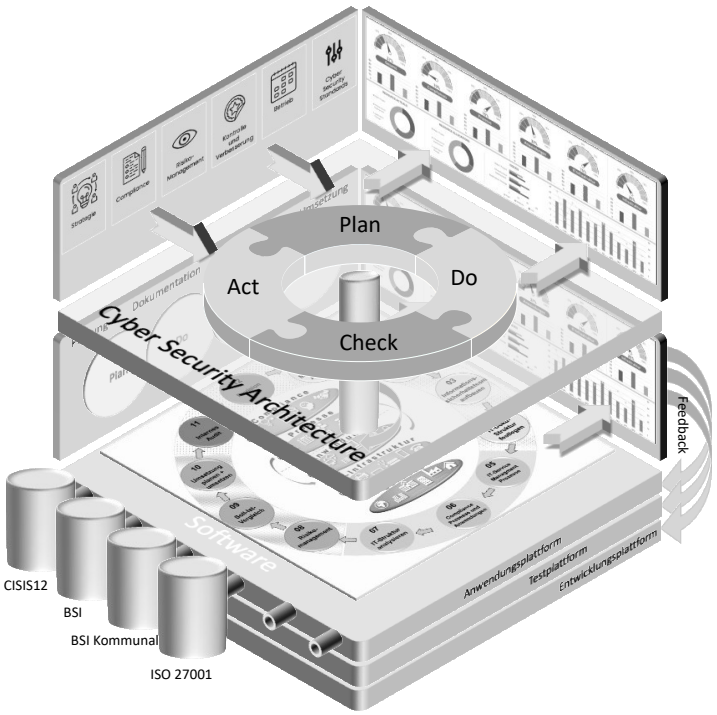

Abbildung 10 Cyber Security Architecture with ISMS

The elements of the cybersecurity strategy are complemented by the cybersecurity strategy (Abbildung 10 Cyber Security Architecture with ISMS). After the theoretical derivation, strategy, requirements, and implementation measures must now be transferred to a practicable procedural model. First and foremost, the requirements of the core processes of the cybersecurity architecture act on an axis of rotation, which in turn drives the development and establishment of an ISMS. With the help of the Deming Circle, individual adaptations from the cybersecurity architecture can be transferred to the ISMS. From the ISMS, aggregated results are fed back into the control centre of the higher-level cybersecurity architecture, which allows the legally required supervisory management to be fulfilled. The user can decide for himself which standard (BSI baseline protection, ISO/IEC 27001, or others) should be used to set up and establish the ISMS.

8.6 CISIS12

Public organisations in particular often lack the necessary resources and expertise to set up an ISMS with which the measures formulated in the NIS 2 Directive can be implemented (Moses et al., 2022a). Here, the CISIS12 (Compliance and Information Security in 12 Steps) process model (Moses & Rehbohm, 2023a) offers a quick and easy introduction to the topic of ISMS for public organizations (Moses & Sandkuhl, 2022).

Step 1 Guideline: The focus of the first step is the creation of a guideline on information security as one of the reference documents of the CISIS12 standard and an essential element of an ISMS (Moses et al., 2022a).

Step 2 Raising awareness among employees: In many projects, the consideration of employees is only at the end of the project (Tatiara et al., 2018). However, it is precisely the issue of cyber security that primarily affects employees and managers. As part of step 2, a process must be established based on an appropriate concept to ensure training, sensitisation, and information for employees. However, it is important that after employees have been sensitized for the first time, sustainability is ensured by the training concept in a target group-specific manner.

Step 3 Information security team: The roles necessary for the development of the ISMS are fixed here in writing, tasks, rights and obligations are defined and an ISMS team is formed. Depending on the size of the organization, it is necessary to determine with which roles the upcoming ISMS project is to be carried out and which employees have roles in the core team and which employees have roles in the extended security team. Regardless of this organizational structure, a member of the organizational leadership must be integrated into the extended team in any case (Choejey et al., 2016).

Step 4 IT documentation structure: The PDCA cycle immanent in a management system focuses on the "P for plan". No successful project, without a good plan. Against this background, step 4 of the CISIS12 process model focuses on the creation and updating of a documentation structure suitable for the ISMS (Susukailo et al., 2022). Documentation that is intended to support the organization in the operation of the ISMS on the one hand, but also serves as proof of certification on the other, must meet the requirements of structure, clarity, completeness, comprehensibility, correctness, traceability, objectivity, integrity, and authenticity. The CISIS12 standard lists the 16 mandatory documents (e.g., guidelines, training and awareness-raising concept, operating manual and network plan to a management report including implementation and risk treatment plan and emergency manual). In addition to these certification-relevant reference documents, further documents are inevitably created when the 12 steps are completed, e.g. work instructions, process descriptions or concepts. Almost all documentation must be made known to the employees and therefore controlled.

Step 5 IT service management: One of the main differences to other ISMS process models is the implementation of IT service management in the CISIS12 process model. The implementation of clearly defined and described IT service management processes is a key success factor for increasing information security and maturity of the ISMS (A-wan, 2017). In step 5, the three essential IT service management processes (maintenance, malfunction and change processes) are to be set up in an organization-specific manner or the processes that already exist in reality are to be integrated into the ISMS and further developed.

Step 6 Compliance, Processes and Applications: CISIS12 has taken up the requirements from practice, namely, to integrate the legal requirements and contractual obligations (compliance) as well as the process view into the management system and includes five levels of consideration, namely the compliance and process layer as well as the

application and infrastructure and building level. Thus, CISIS12 offers a view that corresponds to that of the management level, namely "Which legal requirements and compliance requirements must the management level meet and how can these be implemented in practice (corporate governance)?". Thus, the CISIS12 process model makes it easier for the management level to act and delegate the necessary tasks to set up and establish an ISMS while at the same time meeting the legal requirements and minimizing the liability risks of the management level. This means that in step 6, the business processes that are essential for the organization are identified and evaluated concerning the protection requirements of confidentiality, integrity, and availability. This can be done with the help of tools, as can the assignment of modules and measures.

Step 7 IT infrastructure: The recording of IT infrastructure objects (e.g. servers, clients, active network components, etc.) is derived from the business processes identified in step 6 and the applications necessary for these business processes and forms an important pillar of the ISMS (CHODAKOWSKA et al., 2022). Thus, a simplification for the user also occurs here. In this way, attention can be drawn to the implementation of the module and measure assignment.

Step 8 Risk management: Risk management is a major innovation in the CISIS12 process model (Kitsios et al., 2022). The geopolitical events of the past few months have shown that the development of an information security management system is no longer a hygiene factor (hygiene factor = works without it, but a little worse). No, an ISMS is now a "must-have" (state of the art) for all organizations and a risk management system established in it is an important tool for learning from the past and being able to better assess future events.

Step 9 Target/actual comparison: In step 9, the measures from the CISIS12 building block catalogue modelled in steps 6 and 7 are evaluated concerning the degree of implementation. This evaluation process takes place within the framework of a group dynamic process and represents a self-evaluation. This process may be supported by external third parties.

Step 10 Implementation: The degree of implementation of the individual measures determined in Step 9 can be transferred to an implementation plan in Step 10 with the help of tools, if necessary. Individual measures can be prioritized, their financial and personnel expenses can be recorded, and the roles of the initiator and the implementer can be defined with the help of tools. No system is perfect, and more is always possible. This also applies to the ISMS built with CISIS12. The maturity level of a management system with CISIS12 only develops with several runs. The initial audit is therefore referred to as a system audit, whereby the certification audit focuses on the documentation and implementation of the plan documents (lived security process). The surveillance audit then examines how the ISMS has developed further and how this further development affects the maturity level.

Step 11 Internal Audit: In step 11, CISIS12 requires the organization to create an appropriate audit program. This audit program should then include the respective certification as well as internal audits. With the help of internal audits, the organization itself should be able to examine its own ISMS for weaknesses and improve it accordingly (Pohlmann, 2019).

Step 12 Revision: CISIS12 steps 1 to 11 must be completed regularly (e.g. annually). However, changes and additions can also be introduced into the management system at any time. Step 12 summarizes the results of the final PDCA phase and ends with the preparation of a management report. Step 12 summarizes the results of the final PDCA phase and ends with the preparation of a management report. At the same time, the management report is one of the certification-relevant reference documents. As soon as the management level has approved the management report including its assets, the next PDCA phase can begin and the continuous improvement process can be initiated (Preis & Susskind, 2022). The entire process is supported by the CISIS12 circuit – possibly tool-based.

8.7 Summary, Conclusions and Outlook

The NIS 2 Directive requires in Art. 21 fourteen measures to be implemented by federal states. The developed cybersecurity architecture forms a good procedural model for identifying, planning, implementing and sustainably establishing and controlling these measures and associated requirements. An essential tool here is the selection of a suitable process model for the further implementation of an information security management system as the basis of a higher-level cybersecurity architecture. The presented cybersecurity architecture can be used can be underpinned by the CISIS12 process model. The implementation of CISIS12 is open. An ISMS can be set up with the native CISIS12 catalogue. However, it is also possible to use other module measure catalogues with the process model, e.g., "BSI-IT-Grundschutz", "BSI-Kommunalprofil" or ISO/IEC 27001, CIS-Controls, or other proprietary measures. In particular, the aspects of the NIS 2 guideline such as guidelines, awareness and training measures for employees, incident management, business continuity management and implementation of technical and organizational measures can be implemented in a target group-adapted manner with the help of the CISIS12 process model. The result is an overall cybersecurity architecture that can meet the requirements of the NIS 2 Directive. It does not matter whether users choose a top-down approach or a bottom-up approach. Due to the interlocking of the two architectures, each approach can be started independently of the other and the necessary information can be exchanged via interfaces (Abbildung 9 Cybersecurity Cube (Architecture, Goals, and Processes)).

One limitation of the present work is that the presented theoretical cybersecurity architecture has not yet been evaluated practically. Plans are currently underway to verify the architecture in conjunction with the establishment of an ISMS in a municipal organization.

The logical final step is the evaluation of the overall architecture in the country context. For this purpose, the overall architecture is to be presented within the framework of the working group on the cyber security of the federal states. Depending on the evaluation results, the architecture will be further developed.

9 Entwicklung eines modularen ISMS und DSMS, Datenschutz und Datensicherheit[8]

Zusammenfassung: Der Schutz von Informationswerten erfordert einen interdisziplinären Ansatz und funktionsübergreifende Fähigkeiten. Die Norm ISO/IEC 27701:2019 für Informationssicherheit und Datenschutz bietet Unterstützung für alle Organisationen, die Systeme zur Einhaltung des Datenschutzes einrichten möchten. Der vorliegende Beitrag untersucht, ob und inwieweit das ISO/IEC 27701:2019-Rahmenwerk eine Chance für die Umsetzung der DSGVO über ein Managementsystem darstellt. Es wird ein prozedurales Framework vorgestellt, das unterschiedliche Normen (ISO 27701:2019, SDM 3.0, BSI oder CISIS12 und weitere) verbindet, damit der Aufbau und die Etablierung eines ISMS und eines DSMS in der Praxis leicht umsetzbar werden.

9.1 Einleitung

Die Informationssicherheit ist aufgrund der zunehmenden Angriffe auf Unternehmen eines der größten Probleme und stellt somit ein erhebliches Risiko für die Organisationen dar. Die Sicherheit personenbezogener Daten (PII) ist eines der grundlegenden Menschenrechte des Eigentümers von Informationen. Auf der ganzen Welt gibt es bereits Gesetze zum Schutz dieser Rechte oder sie werden in einem Ökosystem, in dem die Verarbeitung von Daten globalisiert wird und die Besorgnis über die Verwaltung von PII zunimmt, umgesetzt und gestärkt. Die DSGVO (engl. GDPR) ist wahrscheinlich die bekannteste Datenschutzverordnung (University of Technology Sydney, AU et al., 2018), obwohl viele andere Länder wie USA, Korea, die Philippinen und auch China ebenfalls Datenschutzgesetze eingeführt haben. Die Entwicklung eines Systems, das die unterschiedlichen Compliance-Anforderungen aus Datenschutz und Informationssicherheit erfüllt, stellt eine der größten Herausforderungen für Organisationen dar, die mit den notwendigen Anforderungen an die geschäftliche Flexibilität Schritt halten und sich gleichzeitig schützen wollen.

Die Internationale Organisation für Normung (ISO) und die Internationale Elektrotechnische Kommission (IEC) haben diesen dringenden Bedarf an einem allgemeinen Anforderungskatalog für das Management der Sicherheit von personenbezogenen Daten unabhängig von speziellen gesetzlichen oder behördlichen Anforderungen erkannt und die Norm ISO/IEC 27701:2019 vorgestellt, um dafür in einem variierenden regulatorischen Umfeld eine Anleitung zu bieten.

Die Unterschiede in den Datenschutzgesetzen auf der ganzen Welt wurden als Hindernis für die auf dem internationalen Markt tätigen Organisationen erkannt (Bougiakiotis, 2020). Eine allgemeingültige GDPR Zertifizierung (University of Technology Sydney, AU

[8] Der Inhalt dieses Kapitels ist bereits wie folgt veröffentlicht worden: Frank Moses und Thomas Rehbohm (2023), Datenschutz und Datensicherheit, DuD

et al., 2018) für alle Regionen und Branchen ist unerlässlich, um das Risiko zu beherrschen und folglich die Hindernisse für den Handel zwischen Geschäftspartnern zu verringern. Die ISO/IEC 27701:2019 soll ein branchenunabhängiger Standard für den Datenschutz sein, der sicherstellt, dass alle Organisationen, ob klein oder groß, die in verschiedenen Rechtsordnungen tätig sind, die von ihnen gespeicherten personenbezogenen Daten effizient schützen und verwalten. Es wird erwartet, dass der interoperable Standard den Organisationen helfen wird, den Weg zur Einhaltung der Datenschutzgrundverordnung zu beschreiten.

Es ist jedoch unklar, ob ISO/IEC27701:2019, GDPR oder beides implementiert werden muss, um den globalen Compliance-Anforderungen gerecht zu werden. Literaturrecherchen zeigen, dass es kaum Informationen darüber gibt, wie die ISO/IEC27701:2019 mit den am weitesten verbreiteten Vorschriften zum Schutz der Privatsphäre und des Datenschutzes (wie der DSGVO) übereinstimmt (University of Technology Sydney, AU et al., 2018). Daher verfolgt dieser Beitrag den Ansatz, diese elementare und wichtige Lücke zu füllen, indem die Überschneidungen und Unterschiede zwischen der ISO/IEC 27701:2019 und der DSGVO analysiert werden. Hierzu wird das Vorgehensmodell CISIS12 (Moses & Sandkuhl, 2022) verwendet, mit dem Anforderungen aus ISO/IEC 27701:2019 und DSGVO systematisch überprüft und abgebildet werden.

9.2 Unterschiede und Gemeinsamkeiten ISO 27701 vs. DSGVO

Der in der ISO/IEC 27701:2019 vorgeschlagene Ansatz unterscheidet

sich in vielerlei Hinsicht von dem in der DSGVO verankerten:

- Zunächst einmal macht die ISO den Datenschutz von der Informationssicherheit abhängig, während in der DSGVO die Informationssicherheit eine separate Komponente bleibt.
- Die DSGVO bezeichnet den Datenschutz als allgemeines Prinzip.
- Die ISO/IEC 27701:2019 fordert zur Gewährleistung des Datenschutzes einen vollständig risikobasierten Ansatz, der die Identifizierung und Reduzierung von Informationssicherheitsrisiken für IT-Ressourcen ermöglicht, die PII verwalten und speichern. Die DSGVO stützt sich punktuell auf einen risikobasierten Ansatz, um umfassendere Risiken für die Rechte und Freiheiten der betroffenen Personen zu reduzieren.
- Die DSGVO ist eher ein rechtsbasierter Ansatz.
- Darüber hinaus bescheinigen die auf ISO/IEC 27701:2019 basierenden Systeme die Konformität mit einem Managementsystem, aber die DSGVO schließt die Zertifizierung von Managementsystemen aus dem Geltungsbereich der von der DSGVO genehmigten Zertifizierung aus.

- Die ISO-Normen sind privat und durch ein strenges Urheberrecht geschützt, während die DSGVO verlangt, dass die Zertifizierungsanforderungen von einer Aufsichtsbehörde genehmigt und öffentlich und leicht zugänglich gemacht werden.
- Die durch ISO/IEC 27001 und ISO/IEC 27701:2019 geschützten Daten umfassen Datensätze, die in IT-Anlagen strukturiert sind, während die DSGVO auch für unstrukturierte Datensätze gilt, z. B. eigenständige Textdateien, Tabellenkalkulationen und in Schränken aufbewahrte Dateien.
- Darüber hinaus gilt die DSGVO nicht nur für die digitalisierte Datenverarbeitung, sondern auch für die Verarbeitung und Speicherung personenbezogener Daten auf physischen Medien (z. B. papierbasierte Aufzeichnungen).
- Die DSGVO zielt nicht nur auf die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen ab, sie beleuchtet auch die Wahrscheinlichkeit und Schwere (der Risiken) für die Rechte und Freiheiten natürlicher Personen. Demgegenüber definiert die ISO/IEC 27701:2019-Norm ihre eigenen Anforderungen mit ihrer eigenen Terminologie.
- Die Norm ISO/IEC 27701:2019 schlägt ein Managementsystem vor, das mit anderen von der ISO veröffentlichten Managementsystemnormen übereinstimmt; d. h. die ISO 27701 ist kein eigenständiger Standard, der einzig und allein Organisationen hilft, ein DSMS aufzubauen (Sowa & Rost, 2020, S. 659–662). Im Gegenteil: Sie ist als Ergänzung zu einem bestehenden ISMS (gleich welcher Art) zu verstehen. Andererseits bietet die DSGVO kein Managementsystem nach der ISO-Definition.
- Die DSGVO schafft lediglich einen Rechtsrahmen, der Grundsätze und Anforderungen festlegt und nicht darauf abzielt, gebrauchsfertige Leitlinien bereitzustellen, die helfen, die Anforderungen des Rechtsrahmens zu erfüllen. Trotz der Unterschiede verfolgen beide Ansätze das gleiche Ziel. In der Tabelle 6 Gemeinsamkeiten der ISO 27701 und der DSGVO ((International Organization for Standardization, 2019), (Däubler et al., 2024) sind die Gemeinsamkeiten und Ziele gegenübergestellt.

Gemeinsamkeiten und Ziele	ISO 27701	Artikel in der DSGVO
Verstehen der Organisation	5.2.1	24, 25, 28, 32, 40, 41, 42
Identifikation der Stakeholder	5.2.2	31, 35, 36
Rollen und Aufgaben (Verantwortlicher, Auftragsverarbeiter)	7.2.6, 7.2.7, 7.2.8, 7.3.2, 7.3.3, 7.3.5, 7.3.7, 7.3.8, 7.4.9, 8.2.5, 8.3.1, 8.4.2, 8.5.1, 8.5.3, 8.5.4, 8.5.6, 8.5.7, 8.5.8,	5, 11, 13, 14, 15, 18, 20, 21, 24, 26, 28, 44, 45, 46, 47, 49
Scope des ISMS, Risikomanagement und Risikobehandlung	5.2.3, 5.2.4, 5.4.1.2, 5.4.1.3	32

Rollen und Verantwortlichkeiten für Richtlinien, Sensibilisierungs-Maßnahmen und Umgang mit Sicherheitsereignissen	6.3.1.1, 6.3.2.1, 6.4.2.2, 6.5.3.1, 6.8.2.7, 6.9.3.1, 6.9.4.1, 6.9.4.2, 6.10.2.1, 6.10.2.4, 6.13.1.1, 6.13.1.5	27, 28, 33, 34, 37, 38, 39
Durchführung einer Datenschutzfolgen-Abschätzung	7.2.5	35, 36
Identifikation von Compliance-Anforderungen	6.15.1.1, 6.15.2.3	5, 28, 30, 32

Tabelle 6 Gemeinsamkeiten der ISO 27701 und der DSGVO

9.3 SDM 3.0 als Ergänzung zu einen ISMS

Trotz der zahlreichen Gemeinsamkeiten greifen beide Ansätze zu kurz, da wesentliche Elemente nicht betrachtet werden. Diese Lücke kann durch das Standard-Datenschutzmodell (SDM) in der aktuellen Version geschlossen werden. Die ISO 27701 setzt darauf, dass weitere Maßnahmen durch andere Normen aus der Normfamilie abgedeckt werden. Demgegenüber liefert das SDM 3.0 zwar abstrakte (Rost, 2022) Maßnahmen als Umsetzungshinweise (TOMs); detaillierte Handlungsanweisungen fehlen jedoch, was ggf. damit erklärt werden kann, dass der aktuelle IT-Grundschutz in seinem Baustein (CON.2) auf das SDM 3.0 verweist und damit gleichzeitig das SDM sich aus Umsetzungsmaßnahmen aus dem IT-Grundschutz bedient (Deutschland, 2023).

Dennoch ist das SDM 3.0 eine sinnvolle Ergänzung, da es genau die oben geschilderten rechtlichen Anforderungen aufgreift und mit dem in der aktuellen Version vorgestellten SDM-Würfel einen abstrakten, aber sehr treffenden Ansatz vorstellt, der ein ISMS sinnvoll ergänzt und damit zwei wesentliche Elemente eines übergreifenden Managementsystems adressiert werden können – insbesondere Aufbau und Etablierung eines ISMS und eines DSMS. Das SDM fasst mit einem dreidimensionalen Würfel die Anforderungen des Datenschutzes zusammen. Die erste Dimension beleuchtet die Gewährleistungsziele (Datenminimierung, Transparenz, Nichtverkettbarkeit, Intervenierbarkeit, Integrität, Vertraulichkeit und Verfügbarkeit). Auf der zweiten Dimension werden mögliche (Kern-)Verarbeitungsaktivitäten (Kollektion, Bereithaltung, Nutzung und Beseitigung) beschrieben. Diese Verarbeitungsaktivitäten werden in Sub-Aktivitäten aufgeteilt, die ggf. einzelnen Geschäftsprozessen (Fachverfahren) zugeordnet werden können. Diese Sub-Aktivitäten können dann mit einer oder mehreren Anwendungen (Fachapplikationen) betrieben werden (Abbildung 11 SDM 3.0 Würfel (Rost, 2022)).

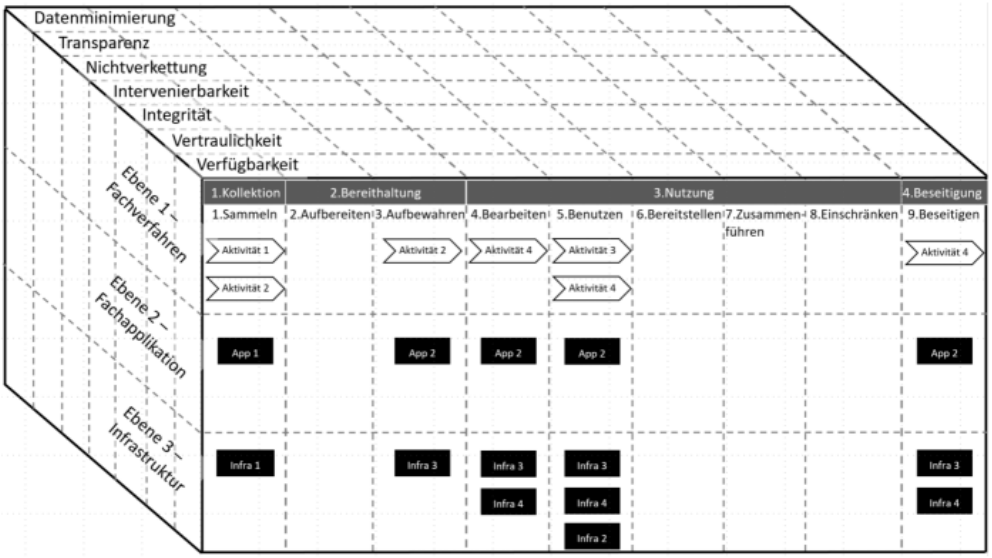

Abbildung 11 SDM 3.0 Würfel (Rost, 2022)

Diese Fachapplikation wird i.d.R. auf einem Server oder Client (IT-Infrastruktur) betrieben. Fachverfahren, Fachapplikation und Infrastruktur bilden somit die Elemente der dritten Dimension des SDM-Würfels.

Auf den ersten Blick bestehen damit (7*3*9) = 189 Kombinationsmöglichkeiten der Elemente der einzelnen Dimensionen des Würfels, um damit „Datenschutz“ zu modellieren (Rost, 2022). Auf den zweiten Blick wird aber sofort deutlich, dass mit Hilfe des Würfels ein Raum für die Bewertung der Risiken für PII aufgespannt wird. Dieser Raum kann über eine einfache Funktion adressiert werden:

Risiko (GZ, VV, VE) = $\sum_1^7 GZ + \sum_1^3 VV + \sum_1^9 VE$

Legende: GZ = Gewährleistungsziel, VV = Verarbeitungsvorgang, VE = Verarbeitungsebene

Damit ist es möglich die auftretenden Risiken für personenbezogene Daten über die einzelnen Dimensionen und darin enthalten Elemente zu modellieren und zu bewerten. Ob in der Praxis jede Kombinationsmöglichkeit modelliert, analysiert und bewertet werden muss, bleibt offen. Durch den aufgespannten Raum besteht aber die Möglichkeit bestimmte Variablen auf einen festen Wert zu setzen und damit vorerst aus der Betrachtung auszublenden. Bei der Restmenge handelt es sich dann nur noch um ein zweidimensionales Objekt, das wesentlich leichter modelliert, analysiert und bewertet werden kann und somit für den Anwender leichter „zugänglich“ ist.

Gerade die Elemente Fachverfahren, Fachapplikation und Infrastruktur werden bereits durch ein ISMS beleuchtet und mit entsprechenden Maßnahmen unterlegt, die der Resilienz dienen. Managementsysteme auf Basis von ISO 27001 oder BSI-Grundschutzes sind oft zu mächtig, um in kleinen Organisationen schnell und einfach eingeführt zu werden.

9.4 Vorgehensmodell CISIS12

Das prozedurale Vorgehensmodell CISIS12 (Abbildung 12 CISIS12-Vorgehensmodell) wurde in dieser Zeitschrift bereits vorgestellt (Moses & Sandkuhl, 2022). CISIS12 steuert entlang eines vorgegebenen Pfades den Aufbau eines ISMS in 12 Schritten. Dabei kann sich das Vorgehensmodell unterschiedlicher Maßnahmenkataloge bedienen, wie z. B. des BSI-IT-Grundschutzes, des BSI-Kommunalprofils, der ISO 27001, CIS-Controls und weiterer beliebiger Kataloge, einzeln oder in einer Mischform.

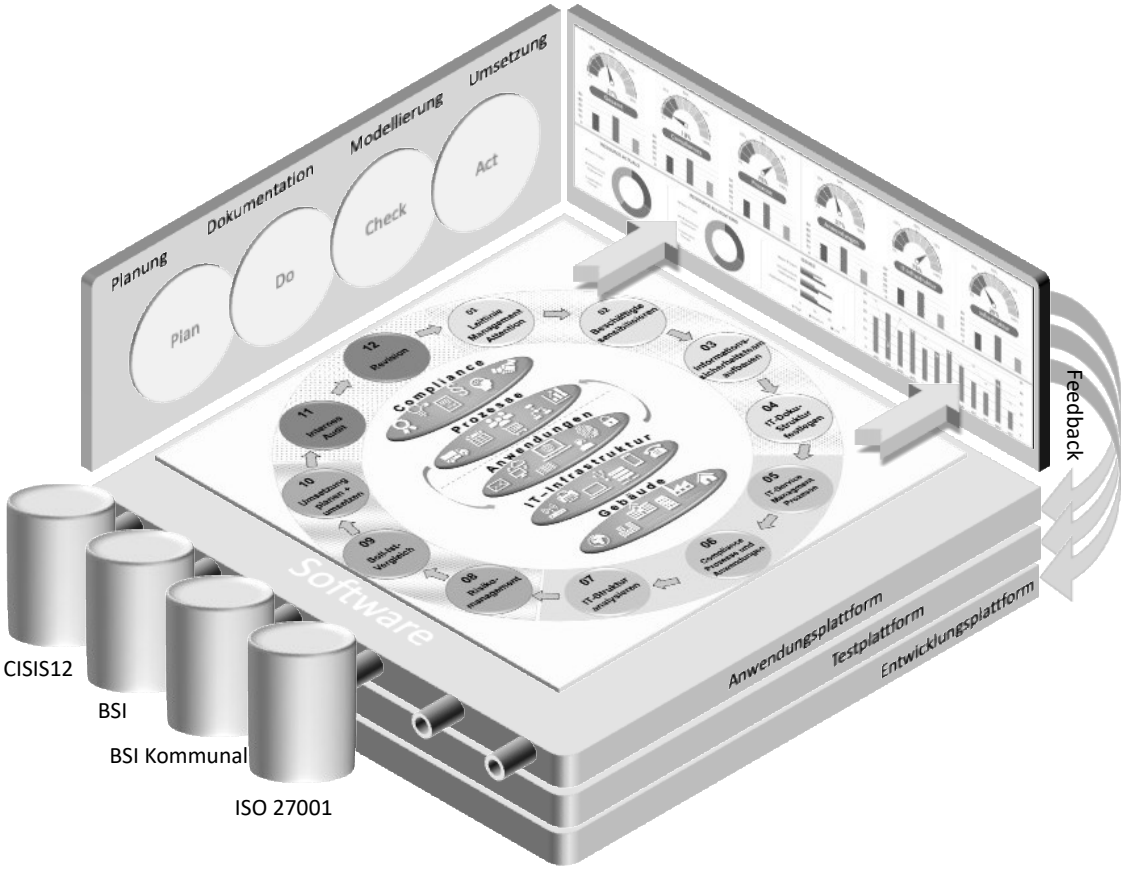

Abbildung 12 CISIS12-Vorgehensmodell

Den Kern des Vorgehensmodells bilden die Assets einer Organisation. Dazu gehören neben den Compliance-Vorgaben und Perimeter (Gebäude) auch die im SDM erwähnten Fachverfahren, Fachapplikationen und Infrastrukturen. Diese Überschneidung kann genutzt werden, um das SDM mit dem CISIS12-Vorgehensmodell zu verbinden. Die Assets werden im Rahmen der Schritte 6 und 7 des Vorgehensmodells modelliert.

Im Schritt 8 können diese einer Risikobetrachtung (in Anlehnung an *Romeike*) in Bezug auf die Gewährleistungsziele unterzogen werden (Romeike & Finke, 2003). Mit Hilfe einer solchen Risikobetrachtung wird im Kontext eines ISMS versucht, die Sicherheit der Verarbeitung zu bewerten und durch entsprechende Maßnahmen aufrechtzuerhalten. Genau an dieser Stelle können die beiden Ansätze verbunden werden, wodurch die vom

SDM vorgeschlagene Risikobetrachtung bzgl. der Gewährleistungsziele mit Hilfe der Risikobetrachtung des ISMS-Vorgehens durchgeführt werden kann und gleichzeitig Maßnahmen zur Risikobehandlung (Reduktion, Vermeidung, Verlagerung oder Akzeptanz) geplant und umgesetzt werden können.

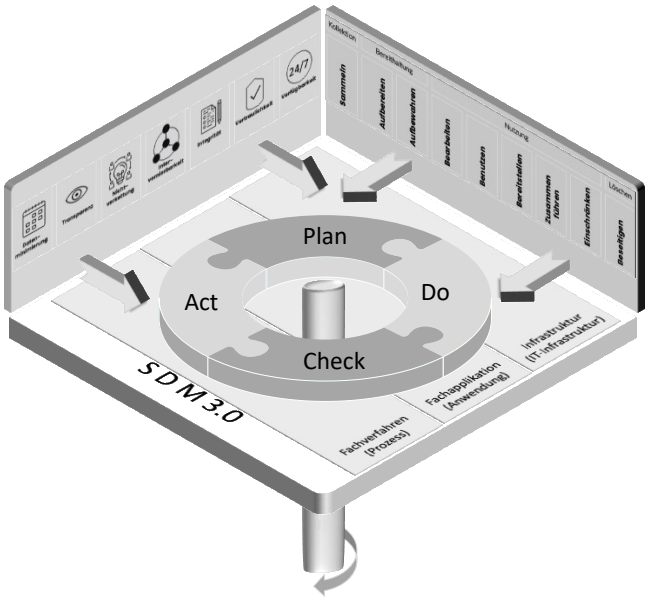

Abbildung 13 SDM Würfel – abgewandelte Darstellung

Art. 32, Abs. 1 lit. d DSGVO fordert „...ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (TOMs) zur Gewährleistung der Sicherheit der Verarbeitung“. Im Schritt 9 wird durch einen Soll-Ist-Vergleich geprüft, welcher Reifegrad bzgl. der TOMs vorliegt. Bei einer Zielabweichung wird die weitere Umsetzung im Schritt 10 geplant. Die jährliche Überprüfung wird durch eine interne und externe Bewertung in den Schritten 11 und 12 sichergestellt.

