Sicher, aber wie?

Strukturelle Herausforderungen für IT-Sicherheit in der freien Wohlfahrt

Eine Fallstudie zur Caritas

Wissenschaftliche Arbeit zur Erlangung des Grades M.Sc.
an der TUM School of Social Science and Technology,
Department of Governance / Hochschule für Politik
der Technischen Universität München

Betreut von	Fabiola Schwarz / Prof. Dr. Katrin Paula
	Professur für Global Security and Technology
Eingereicht von	Katharina Schlotthauer
Eingereicht am	20. März 2025 in München

Abstract (Deutsch)

Die IT-Sicherheit sozialer Organisationen gewinnt zunehmend an Bedeutung, insbesondere angesichts wachsender Cyberbedrohungen auf die Branche. Dennoch gibt es kaum Literatur in diesem Bereich. Daher untersucht diese Masterarbeit die politischen, wirtschaftlichen und organisationalen Rahmenbedingungen für IT-Sicherheit in der freien Wohlfahrt am Beispiel der Caritas. Basierend auf einer Literaturrecherche und auf Experteninterviews mit Führungskräften aus Caritas-Organisationen werden zentrale Herausforderungen und Handlungsoptionen identifiziert.

Die Auswertung der Literatur und Interviews ergibt folgende Faktoren, die das Herstellen von IT-Sicherheit in frei gemeinnützigen Organisationen erschweren: Schlechte IT-Infrastruktur, fehlendes IT-Fachpersonal, geringe IT-Kompetenzen der Mitarbeitenden, eine tendenziell geringe Aufmerksamkeit unter Vorständ:innen und Spitzenverbänden für das Thema IT-Sicherheit, heterogene Strukturen, die Koordination und Kooperation erschweren, Hürden bei der Interessensvertretung, fehlende Refinanzierung von IT-Ausgaben, und mangelndes politischen Interesse. Darüber hinaus leidet die freie Wohlfahrt an sich unter Finanzierungsproblemen, womit die Herausforderungen mit IT-Sicherheit symptomatisch für das System der freien Wohlfahrt an sich sind. Um die IT-Sicherheit zu verbessern, werden eine engere Koordination innerhalb der Verbände, eine gezielte finanzielle Förderung sowie stärkere politische Beachtung der Branche gefordert.

Abstract (English)

Safe, but How? Structural Challenges for IT Security in the Non Profit Welfare Sector. A Case Study on Caritas

IT security in social organizations is becoming increasingly important, particularly considering growing cyber threats to the sector. However, there is little academic literature on this topic. This master's thesis examines the political, economic, and organizational framework conditions for IT security in the nonprofit welfare sector, using Caritas as a case study. Based on a literature review and expert interviews with executives from Caritas organizations, key challenges and potential solutions are identified.

The analysis of the literature and interviews reveals several factors that hinder IT security in nonprofit organizations: poor IT infrastructure, a lack of IT specialists, low IT literacy among employees, limited awareness of IT security among executives and umbrella organizations, heterogeneous structures that complicate coordination and cooperation, obstacles in political advocacy, insufficient funding for IT expenses, and a general lack of political interest in the issue. Additionally, the nonprofit welfare sector faces structural funding problems, making IT security challenges symptomatic of broader systemic issues.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
APT	Advanced Persistent Threat
BAGFW	Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege
BMWi	2013-2021 Bundesministerium für Wirtschaft und Energie, ab Dezember 2021 Bundesministerium für Wirtschaft und Klimaschutz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
Bzw.	Beziehungsweise
DCV	Deutscher Caritasverband
DDoS	Distributed Denial of Service
DiCV	Diözesancaritasverband
ebd.	ebenda
etc.	et cetera
f	folgende
ff	fortfolgende
FINSOZ	Fachverband Informationstechnologie in Sozialwirtschaft und Sozialverwaltung e. V.
IT	Informationstechnologie
KGSt	Kommunale Gemeinschaftsstelle für Verwaltungs-management
KHZG	Krankenhauszukunftsgesetz
KMU	Kleine und mittlere Unternehmen

Kritis	Kritische Infrastrukturen
NGO	Non-Governmental-Organisation (Nicht-Regierungsorganisation)
NPO	Non-Profit-Organisation
SGB	Sozialgesetzbuch
SkF	Sozialdienst katholischer Frauen
SKM	Sozialdienst Katholischer Männer
SROI	Social Return on Invest
NIS-2	Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (Englisch: **N**etwork and **I**nformation **S**ecurity Directive)
NRW	Nordrhein-Westfalen
OCV	Ortscaritasverband
u.a.	unter anderem
usw.	und so weiter
u.v.m.	und vieles mehr
vgl.	vergleiche
WfbM	Werkstätte für behinderte Menschen
z.B.	zum Beispiel

1. Einleitung

Am 10. September 2022 wurde der Caritasverband der Erzdiözese München und Freising Opfer einer Cyber-Attacke. Ein Großteil der Daten des Verbandes wurden verschlüsselt und etwa 5.500 PCs mit Schadsoftware einstweilig unbrauchbar gemacht. Das kabelgebundende Internet durfte nicht mehr genutzt werden, die E-Mail-Accounts von rund 6.000 Mitarbeitenden waren blockiert und auch hunderte Multifunktionskopiergeräte waren nicht betriebsfähig. Insgesamt betraf der Angriff über 10.000 Mitarbeitende an über 360 Standorten. In diesen Einrichtungen der Altenpflege, Kinderbetreuung, Werkstätten für Menschen mit Behinderung, Sozialberatung, etc. werden eine Million Klient:innen betreut. Um die Versorgung dieser Menschen aufrechtzuerhalten, mussten die Mitarbeitenden der Caritas München/Freising monatelang auf improvisierte technische Hilfprozesse zurückgreifen. Auch zwei Jahre nach dem Angriff waren der Wiederauf- und Umbau der IT-Landschaft noch nicht vollständig abgeschlossen.

Die Autorin war zum Zeitpunkt des Vorfalls für den Caritasverband tätig und im Anschluss in die Wiederaufbauarbeiten eingebunden. Während sie dadurch viele technische Einblicke in IT-Sicherheit gewann, ließ sie als Poltikwissenschaftlerin die Frage nicht los, welche strukturellen Faktoren der freien Wohlfahrt, zu der die Caritas gehört, den Angriff begünstigt haben. Diese Arbeit soll daher beantworten, welche politischen wirtschaftlichen und organisationalen Rahmenbedingunen die Fähigkeit der freien Wohlfahrt in Deutschland beeinflussen, gegen Cyberangriffe gerüstet zu sein und wie diese Rahmenbedingungen verbessert werden können. Als Fallbeispiel dient die Caritas. Eine Literaturrecherche soll Auskunft darüber geben, welche Fakoren bereits durch existierende Forschung bekannt sind. Zudem werden acht Expert:innen – Vorständ:innen, Geschäftsführer:innen und Referent:innen aus verschiedenen Caritasorganisationen – befragt, um weitere Herausforderungen sowie Handlungsoptionen zu identifizieren.

Die Arbeit ist wie folgt aufgebaut: Nach der Präzisierung der Fragestellung in Kapitel 2 werden in Kapitel 3 die Sozialwirtschaft und die freie Wohlfahrt definiert, ihre wirtschaftliche Bedeutung dargestellt, die Struktur und Finanzierungsgrundlagen von Wohlfahrtsverbänden umrissen und der Stand von IT und Digitalisierung in der freien Wohlfahrt erläutert. Kapitel 4 widmet sich der Vorstellung der Caritas als Fallbeispiel. IT-Sicherheit steht im Fokus von Kapitel 5: Hier geht es darum, was diese Arbeit unter IT-Sicherheit versteht, wie die aktuelle Gesetzeslage gestaltet ist und was

zur Situation von Cyberangriffen auf die freie Wohlfahrt sowie zu IT-Sicherheit in der Branche bereits durch Forschung bekannt ist. Kapitel 7 bis 8 widmen sich den Experteninterviews, beginnend mit methodischen Erläuterungen in Kapitel 7 und gefolgt von der Auswertung der Gespräche in Kapitel 8. Die Kapitel 9 und 10 enthalten die Diskussion der Ergebnisse und das Fazit.