Im weitesten Sinne wird somit der PDCA-Zyklus in einem ISMS etabliert. Über diese Drehachse können ein ISMS und das SDM verbunden werden. Die nachfolgende Abbildung 13 SDM Würfel – abgewandelte Darstellung, stellt den SDM-Würfel leicht abgewandelt dar. Die Gewährleistungsziele, Verarbeitungsvorgänge und Verarbeitungsebenen sind auch hier in einer dreidimensionalen Darstellung angeordnet. Werden nun beide Denkansätze zusammengefügt entsteht ein neues Gebäude, das in der Fundierung den Aufbau und die Etablierung eines ISMS beinhaltet und über eine Drehachse und Rückkopplungsprozesse Informationen in das SDM übergibt bzw. aus diesem zurückerhält.

Das fundamentale ISMS-Vorgehensmodell ist offen gestaltet, sodass die Vorteile einzelner Standards oder Vorgehensweisen in einem Artefakt vereint werden können. Somit besteht die Möglichkeit ein ISMS auf Basis unterschiedlicher Anforderungen (Normen) und unterschiedlicher Zielrichtungen und Detailtiefen aufzubauen. Eine Integration des

bayrischen LSI-Siegels 3.0 ist ebenso möglich wie die des CISIS12-Bausteinkatalogs, der Bausteine des IT-Grundschutzes oder des BSI-Kommunalprofils bzw. weiterer Profilderivate des IT-Grundschutzes sowie branchenspezifischer Standards (B3S). Nicht zuletzt können die Anforderung des Anhangs A der ISO-Norm-Familie integriert werden, wie ISO 27001 oder 27701. Damit ist sichergestellt, dass auch kleine oder mittelgroße Organisationen unterschiedlicher Branchen aber auch kleine Kommunalverwaltungen oder Stadt- und Landratsverwaltungen einen leichten Einstieg in das komplexe Thema Informationssicherheit finden.

Darauf aufbauend kann in einem weiteren Schritt der Datenschutz in ein ganzheitliches Managementsystem integriert werden. Wesentlich dabei ist, dass keinem der beiden Regelungsbereiche (Informationssicherheit bzw. Datenschutz) das Primat zugeordnet werden kann.

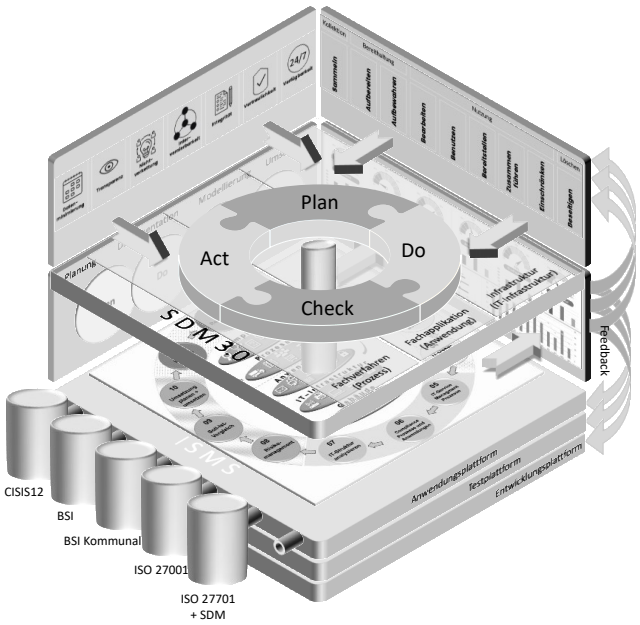

Abbildung 14 Kombination des ISMS-Vorgehensmodells mit dem SDM-Würfel

Die Komplexität der IT, der Grad der Vernetzung, die steigende Abhängigkeit von IT und IT-betriebenen Prozessen und die sich veränderte Gefährdungslage (Boll, 2023), die damit ggf. verbundene Gefahr des Abflusses von Daten sowie die aktuellen Entwicklungen im Kontext der KI verdeutlichen die Notwendigkeit der Verknüpfung der beiden Welten (Pistorius, 2018). Ein handhabbares integriertes Managementsystem ist dann ein Instrument, um sowohl Datenschutz als auch Informationssicherheit dauerhaft zu analysieren, zu systematisieren, zu strukturieren, zu optimieren und proaktiv zu steuern bzw. zu überwachen (Hanschke, 2020). Die hierfür notwendigen Werkzeuge zur Planung, Durchführung und fortlaufenden Optimierung bietet das vorgestellte Vorgehensmodell in Verbindung mit der Erweiterung um das SDM.

9.5 Informationssicherheit und Datenschutz als Teil einer Cybersicherheitsarchitektur

Wird die vorgenannte Vorgehensweise noch weiterentwickelt, kann das etablierte ISMS und DSMS auch als Teil einer übergeordneten Cybersicherheitsarchitektur verstanden werden. In diesem Fall wird eine weitere „Etage“ im Gebäude ergänzt. Sowohl auf föderaler als auch auf Bundesebene wird definiert, welche Elemente des jeweiligen Systems an die übergeordnete – zum Beispiel föderale Cybersicherheitsarchitektur – technisch und organisatorisch angebunden wird, um die Aufsichtspflichten nach der NIS-2-Richtlinie erfüllen zu können (Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie), 2023). Eine wirksame föderale Cybersicherheitsarchitektur soll dabei die strukturellen Rahmenbedingungen, technische Interaktionen und Rechtssicherheit schaffen, die eine gleichberechtigte Teilhabe aller Akteure ermöglichen. Eingebunden werden alle zu identifizierenden Stellen in der Architektur für präventive, situative und reaktive Aufgaben, welche ergänzend durch regulatorische Maßnahmen abgesichert werden. Das bedeutet im Einzelnen, dass nach Einstufung der Akteure in „wesentlich“ oder „wichtig“ für die Daseinsvorsorge, insbesondere Kontrollen, Berichtspflichten und der Echtzeit-Informationsaustausch zu berücksichtigen sein werden. Damit kann das bestehende Managementsystem (ISMS und DSMS) um übergeordnete Strategieelemente ergänzt werden, um die von *Hanschke* formulierte Steuerung auf Managementebene zu zentralisieren und entsprechende Rückkopplungen aus den einzelnen „Gebäudeetagen“ sicherzustellen (Hanschke, 2020). Die Strategie – zum Beispiel in einem Bundesland – wird dabei von intrinsischen und extrinsischen Motiven befördert. Intrinsische Motive liegen in der Wirtschaftlichkeit, Nachhaltigkeit und Widerstandsfähigkeit der angestrebten Lösung. Extrinsische Motive liegen in der Rechtskonformität bzw. Compliance und in der Reputation, also der Glaubwürdigkeit der Organisation und des in sie gesetzten Vertrauens. Die nachstehende Abbildung 15 Cybersicherheitsarchitektur als Ergänzung zum ISMS und SDM fasst die vorgestellte Cybersicherheitsarchitektur kurz zusammen.

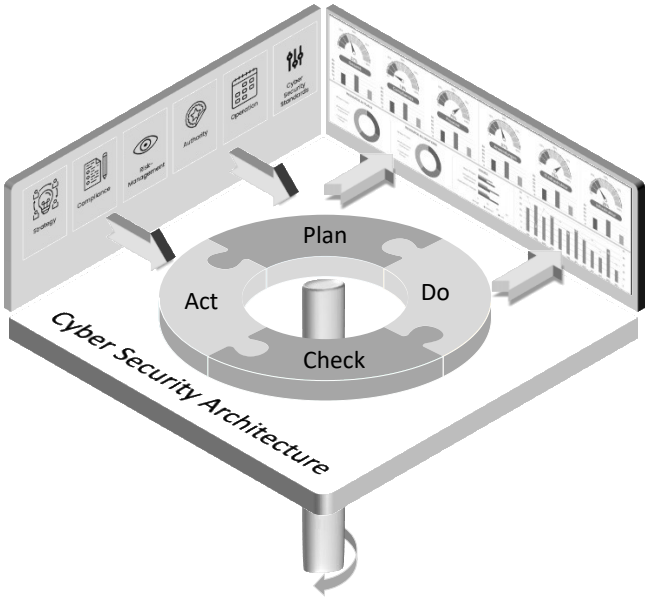

Abbildung 15 Cybersicherheitsarchitektur als Ergänzung zum ISMS und SDM

9.6 Zusammenfassung

Managementsysteme für Datenschutz (ISO 27701, SDM) und Informationssicherheit (ISO 27001, BSI, usw.) sind vorhanden. Dennoch fehlt es an klaren Vorgaben, Leitfäden und einfachen Umsetzungsmöglichkeiten, sprich einfachen und handhabbaren Vorgehensmodellen, die es kleinen bis mittleren Organisationen ermöglichen, die Einführungshürden leichter zu überwinden. Mit dem vorgestellten Vorgehensmodell besteht die Möglichkeit ein ISMS unter dem Motto „...think big, start small and grow step by step“ aufzubauen und sukzessive fortzuentwickeln. Gerade diese einfache „Zugänglichkeit“, die Systemoffenheit und damit die Möglichkeit „the best of bread“ auszuwählen, um schnell und einfach ein Managementsystem für Informationssicherheit aufzubauen, hilft kleinen Organisationen. Durch die Modulstruktur kann ein ISMS als Teil einer übergreifenden Cybersicherheitsarchitektur bzw. -strategie etabliert werden.

Alternativ besteht die Möglichkeit, das ISMS um Datenschutzaspekte zu ergänzen und sich in dem Fall dem SDM als sinnvoller Ergänzung zu bedienen. Es können aber auch alle drei „Etagen“ des Gebäudes genutzt werden, womit eine ganzheitliche Steuerung der Gesamtstrategie (Cybersicherheit, Informationssicherheit und Datenschutz) möglich ist.

Es obliegt der Organisation zu entscheiden, mit welchen Normen ein ISMS oder ein DSMS aufgebaut bzw. ergänzt wird. Hier kann die ISO 27701:2019 hilfreich sein. Die größere Stärke wird aber im SDM gesehen. Ungeachtet der Umsetzung in der jeweiligen Organisation wird die übergeordneten Cybersicherheitsarchitektur überprüfbare Ergebnisse in beiden Domänen fordern.

10 Referenzarchitektur Cybersicherheit im Föderalsystem Deutschlands[9]

Zusammenfassung: Cybersicherheitsarchitekturen sind im Föderalsystem Deutschlands elementarer Bestandteil der digitalen Daseinsvorsorge für Gesellschaft, Wirtschaft und Verwaltung. In Deutschland stehen neben dem Bund alle Länder vor vergleichbaren Herausforderungen, die Akteure ihrer Region dergestalt in eine Architektur einzubinden, dass eine gegenüber Cybersicherheitsbedrohungen resiliente IKT-Infrastruktur entsteht. Sofern die Länder eine harmonisierte Architektur implementiert haben, kann die Gesamtarchitektur im Binnenverhältnis der Länder in kooperativer und komplementärer Zusammenarbeit mit dem Bund und für Europa aufwachsen. Das Ziel der hier vorgestellten Forschungsarbeit ist es, die Verzahnung der systemrelevanten Akteure der regionalen und föderalen Cybersicherheit zu unterstützen und zu vereinfachen. Konkret werden dazu sowohl die inter-organisationalen Prozesse und davon betroffenen Rollen und Organisationseinheiten bei Land, Kommune und Unternehmen der Privatwirtschaft als auch gemeinsam nutzbare Komponenten einer Cybersicherheitsorganisation betrachtet und in Form einer Unternehmensarchitektur dokumentiert, die zu einer Referenzarchitektur weiterentwickelt werden soll. Die Modellierung der Referenzarchitektur in der Modellierungssprache ArchiMate wird in Auszügen vorgestellt.

Schlüsselwörter: Unternehmensarchitektur, Cybersicherheit, föderale Sicherheitsarchitektur, Referenzmodell

10.1 Einleitung

Die neuerlichen Cyberangriffe in verschiedenen Bundesländern und auf Bundes- und Landesbehörden (Heller, 2021)unterstreichen die wachsende Bedeutung eines systematischen Managements der Cybersecurity. Die Komplexität dieses Themas mit so unterschiedlichen Aspekten wie Netzwerksicherheit, Informationssicherheit, Softwaresicherheit oder Emergency Response erfordert koordinierte Maßnahmen auf allen Ebenen der Verwaltung und der Betreiber systemrelevanter Infrastrukturen, um Bedrohungen zu minimieren und Ausfälle zu vermeiden. Für die Gesellschaft ist die Frage nach der Verfügbarkeit von elementaren Verbrauchsgütern und Infrastrukturen so wichtig und aktuell, wie schon seit Jahrzehnten nicht mehr. Der wirtschaftliche und soziale Zusammenhalt ist mittlerweile in einem hohen Maß von Informationstechnik abhängig. Cybersicherheit stellt folglich das Bindeglied zwischen der Informationssicherheit verschiedener staatlicher und privater Organisationen dar.

[9] Der Inhalt dieses Kapitels ist bereits wie folgt veröffentlicht worden: Thomas Rehbohm und Kurt Sandkuhl (2023), HMD Praxis der Wirtschaftsinformatik

In der Cybersicherheitsarchitektur – als Teilmenge der Gesamtsicherheit – Deutschlands kommt den Ländern des Föderalstaates eine exponierte Rolle bei der Digitalen Daseinsvorsorge - und den in ihren Regionen betriebenen Informationstechnik-Infrastrukturen zu (Wenzelburger, 2020, S. 382). Kommunen, deren Bevölkerung und Wirtschaftsunternehmen sind grundsätzlich in der Verantwortung der Länder. Die Kommunen sind prinzipiell mit einem hohen Grad an verfassungskonformer Selbständigkeit ausgestattet. Gleichzeitig sind Kooperationsnormen angesichts der Herausforderungen unterentwickelt, was zu Verfassungsänderungen und Kompetenzverlagerungen zum Bund mündete (von Beyme, 2017, S. 387).

In Deutschland ist die Verlagerung von Kompetenzen auch im Cybersicherheitsbereich zugunsten des Bundes in Diskussion. Weiterhin ist mit dem Vorschlag der Europäischen Union und des Rates eine neue Richtlinie für Netz- und Informationssicherheit in der Union verabschiedet worden (Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie), 2023), die in nationales Recht innerhalb von 21 Monaten umgesetzt werden muss und erheblichen Einfluss auf die föderale Ausgestaltung der Cybersicherheitsarchitektur nimmt.

Das Ziel der hier vorgestellten Forschungsarbeit ist es, einen Beitrag zur weiteren Verzahnung der systemrelevanten Akteure der regionalen und föderalen Cybersicherheit zu leisten. Dazu werden die notwendigen Abläufe zwischen den betroffenen Organisationseinheiten bei Land, Kommune und Unternehmen der Privatwirtschaft betrachtet und inter-organisationale Prozesse sowie gemeinsam nutzbare Komponenten einer Cybersicherheitsorganisation vorgeschlagen. Ein Beispiel ist, wie der sichere, technische und vertrauliche Austausch von Angriffsvektoren zwischen diesen Akteuren erfolgen kann.

Als Mittel für die Darstellung der vorgeschlagenen Cybersicherheitsorganisation wird ein Unternehmensarchitekturmodell gewählt. Unternehmensarchitekturen betrachten typischerweise unterschiedliche Ebenen einer Organisation, wie die Geschäfts-, Informations- und Technologiearchitektur. Da bei der Verzahnung von Land, Kommunen und Unternehmen zur Erzielung einer verbesserten Cyberarchitektur alle Ebene erforderlich sind, bietet sich die Verwendung eines Unternehmensarchitekturansatzes an. Gegenstand der Modellierung muss dabei nicht die komplette Cybersicherheitsarchitektur aller Beteiligten sein, sondern der Fokus kann auf der bisher fehlenden Verzahnung liegen, was konkret die betroffenen Schnittstellenbereiche auf Prozess-, Organisations-, Informations- und Technologieebene sind. Die Entwicklung der Architektur erfolgt beispielhaft für die Freie und Hansestadt Bremen (FHB) mit ihren Kommunen und KRITIS-Unternehmen. Das Ziel ist dabei die Schaffung einer Referenzarchitektur im Sinne eines auf die Bundesländer übertragbaren Ansatzes.

10.2 Grundlagen und bisherige Arbeiten

10.2.1 Notwendigkeit und Bedarf an Cybersicherheitsforschung in föderalem Umfeld

Um die Sicherheit von Technologie zu gewährleisten, ist eine effektive Koordination von Instrumenten von entscheidender Bedeutung. Ein wichtiger Aspekt der Resilienz eines Landes bzw. seiner Metropolregion, ist die vertrauensvolle Zusammenarbeit zwischen den wesentlichen Akteuren, die für das Gemeinwohl verantwortlich sind. Eine solche Kooperation ermöglicht es, Bedrohungen schneller zu erkennen und effektiver zu bekämpfen. Cybersicherheitsbedrohungen sind dynamisch und bedürfen einer zeitnahen Reaktion bei den Angegriffenen sowie deren Initiative. Eine Bewusstseinsbildung für die Cybersicherheitsgefahren in vernetzter Technologie muss hierfür in den Unternehmen und im Regierungshandeln Einzug halten, um Cybersicherheit in einer sich ständig verändernden digitalen Welt zu gewährleisten. Folglich sollen die Technologie und der Technologieeinsatz selbst verbessert werden.

Die aktuelle Forschung zeigt, dass im Umfeld der föderalen Strukturen nur wenige einschlägige Arbeiten entstanden sind, die sich der Herausforderungen von Cybersicherheits-Resilienz in föderalen Strukturen widmen. Mehrheitlich befassen sich europäische Beiträge mit dem Binnenmarktrecht, dem Wettbewerbsrecht und im Kontext von strukturellen und demografischen Wandel, mit den Sozial-, Versorgungs- und Gesundheitssystemen. Dienstleistungen im allgemeinen Interesse oder „services of general interest“ (SGI), im Zusammenhang von Cybersicherheitsstrukturen sind noch unterrepräsentiert. Es wurden in der strukturierten Literaturrecherche relevante Veröffentlichungen aus den Vereinigten Staaten, europäische Beiträge und der Forschungsstand in Deutschland erhoben. Die Literaturrecherchen sind Teil der unter Forschungsansatz benannten Vorfeldstudien.

10.2.2 Unternehmensarchitekturen

Das Gebiet des Unternehmensarchitekturmanagements (UA) (Lankhorst, 2017), (Nurmi et al., 2019) hat sich seit mehr als einem Jahrzehnt als eine Disziplin sowohl in der Forschung als auch für die praktische Unterstützung entscheidungsunterstützender Funktionen und Modelle in Unternehmen und Organisationen entwickelt (D. Simon et al., 2014). Ziel der Unternehmensarchitektur ist es, wichtige Zusammenhänge und Querbeziehungen zwischen betrieblichen bzw. organisatorischen und informationstechnischen Aspekten zu modellieren, abzustimmen und zu verstehen, um so die Voraussetzung für einen gut angepassten und strategisch ausgerichteten Entscheidungsrahmen sowohl für Veränderungen in Organisationen, bspw. bei der Anpassung von Geschäftsmodellen oder der Einführung technologischer Innovationen, zu schaffen (Niemi & Pekkola, 2017).

Unternehmensarchitekturmanagement (UAM), wie es heute durch verschiedene Standards wie ArchiMate (Group, 2017) und TOGAF (*The TOGAF Standard*, 2018) definiert

ist, verwendet unterschiedlicher Sichten und Perspektiven für die Dokumentation, Planung und Visualisierung zentraler Bestandteile einer Organisation bzw. eines Unternehmens (D. Simon et al., 2014). Die Geschäftsarchitektur bildet die zentralen Ziele der Unternehmensstrategie, Geschäftsprozesse, Organisationsstrukturen und Governance-Strukturen des Unternehmens ab. Die Informationsarchitektur besteht meistens aus zwei Ebenen: Datenarchitektur und Anwendungsarchitektur. Weiterhin werden auch die Beziehungen zwischen Anwendungen und Geschäftsprozessen sowie zwischen Daten und Anwendungen erfasst. Die Technologiearchitektur erfasst die physischen IT-Komponenten, deren Zusammenhänge und geographische Verteilung.

Das UAM bildet insgesamt einen Managementansatz, der ein kohärentes Ganzes von Richtlinien, Architekturprinzipien und Governance-Regelungen festlegt, pflegt und verwendet. Ein effektiver Architekturmanagement-Ansatz für Cybersicherheitsarchitekturen sollte zusätzlich die Digitalisierung von Produkten und Dienstleistungen unterstützen (Urbach & Ahlemann, 2019) und sowohl ganzheitlich als auch leicht anpassbar sein.

10.2.3 Vorfeldstudien

Im Vorfeld der in diesem Beitrag dargestellten Ergebnisse wurden verschiedene Studien durchgeführt, die zur Analyse des Problems beitragen sowie zur Entwicklung und ersten Evaluation des Unternehmensarchitekturmodells führten. Insbesondere wurde erarbeitet, welche Aufgaben und Herausforderungen bestehen, um öffentliche, private bzw. zivilgesellschaftliche Akteure der Daseinsvorsorge interagieren zu lassen (Neu, 2009, S. 42). Zusammengefasst hat sich der Bedarf an einem integrierten Ansatz in Form einer Unternehmensarchitektur ergeben, die Empfehlungs-charakter haben sollte und somit als eine Referenzarchitektur bzw. ein Referenzmodell entwickelt werden soll. Insgesamt wurden vier Studien als Grundlage für diesen Artikel durchgeführt.

1. Studie bei den Ländersicherheitsbeauftragten zu den Herausforderungen des Cyber- und Informationssicherheitsmanagements in föderalen Strukturen (Rehbohm et al., 2019): Die mit den CISOs der Länder durchgeführte Studie zu politischen, strategischen, technischen und rechtlichen Herausforderungen in der Cybersicherheit hat gezeigt, dass weder durch den Bund definierte, noch in den Ländern, eine vergleichbare oder belastbare Vorgehensweise zur Lösung des Problems vorliegen. Zusammenfassend konnte bestätigt werden, dass der Bedarf, an spezifischeren Instrumenten zur Koordinierung der Landesebenen, existiert. Organisationsbezogene Informationssicherheitsmanagementansätze greifen zu kurz und adressieren nicht die regionale Daseinsvorsorge. Insbesondere kann unterstellt werden, dass ein Referenzmodell – basierend auf einem Unternehmensarchitekturmodell – eine mögliche Lösung des Problems darstellen kann.
2. Integriertes Sicherheitsmanagement des öffentlichen und privaten Sektors für kritische Infrastrukturen – Problemanalyse (Rehbohm et al., 2021) Die Studie mit

den Unternehmen der regionalen Daseinsvorsorgen in der FHB konnte durchgeführt werden, weil diese die bundegesetzlichen Schwellenwerte nach der Definition der BSI-Kritisverordnung übertrafen und Zugang zu diesen Unternehmen bestand. Die befragten Unternehmen hatten keine vergleichbaren Ansätze oder Architekturen in der Organisation etabliert, die Cybersicherheitsrisiken angemessen adressierten. Insbesondere hatten die kleinen Unternehmen keine Sicherheitsstrategie oder relevante Managementsysteme bzw. auch noch kein Verständnis für die eigene Tätigkeit als Daseinsvorsorgeträger. Technische und organisatorische Maßnahmen waren zum Teil nicht zielführend. Auch hat die FHB keine Strukturen zur Förderung der Zusammenarbeit der relevanten Akteure im Sinne des Gemeinwohls geschaffen. Gleichzeitig existieren keine rechtlichen Bindungsvorgaben im Sinne von gesetzlichen Regelungen.

3. Empirische Studie in deutschen Kommunen zu Sicherheitsmanagement, Cybersicherheit und Daseinsvorsorge: ((Rehbohm et al., 2022): Angelehnt an die Studie bei den Landesinformationssicherheitsbeauftragten, sollte diese Umfrage die politischen, organisatorischen, strategischen und juristischen Perspektiven qualifizieren. In der Gesamtschau ließ sich beweisen, Informationssicherheitsmanagementprozesse sind im Allgemeinen unterentwickelt. Auch wenn Empfehlungen seitens des zuständigen Landes oder von den Deutschen Spitzenorganisationen existieren, werden diese überwiegend nicht befolgt, umgesetzt, ihre Umsetzung nicht unabhängig kontrolliert und die Systeme nicht nachhaltig etabliert. Dabei existiert mit CISIS12 ein Vorgehensmodell, das es grundsätzlich jeder Organisation ermöglicht, externe und interne Anforderungen an ein Informationssicherheitsmanagement systematisiert, effektiv und effizient einzuführen (Moses & Rehbohm, 2022, S. 61). Kleinere Kommunen sind dabei durchweg schlechter aufgestellt als größere Organisationen. Erstaunlicherweise wird die eigene Dienstleistungserbringung im kommunalen Umfeld nicht als kritische Dienstleistung bewertet, gleichwohl wird eingeräumt, für solche Dienstleistungen Verantwortlichkeiten zu besitzen. In diesem Kontext wurde auch geprüft, ob eine Bereitschaft zur technischen Kooperation mit größeren Organisationen oder Kommunalverbünden besteht. Diese Bereitschaft ist jedoch eher auf politischer kommunaler Leitungsebene nachweisbar.

4. Grundforderungen von Informations- und Cybersicherheit in Ländern, Studie zu den rechtlichen Rahmenbedingungen im föderalen Kontext (Rehbohm & Kalmbach, 2021): In der Rechtsstudie wurde erhoben, ob Regelungsdefizite in den Ländern und abseits der Gesetzgebung der europäischen Union und Deutschland bestehen. Die vorliegende Arbeit basiert auf Erkenntnissen von Interview- und Umfragestudien in den Ländern und den zuständigen Ministerien. Dabei wurde erarbeitet, dass es eine rechtsstaatliche Aufgabe ist, die IKT-Infrastrukturen der öffentlichen Gewalt, hier der Länder und der Kommunen, ge-

gen Angriffe abzusichern. Gleichzeitig sind aber auch privatwirtschaftliche Bereiche von dieser staatlichen Verantwortung betroffen. Die Gewährleistungsverantwortung des Staates gegenüber der Bevölkerung ist hier relevant (kollektives Rechtsgut).

5. Das Gefahrenabwehrrecht liegt bei den Ländern, folglich muss das einschlägige Bundesrecht komplementär um Inhalte im Landerechts ergänzt werden. Der Anspruch auf Daseinsvorsorge und das Funktionieren der IKT-Systeme ist rechtlich zu sichern. Sinnlogisch sind Anbieter von Dienstleistungen oder Waren, welche elementar wichtig für große Teile der Bevölkerung sind, also Träger der Daseinsfürsorge als maßgebliche Akteure per Gesetz und nötigenfalls per Verwaltungsakt zu identifizieren und in die Pflicht zu nehmen.

10.3 Forschungsansatz

Das Ziel der hier vorgestellten Forschungsarbeiten ist, die Integration einer Cybersicherheitsstrategie in Cybersicherheitsarchitekturansätzen aufzuzeigen und zu einem Referenzmodell weiterzuentwickeln.

Forschungsmethodisch wird zur Erreichung dieses Ziels ein konstruktionsorientierter Forschungsansatz (Frank, 2009) eingesetzt, wie er besonders in der Wirtschaftsinformatik weit verbreitet ist. Der Unternehmensarchitektur wird dabei nicht als Selbstzweck betrachtet, sondern dezidiert als Mittel zur Erreichung organisatorischer Zielsetzungen verstanden. Der konstruktionsorientierte bzw. gestaltungsorientierte (Österle et al., 2010) Forschungsansatz wird im internationalen Umfeld auch als „Design Science (A. R. Hevner et al., 2004), (Peffers et al., 2007)“ bezeichnet.

Während konstruktionsorientierte Forschung den Gesamtansatz darstellt, wird bei der Durchführung der Forschungsarbeiten eine Vielzahl von Einzelmethoden eingesetzt, die im Wesentlichen zur Begründung der Forschungsresultate erforderlich sind. Da Begründung von Forschungsergebnissen etwa durch einen formalen Beweis oder durch eine empirisch bestätigte Theorie aufgrund der Natur der Fragestellung oder fehlender Daten häufig nicht möglich ist, sind in der Regel alle Annahmen, die dem Entwurf einer Konstruktion zugrunde liegen, explizit machen. Dazu gehören Annahmen, die Anforderungen, Entwurfsentscheidungen wie auch die Evaluation des „Artefakts“ (in unserem Fall: der Referenzarchitektur) betreffen (Frank, 2008).

Konstruktionsorientierte Forschung beinhaltet in der Regel drei miteinander integrierte Forschungszyklen, die auch für die Entwicklung der Referenzarchitektur gelten:

- Der Relevanzzyklus verankert die Entwurfsentscheidungen und Merkmale der Referenzarchitektur in Anforderungen des betreffenden Handlungskontextes, also der Verbindung zwischen Land, Kommune und relevanten Wirtschaftsunternehmen. Dies erfolgte durch die in Abschnitt 2 beschriebenen Vorfeldstudien.

- Der Rigorositätszyklus setzt die Forschungsresultate in Verbindung zum Stand des Wissens im jeweiligen Fachgebiet, was über Literaturanalysen erfolgen kann. Auch dies in den Publikationen zu den Vorfeldstudien erfolgt.
- Die Entwurfs-/Evaluationszyklus dient der eigentlichen Konstruktion der Referenzarchitektur auf Grundlage der Ergebnisse aus dem Relevanzzyklus und unter Berücksichtigung der Resultate des Rigorositätszyklus. In der Regel wechseln sich hier Entwurf- und Validierungsschritte bzw. Verbesserungs- und Validierungsschritte ab. Die Abschnitte 4 und 5 beschreiben einen solchen Zyklus.

Die zentrale Forschungsfrage für diesen Beitrag ist: Kann die vorgestellte Referenzarchitektur für Länder Deutschlands einen wesentlichen Beitrag zur Nationalen Cybersicherheitsarchitektur leisten? Die zur Beantwortung dieser Forschungsfrage und die angewandte Forschungsmethode ist eine Kombination aus Literaturrecherche, konzeptionell-deduktiver Arbeit und Evaluation. Die Referenzarchitektur wurde mit der Modellierungssprache ArchiMate dokumentiert.

10.4 Anforderungen und Lösungsansatz der Referenzarchitektur

10.4.1 Anforderungen an eine föderale Architektur

Eine wirksame föderale Cybersicherheitsarchitektur soll strukturelle Rahmenbedingungen, technische Interaktionen und Rechtssicherheit schaffen, die eine gleichberechtigte Teilhabe aller Akteure ermöglicht. Zum Schutz der Bevölkerung in der jeweiligen Region ist es notwendig, Akteure in den Kommunen eines Landes oder Metropolregion unter regulierender Aufsicht eines Landes mit den systemrelevanten Unternehmen zu vernetzen (vgl. Abbildung 16 Akteure). Systemrelevante Unternehmen sind die Summe aus kritischen Infrastrukturen nach Definition und Regulierung des Bundes, Infrastrukturen nach Regulierung der EU und wesentliche und wichtige Einrichtungen, die durch das jeweilige Land zu identifizieren sind. Staatliche Akteure der Landesverwaltung müssen rechtliche, technische und organisatorische Rahmenbedingungen schaffen, die eine Kollaboration zulassen und nötigenfalls erzwingen.