2. Fragestellung

Diese Arbeit widmet sich der Frage, welche politischen, wirtschaftlichen und organisationalen Rahmenbedingungen die Fähigkeit der freien Wohlfahrt in Deutschland beeinflussen, gegen Cyberangriffe gerüstet zu sein und wie diese Rahmenbedingungen verbessert werden können. Dabei sind *Cyberangriffe* vorsätzliche Angriffe auf die Vertraulichkeit, Integrität oder Verfügbarkeit von elektronisch gespeicherten Daten bzw. Informationen einer Organisation, mit dem Ziel, der Organisation dadurch Schaden zuzufügen (siehe *5.1 Definitionen*). *Organisational* bezieht sich auf die strukturellen Eigenheiten der freien Wohlfahrt, beziehungsweise speziell der Caritas. Unter *freie Wohlfahrt* wird dabei ein Teil der Sozialwirtschaft verstanden, nämlich die freigemeinnützigen, also nichtgewinnorientierten, nicht-staatlichen Träger von sozialen Einrichtungen. Die Sozialwirtschaft wiederum umfasst alle Produzenten von sozialen und gesundheitsbezogenen Dienstleistungen (für eine ausführliche Definition siehe *3.1 Definition der Sozialwirtschaft und freien Wohlfahrt in Deutschland*). Der Fokus dieser Arbeit liegt aus zwei Gründen auf der freien Wohlfahrt anstatt auf der Sozialwirtschaft: Zum einen spielt die freie Wohlfahrt in der Sozialwirtschaft in Deutschland nach wie vor eine wichtige Rolle (siehe *3.1 Definition der Sozialwirtschaft und freien Wohlfahrt in Deutschland*); zum anderen gibt es Indizien, dass der Zustand der IT-Infrastruktur in der freien Wohlfahrt aufgrund ihrer Nonprofit-Natur und aufgrund des langen Bestehens vieler Einrichtungen im Vergleich zu kommerziellen Anbietern schlechter ausfällt. So steht beispielsweise in privaten Krankenhäusern mehr IT-Fachpersonal zur Verfügung als in freigemeinnützigen (siehe *3.5 IT und Digitalisierung in der freien Wohlfahrt*).

Die Forschungsfrage untergliedert sich in vier Unterfragen:

- Welche politischen, wirtschaftlichen und organisationalen Rahmenbedingungen lassen sich in der Literatur finden?
- Gibt es Herausforderungen für die Branche bezüglich IT-Sicherheit, die von bisheriger Literatur noch nicht erfasst wurden?
- Wie begegnet die Branche den Herausforderungen aktuell?

- Welche Handlungsoptionen sieht die freie Wohlfahrt, beziehungsweise welche Forderungen stellt sie, um die Rahmenbedingungen für IT-Sicherheit zu verbessern?

Während die erste Unterfrage aus bestehender Literatur heraus bearbeitet wird (Kapitel 3 bis 6), werden zur Beantwortung der anderen drei Fragen Experteninterviews geführt (Kapitel 8 bis 10).

Die Relevanz des Themas begründet sich sowohl wissenschaftlich als auch gesellschaftlich. Wissenschaftlich leistet diese Masterarbeit einen Beitrag zu einem untererforschten Gebiet: Wie in *5.5 Forschung zu IT-Sicherheit in angrenzenden Bereichen: KMU, Gesundheitswesen, NPOs und NGOs* und *5.6 Forschungsstand zu Cyberbedrohungen in der Sozialwirtschaft* dargestellt, existiert – abgesehen vom Klinikbereich – kaum Literatur zu IT-Sicherheit in der Sozialwirtschaft. Zudem zeichnet sich die Arbeit durch einen besonderen Feldzugang aus. In den Experteninterviews werden Vorständ:innen und Geschäftsführer: innen von Caritas-Organisationen befragt. Wegen ihrer Position und den damit einhergehenden zeitlichen Verpflichtungen ist es nicht leicht, diese Personengruppe für Interviews zu gewinnen. Darüber hinaus handelt es sich bei IT-Sicherheit um ein sensibles Thema, für das es einer gewissen Vertrauensbasis bedarf, um offen mit Forscher:innen darüber zu sprechen. Die Autorin dieser Arbeit war zum Zeitpunkt des Forschungsprojekts für den Caritas-Netzwerk IT e. V. tätig. Der Verein wurde 2021 von ca. 100 Caritas-Organisationen gegründet, um gemeinsame IT-Strategien zu entwickeln, die Vernetzung in der Informationstechnologie innerhalb der Caritas zu fördern und eine IT-Standardisierung für die Sozialwirtschaft zu erwirken (Caritas-Netzwerk IT e. V. 2024). Stand März 2025 sind etwa 150 Rechtsträger Mitglieder im Verein. Durch ihre Arbeit für den Caritas-Netzwerk IT e. V. hat die Autorin Kontakt zu Vorständ:innen und Geschäftsführer:innen von Caritas-Organisationen, aufgrund deren Mitgliedschaft im Verein davon ausgegangen werden kann, dass sie ein gewisses Interesse an und Verständnis für Informationstechnologie in der Sozialwirtschaft und den damit verbundenen Herausforderungen mitbringen.

Die gesellschaftliche Relevanz des Themas leitet sich aus der Bedeutung der Sozialwirtschaft im Bereich der sozialen Fürsorge und Absicherung sowie für den Arbeitsmarkt und in Folge aus beiden auch für die Volkswirtschaft ab (siehe *3.2 Wirtschaftliche Bedeutung der freien Wohlfahrt*). Zudem stellen Shandler und Gomez am Beispiel eines Ransomware-Angriffs auf das Universitätsklinikum Düsseldorf im Jahr 2020 fest, dass Cyberangriffe auf öffentliche Einrichtungen das Vertrauen in die Regierung senken und somit potenziell eine Gefahr für die Demokratie darstellen (Shandler und Gomez 2023). Ebenso dürfte der Schutz anderer sozialer Einrichtungen als Krankenhäuser wichtig für das Vertrauen in demokratische Regierungen sein. Darüber hinaus betrifft IT-Sicherheit

in der Sozialwirtschaft nicht nur die Gesellschaft als Ganzes, sondern ist auch auf individueller Ebene relevant. Zum einen arbeitet die Sozialwirtschaft mit sensiblen personenbezogenen Daten, und ein Datenabfluss kann schwere Auswirkungen auf die Betroffenen haben. Beispiele hierfür wären, wenn die Namen und Adressen von Menschen, die Schuldnerberatung in Anspruch nehmen, sich in Rehabilitation von einer Suchterkrankung befinden oder in Gewaltschutzhäusern leben, an die Öffentlichkeit gelangen würden. Zum anderen kann ein Ausfall der IT-Systeme zur Einschränkung oder zum temporären Wegfall von Dienstleistungen führen. Wenn etwa die elektronische Routen-/Tagesplanung eines ambulanten Pflegedienstes ausfällt, kann es sein, dass eine pflegebedürftige Person nicht aufgesucht und versorgt wird. Auch der unangekündigte Ausfall eines Onlineberatungstermins, beispielsweise im Bereich Sucht, Trauer oder Suizidprävention, kann eine hilfesuchende Person tief verunsichern.

3. Die freie Wohlfahrt in Deutschland

3.1 Definition der Sozialwirtschaft und freien Wohlfahrt in Deutschland

Der Begriff „Sozialwirtschaft“ bezeichnet den sozialen Dienstleistungssektor (Schneiders 2021), also die „Gesamtheit der Produzenten sozialer und gesundheitsbezogener Dienstleistungen“ (Grunwald und Langer 2018, 49). Diese sozialen und gesundheitsbezogenen Dienstleistungen umfassen die Arbeitsbereiche Gesundheitshilfe (u.a. den Betrieb von Krankenhäusern), Kinder- und Jugendhilfe (inklusive den Betrieb von Kindergärten), Familienhilfe, Altenhilfe (v.a. die stationäre und ambulante Pflege), Eingliederungshilfe (Hilfen für Menschen mit Behinderung und psychischen Erkrankungen), Angebote für Geflüchtete und Eingewanderte, Hilfe für Personen in besonderen sozialen Situationen (Obdachlosigkeit, Verschuldung, Sucht, usw.) sowie die Ausbildung für soziale und pflegerische Berufe (Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege 2023, 4).

Erbracht werden diese sozialen Dienstleistungen von öffentlichen Trägern oder freien, also nichtstaatlichen Trägern (Bieker 2022; Brinkmann 2009, 58ff). Öffentliche Träger fungieren primär als Kostenträger, die für die Vergabe von Sozialleistungen zuständig sind, etwa Sozial- und Jugendämter oder die Sozialversicherungen. Manche öffentlichen Träger können zugleich Träger eigener Dienste sein, zum Beispiel Kommunen als Betreiber von kommunalen Kindergärten, Krankenhäusern, Jugendeinrichtungen etc., oder Bundesländer als Träger von Universitätsklinken (ebd.). Freie Träger lassen sich in privatwirtschaftliche und freigemeinnützige Träger unterscheiden (ebd.).

Während privatgewerbliche Anbieter gewinnorientiert arbeiten, sind freigemeinnützige Träger dem Gemeinwohl und der Gemeinnützigkeit verpflichtet. In Deutschland ist der gemeinnützige Bereich der Sozialwirtschaft beinahe gleichzusetzen mit den sechs Spitzenverbänden der freien Wohlfahrtspflege (Zimmer und Paul 2024, 93): Deutscher Caritasverband (DCV), Diakonisches Werk (DW), Paritätischer Wohlfahrtsverband (DPWV) Deutsches Rotes Kreuz (DRK), Arbeiterwohlfahrt (AWO) und die Zentralwohlfahrtsstelle der Juden in Deutschland (ZWST). Auch wenn es immer mehr privat-kommerzielle Anbieter gibt, so werden auch heute noch – je nach Arbeitsbereich – 32 bis 64 Prozent aller sozialen Dienstleistungen von Mitgliedsorganisationen dieser sechs Verbände erbracht (Zimmer und Paul 2024, 90).

Diese Arbeit betrachtet schwerpunktmäßig die freie Wohlfahrt. Da viele Zahlen jedoch nicht nach Träger differenziert vorliegen, wird im Laufe der Arbeit immer wieder auf die Sozialwirtschaft als Ganzes verwiesen. Sobald von „Sozialwirtschaft" die Rede ist, sind also sowohl freigemeinnützige als auch private und öffentliche Leistungsträger gemeint.

3.2 Wirtschaftliche Bedeutung der freien Wohlfahrt

Wegen mangelnder Zahlen und aufgrund der Natur von sozialwirtschaftlichen Dienstleistungen lässt sich ihre Wirtschaftsleistung nur schwer berechnen. Die Deutsche Bank schätzt für 2008, dass sich das Leistungsvolumen der freien Wohlfahrt auf knapp 38 Milliarden Euro belief, und das allein für die marktnahen Bereiche der Gesundheits- und Altenhilfe und Teile der Jugendhilfe (Falter 2010). Marktferne Bereiche wie Beratungsstellen und therapeutische Selbsthilfegruppen fallen aufgrund anderer Finanzierungsstrukturen aus der Berechnung der Deutschen Bank heraus, und auch Kindertagesstätten wurden mangels geeigneter Daten nicht berücksichtigt. Die Deutsche Bank schlussfolgert daher, „dass der genannte Wert die FW [Freie Wohlfahrt] als Wirtschaftsfaktor unterschätzt" (Falter 2010, 8).

Ein Versuch, den wirtschaftlichen Beitrag von sozialen Organisationen messbar zu machen, sind Social-Return-on-Invest-Analysen (SROI-Analysen). Dabei wird eine „Sonzialrendite" berechnet, indem Investitionen zusätzlicher Wertschöpfung und vermiedenen Kosten gegenübergestellt werden (Kehl und Then 2024, 935). Zusätzliche Wertschöpfung sind zum Beispiel Sozialversicherungsbeiträge, Lohnsteuer und Mehrwertsteuer, die Mitarbeitende in der Sozialwirtschaft von ihrem Einkommen bezahlen. Der Sozialreport Bayern 2018 berechnet, dass allein dadurch 48 % der öffentlichen Investitionen in die bayerische Sozialwirtschaft wieder an die öffentliche Hand

zurückfließen (Schellberg 2018, 27). Des Weiteren findet Wertschöpfung dadurch statt, dass Menschen in Arbeit gebracht werden und ebenfalls Steuern zahlen, die ohne Unterstützung der Sozialwirtschaft – etwa durch Bildungs-, Gesundheits- oder Therapiemaßnahem – nicht oder nur eingeschränkt erwerbsfähig wären. Gleichzeitig werden dadurch Ausgaben für Arbeitslosengeld, Wohngeld, etc. reduziert. Im Justiz- und Sicherheitswesen werden ebenfalls Kosten vermieden, beispielsweise durch Gewaltpräventionsmaßnahmen oder Resozialisierungsarbeit. Einen großen Anteil macht auch die Betreuung von Kindern und Pflegebedürftigen aus, die andernfalls unter Reduzierung der Arbeitszeit privat organisiert werden müsste, was wiederum geringere Steuereinnahmen nach sich zöge.

SROI-Analysen gibt es in unterschiedlichen Formen, die zu verschiedenen Zwecken unter Einbezug verschiedener Dimensionen und in verschiedener Ausführlichkeit vorgenommen werden (Then und Schober 2015, 17ff). Um SROI-Werte wirklich miteinander vergleichen zu können, muss man sich daher mit den entsprechenden Analysen auseinandersetzen. Dennoch hier ein paar Beispiele, die illustrieren, dass Investitionen in die Sozialwirtschaft nicht nur einen ethischen, sondern auch monetären Mehrwert für die Gesellschaft erzeugen:

- Der Bundesverband Werkstätten für behinderte Menschen berechnet, dass 100 € an investierten Mitteln in eine Werkstätte Rückflüsse und Einsparungen von 108 € erbringen (Bundesarbeitsgemeinschaft Werkstätten für behinderte Menschen e. V. et al. 2015).
- Die Sozialwirtschaftsstudie Hessen kommt zu dem Schluss, dass jeder investierte Euro in Schuldnerberatungsstellen 6,60 € Sozialrendite generiert (Rada und Stahlmann 2016, 102).
- Im Bergischen Städtedreieck liegt der SROI für Kitas zwischen 4,70 € und 6,70 € (Betzer et al. 2025, 44).
- Eine Analyse des SROI der Psychosozialen Beratungs- und Behandlungsstelle Görlitz (Sozialteam GmbH) kommt sogar auf einen Wert von 27 € pro investiertem Euro (Pfahler und Packmohr 2021).

Eindeutiger beziffern lässt sich die volkswirtschaftliche Bedeutung der freien Wohlfahrt in Bezug auf den Arbeitsmarkt: Zum Stichtag 1. Januar 2020 waren in der Freien Wohlfahrtspflege 2.076.535 Menschen hauptamtlich beschäftigt – das sind 4,5 % aller Erwerbstätigen in Deutschland (Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege 2023). Zum Vergleich: Im Baugewerbe arbeiteten 2021 etwa 946.000, in der Automobilindustrie knapp 786.000 Personen (Statistisches Bundesamt 2023; Bundesministerium für Wirtschaft und Klimaschutz o.D.). Mit je knapp 696.000 und 627.000 Mitarbeitenden sind die Caritas und die Diakonie zudem die größten privaten Arbeitgeber

in Deutschland (Zentralstatistik des Deutschen Caritasverbandes e.V. 15.10.2022; Diakonie Deutschland 2023b; Ver.di o.D.).

Eine Kenngröße für die wirtschaftliche Bedeutung der freien Wohlfahrt, die einen Bezug zu IT-Sicherheit hat, ist die Summe der IT-Aufwendungen. Helmut Kreidenweis und Dietmar Wolff berechnen, dass die Sozialwirtschaft jährlich etwa 1,5 Milliarden Euro für Hardware, Netzwerke, Software, eigenes IT-Personal, externe Dienstleister und IT-Verbrauchsmaterial aufwendet (Kreidenweis und Wolff 2023, 13). Da sie jedoch auch privatwirtschaftliche Träger in ihre Rechnung miteinbeziehen, fällt der Wert für die freie Wohlfahrt allein niedriger aus.