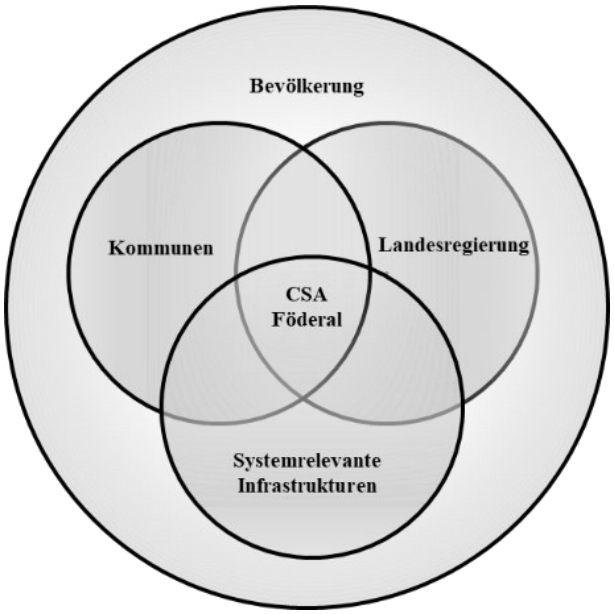

Abbildung 16 Akteure

Die Architektur muss es zulassen, Forschungs- und Entwicklungseinrichtungen in einem Teilhabeprozess einzubinden. Diese Aufgabe kann durch organisatorische Regelungen der Landesverwaltung erfolgen. Die Weiterentwicklung der Architektur muss aktuelle Entwicklungen der Cybersicherheitsforschung berücksichtigen. Auch ist die Architektur darauf auszurichten, dass Digitale Kompetenzen aufgebaut und erhalten werden. Themen, wie die Aus und Fortbildung, Awareness, Fachkräfteaquirierung Fachkräftebindung und Arbeitgebermarkenbildung können das Handlungsfeld Forschung und Entwicklung flankieren.

Auf Seiten der öffentlichen Verwaltung sind neben externen Kooperationen weitere Anforderungen an die Architektur zu berücksichtigen, z. B. Adressierung von Polizei und Verfassungsschutz.

10.4.2Lösungsansatz

Die erstellte Architektur soll zeigen, dass ein übergreifendes Informationssicherheitsmanagement zwischen den Ländern zum einen und zum Bund zum anderen entstehen soll. Das Bild soll (Abbildung 17 Cybersicherheitsarchitektur Land) illustrieren, welche Akteure, mit Aufgaben und verbundenen Methode zu adressieren sind. Der im ersten Ring beschriebene Teil der Cybersicherheitsarchitektur (CSA) Föderal muss die Akteure der Verwaltung (Herpig & Rupp, 2022, S. 173) um Wirtschaft und Gesellschaft erweitern und derart integrieren, dass ein kooperativer Baustein in der deutschen Gesamtarchitektur entsteht und die Cybersicherheitsstrategie Deutschlands ergänzt (Bundesministerium des Innern, für Bau und Heimat, 2021b, S. 21).

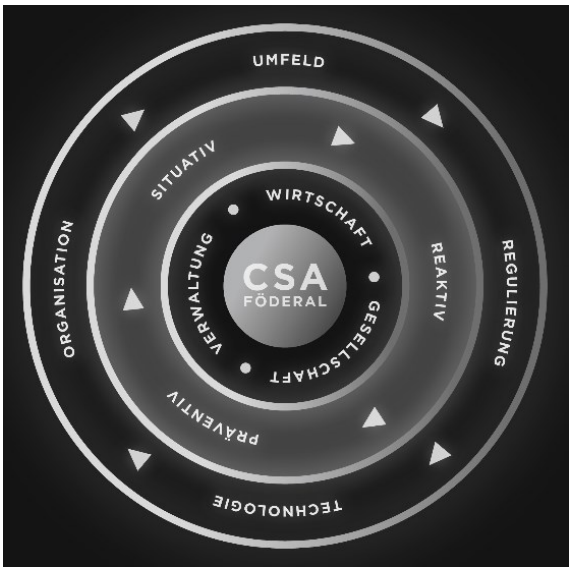

Abbildung 17 Cybersicherheitsarchitektur Land

Auf Seiten der Verwaltung werden hierfür die Ebenen der deutschen Verwaltungsgliederung adressiert, auf Seiten der Wirtschaft werden die kritischen Infrastrukturen nach Definition des Bundes (Kritis) sowie die Wirtschaftsunternehmen der Daseinsvorsorge der Region (Subkritis) in den Fokus genommen.

Eingebunden werden alle zu identifizierenden Stellen der Architektur für die im Einzelnen subsummierten präventiven, situativen und reaktiven Aufgaben, welche ergänzend durch regulatorische Maßnahmen umrahmt werden. Das bedeutet im Einzelnen, dass nach Abstufung der Unternehmen in „wesentlich“ oder „wichtig“ für die Daseinsvorsorge insbesondere Kontrollen, Berichtspflichten und Informationsaustausch zu berücksichtigen sind (EUR-Lex - 32022L2555 - EN - EUR-Lex, 2022, S. 39).

10.5 Unternehmensarchitektur

10.5.1 Strategische und Motivatorische Betrachtung der CSA Land

Das strategische Ziel eines übergreifenden Cybersicherheitsmanagements in einem Land wird von intrinsischen und extrinsischen Motivationen befördert. Intrinsische Motive liegen dabei in der Wirtschaftlichkeit, Nachhaltigkeit und Widerstandsfähigkeit der angestrebten Lösung. Extrinsische Motive liegen in der Rechtskonformität bzw. Compliance und in der Reputation, also der Glaubwürdigkeit der Organisation und das in dieses gesetzte Vertrauen. Aufgrund der zahlreichen parlamentarischen und medialen Anfragen in den Ländern, stehen die Landesregierungen unter enormen Erfolgsdruck. Sowohl die eigenen IT-Infrastrukturen der öffentlichen Verwaltung, als auch die Wirtschaftsunternehmen der Daseinsvorsorgen sind Ziel von politischen Anfragen.

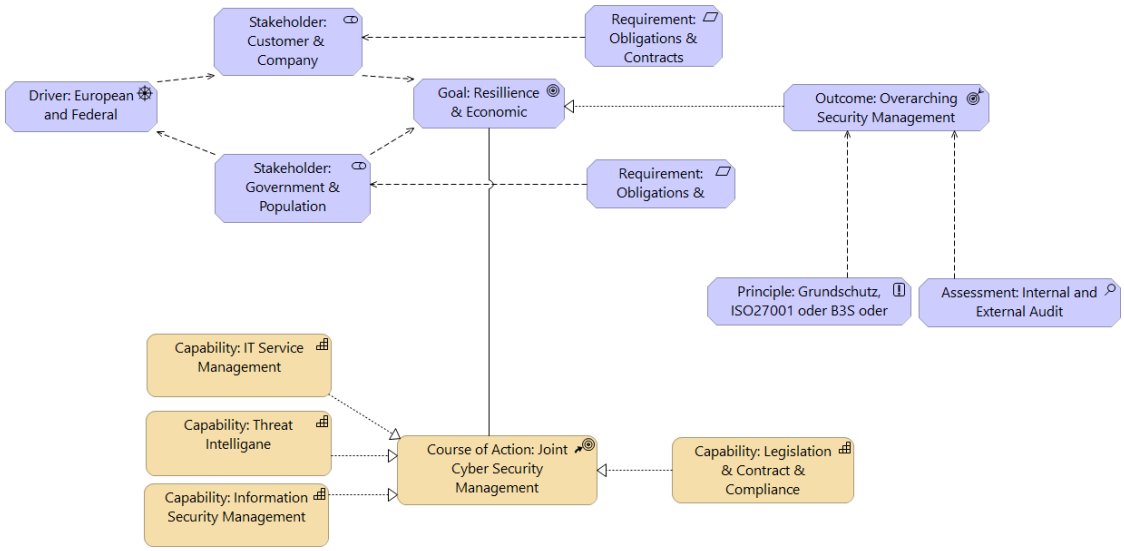

Abbildung 18 CSA-Land-Strategie

In Abbildung 18 CSA-Land-Strategie wird veranschaulicht, welche Fähigkeiten das Land mindestens vorhalten soll, um die strategischen Ziele erreichen zu können. Die drei elementaren Aufgabenbereiche sind zuvorderst den Themenfeldern IT-Servicemanagement, IT-Securitymanagement und Threat-Intelligence-Management zuzuordnen. Für ausgewählte Sektoren der kritischen Infrastrukturen gelten Mindestanforderungen, die der Beherrschung von Cybersicherheitsrisiken dienen. Die Einhaltung der NIS-2-Richtlinie wird durch nationale Behörden überwacht und bei Nichteinhaltung auch sanktioniert werden können.

Neben den verpflichtenden Regelungen aus der Richtlinie existieren weitere Handlungsfelder der föderalen Cybersicherheitsarchitektur, wie insbesondere die Förderung von digitalen Kompetenzen, die Aus- und Fortbildung, die Awarenessbildung und Bekämpfung des Fachkräftemangels, welche in den Bereich von organisatorischen Regelungen fallen und die Beschäftigten in Wirtschaft, Verwaltung und Gesellschaft adressieren. Zudem wird in der Architektur berücksichtigt, dass die einem Land zustehende Fähigkeit einer gesetzgebenden Unterstützung dieser Managementbereiche gegeben ist.

Mindestanforderungen an die Architektur, die unter Präventiv subsummiert werden, sind als Business, Application und Technology modelliert. Hierbei handelt es sich um Applikationen die zu Exchange & Advisory gezählt werden. Weitere Teile der Architektur CSA-Land sind den Abschnitten Situativ und Reaktiv zuzuordnen und definieren Business Architekturen.

10.5.2 Erörterung der Business-/Application Ebenen

Für eine föderale Architektur sollen in diesem Abschnitt Anwendungen aus der Prävention und jeweils eine Anwendung aus den Bereichen Situativ und Reaktiv erläutert werden. In der Präventionsarbeit bieten sich zahlreiche Möglichkeiten der Interaktion mit

den Akteuren, wie zum Beispiel Employer Recruitment, Training & Awareness, Research & Development oder auch Exercise an. Dies sind ausbaubare Elemente einer Landes-Architektur.

10.5.2.1 WIS

Ein wesentlicher Baustein der Prävention sind sogenannte Warn- und Information Services (WIS). Diese müssen inhaltlich auf die Organisation zugeschnitten sein und dürfen den Adressaten in Quantität nicht überfordern. Auch müssen die Informationen in der Organisation verarbeitet werden können, das heißt, entsprechende Ressourcen müssen zur Verfügung stehen.

Grundsätzlich werden solche Business Services von den Computer Emergency Response Teams (CERT) angeboten. Hier besteht die Möglichkeit an einem Landes CERT teilzuhaben, welches die verfügbaren Informationen sammelt ggf. erstellt und bereitstellt. Akteure der Daseinsvorsorge sind ausschließlich beim Land, teilweise auch beim Bund bekannt und werden über die Webanwendung zur Registrierung aufgefordert. Hierfür werden bestehende Möglichkeiten der öffentlichen Verwaltung zu Identifizierung solcher Unternehmen insbesondere die Beziehungen zu Branchenverbänden und Kammern genutzt, um unabhängig von der Relevanz für die Daseinsvorsorge jedes Unternehmen der Region teilhaben zu lassen. Gewünschte Informationen werden von der jeweiligen Organisation selbst zusammengestellt, abonniert und ausgewertet. Dabei handelt es sich insbesondere um Informationen von bekannten Schwachstellen in Hard- und Softwareprodukten sowie bekannten Sicherheitslücken bzw. Angriffsmustern. Die in der Plattform integrierten Informationen zu Sicherheitslücken werden aus angebundenen „Common Vulnerabilities and Exposures“ Datenbanken gewonnen. Schwachstellen in Hard- und Software werden regelmäßig bei kommerziellen Anbietern eingekauft, integriert und zur Verfügung gestellt.

10.5.2.2 MISP

Ein weiterer Business Service ist modelliert und beruht auf der “Malware Information Sharing Platform”. Dieser Service wird in den Ländern regelmäßig beim Security Operation Center (SOC) betrieben werden. Die hier über eine Partnerschnittstelle zur Verfügung gestellten Informationen sind anders als im WIS nicht frei verfügbar, sondern teilweise vertraulich, im Sinne von Verschlusssachen nach den jeweiligen gesetzlichen Rahmenbedingungen. Die Prävention schließt aktuelle Ereignisse der Detektion ein (Indicator of Attacks). Der Datenaustausch folgt einer festgelegten Taxonomie (Mokaddem et al., 2019). Wie die Abbildung 4 illustrieren soll, wird der Prozess von externen Ereignissen initiiert. Solche Ereignisse werden unter anderem über Sicherheitsvorfälle und forensischer Aufarbeitung erzeugt bzw. wird aus aktuellen Ergebnissen von Detektoren gespeist. Die Weitergabe von ermittelten Ergebnissen aus Sicherheitsvorfällen, Ereig-

nissen aus “Threat Intelligence” oder Intrusion Detection Systems (IDS)/Security Information and Event Management (SIEM) erfordern in jeder teilnehmenden Organisation Expertise. Diese Expertise muss ggf. aufgebaut und ausgebaut werden. Das Land reichert die auf der Plattform verfügbaren Informationen zudem noch um Erkenntnisse des Bundes an. Solche “Indicator of Compromises” (IoC) können nur unter bestimmten vertraulichen Bedingungen bereitgestellt werden. Die Plattform kann bidirektional genutzt werden, insofern wird beim Land eine Datenqualitätskontrolle der gelieferten IoCs erfolgen müssen. Für die Teilnehmenden aus der Wirtschaft muss ein Vertragskonstrukt gewählt werden, dass die Vertraulichkeit aller Informationen sicherstellt. Auch kann die Integrität des Datenaustausches über kryptografische Maßnahmen verbessert werden (van de Kamp et al., 2016, S. 3). Des Weiteren werden die Akteure der Wirtschaft untereinander nicht identifiziert, da sie auf der Plattform pseudonymisiert werden müssen.

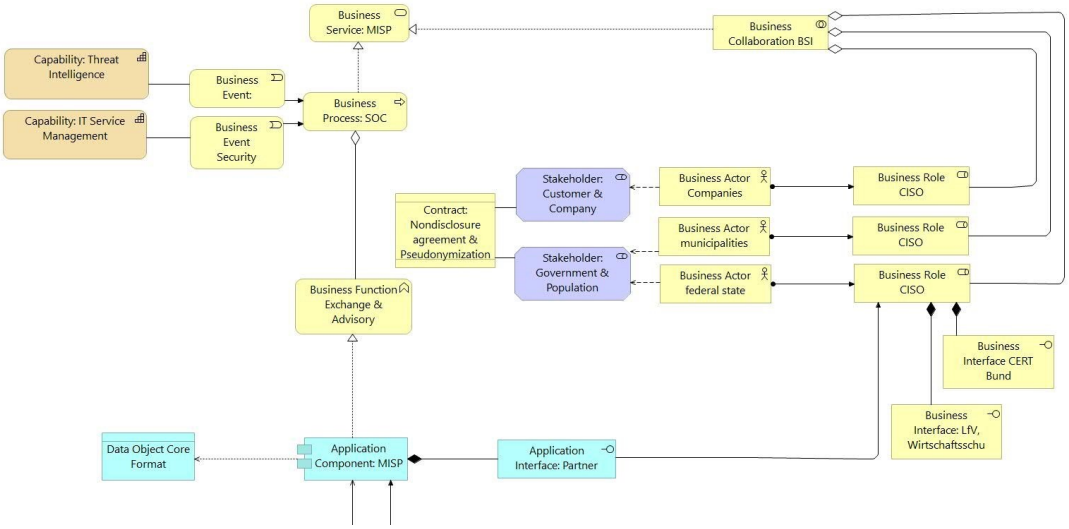

Abbildung 19 MISP

10.5.2.3 SR

In der Architektur sind weitere Themen aus Sicht eines Landes zu bedienen. Zum einen handelt es sich dabei um die Erfassung eines Lagebildes Cybersicherheit für das jeweilige Land. Dies kann nur in Zusammenarbeit der Sicherheitsmanagements und der Organisationen der allgemeinen öffentlichen Sicherheit erfolgen, insbesondere des Katastrophenschutzes. Es handelt sich hierbei um einen Business Prozess, der bislang nicht technisch abgebildet ist.

Das Land muss einen Prozess vorhalten, der geeignet ist, Informationen der beteiligten Akteure regelmäßig und verstetigt entgegenzunehmen, weiterzuverarbeiten und an die nächst höheren Instanzen zu melden (e.g. European Union Agency for Cybersecurity).

10.5.2.4 MIRT

Der zwingend nötige Prozess des Mobile Incident Response greift erst, nachdem eine in der CSA-Land involvierte Organisation Opfer eines Cybersicherheitsangriffes wurde. Es sind in diesem Fall die Beteiligten der öffentlichen Sicherheit zu involvieren. Je nach Typ des Angriffs kann das die Polizei, eine Schwerpunktstaatsanwaltschaft oder der Wirtschaftsschutz sein. Im Vorfeld sind jedoch aktive Maßnahmen des Einsatzes von Hilfskräften zu steuern. Im Grunde muss hierdurch verhindert werden, dass durch unterlassene Hilfe des Landes die Situation für die Organisation oder die abhängigen Dienstleister eskaliert. Ein Security Breach eines involvierten Akteurs übt einen zwingenden Druck auf das Land aus. Die Business Rolle CISO eines Landes ist verantwortlich für die Akquirierung von Kräften des BSI, Kräften des möglichen Partnerlandes oder auch von spezialisierten Unternehmen. Hierfür sind neben rechtlich schon definierten Szenarien zwischen dem Bund und den Ländern auch die vertraglichen Möglichkeiten mit externen Dienstleistern auszuschöpfen.

10.5.2.5 Rechtliche Betrachtung

Eine Länder-Allianz für Cybersicherheit kann nur unter bestimmten Voraussetzungen, insbesondere unter der Abwägung von gesetzlichen bzw. gesetzgeberischen Möglichkeiten oder vertraglichen Regelungen entstehen.

Die durchgeführten Studien haben jedoch gezeigt, dass eine Zusammenarbeit verschiedener Organisationen der Wirtschaft von Misstrauen geprägt ist. Erschwerend kommt hinzu, dass Unternehmen, die im Mitbewerb stehen, nicht willens sind, Informationen mit den Wettbewerbern ohne externe Verpflichtungen auszutauschen. Der Erstautor dieses Beitrags hat hierfür im Rahmen seiner hauptamtlichen Tätigkeit als CISO der FHB, zusammen mit dem Co-Autor der Rechtsstudie, ein IT-Sicherheitsgesetz für die FHB entworfen. Mit dem Gesetz werden die Akteure zur Kooperation verpflichtet und müssen dem Land zudem Kontrollrechte einräumen. Die mit der NIS-2-Richtlinie veröffentlichten Rechte und Pflichten der Mitgliedsstaaten greifen genau diese Regulierungsmöglichkeiten auf.

Solange nicht absehbar ist, dass ein für diesen Zweck hilfreiches Gesetz verabschiedet wird, bleibt für die Entfaltung einer kooperativen Beziehung aller Akteure ausschließlich die Vertragsgestaltung.

10.6 Evaluierung der Architektur

10.6.1 Evaluation der Anforderungen an die Architektur

Die hier vorgestellte Architektur erhebt nicht den Anspruch auf eine vollständige Abdeckung aller heute bekannten technischen und organisatorischen Anforderungen. Vielmehr wird hier und im Forschungsfeld Cybersicherheit in föderalen Strukturen auf die

wesentlich zu gestaltenden informationstechnischen Systeme abgestellt. Dort, wo zeitkritische Informationen unverzüglich den Partnern der CSA zur Verfügung gestellt werden müssen, greift die vorgestellte Architektur zuvorderst.

Weitere Anforderungen an die Architektur sind überwiegend einer rein organisatorischen und rechtlichen Art. Hier kann die Architektur grundsätzlich erweitert werden, im Rahmen der Evaluation und Iteration.

10.6.2 Evaluationsstrategie

Die Evaluationsstrategie sieht vor, dass die entstandene Architektur zusammen mit Kommunen und den Ländern in Episoden verifiziert werden soll. Dies geschieht schrittweise, so dass eine Allgemeingültigkeit der vorgestellten Referenzarchitektur hergestellt werden kann.

Im ersten Evaluationsschritt wurde ein strukturiertes Experteninterview im Zeitraum August 2022 mit den Informationssicherheitsbeauftragten (CISOs) der Länder und sofern notwendig mit den zuständigen Vertretern weiterer Ministerien durchgeführt. Es wurden drei thematische Gebiete in der Kooperation und der komplementären Zusammenarbeit zwischen den Akteuren erörtert. Die Interviews wurden mittels qualitativer Inhaltsanalyse ausgewertet (Mayring, 2008, S. 128–135). Entlang von definierten Fragen wurde festgestellt, ob Kritis-Unternehmen durch den Bund beim Land gemeldet und welche durch das Land selbst identifiziert wurden. Weiterhin sollte festgestellt werden, ob und wie die Länder mit den systemrelevanten Unternehmen zusammenarbeiten. Es bestand grundsätzlich keine Architektur, die eine Zusammenarbeit vergleichbar macht oder eine Allgemeingültigkeit in Anspruch nehmen kann. Die Länder kooperieren derzeit entweder nicht, wenige nur mit staatlichen Beteiligungen an Unternehmen und zudem nur auf freiwilliger Basis. In vereinzelten Fällen bestand die Möglichkeit einer Kooperation (Wissenstransfer) im Land, die von Kommunen und Unternehmen in Anspruch genommen werden können. Die hier vorgestellte Architektur wurde als zuführend bewertet. Die CISOs der Länder sahen den Etablierung eines ISMS als sehr wichtig an. Die Verpflichtung zu einer Zertifizierung war unterdurchschnittlich ausgeprägt. Alle Länder haben auf ministerieller Ebene ein zentrales Informationssicherheitsmanagement eingeführt. Eine Zertifizierung von einzelnen Ressorts besteht allerdings nicht, bzw. ist nur bei einzelnen Ressorts im Planungsstatus (4 von 186 Ministerien). Zentrale Rechenzentrumsdienstleister der ministeriellen Verwaltung sind regelmäßig zertifiziert. Vereinzelt sind auch zentrale Netzwerkinfrastrukturen (wie ein Landesnetz) zertifiziert.

Die Zahl von Unternehmen in kritischen Infrastrukturen, welche durch den Bund identifiziert wurden, liegt in den Ländern zwischen einem einstelligen und einem kleinen dreistelligen Bereich. Unabhängig von einer etwaigen öffentlichen Beteiligung an entsprechenden Unternehmen, liegt die Anzahl subkritischer Infrastrukturen nach Ersterhebung in zwei Ländern um den Faktor 20 bis 100 höher als die kritischen Infrastrukturen

(gemäß Bund). Nur ein Land gab an, dass sie aktiv die Interdependenzen systemrelevanter Infrastrukturen analysieren wollen.

Grundsätzlich sind die Länder von einer harmonisierbaren Architektur, die als Minimalanforderung zu verstehen ist, überzeugt. Andererseits sind derzeit auch Länder unter den Befragten, die das Themenfeld der systemrelevanten Infrastrukturen vollständig dem Bund überlassen wollen und keine eigenen Anstrengungen unternehmen, die Resilienz gegen Cybersicherheitsgefahren in ihrer Region zu erhöhen.

10.7 Schlussfolgerungen und zukünftige Arbeit

Die in diesem Beitrag vorgelegte Architektur ist nach ersten Iterationsschritten Teil einer möglichen Cybersicherheitsstrategie der FHB. In dieser Arbeit wurde eine erste Referenzarchitektur anhand der strategischen Anforderungen konkretisiert, die auch in der FHB relevant sein wird.

Erste Evaluierungsergebnisse liegen aus der Befragung der Länder vor und werden in der Fortschreibung der Architektur berücksichtigt. Idealerweise werden Prozesse erarbeitet, die es einem Land ermöglichen soll, voneinander abhängige Betreiber subkritischer Infrastrukturen, egal welcher Größe, zu identifizieren.

Die vorliegende Arbeit und die Architektur ist Teil weiterer Evaluationsepisoden in Kommunen und bei Vertretern der Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz. Die Einarbeitung der Ergebnisse stellt den finalen Evaluierungsschritt dar und soll die Gesamtarchitektur verbessern.

11 Cybersicherheitsevaluation einer Referenzarchitektur für Land, Kommune und systemrelevante Infrastruktur[10]

Zusammenfassung: Staat, Wirtschaft und Gesellschaft müssen sich vor Cybersicherheitsbedrohungen schützen. Das gilt für die Europäische Union, ihre Mitgliedsstaaten und in Deutschland auch für die Bundesländer. Vor allem die Handlungsfähigkeit und Handlungsgeschwindigkeit von Staat und Verwaltung müssen verbessert werden. In diesem Beitrag wird eine mögliche Unternehmensarchitektur vorgestellt und bewertet, die die Bedürfnisse der Länder, Kommunen und der Wirtschaft angemessen berücksichtigt. Es wird ein architektonischer Ansatz zur Integration von Anforderungen und zur Erreichung von Zielen in einer regionalen Zuständigkeit, wie der eines Bundeslandes, vorgestellt und bewertet. Unternehmensarchitekturen sind bei Dienstleistern in der öffentlichen Verwaltung anerkannt, werden aber auf Seiten der verantwortlichen Ebenen, z. B. der Ministerialverwaltung, überwiegend nicht verwendet. In diesem Beitrag wird anhand einer Architektur evaluiert, wie Herausforderungen und Anforderungen zu einer partiellen Referenzarchitektur führen können.

11.1 Einleitung

Die Informations- und Kommunikationstechnik-Infrastrukturen der öffentlichen Verwaltung sind, wie das Föderalsystem Deutschlands, hierarchisch aufgebaut und auf vertikalen sowie horizontalen Ebenen regelmäßig autark verwaltet. Entsprechend sind die Informationssicherheitsmanagements der Organisationen grundsätzlich getrennt. Die Zusammenarbeit des Bundes und der Länder ist auf dem Gebiet der Informationstechnik bzw. auch Informationssicherheitsmanagement im Grundgesetz verankert und wird insbesondere durch das IT-Netzgesetz und das Onlinezugangsgesetz gleichwohl ermöglicht. Die Länder und der Bund stehen in diesem Kontext prinzipiell nicht im Wettbewerb und sind – wie das Föderalsystem selbst – daher auf Kooperation ausgelegt, um einheitliche Lebensverhältnisse zu ermöglichen (Schubert & Klein, 2021). Die aktuellen Herausforderungen des Bundes, der Länder, seiner Kommunen und der Wirtschaftsunternehmen, im Zusammenhang mit der dynamischen Bedrohungslage für ihre informationstechnischen Systeme (Bundesamt für Sicherheit in der Informationstechnik, 2022b), bestehen im Aufbau von Resilienz-Strukturen. Die gesamte öffentliche Verwaltung muss sich, genau wie die Wirtschaftsunternehmen, gemeinsam zur Abwehr von Cybersicherheitsbedrohungen entwickeln und neu aufstellen. Dabei ist zu berücksichtigen, dass sich die Anforderungen an Sicherheit und deren technische Umsetzungen ebenso schnell weiterentwickeln wie die Bedrohungslagen selbst. Daher ist der Stand der Technik in der

[10] Der Inhalt dieses Kapitels ist bereits wie folgt veröffentlicht worden: Thomas Rehbohm und Kurt Sandkuhl (2024), Fachtagung des Fachbereichs "Sicherheit - Schutz und Zuverlässigkeit" der Gesellschaft für Informatik e.V., GI-Sicherheit 2024

Informationstechnologie relevant. Ferner muss eine solche Allianz unter Berücksichtigung der europäischen Regulierung, wie zum Beispiel der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie), 2023), erfolgen und soll dabei die Daseinsvorsorge stärken (Rehbohm & Moses, 2023a). Teil der digitalen Daseinsvorsorge ist der Portalverbund von Bundes- und Länderportalen der Verwaltungen. Eine Cybersicherheitsarchitektur ist daher auch im Kontext des Onlinezugangsgesetzes und der verbundenen Portalverbundverordnung zu gestalten.

Im Kontext der digitalen Daseinsvorsorge liegt der Fokus dieses Beitrags auf dem Ausschnitt der föderalen Cybersicherheitsarchitektur, die insbesondere das Zusammenwirken von Land, Kommune und Wirtschaft mit Bezug auf systemrelevante Infrastruktur betrifft. Um die Cybersicherheit zu gewährleisten, ist eine effektive Koordination von Instrumenten zwischen den wesentlichen Akteuren von entscheidender Bedeutung. Eine Kooperation ermöglicht es, Bedrohungen schneller zu erkennen und effektiver zu bekämpfen. Es fehlt jedoch bisher an einer definierten föderalen Cybersicherheitsarchitektur in diesem Bereich, die Gegenstand dieses Beitrags ist.

Für die Entwicklung des Konzepts wurde ein Unternehmensarchitekturmodell gewählt. Unternehmensarchitekturen betrachten typischerweise unterschiedliche Ebenen einer Organisation, wie die Geschäfts-, Informations- und Technologiearchitektur. Da bei der Verzahnung von Land, Kommunen und Unternehmen zur Erzielung einer verbesserten Cyberarchitektur alle Ebenen erforderlich sind, bietet sich die Verwendung eines Unternehmensarchitekturansatzes an. Der vorliegende Beitrag präsentiert die Evaluierung einer föderalen Cybersicherheitsarchitektur. Die Anforderungen an die entstandene Architektur und die vorliegende Evaluation dieser Arbeit beruhen auf empirischen Studien bei den Beauftragten für Informationssicherheit der Länder, Betreibern von kritischen Infrastrukturen im Bundesland Bremen und einer bundesweiten Kommunalumfrage. Durch die Evaluierung der Enterprise-Architektur wurden die Angemessenheit und Anwendbarkeit bei den interviewten Kommunen verifiziert und die Möglichkeiten der Weiterentwicklung nachvollzogen (Enterprise Architecture Management (EAM)). Die Einschränkung der Arbeit besteht darin, dass sie auf die öffentliche Verwaltung Deutschlands bezogen ist, hier insbesondere die Domäne Ministerialverwaltung eines Landes. Es soll ein praxisorientierter Ansatz zur Lösung des föderalen Problems aufgezeigt werden.

Im Abschnitt 2 werden die Forschungsmethodik und im Abschnitt 3 der Stand der Forschung erläutert. Der Abschnitt 4 befasst sich mit der föderalen Cybersicherheitsarchitektur und seiner Evaluierung entlang wissenschaftlicher Grundsätze. Im 5. Abschnitt werden die Ergebnisse zusammengefasst und ein Ausblick hinsichtlich möglicher Verbesserungen und weiterer Evaluierungen gegeben.

11.2 Forschungsmethodik

Die in diesem Artikel vorgestellten Arbeiten sind Teil eines Forschungsprojekts, das darauf abzielt, methodische und technologische Unterstützung für die Umsetzung des Cybersicherheitsmanagements an der Schnittstelle Land – Kommune – systemrelevante Unternehmen zu entwickeln. Das angestrebte Ergebnis ist eine partielle Referenz-Unternehmensarchitektur, die alle notwendigen inter-organisationalen Strukturen und Abläufe zwischen den Akteuren mit dem Anspruch definiert, Empfehlungscharakter für die Länder zu haben. Das Forschungsprojekt folgt dem Paradigma des Design Science Research (DSR) (Johannesson & Perjons, 2014). DSR ist ein Forschungsparadigma, das Probleme mit zugleich wissenschaftlicher als auch betrieblicher Relevanz durch einen konstruktionsorientierten Ansatz löst. Dabei steht das zu entwickelnde Artefakt und dessen systematische Entwicklung und Evaluierung im Mittelpunkt. Im hier behandelten Projekt ist das Referenz-Architekturmodell und die methodische Herangehensweise für den Einsatz des Artefakts verifiziert worden. Tabelle 7 „Forschungsarbeiten im DSR Prozess und ihre Ergebnisse“ gibt einen Überblick über die bereits durchgeführten Arbeiten. Sie ist nach den Phasen des DSR-Prozesses gegliedert und enthält die Forschungsaktivitäten, die erzielten Ergebnisse sowie Verweise auf den jeweiligen Abschnitt im Artikel oder auf die entsprechenden früheren Arbeiten. Im Rahmen des DSR-Prozesses befasst sich dieses Papier mit der Evaluierung der Referenz-Architektur im Kontext der Schnittstelle Land und Kommune.