3.3 Struktur der freien Wohlfahrtsverbände

Alle sechs Spitzenverbände der freien Wohlfahrtspflege in Deutschland haben eine verbandliche Doppelfunktion: Zum einen sind sie selbst Erbringer sozialer Dienstleistungen. Zum anderen betreiben sie Lobbyarbeit für die Interessen sozial schwacher Menschen und die ihrer Mitgliedsverbände. Zudem verstehen sie sich als ‚dritter Sozialpartner' und sind als solcher in die Politikformulierung und den bürokratischen Vollzug von Sozialleistungen eingebunden (Schmid und Mansour 2007, 244ff). In ihrer Funktion als Interessensvertreter gegenüber der Politik kooperieren die Verbände auf Bundesebene unter dem Dach der Bundesarbeitsgemeinschaft der freien Wohlfahrtspflege (BAGFW), auf Landesebene in Landesarbeitsgemeinschaften bzw. in sogenannten „Ligen" und auf Ortsebene in Stadt- und Kreisligen. Eine Übersicht über alle Landesarbeitsgemeinschaften befindet sich in *Anhang 1: Liste der Landesarbeitsgemeinschaften der freien Wohlfahrt*. Seit den 1990er Jahren wird die politische Einflussnahme der Verbände immer schwieriger. So beobachtet die Wohlfahrtsverbandsforschung eine Machtverschiebung zulasten der Wohlfahrtsverbände und zugunsten des Staates (siehe auch: Schmid und Mansour 2007, 258; Schroeder 2017, 60; Schmid 2018, 48; Backhaus-Maul 2019, 95f):

> Wurde bisher – unter Wahrung relativer Autonomie – die Institution der Freien Wohlfahrtspflege in den sozialpolitischen Entscheidungs- und Gesetzgebungsprozess einbezogen, so treten mittlerweile einzelne Wohlfahrtsverbände sowie auch einige große Einrichtungen und Dienste als politische Akteure an diese Stelle, wobei sie aber staatlicherseits, d.h. von Bundes- und Landespolitik und Ministerialverwaltung an einer 'kurzen Leine' geführt werden und ihr Handlungsspielraum gesetzgeberisch detailliert geregelt wird. (Backhaus-Maul 2019, 96)

Die Wohlfahrtsverbände sind föderalistisch strukturiert, d.h. neben der Bundesebene gibt es Landes-, Bezirks-, Kreis- und Ortsebenen, auf denen Interessensakkumulation und -vertretung

stattfinden (Schmid und Mansour 2007, 247). Wichtig zu verstehen ist, dass die Mitgliedsorganisationen auf freiwilliger Basis in den Spitzenverbänden organisiert und rechtlich selbstständig sind (ibid; Brinkmann 2009, 71). Aufgrund der hohen Autonomie der Einrichtungsträger verfügen die Spitzenverbände nur über eine geringe Steuerungswirkung ihren Mitgliedern gegenüber (Boeßenecker 2018, 292).

Dieser hohe Autonomiegrad der Mitglieder, die föderalen Struktur sowie historische Gründe haben dazu geführt, dass die Strukturen in der freien Wohlfahrtspflege höchst heterogen sind. Karl-Heinz Boeßenecker geht sogar so weit, die „regionale und organisatorische Unübersichtlichkeit" als ein „Systemmerkmal der deutschen Wohlfahrtspflege" zu bezeichnen (Boeßenecker 2018, 292ff). Die Komplexität der Organisationsstrukturen in der Freien Wohlfahrt ist in einem Schaubild von Ottnad et al. 2000 illustriert:

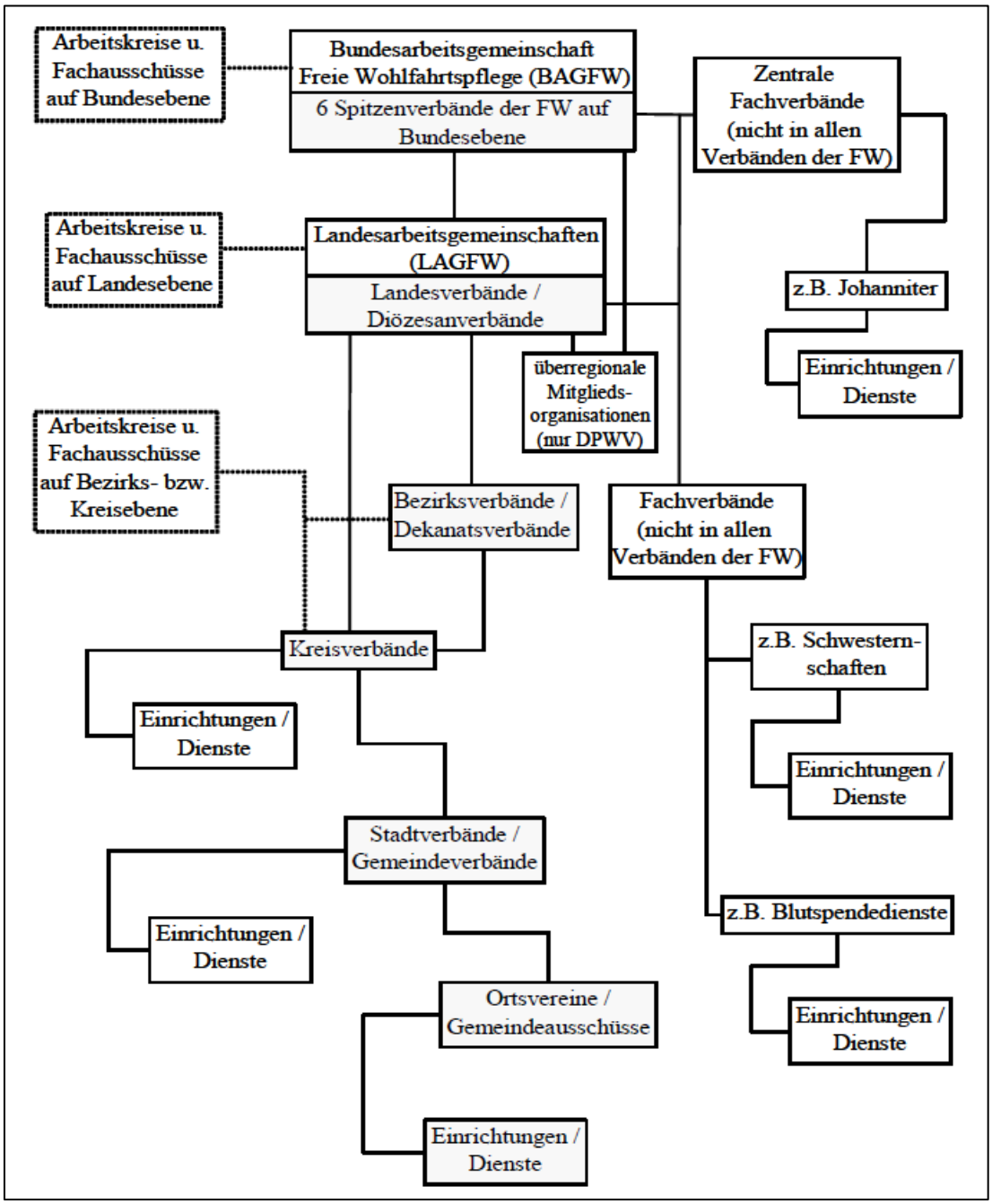

Abbildung 1: Schematische Organisationsstruktur der Wohlfahrtsverbände

Quelle: Ottnad et al. 2000, 19.

Daraus lässt sich ableiten, dass IT-Sicherheit auf verschiedenen Ebenen unterschiedliche Rollen spielt. Die Einrichtungsträger sind in der operativen Verantwortung, IT-Sicherheit in ihren Einrichtungen und Diensten technisch wie organisatorisch zu gewährleisten. Je nachdem, wie die

Träger strukturiert sind, können auch einzelne Einrichtungen und Dienste selbst in dieser Pflicht stehen. Aufgrund der rechtlichen Eigenständigkeit der Einrichtungsträger sind die Verbände nicht in der Lage, verbindliche IT-Sicherheitsvorgaben zu machen. Da aber ein Großteil ihrer Arbeit aus Kommunikations- und Wissensarbeit besteht (Klauß 2014, 41), können Verbände zur IT-Sicherheit bei ihren Mitgliedern beitragen, indem sie Aufmerksamkeit für das Thema schaffen und Wissensressourcen bereitstellen. In ihrer Funktion als politische Interessensvertretung sind außerdem sie die Akteure, die für das Thema IT-Sicherheit in der Wohlfahrt in der Politik sensibilisieren und Forderungen stellen können.

3.4 Finanzierung von Einrichtungsträgern der freien Wohlfahrt

IT-Sicherheit kostet Geld. Weiter unten, im Absatz *IT-Kosten,* wird noch ausführlicher darauf eingegangen, wie knapp die IT-Budgets in der Sozialwirtschaft bemessen sind. Auch wenn Helmut Kreidenweis und Dietmar Wolff betonen, dass die Höhe des IT-Budgets immer auch eine Managemententscheidung ist (Kreidenweis und Wolff 2022, 63), sind die Rahmenbedingungen für die Finanzierung sozialer Dienstleistungen im doppelten Sinne schwierig: Zum einen sind sie komplex und zum anderen durch Knappheit charakterisiert. Klaus Schellberg beschreibt letzteres folgendermaßen:

> Die Finanzierungsmöglichkeiten limitieren die Möglichkeiten, durchaus auch als notwendig erachtete soziale Leistungen zu erbringen. Die sozialwirtschaftliche Finanzierung kann daher durchaus als Engpassfunktion des Managements in Sozialunternehmen bezeichnet werden. (Schellberg 2024, 532)

Folglich ist es essenziell zu verstehen, wie Organisationen der freien Wohlfahrt Einnahmen generieren, aus denen sie wiederum IT-Sicherheitsmaßnahmen finanzieren können – oder eben nicht.

Finanzierungsstrukturen

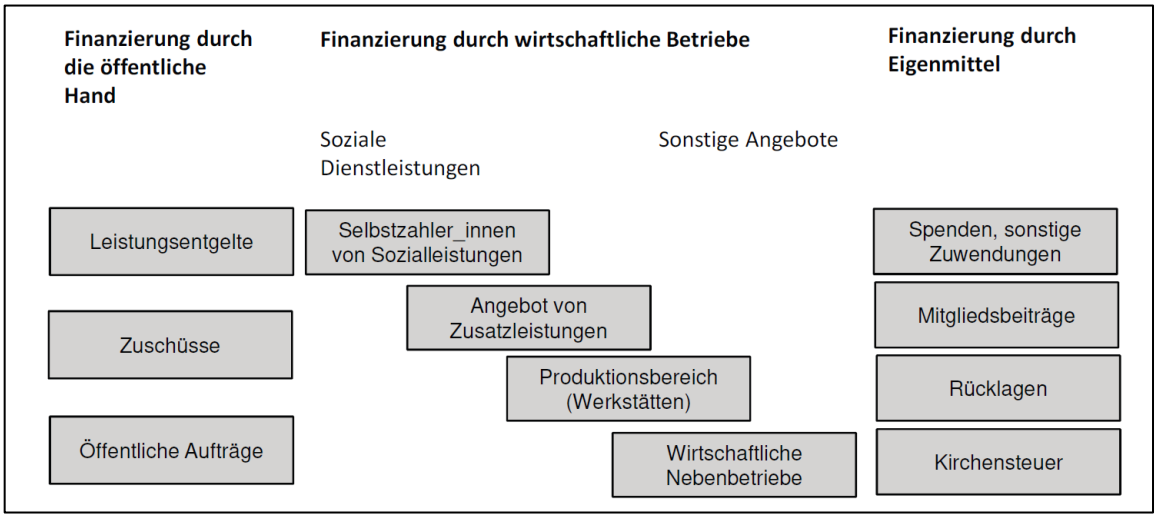

Abbildung 2: Finanzierungselemente eines Sozialunternehmens

Quelle: Schellberg 2024, 533

Prinzipiell stehen Organisationen der freien Wohlfahrt drei Finanzierungsquellen zur Verfügung (siehe *Abbildung 2*): Finanzierung durch die öffentliche Hand, Finanzierung durch Eigenmittel und Finanzierung durch wirtschaftlichen Betrieb. Letzteres kann zum Beispiel über Selbstzahler:innen geschehen, etwa ein Eigenanteil an den Kosten für einen Pflegeheimplatz oder Kitagebühren (Schellberg 2024, 533). Eine weitere Möglichkeit des wirtschaftlichen Betriebs sind Werkstätten für behinderte Menschen (WfbM), wo Produkte hergestellt werden, deren Erlöse zur Finanzierung der Organisation beitragen (ebd.). Eigenmittel können Spenden, Mitgliedsbeiträge, Rücklagen und (im Fall der Caritas und der Diakonie) Kirchensteuern sein, und werden verwendet, um Leistungen anzubieten, die andernfalls nicht oder nur teilweise finanzierbar wären.

Den größten Anteil an der Finanzierung von Leistungsanbietern der freien Wohlfahrt hat die öffentliche Hand: Je nach Quelle wird ihr Anteil auf über 60 bis 75 % geschätzt (ebd.). Die wichtigsten Kostenträger sind hierbei die Sozialversicherungen sowie die Kommunen (Landkreise und kreisfreie Städte), aber auch Länder, Bund sowie weitere administrative Einheiten können als Kostenträger fungieren. Sie finanzieren sowohl Leistungen, auf die Hilfesuchende einen Rechtsanspruch haben (z.B. betreutes Jugendwohnen, Unterbringung von Geflüchteten, Wohnheime für Menschen mit Behinderung, u.v.m.) als auch Leistungen, für die es keinen Rechtsanspruch gibt, die die Kostenträger aber als sinnvoll erachten (z.B. Suchtberatung, Seniorenbegegnungsstätten, Jugendtreffs, Notunterkünfte für Wohnungslose, etc.). Die öffentlichen Kostenträger verteilen die

Finanzmittel für soziale Dienstleistungen über öffentliche Aufträge / Vergabeverfahren, Zuwendungen / Zuschüsse oder über Leistungsentgeltsysteme an die Anbieter. Vergabeverfahren finden nur im Bereich der Sozialgesetzbücher (SGB) II und III[1] statt, z.B. wenn die Bundesagentur für Arbeit Qualifizierungs- und Weiterbildungsmaßen für Arbeitssuchende an Bildungsträger auslagert (vgl. Kolhoff 2019, 167). Zuschüsse hingegen sind direkte Geldzahlungen der Kommunen, Länder, des Bundes oder der EU an die Leistungserbringer (ebd. 158). Sie können als institutionelle Förderung erfolgen, die die Einrichtung als Ganzes fördert oder als Projektförderung, die zeitlich wie inhaltlich genaue abgesteckt ist (ebd.). Allerdings spielen Zuschüsse nur noch in Einzelbereichen eine größere Rolle, etwa bei Beratungsstellen, Jugendzentren und Modellprojekten (Schellberg 2024, 535).

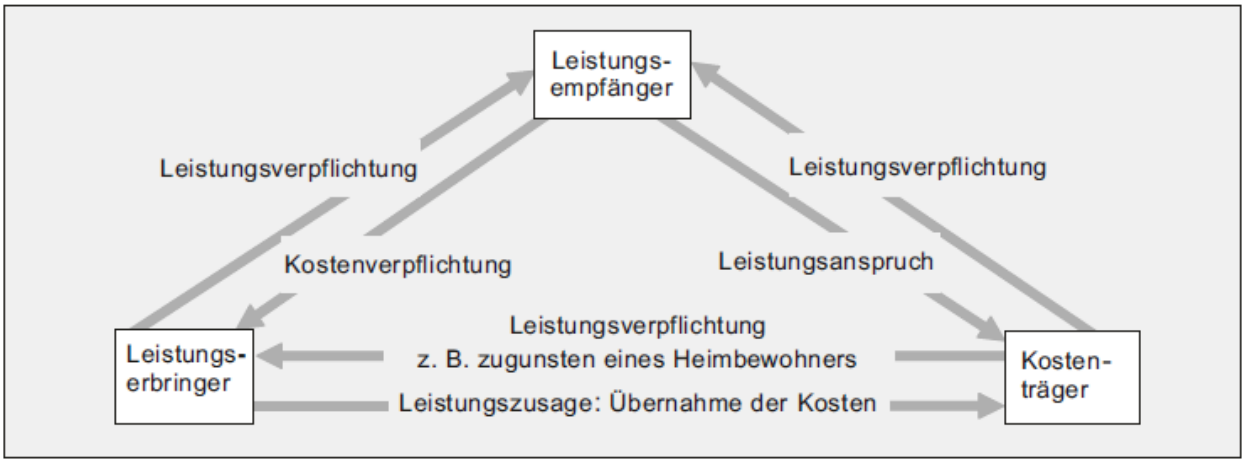

Abbildung 3: Sozialrechtliches Dreiecksverhältnis

Quelle: Kolhoff 2019, 161

Die wichtigste Finanzierungsform in der Sozialwirtschaft ist die Finanzierung über Leistungsentgelte, die über das sozialrechtliche Dreiecksverhältnis erfolgt (siehe *Abbildung 3*). Anders als in der freien Wirtschaft findet hier keine direkte Transaktion zwischen Leistungsempfänger (Klient:in / Patient:in) und Leistungserbringer (hier: ein Einrichtungsträger der freien Wohlfahrt) von sozialer Dienstleistung gegen Bezahlung statt; stattdessen kommt der Kostenträger (auch: Leistungsträger) für die entstandenen Kosten auf. Voraussetzung hierfür ist, dass der Leistungsempfänger einen

[1] SGB II regelt die Grundsicherung für Arbeitsuchende, SGB III die Arbeitsförderung.