DSR-Phase	Durchgeführte Arbeiten	Ergebnis
Problemdefinition	Literaturanalyse zur Ermittlung des Stands der Forschung und relevanter Arbeiten.	Bedarf bestätigt, aber keine wissenschaftlichen Publikationen verfügbar, die eine Architektur definieren (s. Kapitel 3)
	Experteninterviews mit den Chief Information Security Officers (CISO) bzw. Landesbeauftragte für Informationssicherheit mehrerer Bundesländer.	Problem fehlender Mechanismen zur Abstimmung zwischen Land / Kommune / Unternehmen wird bestätigt (Rehbohm et al., 2019).
Anforderungen ermitteln	Argumentative-deduktive Arbeit zur Ableitung von Anforderungen an methodische Unterstützung inkl. rechtlicher Rahmenbedingungen und technologisch-methodischer Anforderungen	Anforderungen basierend auf Experteninterviews, einer bundesweiten Umfrage in Kommunen, Rechtsstudien und eigenen Erfahrungen (Rehbohm et al., 2021), (Rehbohm et al., 2022), (Rehbohm & Kalmbach, 2021), (Rehbohm & Kalmbach, 2023).
Designzyklen des Artefakts	Konzeptionell-deduktive Entwicklung eines Architekturmo-	Mehrere Architekturversionen. Siehe Kapitel 4.

	dells mit ArchiMate (Modellierungssprache für Unternehmensarchitektur).	
Demonstration	Anwendung des Architekturmodells in konkretem Beispiel (Fallstudie)	Architektur (Rehbohm & Sandkuhl, 2023) in Bremerhaven/Würzburg/Hamburg.
Evaluierung	Evaluationsepisoden gemäß des FEDS-Ansatzes, d. h. formative und summative sowie artifiziell und in Realumgebung.	Relevanz und Nutzbarkeit bestätigt. Siehe Kapitel 4 und 5.

Tabelle 7 „Forschungsarbeiten im DSR Prozess und ihre Ergebnisse“

11.3 Stand der Forschung

Forschungsbeiträge im Umfeld der Cybersicherheit betreffen aktuell viele Disziplinen, insbesondere Künstliche Intelligenz, Internet of Things oder auch Cloud-Sicherheit. Das hier einschlägige Forschungsfeld ist im Kontext der Bedrohungsabwehr bei Dienstleistungen von allgemeinem Interesse zu fassen, der Gefahrenabwehr und Daseinsvorsorge in Verantwortung der Länder. In föderalen Strukturen wie in den USA, sind die Herausforderungen vergleichbar. Auch hier werden nahtlose Architekturen der Zusammenarbeit (Andreasson, 2012, S. 124), ein Cybersicherheitsframework (Rodin, 2015, S. 519) und ein Umdenken bei der Verantwortung einzelner Akteure eingefordert (Harknett & Stever, 2011, S. 455). Den europäischen Kontext betreffende Forschungsthemen zur Daseinsvorsorge tangieren Binnenmarktrecht, Wettbewerbsrecht und das öffentliche Auftragsvergaberecht. Die mittelbare Zuständigkeit für die Bereitstellung, Beauftragung und Organisation von Dienstleistungen von allgemeinem Interesse, mithin auch die Cybersicherheit auf föderalen Ebenen, ist in Forschungsarbeiten adressiert (Krajewski, 2015, S. 237). Was im allgemeinen Interesse der Gesellschaft steht, muss die jeweilige Gesellschaft definieren (Zhu, 2020, S. 31). Beschränkungen und Hemmnisse von Zusammenarbeitsbereichen von öffentlichen und privatrechtlich organisierten Akteuren wurden wissenschaftlich aufgearbeitet (Lange & Bötticher, 2015, S. 110). Forschungsbeiträge auf nationaler Ebene befassen sich zuvorderst mit Themen der Digitalisierung und des Onlinezugangsgesetzes (Seckelmann & Brunzel, 2021, S. 165). Die Zusammenarbeit von behördlichen und privatwirtschaftlichen Akteuren bei Cybersicherheitsbedrohungslagen ist Teil der aktuellen Forschung (Bretschneider et al., 2020, S. 53), insbesondere auch im Zusammenhang mit der Digitalisierung (Klenk et al., 2020, Teil 3). Eine funktionsfähige IT, beginnend mit der Öffentlichen Verwaltung (H. Becker, 2019, S. 19) und zusammen mit Unternehmen (Dürig & Fischer, 2018, S. 213), ist eine staatliche Aufgabe. Auf dem Gebiet des Cybersicherheitsmanagements sind in der Forschung eine Reihe von Arbeiten zum Thema Architektur von Cybersicherheitsmanagement durchgeführt worden. Es gibt jedoch einen Mangel an Forschung mit Bezug auf den öffentlichen

Sektor in föderativen Verwaltungsstrukturen und keine Arbeiten, die diesbez. die Konstellation Land – Kommune – systemrelevante Unternehmen adressieren (s.o.).

11.4 Föderale Cybersicherheitsarchitektur

11.4.1 Anforderungen an die Architektur

Die Anforderungen an die Architektur sind das Ergebnis von drei initialen Studien bei Stakeholdern und relevanten Akteuren sowie zwei begleitenden Rechtsstudien. Die mit den Landesbeauftragten für Informationssicherheit in den Ländern durchgeführte Studie zu politischen, strategischen, technischen und rechtlichen Herausforderungen in der Cybersicherheit haben gezeigt, dass die Länder verschiedene Herangehensweisen zur Lösung des Problems hatten. Insbesondere wurde geprüft, ob Verpflichtungen von Kommunen oder Wirtschaftsunternehmen zur Kooperation bestehen, oder diese Kooperation als freiwillige Leistung des Landes bzw. als Beratungsangebot bestand. Gleichzeitig wurde deutlich, dass keine zwischen den Ländern vergleichbare oder harmonisierte Vorgehensweisen vorlagen. Deutlich wurden die Unterschiede dort, wo die strategische und politische Willensbildung, zu Veränderungsprozessen im IT-Management oder IT-Sicherheitsmanagement, abgeschlossen war (Rehbohm et al., 2019).

Weiterhin beruht die Architektur auf Anforderungen, die mit Unternehmen der Freien Hansestadt Bremen durchgeführt wurden und als kritische Infrastrukturen (Kritis) nach Definition des Bundes gelten. Die Unternehmen waren, abhängig von ihrer Größe, sowohl im IT-Servicemanagement als auch im IT-Sicherheitsmanagement höchst unterschiedlich aufgestellt. Cybersicherheitsrisiken, Sicherheitsstrategien oder einschlägige Managementsysteme sind überwiegend nicht angemessen adressiert worden. Eine inhaltliche Zusammenarbeit mit der Landesverwaltung war auf Ebenen von Strafverfolgungsbehörden rudimentär gegeben. Es bestanden im Land Bremen auch keine rechtlichen Anknüpfungspunkte um eine Zusammenarbeit zu gewährleisten. Gleichzeitig ist der Wunsch nach weiterer Regulierung auch nicht artikuliert worden (Rehbohm et al., 2021). Ein weiterer Aspekt der Anforderungen an die Architektur wurde mittels einer Studie mit den Kommunen erhoben. Hierfür wurde bundesweit eine Onlineumfrage zum Sicherheitsmanagement bzw. Cybersicherheitsmanagement, auch als Träger der Daseinsvorsorge, durchgeführt.

Grundsätzlich ließ sich belegen, dass Informationssicherheitsmanagementprozesse unterentwickelt sind. Auch hier sind kleinere Kommunen deutlich schlechter als größere Kommunen aufgestellt. Zudem wird die eigene Dienstleistung überwiegend nicht als kritische Dienstleistung der Daseinsvorsorge verstanden. Gleichwohl wird aber Verantwortung für kommunale Dienste außerhalb der Verwaltung wahrgenommen. Verpflichtende rechtliche Bindungen an die Länder konnten auch nicht nachgewiesen werden. Ob und wie eine Kommune mit seinen Wirtschaftsunternehmen oder dem Land kooperiert, ist im

Benehmen der Kommune (Kommunale Selbstverwaltung) (Rehbohm et al., 2022). Neben den Studien bei den relevanten Akteuren, wurde initial eine Studie zu Grundforderungen von Informations- und Cybersicherheit in Ländern erstellt. Ergebnis dieser Arbeit ist, wer elementar wichtige Dienstleistungen oder Waren für große Teile der Bevölkerung anbietet, ist Teil der Daseinsvorsorge. Solche Akteure müssen identifiziert werden und sind nötigenfalls gesetzlich oder auf dem Verordnungswesen in die Pflicht zu nehmen. Ermächtigungen zur Kontrolle und zum Ergreifen von Maßnahmen ggf. Sanktionen sind im Ermessen des jeweiligen Gesetzgebers im Land. Cybersicherheit kann als Teil des Ordnungsrechts im jeweiligen Land ausgebaut werden (Rehbohm & Kalmbach, 2021).

Eine zweite Studie befasste sich mit der von der Bundesinnenministerin postulierten Absicht einer Grundgesetzänderung, welche die Gesamtzuständigkeit für die Cybersicherheit beim Bund verorten will. Im Beitrag *Herausforderungen der föderalen Cybersicherheit vs. Änderung in der Bund-Länder Gewaltenteilung* wird herausgearbeitet, welche Gefahren und Möglichkeiten mit einer Zentralisierung der Verantwortung einhergehen. Grundsätzlich können durch die Mandatserhöhung beim Bund auch Chancen für die Länder und somit für die gesamte Resilienz entstehen, gleichzeitig sind jedoch die Folgen einer Zentralisierung nicht abschließend aufgearbeitet worden (Rehbohm & Kalmbach, 2023). Die hier vorgestellte föderale Cybersicherheitsarchitektur ist das Ergebnis mehrerer empirischer Studien, der Erarbeitung von Anforderungen an eine Architektur und die nachstehend abgeleiteten Ziele. Zusammenfassend und auf einem hohen Abstraktionsniveau gesehen, sind dies die Ziele Rechtssicherheit, Anwendbarkeit, Resilienz, Nachhaltigkeit und Kooperation. Die Cybersicherheitsarchitektur soll strukturelle Rahmenbedingungen, technische Interaktionen und Rechtssicherheit schaffen, die eine gleichberechtigte Teilhabe aller Akteure ermöglicht.

11.4.2 Architektur

Die erstellte Architektur soll ein funktionsfähiges Bindeglied zwischen den Ländern, dem Bund und den Verwaltungen, insbesondere Ministerialverwaltungen sowie den Kommunen präsentieren (Rehbohm & Sandkuhl, 2023). Für die Wirtschaft kommen derzeit verschiedene Mechanismen zur Identifizierung und zur Einbindung in die Prozesse zur Anwendung. Insbesondere werden kritische Infrastrukturen derzeit nach Definition des Bundes (Kritis) sowie die Wirtschaftsunternehmen der Daseinsvorsorge der Region (Subkritis) adressiert. Kritische und subkritsiche Infrastrukturen werden in der vorliegenden Studie als systemrelevante Infrastrukturen der Daseinsvorsorge im Land definiert. Das angewendete Unternehmensarchitekturmanagement verwendet unterschiedliche Sichten und Perspektiven für die Dokumentation, Planung und Visualisierung zentraler Bestandteile eines Unternehmens bzw. einer Organisation wie der Landesverwaltung (D. Simon et al., 2013). Die Geschäftsarchitektur soll die zentralen Ziele der Unternehmensstrategie bedienen, die Geschäftsprozesse visualisieren, die erforderlichen Organisationsstrukturen aufzeigen und Governance-Strukturen des Unternehmens abbilden.

Das in Abbildung 20 "Auszug der vorgeschlagenen föderalen Cybersicherheitsarchitektur: Prozesse" dargestellte Bild (Anlagen), zeigt die fünf Kernprozesse, zwei Supportprozesse und den Prozess zur übergeordneten Strategie der Gesamtarchitektur auf. ***Strategie und Motivation*** ist der übergeordnete Prozess, der zum einem die Erwartungshaltung der Stakeholder visualisiert und zum anderen strategische Ziele eines übergreifenden Cybersicherheitsmanagements in einem Land beinhaltet. Intrinsische Motive wie zum Beispiel Wirtschaftlichkeit, Nachhaltigkeit oder Widerstandsfähigkeit sowie die extrinsischen Motive im Kontext von eigenen IT-Infrastrukturen und die Fähigkeiten diese zu betreiben oder betreiben zu lassen, sind adressiert. Elementare Fähigkeiten sind in diesem Zusammenhang mit IT-Servicemanagement, IT-Sicherheitsmanagement und Threat-Intelligence-Management verbunden. Zwei Supportprozesse unterstützen die eigentlichen fünf Kernprozesse. Zur Erreichung des Ziels Rechtssicherheit ist der Prozess zur ***Regulation/Legislation/Obligation*** angelegt. Hierunter ist ein wesentlicher Unterstützungsprozess zu verstehen, der die Verpflichtung der Föderalstaaten umfasst, entlang der europäischen und deutschen regulatorischen Anforderungen, eigene Gesetzgebungen und Verordnungen zu entwickeln und an den dynamischen Herausforderungen anzupassen. Ein klassischer Compliance Prozess, der um die Möglichkeit der eigenen Gesetzgebungskompetenz erweitert ist. Der zweite Unterstützungsprozess *Human Resources/Communication/Cooperation* umfasst die Entwicklung eines regionalen Netzwerkes von eigenen und im Auftrag tätigen Beschäftigten der betroffenen Organisationen sowie Dienstleistern oder Partnern. Dies können insbesondere Unternehmen, andere Föderalstaaten, der Bund und auch jede andere Organisation in Europa oder in der Welt sein, um die eigenen Fähigkeiten partnerschaftlich zu entwickeln. Die fünf Kernprozesse werden bestimmt von ***Identification/Compliance***, um initial und fortwährend die Bestimmung wesentlicher und wichtiger Organisationen der Region, in Wirtschaft und Verwaltung sowie entlang der rechtlichen Anforderungen zu identifizieren. Dabei ist die Registrierung und Bekanntmachung der betroffenen Daseinsvorsorgeträger in Bund und Länder gleichermaßen und synchron sicherzustellen, um eindeutige Zuständigkeiten zu definieren. Der nächste Kernprozess bezieht sich auf ***Risk/Performance*** und betrifft den Aufbau und die Überwachung der Veränderung der Bedrohungslage auf die föderalen Infrastrukturen, seinen Akteuren und den damit einhergehenden Risiken für diese. Fähigkeiten der betroffenen Organisationen, wie Informationssicherheitsmanagement, liefern regelmäßig Kennzahlen, welche in einem ganzheitlichen Monitoring des Risikos der Region weiterverwendet werden sollen. Die im Prozess ***Operation*** beschriebenen Funktionalitäten existieren teilweise als Softwarelösung oder Anwendung und müssen zwischen den Akteuren etabliert werden. Insbesondere handelt es sich um den technischen Echtzeit-Austausch von Angriffsvektoren, die Lagebilderhebung oder die Koordinierung von Unterstützungskräften in der Region. Der Kernprozess ***Super Authority/Sanctioning*** betrifft die jeweilige Landesverwaltung und die Pflicht zur Institutionalisierung in einer behördlichen Struktur. Die Prozesse zur Steuerung der Cybersicherheit beinhalten insbesondere Mandate zur Einsichtnahme und Kontrolle von Akteuren, um die Einhaltung der Ziele und die Konformität sicherzustellen. Auch ist das Auslösen von

Sanktionsmechanismen und Maßnahmen zur Aufrechterhaltung bzw. Verbesserung des Gesamtsystems sicherzustellen. Der Kernprozess ***Cyber Security Standards*** umfasst alle Hilfsmittel, Maßnahmen und Vorgehen, die den Betrieb und die Resilienz der Cybersicherheitsarchitektur fördern, insbesondere aus dem Bereich der Informationssicherheit. Beinhaltet ist auch die Mitwirkung der jeweiligen Länder bei der Entwicklung- und fortlaufenden Prüfung der Anwendbarkeit von Sicherheitsstandards auf die Akteure der Region.

11.4.3 Evaluierungsstrategie und Grundsätze ordnungsgemäßer Modellierung

Die Cybersicherheitsarchitektur ist entlang des Designs Science Research (DSR) entstanden. Das DSR Vorgehensmodell zielt darauf ab, anhand eines Sollzustandes ein Artefakt zu entwickeln; dies kann insbesondere eine Methode oder wie in diesem Beitrag eine Architektur sein. Neben der eigentlichen Entwicklung des Design-Artefakts, liegt eine weitere Herausforderung darin, dass der Evaluierungsprozess sichergestellt, dass Anhaltspunkte für die Verbesserung und Weiterentwicklung – die dem Anspruch an der Forschung genügen – generiert werden.

Als *Evaluationskriterien* werden in dieser Arbeit die Grundsätze ordnungsmäßiger Modellierung (GoM) herangezogen und überprüft (J. Becker et al., 2012, S. 32), da es sich bei der CSA um ein Modell handelt. Es wird ein Interviewleitfaden entwickelt, dessen Fragestellungen inhaltlich auf diese Grundsätze ausgerichtet sind. Dabei handelt es sich um folgende Inhalte:

- Grundsatz der Richtigkeit wird erfüllt, wenn eine inhaltliche und widerspruchsfreie Syntax verwendet wird sowie die beschriebenen Rollen und Namenskonventionen anerkannt werden und konsistent sind.
- Grundsatz der Relevanz wird erfüllt, wenn die definierten Ziele mit der Architektur und den Anforderungen der Stakeholder im Einklang stehen.
- Grundsatz der Wirtschaftlichkeit wird erfüllt, wenn die mit der Umsetzung der Architektur stehenden Aufgaben in einem definierten Zeitraum leistbar sind. Dabei stellt die Architektur einen Kompromiss dar, der abhängig von den Ländern unterschiedlich mit Ressourcen unterstützt wird um folglich detaillierte Ziele umzusetzen.
- Grundsatz der Klarheit wird erreicht, wenn das entwickelte Artefakt für die Akteure und Stakeholder als eindeutige und anschauliche Interpretation verstanden wird.
- Grundsatz der Vergleichbarkeit wird erreicht, wenn die Vorgehensweise zur Entwicklung des Artefakts mit anderen Entwicklungen, zum Beispiel im Umfeld von EAM mit ArchiMate, nachvollzogen werden kann.
- Grundsatz des systematischen Aufbaus wird erreicht, wenn der logische Aufbau verifiziert werden kann und widerspruchsfrei ist.

Eine in der Wissenschaft anerkannte Evaluierungsstrategie bietet das *Framework for Evaluation in Design Science Research* (FEDS), welches in diesem Beitrag angewendet

wird (Venable et al., 2016). Mit der FEDS-Evaluationsstrategie soll sichergestellt werden, dass die beinhalteten Fragestellungen im Entstehungsprozess des Artefakts evaluiert werden. Die DSR-Evaluierungsepisoden werden in zwei Dimensionen ausgeprägt. Eine Dimension berücksichtigt den formativen bzw. summativen Zweck- und die zweite Dimension die künstliche oder naturalistische Evaluierung. Schritte im FEDS-Evaluierungsprozess:

1. Erläuterung der Evaluationsziele: Darstellung der Ziele der Evaluation des Artefakts und mögliche Alternativziele. Dabei werden Effizienz (Artificial Evaluation, das beobachtete Ergebnis wird nicht von Störvariablen beeinflusst) und Effektivität (Summative Evaluation der Wirksamkeit in einem realen Umfeld). Ungewissheiten und Risikominderung, wie z. B. Nutzungsrisiken (die Architektur kommt nicht zum Einsatz) sollten in einer frühen Phase der Evaluationen bewertet werden.
2. Auswahl der Evaluationsstrategie: Je nach Ziel der Evaluierung können mehr als eine Strategie zur Anwendung kommen oder deren Kombination. 1. Bewertung von Designrisiken im Hinblick auf technologische oder menschliche Nutzungsrisiken. 2. Bewertung von Wirtschaftlichkeitsaspekten, wie Ressourcenverfügbarkeit im Verhältnis Umsetzungsmöglichkeiten in Evaluierungsepisoden. 3. Bewertung des Artefakts im Hinblick auf den gegenwärtigen oder zukünftigen Einsatz, als rein technische Lösung, ohne menschliche Nutzung. 4. Bewertung der Komplexität des Artefakts.
3. Bestimmung der zu evaluierenden Eigenschaften: In diesem Schritt müssen die Kriterien, Merkmale und Anforderungen des Artefakts für die Bewertung definiert werden. Dies können insbesondere bestehende Anforderungen aus Frameworks oder Standards sein und werden in jedem Fall individuell auf das Artefakt abgestellt.
4. Gestaltung der einzelnen Evaluationsabschnitte: Festlegung der konkreten Evaluierungsepisoden. 1. Identifikation von Beschränkungen, wie Ressourcen. 2. Priorisierung von wesentlichen, wichtigen, weniger wichtigen, "nice to have" oder irrelevanten Aspekten. 3. Festlegung der Anzahl und Art von Evaluierungsepisoden.

11.4.4 Evaluierungsepisode Kommunen

Die Evaluierung wurde mit den Kommunen Bremerhaven, Hamburg und Würzburg durchgeführt. Grundsätzlich wurden in diesem Evaluationsschritt große Kommunen gewählt, da diese zur unmittelbaren Einbeziehung der Umsetzungsanforderungen der NIS-2-Richtlinie (EUR-Lex - 32022L2555 - EN - EUR-Lex, 2022) in Diskussion standen. Gleichwohl ist der Architekturvorschlag für die deutsche Verwaltungsgliederung konzipiert und nicht an Einwohnerzahlen einer Gebietskörperschaft gebunden. Für Bremerhaven war ausschlaggebend, dass die Architektur in Land Bremen entstanden ist und

somit schon in der Konzeptionsphase Berücksichtigung fand. Des Weiteren bietet sich das kleinste Bundesland mit einer weiteren Kommune auch für eine praktische Umsetzung als Verprobungsregion an. Die Stadt Würzburg wurde als weitere Referenz aus einem Flächenland hinzugezogen, um den Vergleich mit einem großen Föderalstaat zu ermöglichen. Die Stadt Hamburg wurde als Stadtstaat hinzugezogen und kann zusätzlich für eine Evaluierung als Land genutzt werden. In Bremerhaven wurden am 24. Mai 2023, in Hamburg am 13.10.2023 und in Würzburg am 12. Juni 2023 die Experteninterviews mit folgenden Teilnehmern durchgeführt: Stefan J., Magistratskanzlei der Stadt Bremerhaven, Leitung des Digitalisierungsbüros, Lars J., Betriebsleiter des Betriebs für Informationstechnologie Bremerhaven (BIT), Wirtschaftsbetrieb der Stadt Bremerhaven, Frank S., IT-Sicherheitsbeauftragter des Betriebs für Informationstechnologie Bremerhaven, Marc B., Informationssicherheitsbeauftragter (CISO), Stadt Würzburg und Carsten. B., Senat der Freien und Hansestadt Hamburg, Senatskanzlei, CISO, Amt für IT und Digitalisierung (ITD). Den Experten wurde der Architekturansatz zunächst hinsichtlich der generellen Struktur vorgestellt und danach die wesentlichen Prozesse – wie in Abbildung 21 "Strategy and Motivation" exemplarisch illustriert (Anlagen) – im Architekturmodell erläutert. Weiterhin wurden entlang des Design Science Process die Iterationsschritte zur Entwicklung des Artefakts diskutiert. Der Lösungsansatz einer formalen Architekturentwicklung wird grundsätzlich als hilfreich und zielführend für die Herausforderungen der Cybersicherheit angesehen. Unklarheiten bestehen jedoch über die zu erfüllenden Anforderungen in kommunalen Strukturen. Insbesondere die Gesetzgebungsverfahren in Europa, dem Bund und den Ländern können derzeit nicht auf konkrete Anforderungen oder Erfüllungsaufwände umgesetzt werden. Die verfolgten Ziele sind in Bezug auf die Anforderungen an eine Resilienz-Architektur nachvollziehbar, richtig und vollständig. Der strategische und motivatorische Prozess ist korrekt dargestellt. Insbesondere motivatorische Elemente sind auch in den Kommunen gleichgelagert und werden als richtig gesehen. Strategische Ziele sind zu diesem Zeitpunkt nicht von der Landesregierung kommuniziert und insofern derzeit nicht nachvollziehbar. Die Darstellung der einzelnen Akteure – insbesondere die Kommunen – sind korrekt ausgewiesen. Die beschriebenen Kernprozesse stellen die Kommunen vor Herausforderungen, für die sie derzeit nicht aufgestellt sind. Bei den Kernprozessen selbst und den verbundenen Aufgaben bestehen hingegen keine Bedenken. Die mit den Prozessen verbundenen Fähigkeiten müssen in den Kommunen teilweise aufgebaut werden, insbesondere im Bereich Operations. Die mit den Supportprozessen verbundenen Aufgaben sind nachvollziehbar ausgewiesen und müssen zuvorderst durch die Länder etabliert werden. Dies gilt vor allem für die Ausgestaltung des mit Rechtssicherheit ausgewiesenen Ziels. Kooperationen auszubauen und Fachkräftegewinnung wird auch in den Kommunen als leistbar gesehen. Aus Sicht der Kommunen ist die Architektur größtenteils verständlich strukturiert und kann implementiert werden. Die mit diesem Modell vorgestellte Vorgehensweise und der erforderliche Aufbau von ergänzenden Infrastrukturen wird als übertragbar auf an-

dere Organisationen gesehen, auch im Hinblick auf wirtschaftliche Aspekte. Ob das vorliegende Modell auch Hinsicht der Kooperation mit Wirtschaftsunternehmen hilfreich sein wird, konnte durch die Befragten nicht bestätigt werden.

11.5 Schlussbetrachtung

Die Cybersicherheitsarchitektur ist das Ergebnis einer mehrjährigen Forschungsarbeit. Die in diesem Beitrag behandelte Evaluierungsepisode soll dazu beitragen, eine belastbare und auf weitere Länder übertragbare Architektur zu entwickeln. Besondere Berücksichtigung findet dabei die Dynamik von Bedrohungen für die IKT Infrastrukturen. Insofern soll die Architektur ein offenes System sein, welches auch den Anforderungen an Agilität standhält. Die Evaluationsstrategie soll das Artefakt und die inhaltlichen Schwerpunkte erfüllen und möglichst verbessern. Die hier aufgezeigte Evaluierungsepisode bei den Kommunen, wurde von den Befragten als grundsätzlich belastbare Architektur eingeschätzt. Gleichzeitig bestehen Bedenken, hinsichtlich der Umsetzbarkeit mit den vorhandenen Ressourcen. Zuvorderst ist eine politische Willensbildung gefragt, die folglich auch Steuerungen von Ressourcen beinhalten wird. Diese Willensbildung kann auch per Gesetz erfolgen, insofern existiert auch eine Verpflichtung für die erforderlichen Schritte. Aus Sicht der Befragten in den Kommunen kann die Cybersicherheitsarchitektur umgesetzt werden. Aus Sicht des Autors sind Änderungen am Modell derzeit entbehrlich. In einer nächsten Evaluierungsepisode werden ausgewählte Länder in einem Experteninterview befragt und sollen die Evaluierung der Cybersicherheitsarchitektur abschließen.

11.6 Anlagen

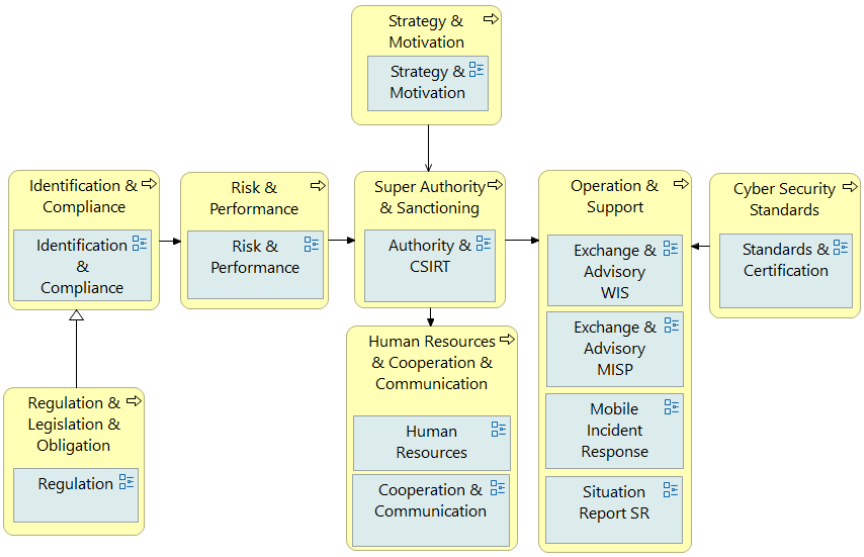

Abbildung 20 "Auszug der vorgeschlagenen föderalen Cybersicherheitsarchitektur: Prozesse"

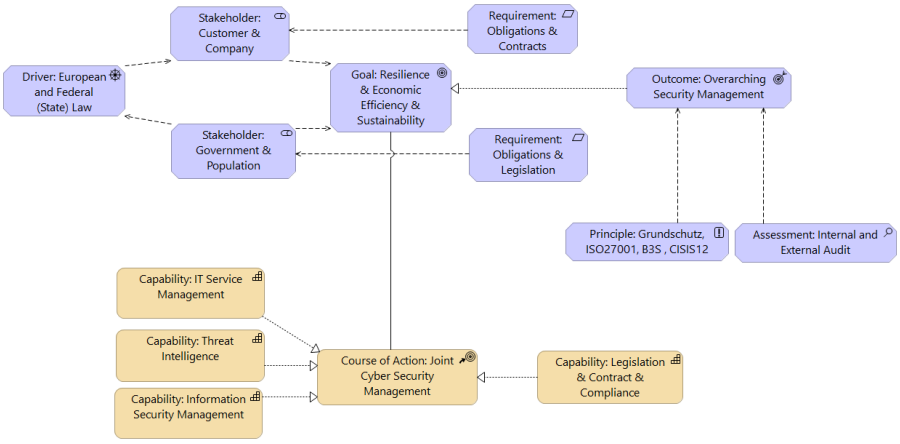

Abbildung 21 "Strategy and Motivation"

12 Evaluation einer föderalen Referenzarchitektur für Cybersicherheit[11]

Zusammenfassung. Öffentliche Verwaltungen, Unternehmen und Bürger sind das Ziel von Angriffen aus dem Cyberraum. Staat, Wirtschaft und Gesellschaft müssen sich daher vor Bedrohungen im Bereich der Cybersicherheit schützen. Die deutsche Cybersicherheitsarchitektur (CSA) von Bund und Ländern ist grundsätzlich unabhängig und greift an ausgewählten Stellen ineinander. Europäische Regelungen betreffen in erster Linie die Mitgliedsstaaten und nur teilweise auch die Bundesländer. Die Verwaltungsgliederung und folglich die Kompetenzen zur Abwehr von Gefahren für ein Bundesland können nur von einem Bundesland bestimmt werden, um die Handlungsfähigkeit und die Geschwindigkeit des Agierens zu verbessern. In diesem Artikel wird eine Unternehmensarchitektur vorgeschlagen, die sich insbesondere auf die Bundesländer und deren Möglichkeiten und Fähigkeiten konzentriert. Der architektonische und föderale Ansatz zur Integration von Anforderungen und zur Zielerreichung wird vorgestellt und evaluiert. Unternehmensarchitekturen werden in der öffentlichen Verwaltung bisher wenig oder gar nicht eingesetzt. In diesem Artikel wird eine Cybersicherheitsarchitektur mit Bundesländern evaluiert, um eine partielle Referenzarchitektur zu verifizieren.