Anspruch auf die Leistung hat und eine Vereinbarung zwischen Kostenträger und Leistungserbringer zur Kostenübernahme besteht. Der Leistungsempfänger hat dabei ein Wunsch- und Wahlrecht, das heißt er:sie kann nicht gezwungen werden, die Leistung bei einem bestimmten Leistungserbringer in Anspruch zu nehmen sondern darf zwischen verschiedenen Anbietern frei entscheiden (vgl. Gerlach und Hinrichs 2018, 168–171).

Grundlage für die Finanzierung von Leistungsentgelten bzw. Pflegesätzen sind Leistungsvereinbarungen und Entgeltvereinbarungen. In den Leistungsvereinbarungen sind die Art, das Ziel und die Qualität der Leistung festgesetzt, der zu betreuende Personenkreis definiert, sowie Angaben zu Qualität und Quantität des Personals und zur sachlichen Ausstattung enthalten (Gerlach und Hinrichs 2018, 183). Entgeltvereinbarungen können erst bei Vorliegen der Leistungsvereinbarungen geschlossen werden (Schellberg 2024, 537). Sie sind prospektiv, d.h. sie setzen zukünftige Preise fest und dürfen nicht rückwirkend angepasst werden (Gerlach und Hinrichs 2018, 178). Zudem müssen sie leistungsgerecht sein, also ausreichen, um die Kosten des Leistungsträgers für die erbrachte Leistung zu decken (ebd. 174). Die Auszahlung der Leistungsentgelte erfolgt nur bei tatsächlicher Inanspruchnahme der Leistung durch Klient:innen / Patient:innen (Schellberg 2024, 537). Die Leistungsvereinbarungen und Entgeltvereinbarungen werden auf einrichtungsindividueller Ebene, also lokal zwischen dem Leistungsträger und dem Kostenträger geschlossen (ebd.). Wer der zuständige Kostenträger ist, variiert zwischen Hilfefeldern und Bundesländern. Für Gesundheitsleistungen, beispielsweise Ergo- oder Physiotherapie im Rahmen der kindlichen Frühförderung, sind die gesetzlichen Krankenkassen verantwortlich, für Pflegeleistungen die Pflegekassen (vgl. Gerlach und Hinrichs 2018, 170). In der Kinder- und Jugend- sowie der Sozialhilfe sind die Landreise und kreisfreien Städte die Kostenträger (Kolhoff 2019, 156). Die einzelnen Leistungen in verschiedenen Hilfefeldern fallen wiederum in den Zuständigkeitsbereich unterschiedlicher Stellen innerhalb der Kommunalverwaltungen, zum Beispiel die Kinder- und Jugendhilfe in die des jeweiligen Jugendamtes. In der Sozialhilfe sowie der Eingliederungshilfe gibt es zudem eine überörtliche Ebene (ebd. 166). Diese ist entweder in Trägerschaft der Länder bzw. Stadtstaaten (z.B. Thüringen, Saarland, Berlin) oder höherer Kommunalverbände (z.B. die Bezirke in Bayern, die Landschaftsverbände Westfalen-Lippe und Rheinland in NRW, oder der Kommunale Sozialverband Sachsen) (Bundesarbeitsgemeinschaft der überörtlichen Träger der Sozialhilfe und der Eingliederungshilfe 2024). Diese können mandatiert sein, Leistungs- und Entgeltvereinbarungen zu schließen (Kolhoff 2019, 166). Die meisten dieser Vereinbarungen basieren auf

Rahmenverträgen, die auf Landesebene zwischen den Verbänden der Leistungsträger (z.B. Städte- und Gemeindetag, Landesverbände der Pflegekassen) und den Spitzenverbänden der freien Wohlfahrtspflege ausgehandelt werden (Schellberg 2024, 536f). Für die einrichtungsspezifischen Leistungs- und Entgeltvereinbarungen gelten diese Rahmenverträge allerdings nur, wenn beide Seiten Teil der Rahmenvereinbarung sind (Gerlach und Hinrichs 2018, 192).

Herausforderungen in der Finanzierung

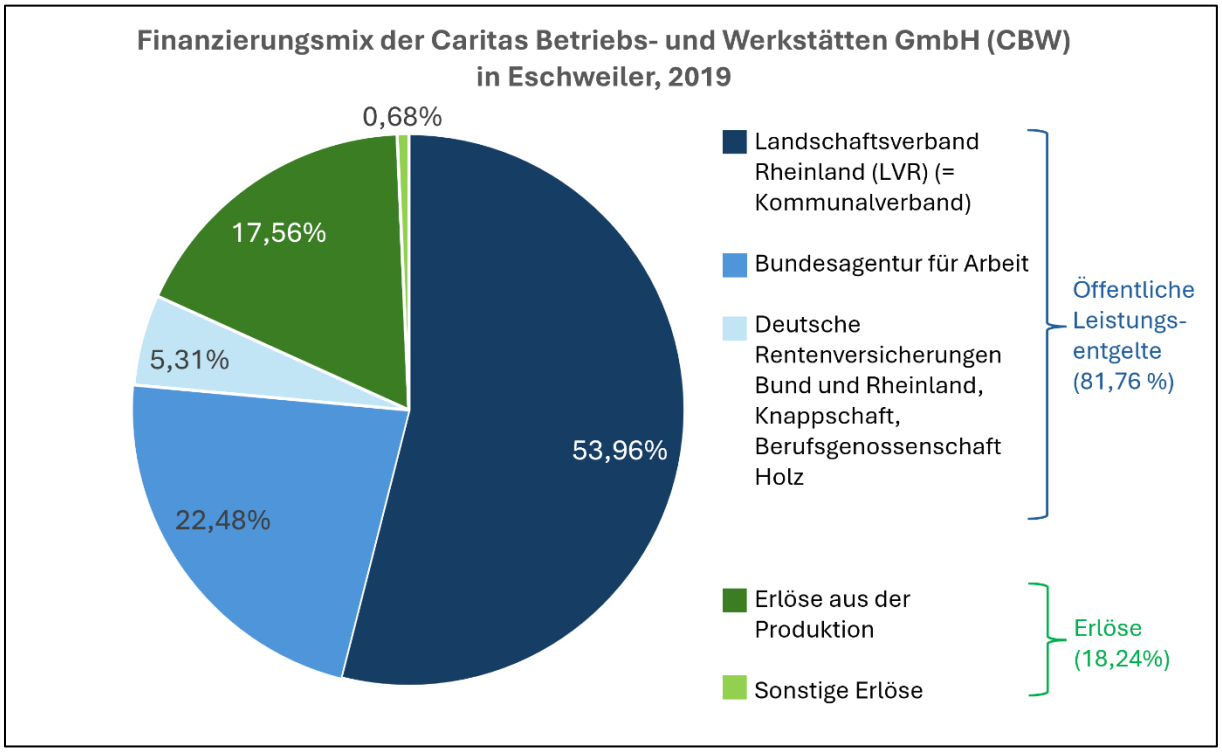

Abbildung 4: Finanzierungsmix der Caritas Betriebs- und Werkstätten GmbH (CBW) in Eschweiler, 2019. Eigene Darstellung.

Datenquelle: Heidrich 2021.

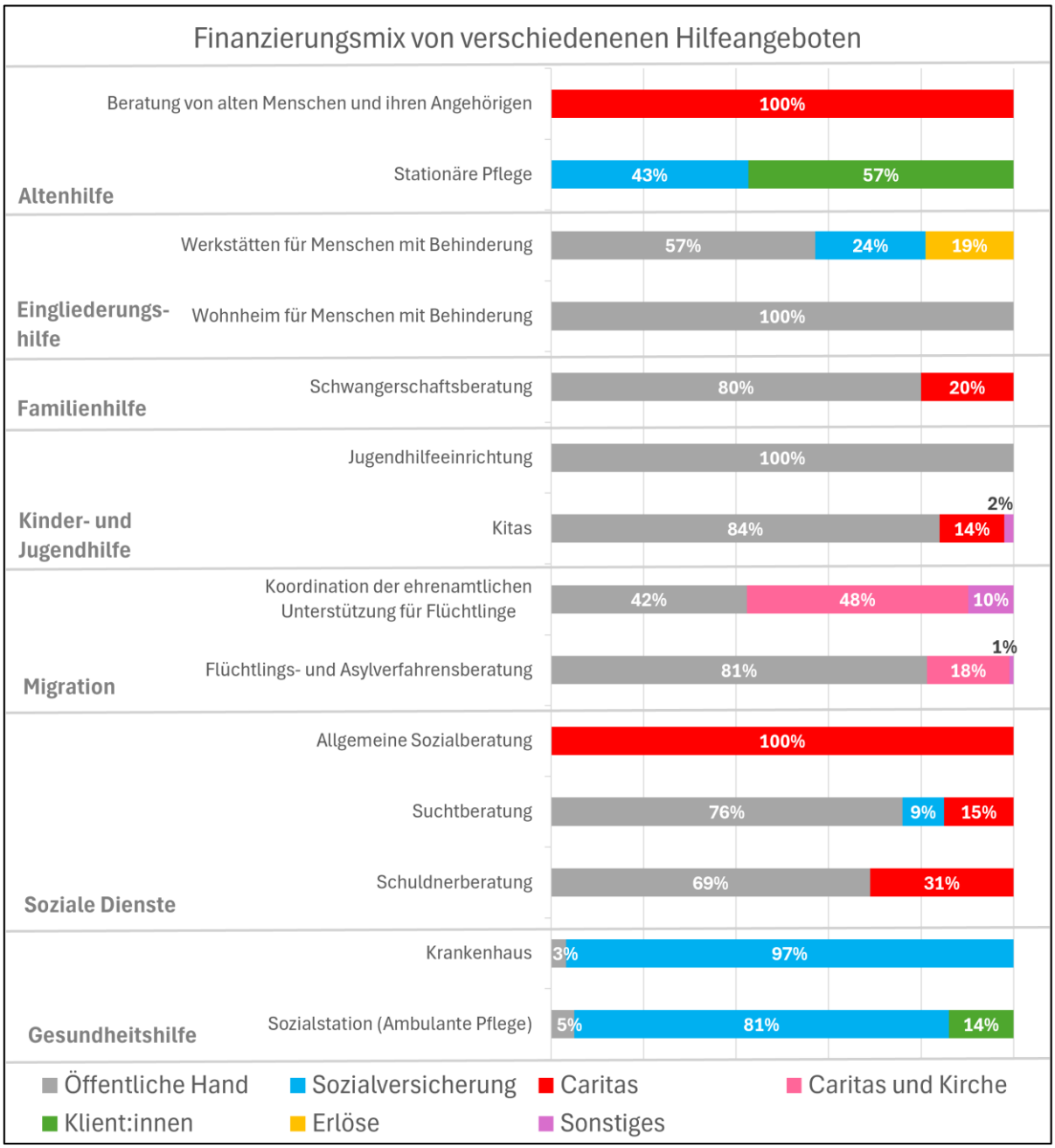

Abbildung 5: Finanzierungsmix verschiedener Hilfeangebote. Eigene Darstellung.

Datenquellen: Deutscher Caritasverband 2019.

Die Finanzierungsstrukturen in der Sozialwirtschaft bringen einige Herausforderungen für die Organisationen mit sich. Erstens sind sie ungemein komplex und binden sowohl auf Leistungserbringer- als auch Kostenträgerseite Personal- und Zeitressourcen für das Aushandeln der zahlreichen Vereinbarungen. *Abbildung 4* zeigt exemplarisch, wie sich die Caritas Betriebs- und Werkstätten

GmbH in Eschweiler (NRW), eine Werkstätte für behinderte Menschen (WfbM), finanziert. Über 80 % der Finanzierung erfolgen über öffentliche Leistungsentgelte, allerdings nicht aus einer Hand, sondern über verschiedene Stellen. Der größte Teil (insgesamt knapp 54 %) stammen vom Landschaftsverband Rheinland (LVR), dem für Eschweiler zuständigen überörtlichen Kommunalverband. Die Bundesagentur für Arbeit steuert weitere 22 % bei. Ein vergleichsweise kleiner Anteil von 5,3 % entfällt auf vier Akteure: die Deutsche Rentenversicherung Bund, die Deutsche Rentenversicherung Rheinland, die Knappschaft und die Berufsgenossenschaft Holz. Die WfbM hat also mit sechs verschiedenen öffentliche Stellen zu tun, mit denen sie und / oder der für sie zuständige Spitzenverband Leistungs- und Entgeltvereinbarungen aushandelt und denen gegenüber sie ihre IT-Kosten als Teil der Entgelte plausibel machen muss. Dabei hat die Caritas Betriebs- und Werkstätten GmbH im Vergleich zu anderen Einrichtungsträgern sogar den Vorteil, dass sie durch diverse Produktionen und Dienstleistungen, die von den dort angestellten Menschen mit Behinderung geleistet werden, Erlöse erwirtschaftet, über die der Träger mögliche Lücken in der Refinanzierung stopfen kann. Schließlich stellt die WfbM sogar einen einfachen Fall von Finanzierungsstrukturen dar, weil sie nur ein Hilfefeld bedient, nämlich das der Eingliederungshilfe. Viele Leistungsträger sind jedoch in mehreren Hilfefeldern tätig, das heißt sie müssen für jedes Hilfefeld andere Verträge auf Grundlage anderer Abschnitte des Sozialgesetzbuches mit anderen Ansprechpartnern der öffentlichen Hand schließen. *Abbildung 5* stellt Finanzierungsbeispiele für Hilfeleistungen in verschiedenen Hilfefeldern gegenüber. Die Zahlen stammen vom Deutschen Caritasverband und sind exemplarische Fälle, nicht allgemeingültig. Aus der Darstellung wird ersichtlich, wie sehr die Anteile von Sozialversicherungen, anderen Quellen der öffentlichen Hand und Eigenmitteln an der Finanzierung zwischen den Leistungen variieren. Was die Grafik nicht zeigt, ist, dass hinter jeder dieser drei Hauptfinanzierungsquellen wiederum verschiedene ‚Töpfe' bzw. Kostenträger stehen. Gerade für operativ tätige Caritasverbände ist es nichts Ungewöhnliches, eine Vielzahl an Leistungen in mehreren Hilfefeldern anzubieten – beispielweise hält der Caritasverband der Erzdiözese München und Freising e.V. bis auf Krankenhäusern alle in der Grafik dargestellten Leistungen in 15 Landkreisen und zwei kreisfreien Städten vor (Caritasverband der Erzdiözese München und Freising e.V. o.D.a). Die Anzahl der Verhandlungspartner:innen aus dem Beispiel für die WfbM kann sich bei einem Komplexträger also schnell vervielfachen.

Eine weitere Herausforderung sind Probleme bei der Rücklagenbildung. Aus Zuschüssen können Einrichtungsträger keine Rücklagen bilden, da sie fürchten müssen, nicht verwendete Mittel

entweder zurückzahlen zu müssen oder bei der der nächsten Förderrunde entsprechend geringere Mittel bewilligt zu bekommen (Patjens 2017, 147). Bei Rücklagenbildung aus anderen Finanzierungsquellen unterliegen die meisten sozialen Unternehmen aufgrund ihrer Gemeinnützigkeit den Einschränkungen der Abgabenordnung. Viele Einrichtungsträger sind steuerbegünstigte Körperschaften laut Abgabenordnung, was im Allgemeinen als ‚gemeinnützig' bezeichnet wird (Schick 2024, 587). Dadurch sind sie von der Körperschafts- und Gewerbesteuer sowie Erbschafts- und Schenkungssteuer befreit (ebd.). Zugleich sind sie aber auch verpflichtet, alle ihre Einnahmen zeitnah, also im Jahr des Zuflusses oder spätestens in einem der beiden Folgejahre, für einen gemeinnützigen Zweck zu verwenden (ebd. 595). Auch wenn es Ausnahmeregelungen, z.B. für Projektrücklagen oder Betriebsmittelrücklagen bei unsicheren Einnahmen und sicheren Ausgaben gibt (ebd. 597f), ist die Verpflichtung zur zeitnahem Mittelverwendung der Regelfall (Koglin 2023). Dies erschwert Investitionen in eine bessere IT-Infrastruktur. Entsprechend fordert die Bank für Sozialwirtschaft eine Anpassung der Regelungen zur Rücklagenbildung im Gemeinnützigkeitsrecht, um die Digitalisierung in der Sozialwirtschaft voranzutreiben (Klemm et al. 2020, 41).