Schlüsselwörter: Cybersicherheit, Informationssicherheit, Cybersicherheitsarchitektur, Unternehmensarchitektur, Referenzmodell, Referenzarchitektur

12.1 Einleitung

Die Verwaltungsstruktur in Deutschland hat eine in ihren Säulen voneinander unabhängige vertikale Struktur. Die Staatsgewalt ist zwischen dem Bund und den Ländern aufgeteilt. Das Grundgesetz legt fest, dass die Bundesländer für die Gesetzgebung, Verwaltung und Rechtsprechung zuständig sind, soweit es um föderal relevante Regelungsinhalte geht. Für die Zusammenarbeit in der Informationstechnik wurde im Zuge der Föderalismusreform das Grundgesetz konsequent so ausgestaltet, dass Bund und Länder auf dem Gebiet der Informationstechnologie zusammenarbeiten dürfen (GG - Grundgesetz für die Bundesrepublik Deutschland, 1949, Article 91c). Die Kommunen sind Teil der Bundesländer und stellen in diesem Kontext keine weitere Ebene im Staatsgefüge dar. Dennoch haben sie das garantierte Recht der Selbstverwaltung (GG - Grundgesetz für die Bundesrepublik Deutschland, 1949, Article 28). Die Organisation der technischen Zusammenarbeit ist im Gesetz über die Zusammenschaltung der informationstechnischen Netze des Bundes und der Länder verankert (Bundesministerium der Justiz, 2019). Die informationstechnischen Infrastrukturen und die darauf aufbauenden Sicherheitsmanagementsysteme sind dennoch unabhängig voneinander entwickelt worden

[11] Der Inhalt dieses Kapitels ist bereits wie folgt veröffentlicht worden: Thomas Rehbohm und Kurt Sandkuhl, Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023) der Gesellschaft für Informatik e.V., in "Praxishandbuch Verwaltungsinformatik" (Pidun & Auth, 2025)

und greifen auf der Anwendungsebene nur dann ineinander, wenn ebenenübergreifende Prozesse genutzt werden. Überall dort, wo der Bund die ausschließliche Verantwortung übernimmt, sind die Anforderungen an die Informationssicherheit gesetzlich verankert, zum Beispiel im Onlinezugangsgesetz und der darauf basierenden Portalnetzverordnung (OZG - Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen, 2017). Grundsätzlich stehen die Länder und der Bund hier nicht in Konkurrenz zueinander und sollten zusammenarbeiten, um einheitliche und sichere Lebensverhältnisse zu ermöglichen (Krumm, 2015, S. 170). Die mit den dynamischen Bedrohungssituationen (Bundesamt für Sicherheit in der Informationstechnik, 2023) verbundenen Herausforderungen für die informationstechnischen Systeme von öffentlichen Verwaltungen und Wirtschaftsunternehmen sind grenzüberschreitend und erzwingen einen kooperativen Ansatz zum Aufbau belastbarer Infrastrukturen und eines gemeinsamen Sicherheitsmanagements. Zusammenhängende Problemstrukturen machen Kooperationen erforderlich (Kropp, 2010, S. 125).

Die regionalen Akteure eines Bundeslandes sind in die Cybersicherheitsarchitektur des Bundes und der Länder involviert und müssen nahtlos in die gesamtdeutsche Cybersicherheitsarchitektur integriert werden. Die föderale Cybersicherheitsarchitektur muss der aktuellen europäischen Regulierung entsprechen, insbesondere der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie), 2023). Regionale und digitale Dienstleistungen von allgemeinem Interesse stehen somit im Mittelpunkt dieses Artikels. Das Zusammenspiel von Staat, Kommunen und Wirtschaft wird als systemrelevante Infrastruktur betrachtet. Eine effektive Koordination der Instrumente zwischen den relevanten Akteuren ist entscheidend für die Gewährleistung der Cybersicherheit. Die Zusammenarbeit ermöglicht es, Bedrohungen schneller zu erkennen und effektiver darauf zu reagieren. Eine definierte Cybersicherheitsarchitektur des Bundes in diesem Bereich, um die es in diesem Artikel geht, fehlt jedoch noch.

Dieser Artikel stellt die Evaluierung einer föderalen Cybersicherheitsarchitektur in ausgewählten Bundesländern vor. Für die Konkretisierung des Cybersicherheitskonzepts wurde ein Unternehmensarchitekturmodell gewählt. Unternehmensarchitekturen berücksichtigen typischerweise verschiedene Ebenen einer Organisation, wie die Geschäfts-, Informations- und Technologiearchitektur. Da bei der Vernetzung von Land, Kommunen und Unternehmen alle Ebenen für eine verbesserte Cyber-Architektur benötigt werden, ist es sinnvoll, einen Enterprise-Architekturansatz zu verwenden.

Die Anforderungen an die resultierende Architektur basieren auf empirischen Untersuchungen der Informationssicherheitsbeauftragten der Bundesländer, der Betreiber kritischer Infrastrukturen im Land Bremen und einer bundesweiten Befragung von Kommunen. Durch die Evaluierung der Unternehmensarchitektur wurden die Angemessenheit und Anwendbarkeit in den befragten Bundesländern überprüft und die Möglichkeiten zur Weiterentwicklung analysiert. Die Beschränkung der Arbeit liegt darin, dass sie sich auf

die öffentliche Verwaltung in Deutschland bezieht. Ziel ist es, einen praxisnahen Ansatz zur Lösung der föderalen Problematik aufzuzeigen.

Abschnitt 2 beschreibt die Forschungsmethodik und Abschnitt 3 den aktuellen Stand der Forschung. Abschnitt 4 befasst sich mit der Cybersicherheitsarchitektur und ihrer Bewertung nach wissenschaftlichen Grundsätzen. Abschnitt 5 fasst die Ergebnisse zusammen und gibt einen Ausblick auf mögliche Verbesserungen und weitere Bewertungen.

12.2 Forschungsmethodik

Die in diesem Beitrag vorgestellten Arbeiten sind Teil eines Forschungsprojekts, das zum Ziel hat, methodische und technologische Unterstützungen für die Umsetzung eines Cybersicherheitsmanagements an der Schnittstelle zwischen Land, Kommune und systemrelevanten Unternehmen zu entwickeln. Das angestrebte Ergebnis ist eine partielle Referenz-Unternehmensarchitektur, die alle notwendigen interorganisatorischen Strukturen und Prozesse zwischen den Akteuren definiert, mit dem Ziel, Empfehlungen für die Bundesländer zu geben. Das Forschungsprojekt folgt dem Paradigma der Design Science Research (DSR) (Johannesson & Perjons, 2014) und basiert auf Design Science in Information Systems Research (A. R. Hevner et al., 2004).

DSR ist ein Forschungsparadigma, das Probleme mit wissenschaftlicher als auch operativer Relevanz mit einem designorientierten Ansatz löst. DSR wird als Forschungsmethode in verschiedenen Disziplinen eingesetzt, insbesondere in den Bereichen Informationssysteme und Informatik. Das Ziel der designwissenschaftlichen Forschung ist es, praktische Lösungen für komplexe Probleme zu entwickeln und Erkenntnisse über das Design neuer Artefakte zu schaffen. Der designwissenschaftliche Ansatz umfasst oft mehrere iterative Zyklen, beginnend mit der Identifizierung und Definition eines Problems, gefolgt von der Entwicklung eines Artefakts zur Lösung dieses Problems. Der entwickelte Lösungsansatz wird dann evaluiert und iterativ verbessert. Der Schwerpunkt liegt dabei auf dem zu erstellenden Artefakt und dessen systematischer Entwicklung und Bewertung.

In diesem Artikel wurden die Referenzarchitektur und der methodische Ansatz für die Nutzung des Artefakts mit drei Bundesländern evaluiert. Der folgende Abschnitt gibt einen Überblick über die bereits durchgeführten Arbeiten. Der Abschnitt ist nach den Phasen des DSR-Prozesses gegliedert und enthält die Forschungsaktivitäten, die erzielten Ergebnisse und Verweise auf die entsprechenden Abschnitte in diesem Artikel oder auf die entsprechenden veröffentlichten Arbeiten.

***Explicate Problem*:** Durchführung einer systematischen Literaturanalyse zur Ermittlung des aktuellen Forschungsstandes und der einschlägigen Arbeiten. Ergebnis: Der Bedarf an Forschung konnte bestätigt werden, da keine relevanten wissenschaftlichen Publikationen verfügbar sind, die eine föderale Architektur definieren (siehe Abschnitt 3). Initiale

Durchführung eines Experteninterviews mit den Chief Information Security Officers (CISO), den Landesbeauftragten für Informationssicherheit der Bundesländer. Ergebnis: Das Problem fehlender Mechanismen zur Abstimmung zwischen Land, Kommunen und Unternehmen konnte bestätigt werden (Rehbohm et al., 2019).

***Define Requirements*:** Die argumentative-deduktive Arbeit zur Ableitung von Anforderungen an methodische Unterstützung inklusive rechtlicher Rahmenbedingungen und technologisch-methodischer Anforderungen. Ergebnis: Die Anforderungen konnten basierend auf Experteninterviews mit Betreibers systemrelevanter Infrastrukturen, einer bundesweiten Umfrage in Kommunen, einer Rechtsstudie und eigener Expertise definiert werden (Rehbohm et al., 2021), (Rehbohm et al., 2022), (Rehbohm & Kalmbach, 2021).

Design and Develop Artefact: Konzeptionell-deduktive Entwicklung eines Architekturmodells mit ArchiMate (Modellierungssprache für Unternehmensarchitektur), unter Berücksichtigung von geänderten rechtlichen Rahmenbedingungen (Rehbohm & Kalmbach, 2023). Ergebnis: Anpassungen und Änderungen der entworfenen Architektur, entlang der sich ergebenden Anforderungen (Rehbohm & Moses, 2023a) (siehe Abschnitt 4).

***Demostrate Artefact*:** Anwendung des Architekturmodells, um die Bedeutung des Artefakts nachzuweisen bzw. die Verallgemeinerung des Designs zu erreichen (Rehbohm & Sandkuhl, 2023). Fallstudien in Bremerhaven, Hamburg und Würzburg.

***Evaluate Artefact*:** Durchführung von Evaluationsepisoden gemäß des FEDS-Ansatzes (Venable et al., 2016, S. 16), d. h. formative und summative sowie artifiziell und in Realumgebung.

Kommunale Evaluation: Zur Veröffentlichung angenommen im April 2024, auf der „GI Sicherheit 2024“, Fachtagung des Fachbereichs "Sicherheit - Schutz und Zuverlässigkeit" der Gesellschaft für Informatik e.V. (Rehbohm & Sandkuhl, 2024).

Bundesländer Evaluation: Die Relevanz und Nutzbarkeit der Architektur wurde bestätigt (siehe Abschnitte 4 und 5).

12.3 Stand der Forschung

Die aktuellen Forschungsbeiträge im Umfeld der Cybersicherheit betreffen diverse Disziplinen, insbesondere Künstliche Intelligenz oder auch Cloud-Sicherheit. In der Domäne „Öffentliche Verwaltung“ des föderalen Deutschlands sind weiterhin Beiträge im Umfeld der Verwaltungsdigitalisierung relevant. Das hier einschlägige Forschungsfeld ist im Zusammenhang der Gefahrenabwehr bei Dienstleistungen von allgemeinem Interesse zu fassen. Das heißt, die fortwährende Bewältigung von Bedrohungslagen für die Informationssicherheit von Daseinsvorsorgeträgern in Verantwortung der Länder. Diese Herausforderungen sind durchaus vergleichbar, insbesondere in föderalen Strukturen wie in den USA. Grundsätzlich sind Architekturen der Zusammenarbeit (Andreasson, 2012, S.

125), ein Cybersicherheitsframework (Rodin, 2015, S. 519) und ein Umdenken bei der Verantwortung einzelner Akteure gefordert (Harknett & Stever, 2011, S. 455). Europäische Forschungsthemen zur Daseinsvorsorge tangieren vornehmlich Themen des Binnenmarktrechts, Wettbewerbsrechts und das öffentliche Auftragsvergaberecht. Die mittelbare Zuständigkeit für die Bereitstellung, Beauftragung und Organisation von Dienstleistungen von allgemeinem Interesse, mithin auch die Cybersicherheit auf föderalen Ebenen, ist in Forschungsarbeiten adressiert (Krajewski, 2015, S. 237). Was im allgemeinen Interesse der Gesellschaft steht, muss die jeweilige Gesellschaft definieren (Zhu, 2020, S. 31). Beschränkungen und Hemmnisse von Zusammenarbeitsbereichen von öffentlichen und privatrechtlich organisierten Akteuren wurden wissenschaftlich aufgearbeitet (Lange & Bötticher, 2015). Forschungsbeiträge auf nationaler Ebene befassen sich zuvorderst mit Themen der Digitalisierung und des Onlinezugangsgesetzes (Seckelmann & Brunzel, 2021, S. 165). Die Zusammenarbeit von behördlichen und privatwirtschaftlichen Akteuren bei Cybersicherheitsbedrohungslagen ist Teil der aktuellen Forschung (Bretschneider et al., 2020, S. 53), insbesondere auch im Zusammenhang mit der Digitalisierung (Klenk et al., 2020, Teil 3). Eine funktionsfähige IT, beginnend mit der Öffentlichen Verwaltung (H. Becker, 2019, S. 19) und zusammen mit Unternehmen (Dürig & Fischer, 2018, S. 209–213), ist eine staatliche Aufgabe.

Auf dem Gebiet des Cybersicherheitsmanagements sind in der Forschung eine Reihe von Arbeiten zum Thema Architektur durchgeführt worden. Es gibt jedoch einen Mangel an Forschungen mit Bezug auf den öffentlichen Sektor in föderativen Verwaltungsstrukturen und keine Arbeiten, die diesbezüglich die Konstellation Land, Kommune und systemrelevante Unternehmen adressieren.

12.4 Föderale Cybersicherheitsarchitektur

12.4.1 Anforderungen an die Architektur

Die initialen Anforderungen an die Architektur sind das Ergebnis von drei initialen Studien bei Stakeholdern und relevanten Akteuren sowie zwei begleitenden Rechts-studien. Die mit den Landesbeauftragten für Informationssicherheit in den Ländern durchgeführte Studie zu politischen, strategischen, technischen und rechtlichen Herausforderungen in der Cybersicherheit haben gezeigt, dass die Länder verschiedene Herangehensweisen zur Lösung des Problems hatten. Auch hat sich gezeigt, dass die Verortung der CISO-Bereiche relevant sein kann. Cybersicherheit wird regelmäßig als Teil der Gefahrenabwehr betrachtet, was für eine Zuordnung des Informationssicherheitsmanagements der Öffentlichen Verwaltung (CISO) in den ministeriellen Innenbereichen von Vorteil erscheinen lässt. Tatsächlich sind die CISO-Bereiche oftmals bei den Finanzministerien, Digitalisierungsministerien oder in den Staats- bzw. Senatskanzleien zugeordnet, was folglich höhere Abstimmungsaufwände erforderlich macht. Unabhängig von der Verortung wurde geprüft, ob rechtliche Verpflichtungen (Barudi et al., 2023, Kapitel 15.3) von Kommunen oder Wirtschaftsunternehmen zur Kooperation bestehen, oder diese Kooperation

als freiwillige Leistung des Landes bzw. als Beratungsangebot bestand. Gleichzeitig wurde deutlich, dass keine zwischen den Ländern vergleichbare oder harmonisierte Vorgehensweisen vorlagen (Rehbohm et al., 2019).

Weiterhin beruht die Architektur auf Anforderungen, die mit Unternehmen der Freien Hansestadt Bremen durchgeführt wurden und zu diesem Zeitpunkt als kritische Infrastrukturen (Kritis) nach Definition des Bundes (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 2015) galten. Die Anzahl solcher Unternehmen ist durch die neueren europäischen Gesetzgebungen weiter angewachsen. Die Unternehmen waren, abhängig von ihrer Größe, sowohl im IT-Servicemanagement als auch im IT-Sicherheitsmanagement höchst unterschiedlich aufgestellt. Cybersicherheitsrisiken, Sicherheitsstrategien oder einschlägige Managementsysteme sind überwiegend nicht angemessen adressiert worden. Eine inhaltliche Zusammenarbeit mit der Landesverwaltung war auf Ebenen von Strafverfolgungsbehörden rudimentär gegeben. Es bestanden im Land Bremen auch keine rechtlichen Anknüpfungspunkte um eine Zusammenarbeit zu gewährleisten. Gleichzeitig ist der Wunsch nach weiterer Regulierung auch nicht artikuliert worden (Rehbohm et al., 2021).

Ein weiterer Aspekt der Anforderungen an die Architektur wurde mittels einer Studie mit den Kommunen erhoben. Hierfür wurde bundesweit eine Onlineumfrage zum Sicherheitsmanagement bzw. Cybersicherheitsmanagement, auch als Träger der Daseinsvorsorge, durchgeführt. Grundsätzlich ließ sich belegen, dass Informationssicherheitsmanagementprozesse unterentwickelt sind. Auch hier sind kleinere Kommunen deutlich schlechter als größere Kommunen aufgestellt. Zudem wird die eigene Dienstleistung überwiegend nicht als kritische Dienstleistung der Daseinsvorsorge verstanden. Gleichwohl wird aber Verantwortung für kommunale Dienste außerhalb der Verwaltung wahrgenommen. Ob und wie eine Kommune mit seinen Wirtschaftsunternehmen oder dem Land kooperiert, ist im Benehmen der Kommune (Kommunale Selbstverwaltung) (Rehbohm et al., 2022).

Neben den Studien bei den relevanten Akteuren, wurde initial eine Studie zu Grundforderungen von Informations- und Cybersicherheit in Ländern erstellt. Ergebnis dieser Arbeit ist, wer elementar wichtige Dienstleistungen oder Waren für große Teile der Bevölkerung anbietet, ist Teil der Daseinsvorsorge. Solche Akteure müssen identifiziert werden und sollen nötigenfalls gesetzlich oder auf dem Verordnungswesen in die Pflicht genommen werden. Ermächtigungen zur Kontrolle und zum Ergreifen von Maßnahmen ggf. Sanktionen sind im Ermessen des jeweiligen Gesetzgebers im Land. Cybersicherheit kann als Teil des Ordnungsrechts im jeweiligen Land ausgebaut werden (Rehbohm & Kalmbach, 2021). Eine zweite Studie befasste sich mit der von der Bundesinnenministerin postulierten Absicht einer Grundgesetzänderung, welche die Gesamtzuständigkeit für die Cybersicherheit beim Bund verorten will. Im Beitrag Herausforderungen der föderalen Cybersicherheit vs. Änderung in der Bund-Länder Gewaltenteilung wird herausgearbeitet, welche Gefahren und Möglichkeiten mit einer Zentralisierung der Verantwortung einhergehen. Grundsätzlich können durch die Mandatserhöhung beim Bund

auch Chancen für die Länder und somit für die gesamte Resilienz entstehen, gleichzeitig sind jedoch die Folgen einer Zentralisierung nicht abschließend aufgearbeitet worden (Rehbohm & Kalmbach, 2023).

Die hier vorgestellte föderale Cybersicherheitsarchitektur ist das Ergebnis mehrerer empirischer Studien, der Erarbeitung von Anforderungen an eine Architektur und die nachstehend abgeleiteten Ziele. Zusammenfassend und auf einem hohen Abstraktionsniveau gesehen, sind dies die Ziele Rechtssicherheit, Anwendbarkeit, Resilienz, Nachhaltigkeit und Kooperation. Die Cybersicherheitsarchitektur soll strukturelle Rahmenbedingungen, technische Interaktionen und Rechtssicherheit schaffen, die eine gleichberechtigte Teilhabe aller Akteure ermöglicht.

12.4.2 Architektur

Die erstellte Architektur soll ein funktionsfähiges Bindeglied zwischen den Ländern, dem Bund und den Verwaltungen, insbesondere Ministerialverwaltungen sowie den Kommunen präsentieren (Rehbohm & Sandkuhl, 2023). Für die Wirtschaft kommen derzeit verschiedene Mechanismen zur Identifizierung und zur Einbindung in die Prozesse zur Anwendung. Insbesondere werden kritische Infrastrukturen derzeit nach Definition des Bundes (Kritis), nach der europäischen Richtlinie zur Netz und Informationssicherheit (NIS-2-Richtlinie) (EUR-Lex - 32022L2555 - EN - EUR-Lex, 2022) sowie die Wirtschaftsunternehmen der Daseinsvorsorge der Region (Kritis unterhalb von Schwellenwerten) adressiert. Kritische und subkritische Infrastrukturen werden in der vorliegenden Studie als systemrelevante Infrastrukturen der Daseinsvorsorge im Land definiert. Das angewendete Unternehmensarchitekturmanagement verwendet unterschiedliche Sichten und Perspektiven für die Dokumentation, Planung und Visualisierung zentraler Bestandteile eines Unternehmens bzw. einer Organisation wie der Landesverwaltung (D. Simon et al., 2013). Die Geschäftsarchitektur soll die zentralen Ziele der Unternehmensstrategie bedienen, die Geschäftsprozesse visualisieren, die erforderlichen Organisationsstrukturen aufzeigen und IT-Governance Strukturen des Unternehmens abbilden. Die vorgeschlagene föderale Cybersicherheitsarchitektur beinhaltet fünf Kernprozesse, zwei Supportprozesse und den Prozess zur übergeordneten Strategie der Gesamtarchitektur.

Strategie und Motivation ist der übergeordnete Prozess, der zum einem die Erwartungshaltung der Stakeholder visualisiert und zum anderen strategische Ziele eines übergreifenden Cybersicherheitsmanagements in einem Land beinhaltet. Intrinsische Motive wie zum Beispiel Wirtschaftlichkeit, Nachhaltigkeit oder Widerstandsfähigkeit sowie die extrinsischen Motive im Kontext von eigenen IT-Infrastrukturen und die Fähigkeiten diese zu betreiben oder betreiben zu lassen, sind adressiert. Elementare Fähigkeiten sind in diesem Zusammenhang mit IT-Servicemanagement, IT-Sicherheitsmanagement und Threat-Intelligence-Management verbunden.

Zwei Supportprozesse unterstützen die eigentlichen fünf Kernprozesse. Zur Erreichung des Ziels Rechtssicherheit ist der Prozess zur *Regulation/Legislation/Obligation* angelegt. Hierunter ist ein wesentlicher Unterstützungsprozess zu verstehen, der die Verpflichtung der Föderalstaaten umfasst, entlang der europäischen und deutschen regulatorischen Anforderungen, eigene Gesetzgebungen und Verordnungen zu entwickeln und an den dynamischen Herausforderungen anzupassen. Ein klassischer Compliance Prozess, der um die Möglichkeit der eigenen Gesetzgebungskompetenz erweitert ist. Der zweite Unterstützungsprozess *Human Resources/Communication/Cooperation* umfasst die Entwicklung eines regionalen Netzwerkes von eigenen und im Auftrag tätigen Beschäftigten der betroffenen Organisationen sowie Dienstleistern oder Partnern. Dies können insbesondere Unternehmen, andere Länder, der Bund und auch jede andere Organisation in Europa oder in der Welt sein, um die eigenen Fähigkeiten partnerschaftlich zu entwickeln.

Die fünf Kernprozesse werden bestimmt von *Identification/Compliance*, um initial und fortwährend die Bestimmung wesentlicher und wichtiger Organisationen der Region, in Wirtschaft und Verwaltung sowie entlang der rechtlichen Anforderungen zu identifizieren. Dabei ist die Registrierung und Bekanntmachung der betroffenen Daseinsvorsorgeträger in Bund und Länder gleichermaßen und synchron sicherzustellen, um eindeutige Zuständigkeiten zu definieren. Der nächste Kernprozess bezieht sich auf *Risk/Performance* und betrifft den Aufbau und die Überwachung der Veränderung der Bedrohungslage auf die föderalen Infrastrukturen, seinen Akteuren und den damit einhergehenden Risiken für diese. Fähigkeiten der betroffenen Organisationen, wie Informationssicherheitsmanagement, liefern regelmäßig Kennzahlen, welche in einem ganzheitlichen Monitoring des Risikos der Region weiterverwendet werden sollen. Die im Prozess *Operation* beschriebenen Funktionalitäten existieren teilweise als Softwarelösung oder Anwendung und müssen zwischen den Akteuren etabliert werden. Insbesondere handelt es sich um den technischen Echtzeit-Austausch über aktuelle Angriffsvektoren, die Lagebilderhebung oder die Koordinierung von Unterstützungskräften in der Region. Der Kernprozess *Super Authority/Sanctioning* betrifft die jeweilige Landesverwaltung und die Pflicht zur Institutionalisierung in einer behördlichen Struktur. Die Prozesse zur Steuerung der Cybersicherheit beinhalten insbesondere Mandate zur Einsichtnahme und Kontrolle von Akteuren, um die Einhaltung der Ziele und die Konformität sicherzustellen. Auch ist das Auslösen von Sanktionsmechanismen und Maßnahmen zur Aufrechterhaltung bzw. Verbesserung des Gesamtsystems sicherzustellen. Der Kernprozess *Cyber Security Standards* umfasst alle Hilfsmittel, Maßnahmen und Vorgehen, die den Betrieb und die Resilienz der Cybersicherheitsarchitektur fördern, insbesondere aus dem Bereich der Informationssicherheit. Beinhaltet ist auch die Mitwirkung der jeweiligen Länder bei der Entwicklung- und fortlaufenden Prüfung der Anwendbarkeit von Sicherheitsstandards auf die Akteure der Region.

12.4.3 Evaluierungsstrategie und Grundsätze ordnungsgemäßer Modellierung

Die Cybersicherheitsarchitektur ist entlang des Designs Science Research (DSR) entstanden. Das DSR Vorgehensmodell zielt darauf ab, anhand eines Sollzustandes ein Artefakt zu entwickeln; dies kann insbesondere eine Methode oder wie in diesem Beitrag eine Architektur sein. Neben der eigentlichen Entwicklung des Design-Artefakts, liegt eine weitere Herausforderung darin, dass der Evaluierungsprozess sichergestellt, dass Anhaltspunkte für die Verbesserung und Weiterentwicklung – die dem Anspruch an der Forschung genügen – generiert werden.

Als Evaluationskriterien werden in dieser Arbeit die Grundsätze ordnungsmäßiger Modellierung (GoM) herangezogen und überprüft (J. Becker et al., 2012, S. 32), da es sich bei der CSA um ein Modell handelt. Es wird ein Interviewleitfaden entwickelt, dessen Fragestellungen inhaltlich auf diese Grundsätze ausgerichtet sind. Dabei handelt es sich um folgende Inhalte:

- Grundsatz der Richtigkeit wird erfüllt, wenn eine inhaltliche und widerspruchsfreie Syntax verwendet wird sowie die beschriebenen Rollen und Namenskonventionen anerkannt werden und konsistent sind.
- Grundsatz der Relevanz wird erfüllt, wenn die definierten Ziele mit der Architektur und den Anforderungen der Stakeholder im Einklang stehen.
- Grundsatz der Wirtschaftlichkeit wird erfüllt, wenn die mit der Umsetzung der Architektur stehenden Aufgaben in einem definierten Zeitraum leistbar sind. Dabei stellt die Architektur einen Kompromiss dar, der abhängig von den Ländern unterschiedlich mit Ressourcen unterstützt wird um folglich detaillierte Ziele umzusetzen.
- Grundsatz der Klarheit wird erreicht, wenn das entwickelte Artefakt für die Akteure und Stakeholder als eindeutige und anschauliche Interpretation verstanden wird.
- Grundsatz der Vergleichbarkeit wird erreicht, wenn die Vorgehensweise zur Entwicklung des Artefakts mit anderen Entwicklungen, zum Beispiel im Umfeld von EAM mit ArchiMate, nachvollzogen werden kann.
- Grundsatz des systematischen Aufbaus wird erreicht, wenn der logische Aufbau verifiziert werden kann und widerspruchsfrei ist.

Eine in der Wissenschaft anerkannte Evaluierungsstrategie bietet das Framework for Evaluation in Design Science Research (FEDS), welches in diesem Beitrag angewendet wird (Venable et al., 2016). Mit der FEDS-Evaluationsstrategie soll sichergestellt werden, dass die beinhalteten Fragestellungen im Entstehungsprozess des Artefakts evaluiert werden. Die DSR-Evaluierungsepisoden werden in zwei Dimensionen ausgeprägt. Eine Dimension berücksichtigt den formativen bzw. summativen Zweck- und die zweite Dimension die künstliche oder naturalistische Evaluierung. Schritte im FEDS-Evaluierungsprozess:

1. Erläuterung der Evaluationsziele: Darstellung der Ziele der Evaluation des Artefakts und mögliche Alternativziele. Dabei werden Effizienz (Artificial Evaluation,

das beobachtete Ergebnis wird nicht von Störvariablen beeinflusst) und Effektivität (Summative Evaluation der Wirksamkeit in einem realen Umfeld). Ungewissheiten und Risikominderung, wie z. B. Nutzungsrisiken (die Architektur kommt nicht zum Einsatz) sollten in einer frühen Phase der Evaluationen bewertet werden.

2. Auswahl der Evaluationsstrategie: Je nach Ziel der Evaluierung können mehr als eine Strategie zur Anwendung kommen oder deren Kombination. 1. Bewertung von Designrisiken im Hinblick auf technologische oder menschliche Nutzungsrisiken. 2. Bewertung von Wirtschaftlichkeitsaspekten, wie Ressourcenverfügbarkeit im Verhältnis Umsetzungsmöglichkeiten in Evaluierungsepisoden. 3. Bewertung des Artefakts im Hinblick auf den gegenwärtigen oder zukünftigen Einsatz, als rein technische Lösung, ohne menschliche Nutzung. 4. Bewertung der Komplexität des Artefakts.
3. Bestimmung der zu evaluierenden Eigenschaften: In diesem Schritt müssen die Kriterien, Merkmale und Anforderungen des Artefakts für die Bewertung definiert werden. Dies können insbesondere bestehende Anforderungen aus Frameworks oder Standards sein und werden in jedem Fall individuell auf das Artefakt abgestellt.
4. Gestaltung der einzelnen Evaluationsabschnitte: Festlegung der konkreten Evaluierungsepisoden. 1. Identifikation von Beschränkungen, wie Ressourcen. 2. Priorisierung von wesentlichen, wichtigen, weniger wichtigen, "nice to have" oder irrelevanten Aspekten. 3. Festlegung der Anzahl und Art von Evaluierungsepisoden.

12.4.4 Evaluierungsepisode Länder

Die Länder und der Bund haben zwischenzeitlich im Kontext der NIS-2-Richtlinie (EUR-Lex - 32022L2555 - EN - EUR-Lex, 2022) den Anwendungsbereich der Öffentlichen Verwaltung mittels eines abgestimmten Identifizierungskonzeptes festgelegt. Dabei wurden die ministeriellen Ebenen und ausgewählte Bereiche der Landes- und Bundesverwaltung als von der NIS-2-Richtlinie betroffen definiert. Für diesen Anwendungsbereich sind die Kommunen vorerst nicht betrachtet worden. Eine Involvierung dieser ist mit den jeweiligen Landesgesetzgebungen bzw. untergesetzlichen Regelungen geplant.

Die Evaluierung wurde mit den Ländern Hamburg (HH), Niedersachsen (NI), Nordrhein-Westfalen (NW) und einem weiteren Flächenland (FL) mit ca. 1000 Kommunen durchgeführt. Relevant für die Auswahl waren zum einen, dass Experten bzw. Entscheidungsträger aus Stadtstaaten und Flächenländer zur Verfügung standen und zum anderen deren Verortung in der Landesverwaltungsorganisation Berücksichtigung fanden. Die CISO-Stelle des Landes Niedersachsens ist im Ministerium für Inneres und Sport, beim Stabsreferat *Informations- und Cybersicherheit* verortet. In der Freien und Hansestadt

Hamburg wird im Referat *Infrastruktur und Sicherheit* des Amtes für IT und Digitalisierung (ITD) die Informationssicherheit der Öffentlichen Verwaltung (CISO) wahrgenommen. Dabei ist das ITD eine nachgeordnete Behörde der Senatskanzlei Hamburg. Im Referat *Informationssicherheit in der Landesverwaltung* ist die CISO-Stelle im Ministerium für Heimat, Kommunales, Bau und Digitalisierung des Landes Nordrhein-Westfalen lokalisiert. Zudem konnte ein weiterer Entscheidungsträger aus dem Referat der *Koordinierungsstelle für Cybersicherheit NRW sowie Informationssicherheit* im Ministerium des Innern des Landes (NW) und im Geschäftsbereich gewonnen werden. Die Freie Hansestadt Bremen hat wie NW eine geteilte Zuständigkeit, im Referat *Zentralstelle Cybersicherheit* beim Senator für Inneres und den Bereich Informationssicherheit (CISO, der Autor) beim Senator für Finanzen. Die vorgeschlagene Architektur ist im Land Bremen entstanden und somit Teil der anwendbaren und übertragbaren partiellen Referenzarchitektur, unabhängig von der Verortung bestimmter Rollen der Cyber- und Informationssicherheit.

In Niedersachsen und Hamburg fanden die Experteninterviews am 22. Januar 2024 mit den jeweiligen CISOs statt. In einem weiteren Flächenland fand das Interview mit einem Experten am 12. März 2024 und in Nordrhein-Westfalen mit mehreren Entscheidungsträgern verschiedener Referate am 22. März 2024 statt. Den Experten wurde der Architekturansatz zunächst hinsichtlich der generellen Struktur vorgestellt und danach die wesentlichen Prozesse im Architekturmodell erläutert. Weiterhin wurden entlang des Design Science Process die Iterationsschritte zur Entwicklung des Artefakts diskutiert. Der Vorschlag zu einer formalen Architekturentwicklung wird grundsätzlich als hilfreich und zielführend für die Herausforderungen der Cybersicherheit erachtet. Die verfolgten Ziele sind in Bezug auf die Anforderungen an eine Resilienz-Architektur nachvollziehbar, richtig und vollständig. Der strategische und motivatorische Prozess ist korrekt dargestellt. Die Darstellung der einzelnen Akteure sind korrekt ausgewiesen. Bei den Kernprozessen und den verbundenen Aufgaben besteht grundsätzlich Zustimmung. Die mit den Prozessen verbundenen Fähigkeiten müssen bei allen Akteuren aufgebaut werden. Die mit den Supportprozessen verbundenen Aufgaben sind nachvollziehbar und durch die Länder zu gestalten. Kooperationen auszubauen und die Fachkräftesicherung sind grundsätzlich korrekte Vorgehen. Die mit diesem Modell vorgestellte Vorgehensweise, der erforderliche Aufbau von ergänzenden Infrastrukturen sind im Modell verständlich strukturiert und können implementiert werden. Für die Implementierung der Architektur sind folgende Statements der Interviewpartner zu berücksichtigen:

HH: Hamburg hat mehr kritische Infrastrukturen, als die durch den Bund und durch neuere europäische Gesetzgebung identifizierten Unternehmen. Die Gesamtheit der systemrelevanten Infrastrukturen muss Hamburg bekannt sein oder gemacht werden, sofern die Aufsicht in Teilbereichen beim Bund wahrgenommen wird. Die jeweilige Compliance (hier Bezirksämter und Unternehmen) muss folglich dem Land gegenüber bekannt gemacht werden. Alle Akteure müssen im gemeinsamen Risikomanagement eingebunden werden. Die Institutionalisierung (Authority) ist in Hamburg angedacht. Es

braucht eine eigene Aufsichtsbehörde, welche auch Sanktionsmöglichkeiten gesetzlich vorsehen wird. Aus Sicht Hamburgs muss eine Pflicht zur Unterstützung bei Cybersicherheitsvorfällen etabliert werden, sofern es dem Gemeinwohl dient. Kooperationen und die Vernetzung mit IT-Spezialunternehmen bzw. auch die Branchenvernetzung sind erforderlich. Eine Fachkräftesicherung als Teil der Architektur wird eher skeptisch gesehen, da dies eine Aufgabe des allgemeinen Human Ressources sein sollte. Der Austausch von Informationen (Operations) muss stärker qualifiziert und auf die Bedürfnisse der Akteure ausgerichtet werden. Frühwarnsysteme sollen in Hamburg ergänzend und unter Zuhilfenahme von Partnern entstehen. Der Austausch von Angriffsvektoren soll eine volle Ausbreitung in der Region und bestenfalls über alle Akteure haben. Ein regionales Lagebild wird für absolut realistisch gehalten, etwaig auch für die Metropolregion Hamburg. Die Mitwirkung Hamburgs bei der Entwicklung und Erklärung der Anwendbarkeit von Informationssicherheitsstandards auf Akteure der Region soll vom Land beeinflussbar sein. Mögliche Zertifizierungen sollen nach Maßgabe des Landes erfolgen. Die politische Willensbildung und Ausrichtung muss erfolgen.

NI: Niedersachsen hat eine große Anzahl systemrelevanter Infrastrukturen. Im niedersächsischem Gesetz über digitale Verwaltung und Informationssicherheit (NDIG) (Niedersächsisches Vorschrifteninformationssystem (NI-VORIS), 2019) sind im Geltungsbereichs zuvorderst die allgemeine Landesverwaltung (Ministerien, Landesämter, Landesbetriebe) sowie Kommunen adressiert. Dabei sind die Regelungsinhalte für die Landesverwaltung deutlich weitgehender als für übrige Behörden oder Kommunen. Die Kommunen durchgängig zu verpflichten birgt derzeit zu viele Risiken in einem Flächenland. Es besteht derzeit keine politische Einigkeit darüber, welche Regelungen im Land durchsetzbar und finanzierbar sind. Dabei ist unbestritten, dass eine elementare Abhängigkeit von Informationstechnik durchgängig in allen Verwaltungsebenen gegeben ist. Aus Sicht Niedersachsens gehört das Kontinuitätsmanagement zum Cybersicherheitsmanagement, dazu und sollte in *Strategie und Motivation* ergänzt werden. Resiliente Infrastrukturen und Prozesse sind erforderlich.

„Wir werden in der Zukunft erfolgreich angegriffen sein!“

Kritische Infrastrukturen müssen sinnlogisch auf Landesebene identifiziert und ergänzend bei den zuständigen Ressorts bekannt gegeben werden. Schnittmengen sind zu identifizieren und zu konsolidieren. Ein Risikomanagement fürs Land wird übergreifend aufgebaut werden müssen, beinhaltet in den derzeitigen Planungen jedoch nur das Land und die nicht darüberhinausgehenden Bereiche. Lagebilder sollen vorerst für den eingeschränkten Bereich der Landesverwaltung entstehen. Die Versorgungssicherheit wird klar vor Sanktionsmechanismen priorisiert. Das Prinzip von Fordern und Fördern soll Anwendung finden.

FL: Grundsätzlich wird die Herleitung der in der Architektur adressierten Bereiche als korrekte Veranschaulichung der notwendigen Aufgaben in einem Flächenland bestätigt. Der Anwendungsbereich – der Scope der Betrachtung – ist elementar für die Architektur.

Insbesondere stellt die Involvierung der Kommunen eine große Herausforderung dar. Sofern sich die Kommunen in einer eigenen Organisation zusammenfinden würden, könnte man ersatzweise ausschließlich die Spitzenorganisation in der Architektur berücksichtigen. Gleiches gilt für die Erfordernisse für bestimmte Qualifikationen der Akteure. Sollten überdurchschnittlich viele Akteure (ca. 1000 Kommunen) in der Architektur Berücksichtigung finden müssen, erhöhen sich die Anforderungen, zum Beispiel an die Ausgestaltung von Fortbildungen. Im deklaratorischen Teil der Cybersicherheitsarchitektur sollte eine auf das jeweilige Land abgestimmte Definition der CSA erfolgen, insbesondere die Rollen und die Verantwortungsübernahme im Land definieren. Die Involvierung des bzw. Schnittmengen zum Katastrophenschutz und ggf. zur zivilen Alarmplanung könnten in der Architektur berücksichtigt werden. Insbesondere muss im Land identifiziert werden, wo gleiche Akteure in den Ländern zu finden sind, die in unterschiedlichen Rollen des Landes verortet sind. Ob und welche Möglichkeiten im Land bestehen, um auf Informationssicherheitsstandards und deren Zertifizierung Einfluss zu nehmen, wird grundsätzlich befürwortet, insbesondere, weil schon landesspezifische Informationssicherheitskonzepte oder auch branchenspezifische Sicherheitsstandards (B3S) bestehen. Komplementäre Entwicklungen von Sicherheitsstandards sowie Anforderungen – wie z. B. die Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) – des IT-Planungsrates müssen vereinbar sein.

NW: Neben den mir als Experten und gleichfalls Entscheidungsträger zur Verfügung stehenden Interviewpartnern existiert ein dritter zuständiger Bereich für die Cybersicherheit in der Wirtschaft, im Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen. Alle Stellen sind in einer Ministeriumsübergreifenden Arbeitsgruppe organisiert und treffen sich regelmäßig. Die Zusammenarbeit funktioniert hervorragend, auch in geteilter Verantwortung. Es braucht nach Aussagen von NW jedoch Strukturen, die auch ohne persönliche Kontakte funktionieren sollen. Die funktionale Architektur insgesamt kann zur Problemlösung beitragen, ist zudem sehr gut aufgebaut und trägt zum politischen Verständnis bei.

Aufgrund der NIS-2-Richtlinie geht NW davon aus, das nicht zwangsläufig ein eigenes Identifizierungssystem für systemrelevante Infrastrukturen erarbeitet werden muss. Derzeit hat NW jedoch keine Infos über die gemeldeten Betreiber nach dieser Richtlinie. Vielmehr müssen sie sich bei einer BSI-Länderstelle melden, um die Betroffenheit im eigenen oder in einem anderen Land aufzuklären. Insofern plädiert NW für die vollständige Bekanntmachung der Unternehmen im jeweiligen Land. Auch würde man Angriffsvektoren in dieser Zusammenarbeit mit diesen Unternehmen teilen wollen. Bei besonders schützenswerten Daten müssten diese ggf. vorab sanitarisiert werden.

Kompetenzen und Mandate sind im Land geklärt. Dass der Katastrophenschutz, das Krisenmanagement oder auch das Kontinuitätsmanagement in der Architektur aufgenommen werden sollte, wird klar verneint. Katastrophen bzw. Großschadensereignisse sind regelmäßig regional, Cybersicherheitsbedrohungen hingegen mehrheitlich nicht. Das Kontinuitätsmanagement ist Teil des allgemeinen IT-Betriebs, hier werden weitere

Themen als die Cybersicherheit adressiert, insbesondere Strom- oder Personalausfall. Elementarer Teil der Architektur sollte der Datenschutz sein, wenn hier keine konkurrierenden Interessen vorliegen.

Für Kommunen und kommunale Rechenzentren hat das Land einen Kommunalen Warn- und Informationsdienst (KWID) eingeführt, der den Teilprozess WID in *Operation* der vorgeschlagenen Architektur schon erfüllt. Tatsächlich ist es denkbar und auch beabsichtigt, den Informationsdienst für die Kommunen um den Teil *Mobile Incident Response* (MIRT) zu erweitern. Der politische Wille zur Hilfe der Kommunen ist vorhanden. Mit der Gründung der *Agentur Digital Sicher NRW* (Kompetenzzentrum für kleine und mittlere Unternehmen in NRW) stehen schon heute Ansprechpartner für Unternehmen in Fragen der Cybersicherheit und Fortbildung zur Verfügung, der auch in Richtung Kommunen ausgebaut werden kann. Es ist wichtig, dass man Angebote für alle Akteure Region schafft und auf sie (die Akteure) zugeht. Staatliche und nichtstaatliche Stellen müssen in den Prozess *Communiaction & Cooperation* eingebunden werden. Kooperationen sind notwendiger Bestandteil der Architektur, insbesondere auch mit den Hochschulen.

„Die Bedarfe und Bedarfsträger sind nicht zusammengekommen."

Im Idealbild wäre es sicher richtig, die geltenden Standards im Land (BSI-Grundschutz) auf alle Akteure zu übertragen. Hinsichtlich der heterogenen Struktur der Akteure ist es angemessen, dass die anwendbaren Standards in einem Kernprozess der Architektur durch das Land zu begleiten sind.

Das Personalproblem ist in NW eine enorme Herausforderung, die Altersstruktur ist sehr hoch, die offenen Stellen können aus verschiedenen Gründen nicht besetzt werden. Der Vorschlag, *Human Resources* innerhalb der Architektur zu behandeln, wird nach ausführlicher Diskussion begrüßt. Das Land muss mehr in die spezifische Ausbildung investieren um die Bedarfe an Fachkräften selbst zu steuern. In NW werden Nachwuchskräfte nach den Anforderungen der Cybersicherheit ausgebildet. Grundsätzliche Problematiken sind im Besoldungsbereich bzw. den Entgeltordnungen zu finden. Der öffentliche Dienst ist nicht flexibel genug, Fachpersonal mit ihren Fähigkeiten zu gewinnen und zu binden, ohne eine Formalqualifikation nachzuweisen. Daher sollte es ein Architekturthema sein. Tatsächlich sind die öffentlichen IT-Dienstleister flexibler und stehen somit in unmittelbarer Konkurrenz zu den Ministerien. Zudem ist es wichtig, dass die Aufgaben interessant bleiben und durch die Führung nachhaltig unterstützt werden. Das Landes-CERT hat entsprechend dieser Anforderungen ein Förderprogramm zum Bachelor/Master mit finanziellen und zeitlichen Ressourcen unterstützt. Grundsätzlich ist jedoch die administrative Wirklichkeit in Ministerien für Juristen deutlich besser als zum Beispiel für Ingenieure, Informatiker oder perspektivisch auch Psychologen im öffentlichen Dienst für Angelegenheiten der Cybersicherheit.

„Sachliche und fachliche Erwägungen dürfen nicht zum Ausbremsen der High Potentials führen."

Eine gesetzliche Regelung ist in NW mit einem weitrechenden Charakter geplant, zum Beispiel als NIS-2-Umsetzungsgetz. Der Supportprozess zur Regulation wird folglich begrüßt und ist anhaltend an den sicher verändernden Herausforderungen fortzuentwickeln.

CSA	HH	NI	FL	NW
Strategy & Motivation	Politische Willensbildung ist noch nicht erfolgt, aber zwingend notwendig.	1. Politische Uneinigkeit über die darstellbaren Leistungen des Landes (Ressourcenproblematik). 2. Die Involvierung des Kontinuitätsmanagements erscheint zielführend.	1. Es besteht keine politische Einigkeit darüber, welchen Anwendungsbereich eine CSA haben sollte (Ressourcenproblemantik). 2. Die Involvierung des Katastrophenschutzes erscheint zielführend.	1. Es besteht der politische Willen, sich dem Thema Cybersicherheit ganzheitlich zu widmen. 2. Katastrophenschutz und Kontinuitätsmanagement gehören nicht in die Architektur. 3. Die Involvierung des Datenschutzes sollte geprüft werden.
Identification & Compliance	Zustimmung und Meldung aller Akteure (hier Unternehmen) an das Land.	1. Zustimmung und ergänzende Identifizierung von Unternehmen durchs Land sowie Bekanntgabe in den zuständigen Ressorts. 2. Kommunen zu binden stellt ein zu hohes Risiko dar.	1. Zustimmung mit der Präferenz, einen Spitzenverband der Kommunen einzubinden, um die Anzahl der Akteure überschaubar zu halten. 2. Ergänzende Identifizierung von Unternehmen.	1. Zustimmung mit dem Hinweis, ggf. Sollten alle Unternehmen Deutschlands und deren Verortung in jedem Land bekannt gemacht werden.
Risk & Performance	Zustimmung mit übergreifendem Risikomanagement für die Gemeinwohlträger.	Grundsätzliche Zustimmung mit der Einschränkung, dass derzeit nur die Landes-Akteure einbezogen werden soll.	Zustimmung zum übergreifenden Risikomanagement.	Zustimmung, ein übergreifendes Risikomanagement ist Teil NWs, in Bezug auf die geltenden Standards des BSI.
Authority & CSIRT	Zustimmung, Planung sind in dieser Hinsicht fortgeschritten.	Zustimmung zur Einrichtung einer Zentralstelle, mit eingeschränktem Anwenderkreis.	Zustimmung zur Einrichtung einer koordinierenden Stelle im Land.	Grundsätzliche Zustimmung, die Realität ist geteilte Verantwortung.

CSA	HH	NI	FL	NW
Exchange &Advisory WIS	Der Austausch von qualifizierten Informationen wird bestätigt.	Der Austausch von qualifizierten Informationen wird bestätigt.	Der Austausch von qualifizierten Informationen wird bestätigt.	Der Austausch von qualifizierten Informationen ist Realität geworden.
Exchange & Advisory MISP	Der Austausch von Angriffsvektoren ist zielführend.	Der Austausch von Angriffsvektoren ist zielführend.	Der Austausch von Angriffsvektoren ist zielführend.	Der Austausch von Angriffsvektoren soll entstehen, über alle Akteuren hinweg, mit Sanitarisierung.
Mobile Incident Response	Die Unterstützung für Gemeinwohlträger sollte vom Land initiiert und koordiniert werden.	Grundsätzliche Zustimmung.	Grundsätzliche Zustimmung, sofern die Anzahl der mitwirkenden Akteure über reduziert werden kann.	Grundsätzliche Zustimmung, der Ausbau von personellen Ressourcen ist erforderlich.
Situation Report	Zustimmung und Ergänzung um den Aufbau eines Frühwarnsystems fürs Land, besser noch für die Metropolregion.	Lagebilder sollten vorerst auf die Landesregierung beschränkt bleiben.	Grundsätzliche Zustimmung.	Lagebilder sollen Teil der Architektur sein.
Standards & Certification	Einflussnahme und Zustimmung des Landes ist gewünscht.	Grundsätzliche Zustimmung.	Zustimmung, sofern die entstehenden Standards mit denen des BSI kompatibel sind.	Zustimmung, sofern die Gesamtheit aller Akteure werden sollen.
Regulation	Erforderliche und anhaltende Aufgabe, angesichts der sich anhaltend veränderten europäischen Regulation.	Grundsätzliche Zustimmung, bestehendes Gesetz muss ausgestaltet werden.	Derzeit kein erkennbarer politischer Wille zur Gesetzgebung. Vertragsverletzungsverfahren drohen erst 2027, da Nachweispflichten z. B. für NIS-2-Richtlinie erst dann erforderlich sind..	Erforderliche und fortzuschreibende Aufgabe, die in der Architektur abgebildet sein sollte.
Human Resources	Kann ggf. ausgegliedert werden.	Sollte ausgegliedert werden.	Sollte ausgegliedert werden.	Sollte Teil der Architektur sein, da spezielle Fähigkeiten gesucht sind. Fachkräftesicherung und Ausbildung muss enthalten sein.

CSA	HH	NI	FL	NW
Cooperation & Communication	Zustimmung, da die erforderlichen Kapazitäten nicht im Land vorhanden sind.	Grundsätzliche Zustimmung, für die Landesregierung können ergänzende Partner gewonnen werden.	Zustimmung, da Ressourcen nicht vom Land allein gestellt werden können.	Zustimmung, Kooperationspartnerschaften und offenen Kommunikation mit den Akteuren ist erforderlich.

Tabelle 8 Ergebniszusammenfassung

12.5 Schlussbetrachtung

Die Entwicklung einer föderalen Cybersicherheitsarchitektur ist mit der Evaluationsepisode in den Ländern weiter fortgeschritten. Das Ergebnis der mehrjährigen Forschungsarbeit soll in einer finalen Publikation münden und erfüllt dabei den DSR Prozessschritt Communication. Die in diesem Beitrag behandelte Evaluierungsepisode in den Ländern soll dazu beitragen, das Referenz-Architekturmodell weiter zu verbessern und eine Resilienz-Architektur im föderalen Kontext zu etablieren.

Unter Berücksichtigung der Dynamik von Bedrohungslagen für die Informations- und Kommunikationstechnik-Infrastrukturen und der aktuellen sicherheitspolitischen Lage, muss die vorgeschlagene partielle Referenzarchitektur hinreichend an neue Anforderungen anpassbar bleiben. Beispielsweise kann die Architektur um kooperative KI-Systeme erweitert werden, um Desinformationen und Fake-News entgegenzuwirken. Gleichzeitig verändert sich der regulatorische Rahmen zunehmend, durch europäische und deutsche Gesetzgebungen. In den Interviews wurde deutlich, dass die Länder keine harmonischen rechtlichen Umsetzungen im föderalen Kontext anstreben. Vielmehr wurde deutlich, dass grundsätzlich eine politische Willensbildung in den Ländern zuvorderst angestrebt werden muss, jedoch isoliert für das jeweilige Land. Unbestritten ist das Erfordernis der Steuerungen von Ressourcen und die Fachkräftesicherung, ohne dies in der Architektur exponiert zu betrachten.

In der durchgeführten Evaluationsepisode wurde die Cybersicherheitsarchitektur von den Befragten als grundsätzlich belastbar bewertet. Gleichzeitig zeichnet sich ab, dass die Architektur hinsichtlich der Involvierung des Datenschutzes ggf. des Kontinuitätsmanagements und des Katastrophenschutzes weiterentwickelt werden könnte.

Anhang:

A.1 Deklaration der Forschungsbeiträge

Nr.	Titel	Herausgeber	Akzeptanz
#1	*On Challenges of Cyber and Information Security Management in Federal Structures - The Example of German Public Administration.* (Rehbohm et al., 2019)	Rehbohm, T., Sandkuhl, K., Kemmerich, T., (2019). On Challenges of Cyber and Information Security Management in Federal Structures - The Example of German Public Administration, in: Matulevicius, R., Buchmann, R., Repa, V., Kirikova, M., Sandkuhl, K., Pankowska, M. (Eds.), Joint Proceedings of the BIR 2019 Workshops and Doctoral Consortium Co-Located with 18th International Conference on Perspectives in Business Informatics Research (BIR 2019), Katowice, Poland, September 23-25, 2019, CEUR Workshop Proceedings. CEUR-WS.org, pp. 1–13.	Akzeptanzrate: 41%
Deklaration: Dieser Beitrag wurde von mir als Hauptautor konzipiert und geleitet, insbesondere habe ich die Struktur des Artikels entworfen und zusammengestellt. Die Arbeit basiert auf einer Interviewstudie, die ich durchgeführt und ausgewertet habe. Die im Zusammenhang stehende Literaturanalyse wurde von mir begleitend durchgeführt. Den Empfehlungen der beiden Co-Autoren bin ich gefolgt, weiterhin wurde der Beitrag auf dem BIR-Workshop von einem der Co-Autoren präsentiert.			
#2	*Integrated Security Management of Public and Private Sector for Critical Infrastructures – Problem Investigation.* (Rehbohm et al., 2021)	Rehbohm, T., Sandkuhl, K., Cap, C. H., Kemmerich, T., (2021). Integrated Security Management of Public and Private Sector for Critical Infrastructures – Problem Investigation, in: Abramowicz, W., Auer, S., Stróżyna, M. (Eds.), Business Information Systems Workshops, Lecture Notes in Business Information Processing. Springer International Publishing, Cham, pp. 291–303. https://doi.org/10.1007/978-3-031-04216-4_26	Akzeptanzrate: 35%
Deklaration: Dieser Artikel beruht auf einer vom Hauptautor durchgeführten Interviewstudie. Die Vorgehensweise, Struktur der Veröffentlichung und Durchführung der Vorort-Termine wurden vom Autor vorgenommen. Die Hinweise der Co-Autoren zur Verbesserung des Beitrags wurden umfassend angenommen und erhöhten die wissenschaftliche Qualität. Die erforderliche Literaturrecherche wurde vom mir durchgeführt. Der Vortrag im BITA-Workshop erfolgte als Video-Aufzeichnung im Vorfeld und zusätzlich online für eine Diskussion in der Forschungsgemeinschaft.			

#3	*Sicherheitsmanagement, Cybersicherheit und Daseinsvorsorge: Empirische Studie in deutschen Kommunen.* (Rehbohm et al., 2022)	Rehbohm, T., Kemmerich, R., Cap, C.H., Sandkuhl, K., (2022). Sicherheitsmanagement, Cybersicherheit und Daseinsvorsorge: Empirische Studie in deutschen Kommunen. Datenschutz und Datensicherheit 46, 448–454. https://doi.org/10.1007/s11623-022-1637-0	Akzeptanzrate: ca. 35%
Deklaration: Die Veröffentlichung beruht auf einer empirischen, fragengeleiteten und bundesweiten Umfrage in deutschen Kommunen, welche vom Hauptautor konzipiert wurde. Die technische Umsetzung der Online-Befragung wurde auf einer Plattform der Universität Rostock durchgeführt. Die Auswertung der statistischen Ergebnisse in Kapitel 4.4 fand durch den Co-Autor (Robin Kemmerich) statt. Die Hinweise und Vorschläge der weiteren Co-Autoren wurden umgesetzt. Alle Aspekte dieser Arbeit von der Ideenfindung, der Literaturrecherche, über die inhaltliche Gestaltung bis hin zur finalen Umsetzung, wurden vom Hauptautor geleitet.			
#4	*IT-Sicherheitsrecht der (Bundes) Länder.* (Barudi et al., 2023)	Barudi, M., Kapitel 15.3, Rehbohm, T., Kalmbach, P., (2023). Cybersecurity, 2. Auflage. ed. C.H. Beck, München.	Nicht verfügbar
Deklaration: Für diese Veröffentlichung habe ich als Hauptautor die Konzeption, entlang der Anforderungen des Buches, definiert und die inhaltliche Ausgestaltung vorgenommen. Die Datenerhebung wurde gemeinsam mit dem Co-Autor vorgenommen. Beide Autoren haben die Literaturrecherche und die gesetzlichen Grundlagen geprüft. Die Korrektheit der rechtlichen Aussagen wurde über den Co-Autor sichergestellt, die vollständige inhaltliche Verantwortung lag beim Hauptautor. Hinweise des Herausgebers (Kipker, Professors für Sicherheitsrecht) wurden umgesetzt.			
#5	*Grundforderungen von Informations- und Cybersicherheit in Ländern.* (Rehbohm & Kalmbach, 2021)	Rehbohm, T., Kalmbach, P., (2021). MMR-Aktuell 2021, 438461 - beck-online, Grundforderungen von Informations- und Cybersicherheit in Ländern [WWW Document]. Multimedia und Recht (MMR). URL https://beck-online	Nicht verfügbar
Deklaration: Als Hauptautor habe ich alle Teile dieser Veröffentlichung eigenständig konzipiert, entwickelt und inhaltlich bearbeitet. Der Co-Autor hat mit seiner rechtlichen Expertise die Veröffentlichung ergänzt und sichergestellt, dass eine widerspruchsfreie Argumentation hinsichtlich des Rechtsrahmens entsteht. Die Literaturrecherche fand durch beide Autoren statt.			
#6	*Herausforderungen der föderalen Cybersicherheit vs. Änderung in der Bund-Länder Gewaltenteilung.* (Rehbohm & Kalmbach, 2023)	Rehbohm, T., Kalmbach, P.L., (2023). Herausforderungen der föderalen Cybersicherheit vs. Änderung in der Bund-Länder Gewaltenteilung. Datenschutz und Datensicherheit 47, 338–342. https://doi.org/10.1007/s11623-023-1772-2	Akzeptanzrate: ca. 35%

Deklaration: Diese Veröffentlichung entstand als Reaktion auf die geplanten Rechtsänderungen im Bund. Als Hauptautor habe ich diesen Beitrag konzipiert und entworfen. Alle Teile des Artikels wurden von mir hauptsächlich bearbeitet und für die rechtliche Qualitätssicherung vom Co-Autor - insbesondere Kapitel 7.3 Rechtskonstrukt - ergänzt. Die Literaturrecherche fand durch beide Autoren statt. Hinweise des Gast-Herausgebers (Kipker, Professors für Sicherheitsrecht) wurden umgesetzt.			
#7	*CISIS12.* (Moses & Rehbohm, 2022)	Frank Moses, Thomas Rehbohm (2022). CISIS12 – Vorgehensmodell zur Einführung eines Informationssicherheitsmanagementsystems, kes Ausgabe 1/2022, DATAKONTEXT GmbH.	Nicht verfügbar
Deklaration: Der Beitrag basiert auf einem Entwurf eines prototypischen Prozessmodells sowie einer unterstützenden Software. Die Abbildungen dieser Arbeit wurden vom Hauptautor (Moses) erstellt. Die Beiträge des Co-Autors beziehen sich insbesondere auf die Qualitätssicherung des entworfenen Modells zur Einführung eines Informationssicherheitsmanagementsystems. Die relevante Literaturrecherche wurde von beiden Autoren durchgeführt.			
#8	*Föderale Cybersicherheitsarchitektur und Informationssicherheitsmanagement im Kontext der NIS-2-Richtlinie.* (Rehbohm & Moses, 2023b)	Rehbohm, T., Moses, F., (2023). Föderale Cybersicherheitsarchitektur und Informationssicherheitsmanagement im Kontext der NIS-2-Richtlinie. Datenschutz und Datensicherheit 47, 648–655. https://doi.org/10.1007/s11623-023-1837-2	Akzeptanzrate: ca. 35%
Deklaration: Dieser Beitrag entstand in Absprache der Autoren, als gemeinsame Veröffentlichung und wurde zusammen geplant, entwickelt und geschrieben. Der Abschnitte 1 und 2 wurden gemeinsam entworfen, der Abschnitt 3 wurde von mir erarbeitet, die Abschnitte 4 und 5 sind wiederum vom Co-Autor geschrieben und sind von mir qualitätsgesichert worden. Die Zusammenfassung im Abschnitt 6 ist eine gemeinsame Arbeit. Die verwendete Grafiken stammen ausschließlich vom Co-Autor.			
#9	*CISIS12-Modell – In zwölf einfachen Schritten zum ISMS.* (Moses & Rehbohm, 2023a)	Moses, F., Rehbohm, T., (2023). CISIS12 für kleine und mittelständische Organisationen IN ZWÖLF SCHRITTEN ZUM RECHTSKONFORMEN ISMS. kes, CISIS12 14–19.	Nicht verfügbar
Deklaration: Die im Forschungsprozesses entstandenen Möglichkeiten zur Optimierung und Fortentwicklung des ISMS wurden in diesem Beitrag aufgegriffen und in einem gemeinsamen Beitrag der Autoren erarbeitet. Als Co-Autor habe ich sowohl den Artikel als auch das Prozessmodell, die Software geprüft und Verbesserungsvorschläge eingearbeitet. Dieser Beitrag erweitert die ebenfalls von den beiden Autoren erstellte Publikation des Vorjahres insofern und stellt die Fortentwicklung dar.			
#10	*Entwicklung eines modularen ISMS und DSMS.* (Moses & Rehbohm, 2023b)	Moses, F., Rehbohm, T., (2023). Entwicklung eines modularen ISMS und DSMS. Datenschutz und Datensicherheit 47, 721–726.	Akzeptanzrate: ca. 35%

		https://doi.org/10.1007/s11623-023-1850-5	
Deklaration: Der Co-Autor und ich teilten uns die Verantwortung für den Artikel und strukturierten diesen Beitrag gemeinsam. Insbesondere der Teil 5 wurde von mir entwickelt und verfasst. Darüber hinaus sind die einleitenden Teile und die Zusammenfassung gemeinsam entstanden. Die Literaturrecherche wurde von beiden Autoren und insbesondere für die selbstständig verfassten Teile individuell durchgeführt. Alle Ergebnisse wurden durch die Autoren diskutiert und mögliche Anpassungen im Beitrag umgesetzt. Die verwendeten Grafiken wurden vom Co-Autor erstellt.			
#11	*Federal Cybersecurity Architecture and Information Security Management - Adoption and Diffusion of the NIS-2 Requirements.* (Rehbohm & Moses, 2023a)	Rehbohm, T., Moses, F., (2023). Federal Cybersecurity Architecture and Information Security Management - Adoption and Diffusion of the NIS-2 Requirements, Gesellschaft für Informatik in: GI Edition Proceedings Band 341 6. Fachtagung Rechts- Und Verwaltungsinformatik (RVI 2023). Köllen, Bonn, pp. 14–28. https://doi:10.18420/rvi2023-006	Akzeptanzrate: ca. 48%
Deklaration: Dieser Beitrag wurde von den Autoren gemeinsam konzipiert und umgesetzt. Insbesondere die Abschnitte 1-3, 5 und 7 wurden in Zusammenarbeit geschrieben. Der Abschnitt 6 wurde vom Co-Autor und der Abschnitt 4 von mir geschrieben. Die Literaturrecherche wurde grundsätzlich von beiden Autoren durchgeführt und vom Co-Autor in ihrer Gesamtheit durchgeführt. Sämtliche Grafiken stammen vom Co-Autor. Der Beitrag wurde von mir auf der Fachtagung der Forschungsgemeinschaft präsentiert und Anteile hieraus in einer begleitenden Poster-Session bei der Fachtagung vertreten.			
#12	*Referenzarchitektur Cybersicherheit im Föderalsystem Deutschlands.* (Rehbohm & Sandkuhl, 2023)	Rehbohm, T., Sandkuhl, K., (2023). Referenzarchitektur Cybersicherheit im Föderalsystem Deutschlands. HMD Praxis der Wirtschaftsinformatik. https://doi.org/10.1365/s40702-023-01014-7	Akzeptanzrate: ca. 35%
Deklaration: Dieser Beitrag wurde von den Autoren konzipiert und inhaltlich umgesetzt. Alle Kapitel dieser Publikation von mir erstellt und vom Co-Autor hinsichtlich der Konsistenz und Ergänzungsmöglichkeiten geprüft. Die verwendeten Grafiken und Prozessbilder sind durch mich erstellt worden. Die Literaturrecherche und im Zusammenhang stehenden Vorfeldstudien sind durch mich sowie ergänzend vom Co-Autor durchgeführt worden.			
#13	*Cybersicherheitsevaluation einer Referenzarchitektur für Land, Kommune und systemrelevante Infrastruktur.* (Rehbohm & Sandkuhl, 2024)	Rehbohm, T., Sandkuhl, K., (2024). Cybersicherheitsevaluation einer Referenzarchitektur für Land, Kommune und systemrelevante Infrastruktur. GI Sicherheit 2024, Fachtagung des Fachbereichs "Sicherheit - Schutz und Zuverlässigkeit" der Gesellschaft für Informatik e.V. https://doi.org/10.18420/SICHERHEIT2024_001	Akzeptanzrate: ca. 36%

Deklaration: Die Veröffentlichung wurde von mir konzipiert und in allen Teilen des Beitrags durchgeführt sowie geschrieben. Von der Einleitung, über die Literaturrecherche, die Durchführung und Auswertung der Interviews, der Zusammenfassung sowie der finalen Präsentation des Beitrags auf dem Fachkongress, sind alle Teile dem Hauptautor zuzuordnen. Die Publikation entstand unter der Qualität sichernden Zusammenarbeit mit dem Co-Autor. Vorschläge und Verbesserungsmöglichkeiten des Co-Autors wurden vollumfänglich angenommen und umgesetzt.			
#14	Evaluation einer föderalen Referenzarchitektur für Cybersicherheit (Pidun & Auth, 2025)	Thomas Rehbohm, Kurt Sandkuhl (2025). Evaluation einer föderalen Referenzarchitektur für Cybersicherheit, Gesellschaft für Informatik e. V. (GI), Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023), in "Praxishandbuch Verwaltungsinformatik"	Akzeptanzrate: ca. 39%
Deklaration: Dieser Beitrag ist dem Hauptautor in allen Anteilen der Veröffentlichung zuzuordnen. Die Zusammenarbeit mit dem Co-Autor erfolgte zur Qualitätssicherung. Verbesserungsvorschläge und mögliche Anpassungsbedarfe wurden von mir berücksichtigt und fanden Eingang in der Publikation. Die Literaturrecherche ist von beiden Autoren Bestandteil dieser Arbeit.			

Tabelle 9 Akzeptanz der Forschungsbeiträge

A.2 Cybersicherheitsarchitektur

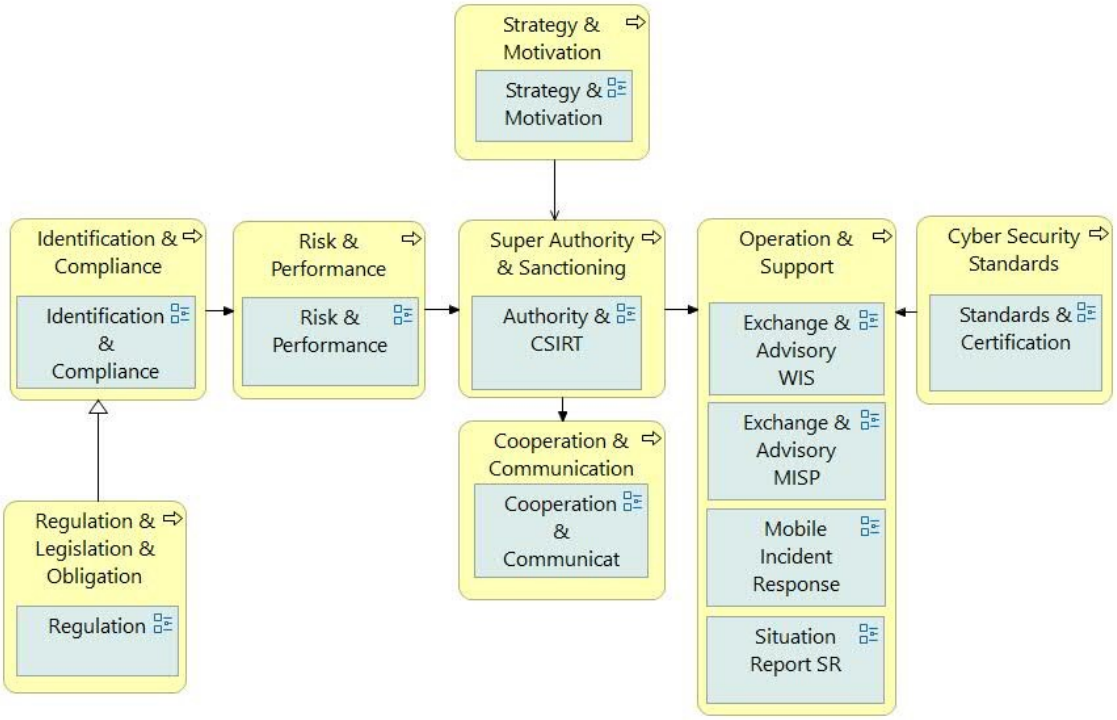

Abbildung 22 Cybersicherheitsarchitektur

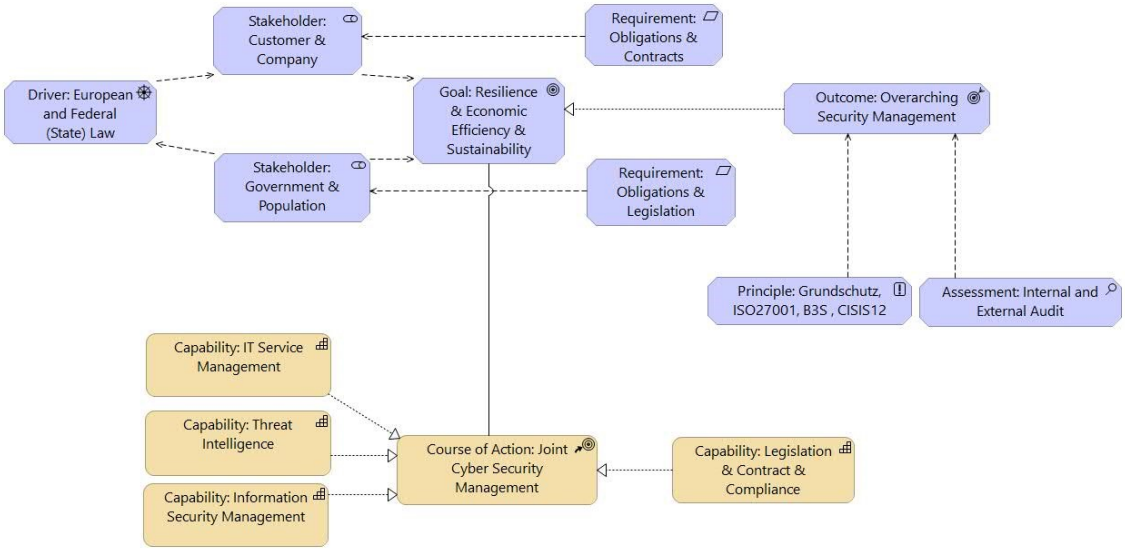

Abbildung 23 Strategy and Motivation

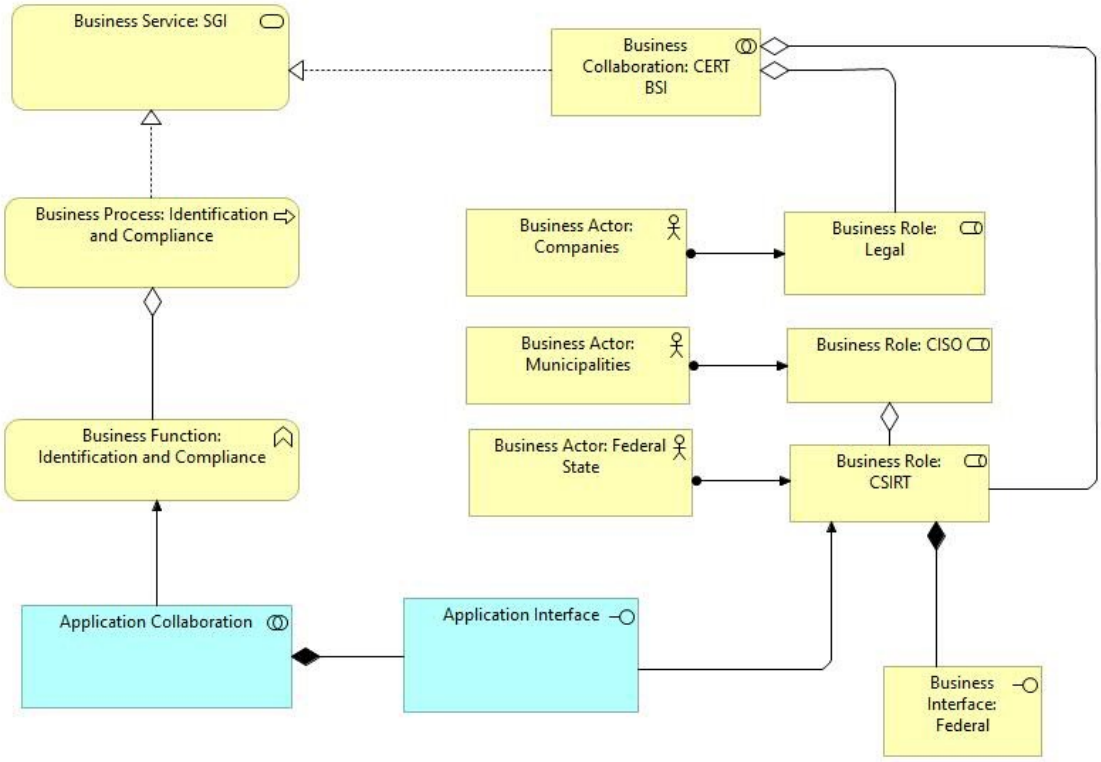

Abbildung 24 Identification and Compliance

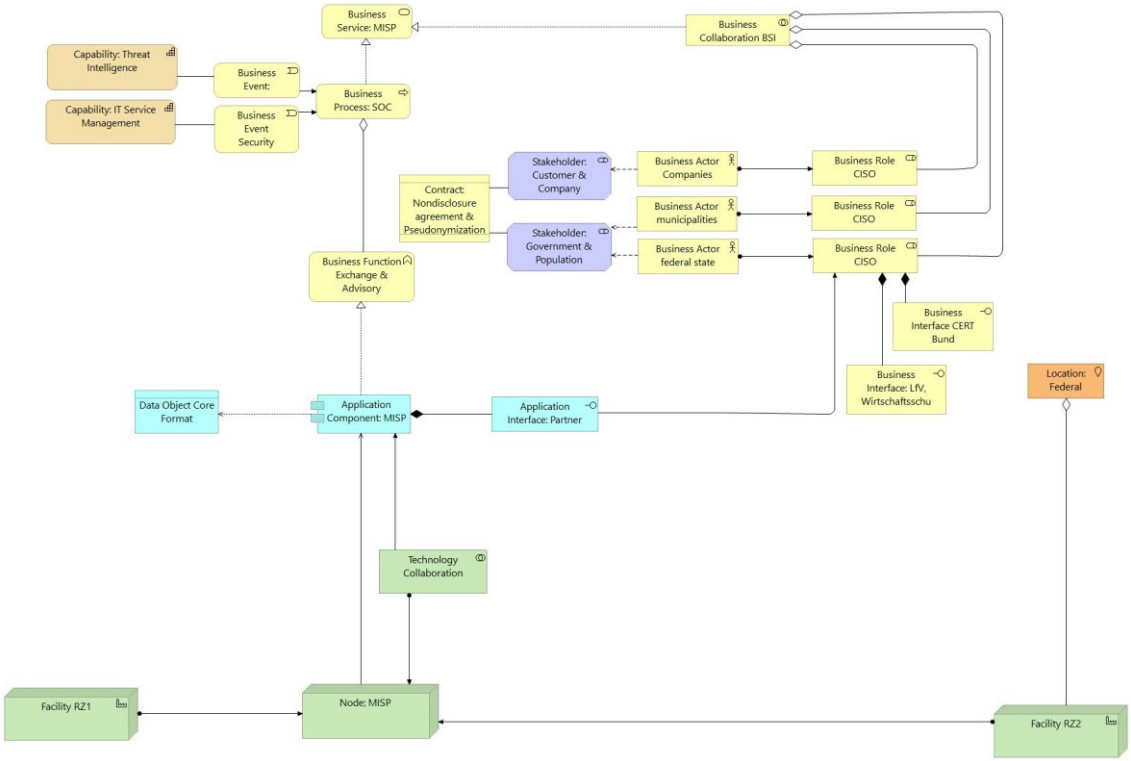

Abbildung 25 Malware Information Sharing Platform

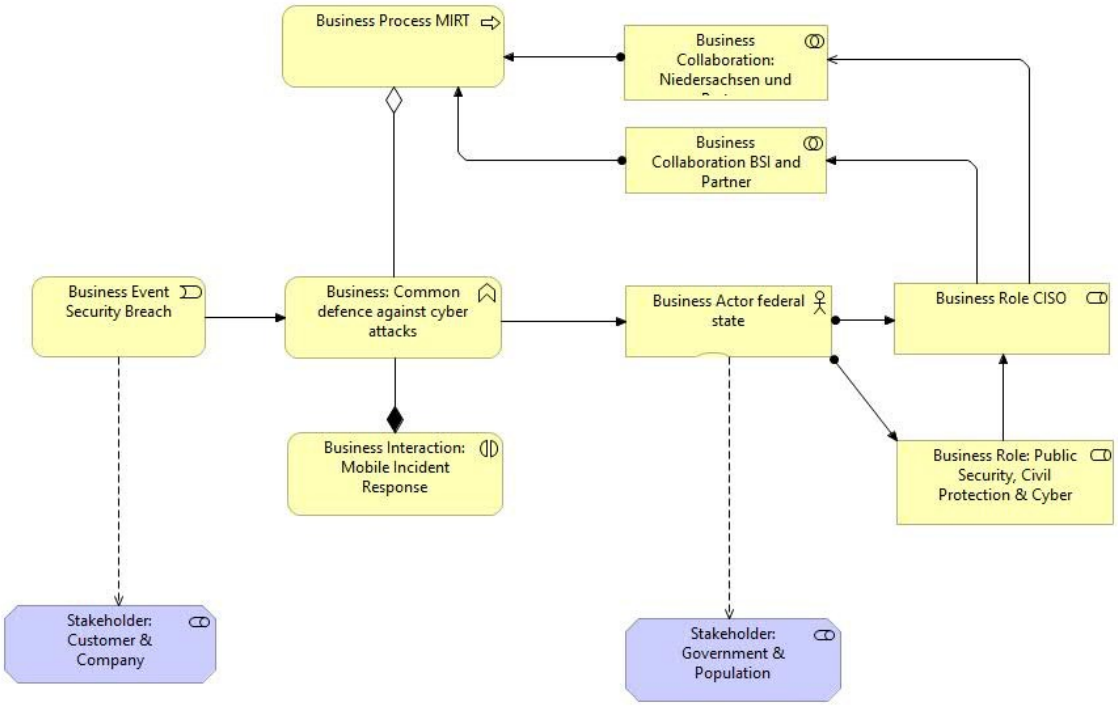

Abbildung 26 Mobile Incident Response Team

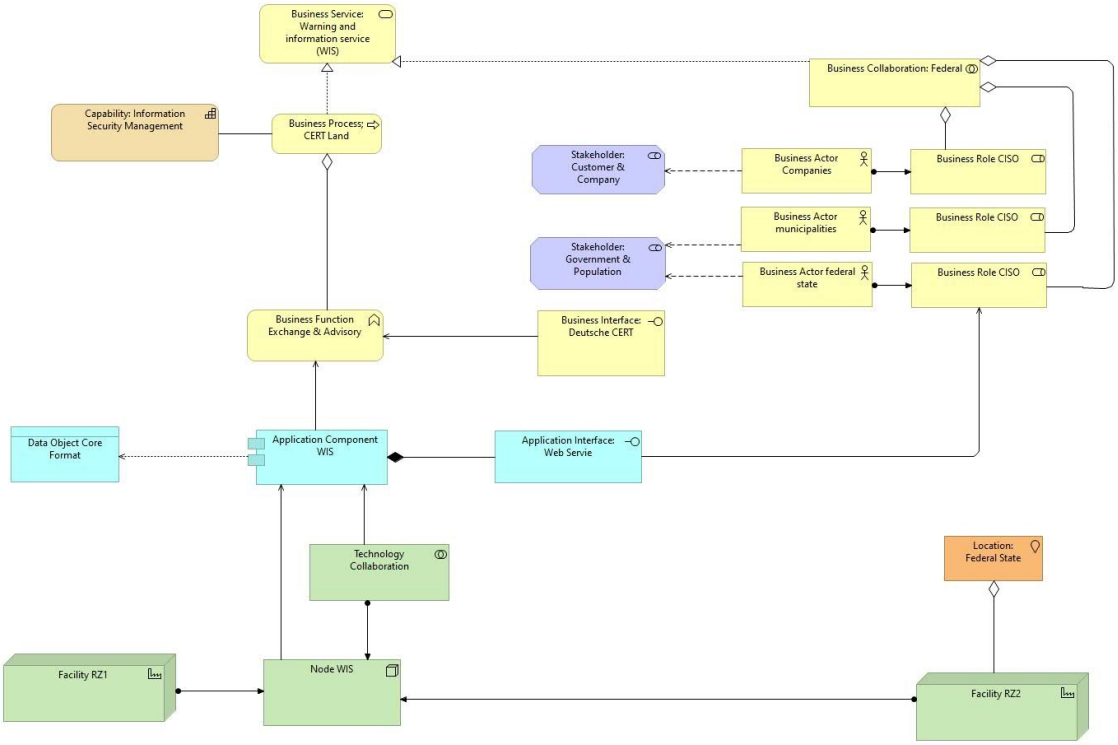

Abbildung 27 Warn and Information Service

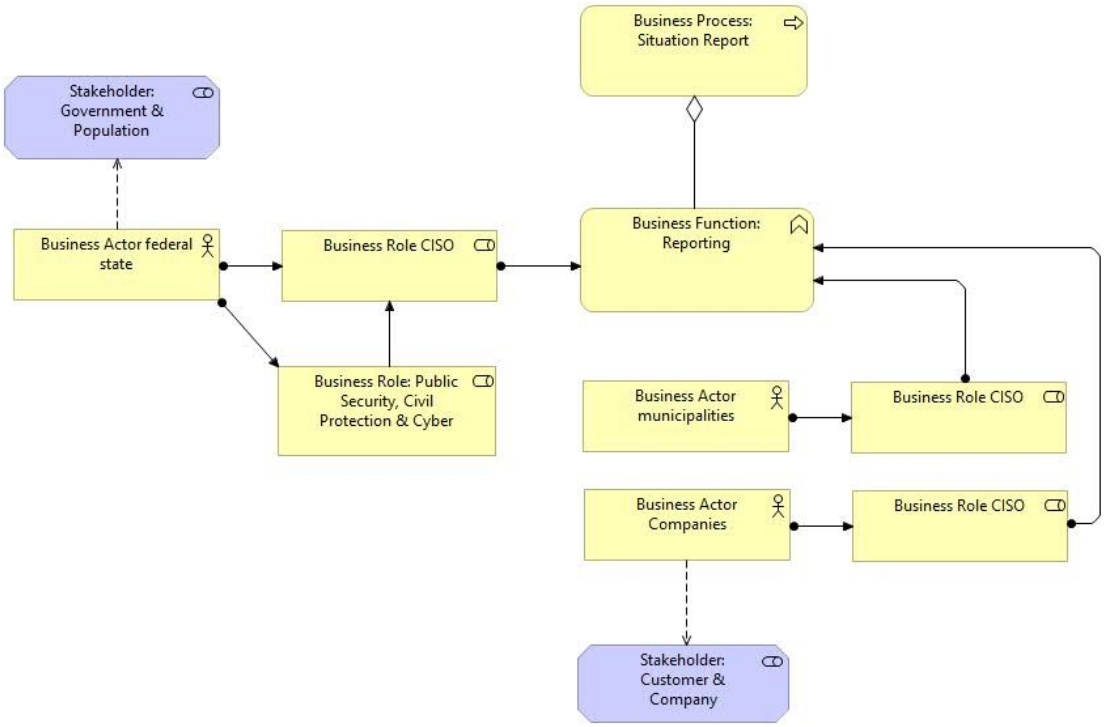

Abbildung 28 Situation Report

Literaturverzeichnis

Ahlemann, F., Stettiner, E., Messerschmidt, M., & Legner, C. (2012). *Strategic Enterprise Architecture Management: Challenges, Best Practices, and Future Developments* (2012. Aufl.). Springer Berlin Heidelberg.

Ali, S., & Green, P. (2007). IT Governance Mechanisms in Public Sector Organisations: An Australian Context. *Journal of Global Information Management (JGIM)*, *15*(4), Article 4. https://doi.org/10.4018/jgim.2007100103

Ambos, K., & Radtke, H. (2017). *Münchener Kommentar zum Strafgesetzbuch. Band 1: §§ 1-37 / Bandredakteur: Professor Dr. Bernd von Heintschel-Heinegg (Vorsitzender Richter am Bayerischen Obersten Landesgericht a.D., Vorsitzender Richter am Oberlandesgericht a.D., Honorarprofessor an der Universität Regensburg, Rechtsanwalt) ; die Bearbeiter des ersten Bandes: Dr. Dr. h.c. Kai Ambos (Professor an der Universität Göttingen, Richter am LG), Dr. Gunnar Duttge (Professor an der Universität Göttingen), Dr. Henning Radtke (Richter am Bundesgerichtshof Karlsruhe, Honorarprofessor an der Universität Hannover) [und 9 weitere]* (B. von Heintschel-Heinegg, Hrsg.; 3. Auflage). C.H. Beck.

Andreasson, K. J. (Hrsg.). (2012). *Cybersecurity: Public sector threats and responses*. CRC Press.

Awan, J. H. (2017). Security strategies to overcome cyber measures, factors and berriers. *Engineering Science and Technology International Research Journal*, *Vol.1, No. 1*.

Axer, P., Isensee, J., & Kirchhof, P. (Hrsg.). (2007). *Handbuch des Staatsrechts der Bundesrepublik Deutschland. Band 4: Aufgaben des Staates / mit Beitr. von Peter Axer* (3., völlig neubearbeitete und erweiterte Auflage). C.F. Müller.

banz. (2009). BGBl I 2009, Nr. 54, S. 2821-2826, Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes. *BGBl I 2009, Nr. 54, S. 2821-2826, Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes*, 2821–2826.

banz. (2015). BGBl I 2015, Nr. 31, S. 1324-1331, Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). *BGBl I 2015, Nr. 31, S. 1324-1331, Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)*, 1324–1331.

Bartsch, M., & Frey, S. (2017). *Cyberstrategien für Unternehmen und Behörden: Maßnahmen zur Erhöhung der Cyberresilienz*. Springer Vieweg. https://doi.org/10.1007/978-3-658-16139-2

Barudi, M., Bird, R., Blunk, R., Beucher, K., Brodowski, D., & Rehbohm, T. (2023). *Cybersecurity* (D.-K. Kipker, Hrsg.; 2. Auflage). C.H. Beck.

Becker, H. (2019). *Handbuch Digitale Verwaltung* (H. Lühr, R. Jabkowski, & S. Smentek, Hrsg.). Kommunal- und Schul-Verlag Wiesbaden.

Becker, H.-J. (1995). Das Gewaltmonopol des Staates und die Sicherheit des Bürgers. *Neue Juristische Wochenschrift*, 2077–2081.

Becker, J., Probandt, W., & Vering, O. (2012). *Grundsätze ordnungsmäßiger Modellierung: Konzeption und Praxisbeispiel für ein effizientes Prozessmanagement*. Springer Gabler.

Benda, E., Maihofer, W., Vogel, H.-J., Hesse, K., & Heyde, W. (Hrsg.). (2012). *Handbuch des Verfassungsrechts der Bundesrepublik Deutschland* (2., neubearbeitete und erweiterte Auflage; Reprint 2012). Walter de Gruyter. https://doi.org/10.1515/9783110890969

Berg, A. (2021). Digitale Teilhabe—Leistungsverwaltung in der Pflicht? *Deutsches Verwaltungsblatt*, 699–705.

Beschluss (EU) 2023/436 des Rates vom 14. Februar 2023 zur Ermächtigung der Mitgliedstaaten, im Interesse der Europäischen Union das Zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität über eine verstärkte Zusammenarbeit und die Weitergabe elektronischen Beweismaterials zu ratifizieren, 063 OJ L (2023). http://data.europa.eu/eli/dec/2023/436/oj/deu

Beyerer, J., Müller-Quade, J., & Reussner, R. (2018). Karlsruher Thesen zur Digitalen Souveränität Europas. *Datenschutz und Datensicherheit - DuD*, *42*(5), Article 5. https://doi.org/10.1007/s11623-018-0940-2

Birkenmaier, P., & Butzer, H. (2018). *GG: Kommentar zum Grundgesetz* (H. Hofmann, H.-G. Henneke, K. von der Decken, B. Schmidt-Bleibtreu, & F. Klein, Hrsg.; 14. Auflage). Heymanns.

Bode, A., Broy, M., Bungartz, H.-J., & Matthes, F. (Hrsg.). (2017). *50 Jahre Universitäts-Informatik in München*. Springer Vieweg.

Boll, A. (2023). Ohne Cybersicherheit kein Datenschutz, ohne Datenschutz keine Cybersicherheit?: Wiederherstellen der Cybersicherheit durch aktive Abwehr von Cyberangriffen. *Datenschutz und Datensicherheit - DuD*, *47*(6), 346–349. https://doi.org/10.1007/s11623-023-1774-0

Borchardt, K.-D. (2020). *Die rechtlichen Grundlagen der Europäischen Union: Eine systematische Darstellung für Studium und Praxis* (7., überarbeitete Auflage). Facultas Verlags- und Buchhandels AG. https://doi.org/10.36198/9783838552781

Bougiakiotis, E. (2020). The layered links model: An alternative approach to international privacy regulation. *International Data Privacy Law*, *10*(3), 253–268. https://doi.org/10.1093/idpl/ipaa002

Bretschneider, W., Rieckmann, J., Stuchtey, T., & Szanto, A. (2020). *Cybersicherheit als Katalysator für Innovation und Wachstum* (Research Report 11–2020; Nummern 11–2020). Studien zum deutschen Innovationssystem. https://www.econstor.eu/handle/10419/222526

Brisch, K., & Rexin, L. (2019). Sicherheit durch Technik: Cyber-Threat-Plattformen in Deutschland: Zur Notwendigkeit einer privaten Initiative zur Stärkung der Cybersicherheit der deutschen Wirtschaft. *Computer Und Recht*, *35*(9), 606–616. https://doi.org/10.9785/cr-2019-350917

Brüsemeister, T. (2008). *Qualitative Forschung: Ein Überblick* (2., überarb. Aufl). VS Verlag für Sozialwissenschaften.

BSI-KritisV Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz, BGBl I 2016, 958 (2016). https://www.juris.de/perma?d=BJNR095800016

Buckl, S., Dierl, T., Matthes, F., & Schweda, C. (2010). *Building Blocks for Enterprise Architecture Management Solutions*. *69*, 17–46. https://doi.org/10.1007/978-3-642-16770-6_2

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. (2021a). *KRITIS - Covid-19: Handlungsempfehlungen für Betreiber Kritischer Infrastrukturen*. https://www.kritis.bund.de/SubSites/Kritis/DE/Aktuelles/Meldungen/210205_Handlungsempfehlungen.html?nn=1902420

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. (2021b, November 20). *KRITIS - Kritische Infrastrukturen Definition und Übersicht*. https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html

Bundesamt für Sicherheit in der Informationstechnik. (2022a). *BSI-Standard 200-4*. Bundesamt für Sicherheit in der Informationstechnik.

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management.html?nn=531576

Bundesamt für Sicherheit in der Informationstechnik. (2022b). *Die Lage der IT-Sicherheit in Deutschland 2022*.

Bundesamt für Sicherheit in der Informationstechnik. (2023). *Die Lage der IT-Sicherheit in Deutschland 2023*.

Bundesministerium der Justiz. (2019). *GGArt91cVtr—Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG (Anlage des Gesetzes zum Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG)*. https://www.gesetze-im-internet.de/ggart91cvtr/BJNR066300010.html

Bundesministerium des Innern, für Bau und Heimat. (2021a). *Cybersicherheitsstrategie für Deutschland*. http://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-artikel.html;jsessionid=A2D24F095A78705EFA547DA2810B70A6.2_cid287?nn=9393618

Bundesministerium des Innern, für Bau und Heimat. (2021b). *Cybersicherheitsstrategie für Deutschland*. http://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-artikel.html;jsessionid=A2D24F095A78705EFA547DA2810B70A6.2_cid287?nn=9393618

Bundesministerium des Innern, für Bau und Heimat. (2021c). *Wegweiser „Einer für Alle/Viele“*. https://www.onlinezugangsgesetz.de/SharedDocs/downloads/Webs/OZG/DE/wegweiser-efa.pdf?__blob=publicationFile&v=4

Bundesministerium des Innern und für Heimat. (2022). *Bundesinnenministerin stellt Cybersicherheitsagenda vor*. Bundesministerium des Innern und für Heimat. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/07/cybersicherheitsagenda.html

Bundesverfassungsgericht. (1982). *Entscheidungen der amtlichen Sammlung—2 BvR 1187/80* (Bd. 61).

Burkett, J. S. (2012). Business Security Architecture: Weaving Information Security into Your Organization’s Enterprise Architecture through SABSA®. *Information Security Journal: A Global Perspective*, *21*(1), Article 1. https://doi.org/10.1080/19393555.2011.629341

Carnap, R. (1998). *Der logische Aufbau der Welt*. Meiner.

CHODAKOWSKA, A., KAŃDUŁA, S., & PRZYBYLSKA, J. (2022). Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done. *Lex Localis - Journal of Local Self-Government*, *Vol. 20, No. 1*.

Choejey, P., Murray, D., & Che Fung, C. (2016). Exploring Critical Success Factors for Cybersecurity in Bhutan’s Government Organizations. *Computer Science & Information Technology (CS & IT)*, 49–61. https://doi.org/10.5121/csit.2016.61505

Daase, C. (Hrsg.). (2013). *Verunsicherte Gesellschaft, überforderter Staat: Zum Wandel der Sicherheitskultur*. Campus Verlag.

Dännart, S., Diefenbach, T., Hofmeier, M., Rieb, A., & Lechner, U. (o. J.). *IT-Sicherheit in Kritischen Infrastrukturen – eine Fallstudien-basierte Analyse von Praxisbeispielen*. 12.

Däubler, W., Wedde, P., Weichert, T., & Sommer, I. (2024). *EU-DSGVO und BDSG: Kompaktkommentar: EU-Datenschutz-Grundverordnung (EU-DSGVO), Bundesdatenschutzgesetz (BDSG), Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)* (3., überarbeitete und aktualisierte Auflage). Bund Verlag.

Daumiller, M. (2018). *Motivation von Wissenschaftlern in Lehre und Forschung*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-21182-0

Degenhart, C. (2007). *Rechtsquellen, Organisation, Finanzen* (J. Isensee & P. Kirchhof, Hrsg.). Müller.

Deutscher Bundestag. (2011). *Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls.* (Drucksache 17/5672; Nummer Drucksache 17/5672). https://dip.bundestag.de/vorgang/.../35375

Deutschland (Hrsg.). (2023). *IT-Grundschutz-Kompendium*. Bundesanzeiger-Verl.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *4*(2), Article 2. https://doi.org/10.4236/jis.2013.42011

Döring, N., & Bortz, J. (with Pöschl-Günther, S.). (2016). *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften* (5. vollständig überarbeitete, aktualisierte und erweiterte Auflage). Springer.

Dürig, M., & Fischer, M. (2018). Cybersicherheit in Kritischen Infrastrukturen: Europäische und deutsche Regulierung — ein Überblick. *Datenschutz und Datensicherheit - DuD*, *42*, 209–213. https://doi.org/10.1007/s11623-018-0909-1

Durning, B., & Jenkins, A. (2005). Teaching/research relations in departments: The perspectives of built environment academics. *Studies in Higher Education*, *30*(4), 407–426. https://doi.org/10.1080/03075070500160046

Eckhardt, P., & Kotovskaia, A. (2023). The EU's cybersecurity framework: The interplay between the Cyber Resilience Act and the NIS 2 Directive. *International Cybersecurity Law Review*, *4*(2), Article 2. https://doi.org/10.1365/s43439-023-00084-z

Ehrenzeller, B., Wallrabenstein, A., Haltern, U., & Et Al. (2014). *Zukunftsgestaltung durch Öffentliches Recht: Referate und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Greifswald vom 2. bis 5. Oktober 2013*. De Gruyter. https://doi.org/10.1515/9783110341386

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (2024).

Ernst, A. (2020, September 17). *Düsseldorfer Uniklinik: Todesfall durch Hacker-Angriff*. Süddeutsche.de. https://www.sueddeutsche.de/panorama/duesseldorf-uniklinikum-erpressung-hacker-angriff-1.5035140

EUR-Lex - 32022L2555 - EN - EUR-Lex (2022). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Europäische Kommission. (2020a). *Proposal for directive on measures for high common level of cybersecurity across the Union | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

Europäische Kommission. (2020b). *The EU's Cybersecurity Strategy for the Digital Decade | Shaping Europe's digital future*. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN

Europäische Kommission. (2021, November 20). *Dienstleistungen von allgemeinem Interesse* [Text]. EU-Kommission - European Commission. https://ec.europa.eu/info/topics/single-market/services-general-interest_de

European Union Agency for Cybersecurity. (2021). *NIS Investments Report 2021* [Report/Study]. https://www.enisa.europa.eu/publications/nis-investments-2021

EUVtr Liss Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft, BGBl II 2008, 1039 (2009). https://www.juris.de/perma?d=BJNR103920008

Fischer, T., Schwarz, O. G., Dreher, E., & Tröndle, H. (2021). *Strafgesetzbuch: Mit Nebengesetzen* (68. Auflage). C.H. Beck.

Fleiner, F. (1920). *Institutionen des Deutschen Verwaltungsrechts* (Fünfte Auflage). J.C.B. Mohr (Paul Siebeck). https://find.ub.uni-rostock.de/id{colon}23425453X

Flick, U. (2011). *Triangulation: Eine Einführung* (3., aktualisierte Aufl). VS, Verl. für Sozialwiss.

Frank, U. (2008). Konstruktionsorientierter Forschungsansatz. In K. Kurbel, J. Becker, N. Gronau, E. Sinz, & L. Suhl (Hrsg.), *Enzyklopädie der Wirtschaftsinformatik: Online-Lexikon*. Oldenbourg. http://www.oldenbourg.de:8080/wi-enzyklopaedie/lexikon/uebergreifendes/Forschung-in-WI/Konstruktionsorientierter-Forschungsansatz

Frank, U. (2009). Die Konstruktion möglicher Welten als Chance und Herausforderung der Wirtschaftsinformatik. In J. Becker, H. Krcmar, & B. Niehaves (Hrsg.), *Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik* (S. 167–180). Physica-Verlag HD. https://doi.org/10.1007/978-3-7908-2336-3_8

German Federal Office for Information Security. (2019). *IT-Grundschutz*. Federal Office for Information Security. https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) (2015). http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf

Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, 1885 (2017). http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s1885.pdf

GG - Grundgesetz für die Bundesrepublik Deutschland (1949). https://www.gesetze-im-internet.de/gg/BJNR000010949.html

Glissmann, S. M., & Sanz, J. (2011). An Approach to Building Effective Enterprise Architectures. *2011 44th Hawaii International Conference on System Sciences*, 1–10. https://doi.org/10.1109/HICSS.2011.48

Group, T. O. (2017). *ArchiMate® 3.0.1 Specification*. Van Haren Publishing.

Gusy, C., Kugelmann, D., & Würtenberger, T. (Hrsg.). (2017). *Rechtshandbuch Zivile Sicherheit*. Springer.

Hackenjos, T., Mechler, J., & Rill, J. (2018). IT-Sicherheit—Ein rechtsfreier Raum? *Datenschutz und Datensicherheit - DuD*, *42*, 286–290. https://doi.org/10.1007/s11623-018-0942-0

Hanschke, I. (2020). *Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten: Eine kompakte Einführung in die Praxis* (2., korrigierte Auflage). Springer Vieweg.

Harknett, R. J., & Stever, J. A. (2011). The New Policy World of Cybersecurity. *Public Administration Review*, *71*(3), Article 3. https://doi.org/10.1111/j.1540-6210.2011.02366.x

Heller, G. (2021). Immer mehr Cyberangriffe: IT-Sicherheitsbehörde BSI schlägt Alarm—Professionalität steigt. *Passau. Neue Presse*.

Herpig, D. S., & Dutke, F. (2023). *-Deutschlands -staatliche Cybersicherheits- architektur*.

Herpig, D. S., & Rupp, C. (2022). *Deutschlands staatliche Cybersicherheits- architektur*. 221.

Hevner, A., & Chatterjee, S. (2010). *Design Research in Information Systems: Theory and Practice* (2010. Aufl.). Springer.

Hevner, A. R. (2007). *A Three Cycle View of Design Science Research*. *19*, 7.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), Article 1. https://doi.org/10.2307/25148625

Hornung, G. (2015). Neue Pflichten für Betreiber kritischer Infrastrukturen: Das IT-Sicherheitsgesetz des Bundes. *Neue Juristische Wochenschrift*, 3334–3340.

International Organization for Standardization. (2019). *ISO/IEC 27701:2019(en), Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines*. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27701:ed-1:v1:en

Isensee, J., & Kirchhof, P. (Hrsg.). (2003). *Handbuch des Staatsrechts der Bundesrepublik Deutschland* (3., völlig neubearbeitete und erw. Aufl). C.F. Müller Juristischer Verlag.

Janssen, M., & Hjort-Madsen, K. (2007). Analyzing Enterprise Architecture in National Governments: The Cases of Denmark and the Netherlands. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 218a–218a. https://doi.org/10.1109/HICSS.2007.79

Jarass, H.-D., Kment, M., & Pieroth, B. (2020). *Grundgesetz für die Bundesrepublik Deutschland: Kommentar* (16. Auflage 2020). C.H. Beck.

Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science*. Springer International Publishing. https://doi.org/10.1007/978-3-319-10632-8

Johnson, P., Ekstedt, M., Silva, E., & Plazaola, L. (2004). *Using Enterprise Architecture for CIO Decision-Making: On the Importance of Theory*. Second Annual Conference on Systems Engineering Research. http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91301

Johnson, P., Lagerström, R., Närman, P., & Simonsson, M. (2007). Enterprise architecture analysis with extended influence diagrams. *Information Systems Frontiers*, *9*(2), Article 2. https://doi.org/10.1007/s10796-007-9030-y

Juhos, B. (1970). Die methodologische Symmetrie von Verifikation und Falsifikation. *Zeitschrift für allgemeine Wissenschaftstheorie / Journal for General Philosophy of Science*, *1*(1), 41–70.

Kalmbach, P. L. (2018). Ermessensübung und Handlungspflichten. *DEUTSCHE VERWALTUNGSPRAXIS*, 386.

Kelle, U. (2017). Die Integration qualitativer und quantitativer Forschung – theoretische Grundlagen von „Mixed Methods". *KZfSS Kölner Zeitschrift für Soziologie und Sozialpsychologie*, *69*(S2), 39–61. https://doi.org/10.1007/s11577-017-0451-4

Kindhäuser, U., Neumann, U., Paeffgen, H.-U., Saliger, F., Albrecht, H.-J., & Eschelbach, R. (2023). *Strafgesetzbuch* (6. Auflage). Nomos.

Kipker, D.-K., & Barudi, M. (Hrsg.). (2020). *Cybersecurity* (1. Auflage). C.H. Beck.

Kirchmair, R. (2022). *Qualitative Forschungsmethoden: Anwendungsorientiert: vom Insider aus der Marktforschung lernen*. Springer.

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability*, *14*(3), Article 3. https://doi.org/10.3390/su14031269

Klein, E. (1989). Grundrechtliche Schutzpflicht des Staates. *Neue juristische Wochenschrift*, *42*(27), 1633–1640.

Klenk, T., Nullmeier, F., & Wewer, G. (Hrsg.). (2020). *Handbuch Digitalisierung in Staat und Verwaltung*. Springer VS. https://doi.org/10.1007/978-3-658-23668-7

Koch, H.-J., Rubel, R., Heselhaus, F. S. M., & Hofmann, E. (2023). *Allgemeines Verwaltungsrecht* (4., neu bearbeitete und erweiterte Auflage). Verlag Franz Vahlen. https://doi.org/10.15358/9783800671960

Kornmesser, S., & Büttemeyer, W. (2020). *Wissenschaftstheorie: Eine Einführung*. J.B. Metzler Verlag.

Krajewski, M. (Hrsg.). (2015). *Services of general interest beyond the single market: External and international law dimensions*. T.M.C. Asser Press.

Krautscheid, A. (Hrsg.). (2009). *Die Daseinsvorsorge im Spannungsfeld von europäischem Wettbewerb und Gemeinwohl: Eine sektorspezifische Betrachtung*. VS Verlag für Sozialwissenschaften / GWV Fachverlage GmbH, Wiesbaden. https://doi.org/10.1007/978-3-531-91841-9

Kropp, S. (2010). *Kooperativer Föderalismus und Politikverflechtung*. VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-92211-9

Krumm, T. (2015). *Föderale Staaten im Vergleich: Eine Einführung*. Springer VS. https://doi.org/10.1007/978-3-658-04956-0

Kuckartz, U. (2016). *Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung* (3., überarbeitete Auflage). Beltz Juventa.

Kuhn, T. S., & Hacking, I. (2012). *The structure of scientific revolutions* (Fourth edition). The University of Chicago Press.

Lagodny, O. (2023). *Rechtswissenschaft als Argumentationswissenschaft: Transnationales Toleranzprinzip oder hegemonialer Letztbegründungsanspruch?* (1. Auflage). Nomos.

Lange, H.-J., & Bötticher, A. (Hrsg.). (2015). *Cyber-Sicherheit*. Springer VS.

Lankhorst, M. (2017). *Enterprise Architecture at Work: Modelling, Communication and Analysis* (4th ed. 2017). Springer Berlin Heidelberg : Imprint: Springer. https://doi.org/10.1007/978-3-662-53933-0

LastG - Gesetz zur Lastentragung im Bund-Länder-Verhältnis bei Verletzung von supranationalen oder völkerrechtlichen Verpflichtungen (2006). https://www.gesetze-im-internet.de/lastg/BJNR210500006.html

Lühr, H. (Hrsg.). (2020). *Digitale Daseinsvorsorge: Bremer Gespräche zur digitalen Staatskunst: Ergebnisse des Kolloquiums im Bremer Rathaus am 24./25. Februar 2020*. Digitale Daseinsvorsorge, Bremen. Kellner Verlag.

Lühr, H., Bremen, & Dataport AöR (Hrsg.). (2019). *Brauchen wir eine neue Staatskunst? Herausforderungen für das Staats- und Verwaltungshandeln durch die digitale Entwicklung: Ergebnisse des Kolloquiums im Bremer Rathaus am 12./13. Februar 2019*. Brauchen Wir eine Neue Staatskunst?, Bremen Boston. Kellner Verlag.

Lurz, H., Scheben, B., & Dolle, W. (2015). Das IT-Sicherheitsgesetz: Herausforderungen und Chancen für Unternehmen - vor allem für KMU. *Betriebs-Berater*, 2755–2762.

Maier, S., & Aengenheyster, S. (2020). *Geschäftsrisiko Cyber-Security: Leitfaden zur Etablierung eines resilienten Sicherheits-Ökosystems*. Springer Gabler.

Mayring, P. (1983). *Qualitative Inhaltsanalyse: Grundlagen und Techniken*. Beltz.

Mayring, P. (2008). *Qualitative Inhaltsanalyse: Grundlagen und Techniken* (10., neu ausgestattete Aufl., Dr. nach Typoskr). Beltz.

Mazaraki, N., & Goncharova, Y. (2022). CYBER DIMENSION OF HYBRID WARS: ESCAPING A 'GREY ZONE' OF INTERNATIONAL LAW TO ADRESS ECONOMIC DAMAGES. *Baltic Journal of Economic Studies*, *8*(2), 115–120. https://doi.org/10.30525/2256-0742/2022-8-2-115-120

Mey, G., & Mruck, K. (Hrsg.). (2010). *Handbuch qualitative Forschung in der Psychologie* (1. Aufl). VS Verlag für Sozialwissenschaften.

Mokaddem, S., Wagener, G., Dulaunoy, A., & Iklody, A. (2019). *Taxonomy driven indicator scoring in MISP threat intelligence platforms* (arXiv:1902.03914; Nummer arXiv:1902.03914). arXiv. http://arxiv.org/abs/1902.03914

Möller, T. A. (2023). Cybersicherheit für Staat, Wirtschaft und Gesellschaft. *Zeitschrift für Außen- und Sicherheitspolitik*, *16*(1), 1–12. https://doi.org/10.1007/s12399-023-00936-w

Moses, F., & Rehbohm, T. (2022). CISIS12. *kes, IT-Sicherheit, Informationssicherheit und Datensicherheit, DATAKONTEXT GmbH*, *1*, Article 1.

Moses, F., & Rehbohm, T. (2023a). CISIS12 für kleine und mittelständische Organisationen IN ZWÖLF SCHRITTEN ZUM RECHTSKONFORMEN ISMS. *kes, IT-*

Sicherheit, Informationssicherheit und Datensicherheit, DATAKONTEXT GmbH, *4*, Article 4.

Moses, F., & Rehbohm, T. (2023b). Entwicklung eines modularen ISMS und DSMS. *Datenschutz und Datensicherheit - DuD*, *47*(11), Article 11. https://doi.org/10.1007/s11623-023-1850-5

Moses, F., & Sandkuhl, K. (2022). Mit CISIS12 ein ISMS aufbauen. *Datenschutz und Datensicherheit - DuD*, *46*(10), Article 10. https://doi.org/10.1007/s11623-022-1677-5

Moses, F., Sandkuhl, K., & Kemmerich, T. (2022a). Empirical Study on the State of Practice of Information Security Management in Local Government. In A. Zimmermann, R. J. Howlett, & L. C. Jain (Hrsg.), *Human Centred Intelligent Systems* (S. 13–25). Springer Nature. https://doi.org/10.1007/978-981-19-3455-1_2

Moses, F., Sandkuhl, K., & Kemmerich, T. (2022b). *Information security management in German local government*. 183–189. https://doi.org/10.15439/2022F162

Neu, C. (Hrsg.). (2009). *Daseinsvorsorge: Eine gesellschaftswissenschaftliche Annäherung* (1. Aufl). VS, Verlag für Sozialwissenschaften.

Neugebauer, R. (Hrsg.). (2018). *Digitalisierung: Schlüsseltechnologien für Wirtschaft und Gesellschaft* (1. Auflage). Springer Vieweg.

Niedersächsisches Vorschrifteninformationssystem (NI-VORIS). (2019). *NDIG,NI - Niedersächsisches Informationssicherheitsgesetz*. Niedersächsisches Vorschrifteninformationssystem (NI-VORIS). https://voris.wolterskluwer-online.de/browse/document/a8cf0d53-edeb-3d90-8bf4-a42dbb4e8799

Niemi, E., & Pekkola, S. (2017). Using enterprise architecture artefacts in an organisation. *Enterprise Information Systems*, *11*(3), Article 3. https://doi.org/10.1080/17517575.2015.1048831

Nurmi, J., Pulkkinen, M., Seppänen, V., & Penttinen, K. (2019). Systems Approaches in the Enterprise Architecture Field of Research: A Systematic Literature Review. In D. Aveiro, G. Guizzardi, S. Guerreiro, & W. Guédria (Hrsg.), *Advances in Enterprise Engineering XII* (Bd. 334, S. 18–38). Springer International Publishing. https://doi.org/10.1007/978-3-030-06097-8_2

Österle, H., Becker, J., Frank, U., & Al., E. (2010). Memorandum zur gestaltungsorientierten Wirtschaftsinformatik. *Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung : Zfbf*, *62*(6), Article 6.

OZG - Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (2017). https://www.gesetze-im-internet.de/ozg/BJNR313800017.html

Pang, M.-S. (2014). IT governance and business value in the public sector organizations—The role of elected representatives in IT governance and its impact on IT value in U.S. state governments. *Decision Support Systems*, *59*, 274–285. https://doi.org/10.1016/j.dss.2013.12.006

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Pfeiffer, S., & Seiffert, M. (2019). Security-Management-as-a-Service. *Datenschutz und Datensicherheit - DuD*, *43*(1), Article 1. https://doi.org/10.1007/s11623-019-1055-0

Pidun, T., & Auth, G. (Hrsg.). (2025). *Praxishandbuch Verwaltungsinformatik* (1. Auflage). UTB.

Pistorius, B. (2018). *Jahrbuch des Föderalismus 2018: Föderalismus, Subsidiarität und Regionen in Europa* (Europäischen Zentrum für Föderalismus-Forschung Tübingen (EZFF), Hrsg.). Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783845296579

Pohlmann, N. (2019). *Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. Springer Vieweg.

Preis, B., & Susskind, L. (2022). Municipal Cybersecurity: More Work Needs to be Done. *Urban Affairs Review*, *58*(2), Article 2. https://doi.org/10.1177/1078087420973760

Raabe, O., Schallbruch, M., & Steinbrück, A. (2018). Systematisierung des IT-Sicherheitsrechts. *Computer und Recht / International*, *34*(11), Article 11. https://doi.org/10.9785/cr-2018-341105

Raithel, J. (2006). *Quantitative Forschung: Ein Praxiskurs* (1. Auflage). VS Verlag für Sozialwissenschaften.

Regulierung digitaler Plattformen als Infrastrukturen der Daseinsvorsorge (with Busch, C.). (2021). Friedrich-Ebert-Stiftung, Abteilung Wirtschafts- und Sozialpolitik.

Rehbohm, T., & Kalmbach, P. (2021). *MMR-Aktuell 2021, 438461—Beck-online, Grundforderungen von Informations- und Cybersicherheit in Ländern*. https://beck-online.beck.de/?vpath=bibdata/zeits/MMRAktuell/2021/438461.htm

Rehbohm, T., & Kalmbach, P. L. (2023). Herausforderungen der föderalen Cybersicherheit vs. Änderung in der Bund-Länder Gewaltenteilung. *Datenschutz und Datensicherheit - DuD*, *47*(6), Article 6. https://doi.org/10.1007/s11623-023-1772-2

Rehbohm, T., Kemmerich, R., Cap, C. H., & Sandkuhl, K. (2022). Sicherheitsmanagement, Cybersicherheit und Daseinsvorsorge: Empirische Studie in deutschen Kommunen. *Datenschutz und Datensicherheit - DuD*, *46*(7), Article 7. https://doi.org/10.1007/s11623-022-1637-0

Rehbohm, T., & Moses, F. (2023a). Federal Cybersecurity Architecture and Information Security Management. In *GI Edition Proceedings Band 341 6. Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023)* (S. 14–28). Köllen.

Rehbohm, T., & Moses, F. (2023b). Föderale Cybersicherheitsarchitektur und Informationssicherheitsmanagement im Kontext der NIS-2-Richtlinie. *Datenschutz und Datensicherheit - DuD*, *47*(10), Article 10. https://doi.org/10.1007/s11623-023-1837-2

Rehbohm, T., & Sandkuhl, K. (2023). Referenzarchitektur Cybersicherheit im Föderalsystem Deutschlands. *HMD Praxis der Wirtschaftsinformatik*. https://doi.org/10.1365/s40702-023-01014-7

Rehbohm, T., & Sandkuhl, K. (2024). *Cybersicherheitsevaluation einer Referenzarchitektur für Land, Kommune und systemrelevante Infrastruktur*. https://doi.org/10.18420/SICHERHEIT2024_001

Rehbohm, T., Sandkuhl, K., Cap, C. H., & Kemmerich, T. (2021). Integrated Security Management of Public and Private Sector for Critical Infrastructures – Problem Investigation. In W. Abramowicz, S. Auer, & M. Stróżyna (Hrsg.), *Business Information Systems Workshops* (S. 291–303). Springer International Publishing. https://doi.org/10.1007/978-3-031-04216-4_26

Rehbohm, T., Sandkuhl, K., & Kemmerich, T. (2019). On Challenges of Cyber and Information Security Management in Federal Structures—The Example of German Public Administration. *BIR 2019*, 13.

Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, OJ L (2016). http://data.europa.eu/eli/dir/2016/1148/oj/deu

Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie), 2022/2555 73 (2023). https://digital-strategy.ec.europa.eu/de/policies/nis2-directive

Riek, M., Bohme, R., & Moore, T. (2016). Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), Article 2. https://doi.org/10.1109/TDSC.2015.2410795

Ritschl, V., Weigl, R., & Stamm, T. A. (Hrsg.). (2023). *Wissenschaftliches Arbeiten und Schreiben: Verstehen, Anwenden, Nutzen für die Praxis* (2. Auflage). Springer.

Rodin, D. N. (2015). THE CYBERSECURITY PARTNERSHIP: A PROPOSAL FOR CYBERTHREAT INFORMATION SHARING BETWEEN CONTRACTORS AND THE FEDERAL GOVERNMENT. *Public Contract Law Journal*, *44*(3), Article 3.

Rohde, M., Bürger, M., Peneva, K., Mock, J., & VDI-VDE Innovation + Technik GmbH (Hrsg.). (2022). *Datenwirtschaft und Datentechnologie: Wie aus Daten Wert entsteht*. Springer Vieweg.

Romeike, F., & Finke, R. B. (Hrsg.). (2003). *Erfolgsfaktor Risiko-Management*. Gabler Verlag. https://doi.org/10.1007/978-3-663-05715-4

Rost, M. (2022). *Das Standard-Datenschutzmodell (SDM): Einführung, Hintergründe und Kontexte zum Erreichen der Gewährleistungsziele*. Springer Vieweg.

Rost, M. (2025). *Das Standard-Datenschutzmodell (SDM): Einführung in die Umsetzung der operativen Anforderungen der DSGVO* (2nd ed. 2025). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-44998-8

Sandkuhl, K., Herzog, H., Timm, F., Stephan, G., & Debski, A. (2018). Eine Referenz für die Compliance-Organisation. *Risk, Fraud & Compliance*, *1*, 5. https://doi.org/10.37307/j.1867-8394.2018.01.05

Schallbruch, M. (2018). *Schwacher Staat im Netz: Wie die Digitalisierung den Staat in Frage stellt*. Springer.

Schladebach, M. (2018). Staatszielbestimmungen im Verfassungsrecht. *Juristische Schulung*, 118–122.

Schliesky, U. (Hrsg.). (2016). *Demokratie im digitalen Zeitalter: Das Grundgesetz im digitalen Zeitalter* (1. Auflage). Nomos.

Schubert, K., & Klein, M. (2021). *Das Politiklexikon: Begriffe, Fakten, Zusammenhänge* (8., vollständig überarbeitete und erweiterte Auflage). Dietz.

Seckelmann, M., & Brunzel, M. (Hrsg.). (2021). *Handbuch Onlinezugangsgesetz: Potenziale - Synergien - Herausforderungen*. Springer.

Seigerroth, U. (2011). Enterprise Modeling and Enterprise Architecture: The Constituents of Transformation and Alignment of Business and IT. *International Journal of IT/Business Alignment and Governance (IJITBAG)*, *2*(1), Article 1. https://doi.org/10.4018/jitbag.2011010102

Sein, Henfridsson, Purao, Rossi, & Lindgren. (2011). Action Design Research. *MIS Quarterly*, *35*(1), 37. https://doi.org/10.2307/23043488

SGB 5 - Sozialgesetzbuch (1988). https://www.gesetze-im-internet.de/sgb_5/

Shackelford, S. J., Russell, S., & Kuehn, A. (2016). Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors. *Chicago Journal of International Law*, *17*, 1.

Simon, D., Fischbach, K., & Schoder, D. (2013). An Exploration of Enterprise Architecture Research. *Communications of the Association for Information Systems*, *32*(1), Article 1. https://doi.org/10.17705/1CAIS.03201

Simon, D., Fischbach, K., & Schoder, D. (2014). Enterprise architecture management and its role in corporate strategic management. *Information Systems and E-Business Management*, *12*(1), Article 1. https://doi.org/10.1007/s10257-013-0213-4

Simon, H. A. (2008). *The sciences of the artificial* (3. ed., [Nachdr.]). MIT Press.

Simonsson, M., Johnson, P., & Ekstedt, M. (2010). The Effect of IT Governance Maturity on IT Governance Performance. *Information Systems Management*, *27*(1), Article 1. https://doi.org/10.1080/10580530903455106

Sodan, H. (2009). Kontinuität und Wandel im Verfassungsrecht. *Neue Zeitschrift für Verwaltungsrecht*, 545–551.

Sowa, A., & Rost, M. (2020). Die ISO 27701 und das SDM-V2 im Lichte der Umsetzung der DSGVO. *Datenschutz und Datensicherheit - DuD*, *44*(10), 659–662. https://doi.org/10.1007/s11623-020-1344-7

Susukailo, V., Opirsky, I., & Yaremko, O. (2022). Methodology of ISMS Establishment Against Modern Cybersecurity Threats. In M. Klymash, M. Beshley, & A. Luntovskyy (Hrsg.), *Future Intent-Based Networking* (S. 257–271). Springer International Publishing. https://doi.org/10.1007/978-3-030-92435-5_15

Szilagyi, T. (2018). *Seminars and Student Projects—Lehrstuhl für Wirtschaftsinformatik—Universität Rostock*. Computer Supported Scientific Work. https://www.wirtschaftsinformatik.uni-rostock.de/en/studies-and-teaching/topics/seminars-and-student-projects/

Tatiara, R., Fajar, A. N., Siregar, B., & Gunawan, W. (2018). Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001. *Journal of Physics: Conference Series*, *978*(1), Article 1. https://doi.org/10.1088/1742-6596/978/1/012039

Tausendpfund, M. (2022). *Quantitative Datenanalyse: Eine Einführung mit SPSS* (2., aktualisierte Auflage). Springer VS.

The TOGAF standard (Version 9.2). (2018). Van Haren Publishing.

University of Technology Sydney, AU, Anwar, M. J., Gill, A. Q., University of Technology Sydney, AU, Beydoun, G., & University of Technology Sydney, AU. (2018). A review of information privacy laws and standards for secure digital ecosystems. In *Australasian Conference on Information Systems 2018*. University of Technology, Sydney. https://doi.org/10.5130/acis2018.bb

Urbach, N., & Ahlemann, F. (2019). Transformable IT Landscapes: IT Architectures Are Standardized, Modular, Flexible, Ubiquitous, Elastic, Cost-Effective, and Secure. In N. Urbach & F. Ahlemann, *IT Management in the Digital Age* (S. 93–99). Springer International Publishing. https://link.springer.com/10.1007/978-3-319-96187-3_10

Valtonen, M. K. (2017). Management Structure Based Government Enterprise Architecture Framework Adaption in Situ. In G. Poels, F. Gailly, E. Serral Asensio, & M. Snoeck (Hrsg.), *The Practice of Enterprise Modeling* (S. 267–282). Springer International Publishing. https://doi.org/10.1007/978-3-319-70241-4_18

van de Kamp, T., Peter, A., Everts, M. H., & Jonker, W. (2016). Private Sharing of IOCs and Sightings. *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, 35–38. https://doi.org/10.1145/2994539.2994544

Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: A Framework for Evaluation in Design Science Research. *European Journal of Information Systems*, *25*(1), Article 1. https://doi.org/10.1057/ejis.2014.36

Vogel, H.-J. (1996). Gewaltenvermischung statt Gewaltenteilung? *Neue Juristische Wochenschrift*, 1505–1511.

von Beyme, K. (2017). Der Föderalismus. In K. von Beyme (Hrsg.), *Das politische System der Bundesrepublik Deutschland: Eine Einführung* (S. 377–417). Springer Fachmedien. https://doi.org/10.1007/978-3-658-14499-9_9

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

VwVfG - Verwaltungsverfahrensgesetz (1977). https://www.gesetze-im-internet.de/vwvfg/

Watson, R. T., & Webster, J. (2020). Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0. *Journal of Decision Systems*, *29*(3), Article 3. https://doi.org/10.1080/12460125.2020.1798591

Weber, A., Heiser, G., Kuhlmann, D., Schallbruch, M., Chattopadhyay, A., Guilley, S., Kasper, M., Krauß, C., Krüger, P. S., Reith, S., & Seifert, J.-P. (2020). Sichere IT ohne Schwachstellen und Hintertüren. *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis*, *29*(1), 30–36. https://doi.org/10.14512/tatup.29.1.30

Weber, K., Christen, M., & Herrmann, D. (2020). Bedrohung, Verwundbarkeit, Werte und Schaden: Cyberattacken und Cybersicherheit als Thema der Technikfolgenabschätzung. *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis*, *29*(1), 11–15. https://doi.org/10.14512/tatup.29.1.11

Wehr, M. (2005). *Rechtspflichten im Verfassungsstaat.* (1. Aufl., Bd. 1003). Duncker & Humblot. https://doi.org/10.3790/978-3-428-51885-2

Weissmann, P. (2023). *Die neue EU NIS 2 Direktive für Cyber Security in KRITIS*. https://www.openkritis.de/it-sicherheitsgesetz/eu-nis-2-direktive-kritis.html

Wenzelburger, G. (2020). Einheit und Vielfalt im Sicherheitsföderalismus: Muster der Sicherheitspolitik in den deutschen Ländern im Vergleich. In F. Knüpling, M. Kölling, S. Kropp, & H. Scheller (Hrsg.), *Reformbaustelle Bundesstaat* (S. 381–405). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-31237-4_22

Wernert, M. (2021). *Internetkriminalität: Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen* (4. Auflage). Richard Boorberg Verlag GmbH & Co KG. https://doi.org/10.5771/9783415068926

Wißotzki, M., & Sandkuhl, K. (2015). Elements and Characteristics of Enterprise Architecture Capabilities. In R. Matulevičius & M. Dumas (Hrsg.), *Perspectives in Business Informatics Research* (S. 82–96). Springer International Publishing. https://doi.org/10.1007/978-3-319-21915-8_6

Zhu, L. (2020). *Services of general economic interest in EU competition law: Striking a balance between non-economic values and market competition*. Asser Press.

Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, 1122 (2021). http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig angefertigt habe. Es wurden nur die in der Arbeit ausdrücklich benannten Quellen und Hilfsmittel benutzt. Wörtlich oder sinngemäß übernommenes Gedankengut habe ich als solches kenntlich gemacht.

Bremen, 18.04.2025 _____

Ort, Datum

_____

Unterschrift

Lebenslauf

Thomas Rehbohm absolvierte bis 1993 eine Ausbildung zum Kommunikationselektroniker bei der Deutschen Telekom und studierte später Elektrotechnik mit der Fachrichtung Informationstechnik an der Hochschule Bremen. Mit seiner Diplomarbeit „Entwicklung eines Schwingungssensors mittels Lasertriangulationsprinzip“ schloss er 1998 das Studium mit dem Dipl.-Ing. (FH) ab. Im Anschluss arbeitete Thomas Rehbohm für die Siemens AG in Hamburg (Information and Communication Networks) und München (Information and Communication Mobile) als Ingenieur. 2002 wechselte er in die Landesverwaltung der Freien Hansestadt Bremen (Senator für Finanzen und Senator für Inneres) und ist dort seit 2012 als Chief Information Security Officer (CISO) tätig. Berufsbegleitend hat er während dieser Tätigkeit ein Studium am University College Dublin (UCD) – zum Master of Science (M.Sc.) in Forensic Computing and Cybercrime Investigation (2010) – absolviert. Seit Ende 2018 war er externer Doktorand der Fakultät für Informatik und Elektrotechnik an der Universität Rostock. Die Betreuung seiner Forschungsarbeit erfolgte am Lehrstuhl für Wirtschaftsinformatik sowie am Lehrstuhl für Informations- und Kommunikationsdienste.