Hinzu kommen aktuelle gesamtgesellschaftliche Herausforderungen. Eine Umfrage der BAGFW im Juni 2024 unter 8297 Organisationen der freien Wohlfahrt hat ergeben, dass knapp zwei Drittel der Organisationen aufgrund von finanziellen Schwierigkeiten Angebote reduzieren oder aufgeben mussten. Mehr als drei Viertel gehen davon aus, ihre Angebote auch 2025 weiter einschränken zu müssen (Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege 2024). Immer mehr Träger müssen ihren Betrieb sogar ganz einstellen (Bingener 01.11.2024). Als Gründe geben Vertreter:innen aller Wohlfahrtsverbände Kürzungen von Sozialausgaben, steigende Personalkosten, steigende Energiekosten vor dem Hintergrund des russischen Angriffskrieg auf die Ukraine sowie rückläufige Kirchensteuern an. Dies führt nicht nur zu einer Einschränkung von Angeboten, sondern treibt immer mehr Träger der freien Wohlfahrt in die Insolvenz (vgl. Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege 2023b; Diakonie Bayern 2024; Curacon 2024; Freie Wohlfahrtspflege Bayern 2024).

Zusammengefasst erschweren die Finanzierungsstrukturen der freien Wohlfahrt Investitionen in IT-Sicherheit: Finanzielle Ressourcen für Sozialleistungen sind ohnehin knapp und die weit verteilten Zuständigkeiten führen dazu, dass die Refinanzierung von IT-Kosten vielen verschiedenen Stellen gegenüber verargumentiert werden muss. Darüber hinaus hat IT-Sicherheit mit dem Präventionsparadox zu kämpfen, d.h. Investitionen in IT-Sicherheit erbringen keine direkte

Wertschöpfung und wenn sich lange keine IT-Vorfälle ereignen, erscheinen Kosten für Sicherheitsmaßnahmen schnell als unnötig hoch. Dies macht es noch schwieriger, Finanzmittel für IT-Sicherheit einzuwerben.

3.5 IT und Digitalisierung in der freien Wohlfahrt

Digitalisierung und IT sind eng miteinander verbunden, können aber nicht gleichgesetzt werden. IT stellt ein Hilfsmittel dar, um Arbeitsprozesse technisch zu unterstützen oder vollständig zu automatisieren (vgl. Wolff 2020, 79). Digitalisierung hingegen geht darüber hinaus: Neben der Automatisierung von Prozessen beschreibt sie die Veränderung von Organisationen durch IT, die Ausbreitung neuer, disruptiver Geschäftsmodelle und einen Wandel der zwischenmenschlichen Kommunikation (Kreidenweis und Wolff 2022; vgl. Kreidenweis 2023, 812ff). Aus diesen Definitionen kann abgeleitet werden, dass Informationstechnologien die Infrastruktur sind, auf deren Grundlage Digitalisierung stattfindet. Aussagen zum Stand der Digitalisierung in einer Branche enthalten folglich auch immer Aussagen zum Stand ihrer IT-Infrastruktur, die wiederum IT-Sicherheit miteinschließt.

Digitalisierungsgrad

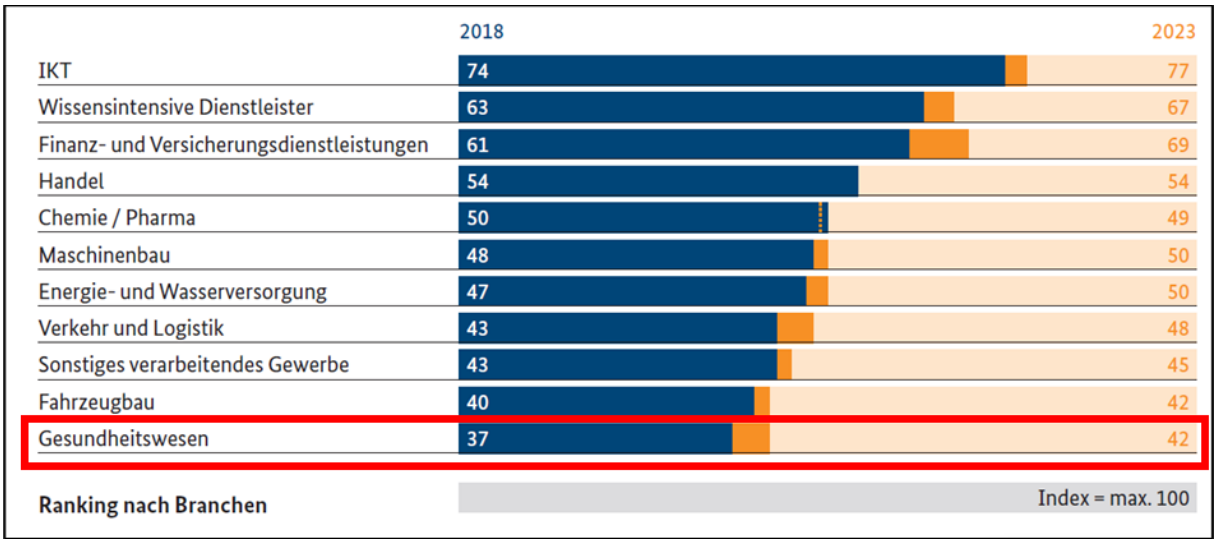

Abbildung 6: Digitalisierungsgrad der Wirtschaftszweige in Deutschland

Quelle: Weber et al. 2018, 13. Die Werte stammen aus einer Befragung des BMWi im April 2018. Die Zahlen für 2023 sind Prognosen.

Laut Bundesministerium für Wirtschaft und Energie (BMWi) ist das Gesundheitswesen unter allen deutschen Wirtschaftszweigen am schlechtesten digitalisiert: Die Branche erreicht nur 37 von 100 Punkten auf dem Digitalisierungsindex und gehört damit in die Kategorie der „Digitalen Anfänger“

(Weber et al. 2018, 12f; Wolff 2020, 78). Das BMWi zählt hierbei unter ‚Gesundheitswesen' auch stationäre soziale Betreuung wie Altenheime, Behindertenheime, Waisenhäuser, stationäre Suchthilfe u.v.m. (Weber et al. 2018, 76; Abschnitt Q). Würde man weitere Bereiche des Sozialwirtschaft (also auch ambulante Hilfen) miteinbeziehen und das klassische Gesundheitswesen herausrechnen, dürfte das Ergebnis noch schlechter ausfallen: Immerhin weist das Gesundheitswesen innerhalb der Sozialwirtschaft noch den höchsten Digitalisierungsgrad auf (Kopf 2020, 50).

IT-Kosten

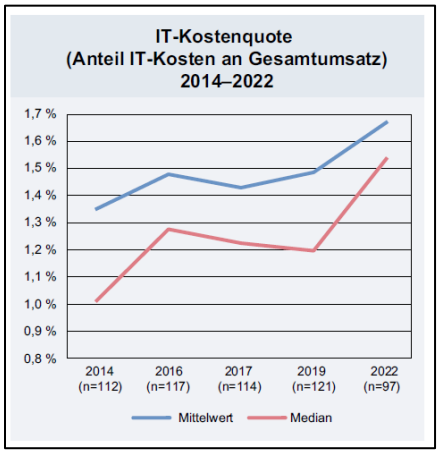

Abbildung 7: Kostenquote in der Sozialwirtschaft, 2014-2022

Quelle: Kreidenweis und Wolff 2022, 18

Tabelle 1: Vergleich durchschnittlicher IT-Kostenquoten 2022 für Sozialwirtschaft, Kliniken und die Gesamtwirtschaft

Sozial-wirtschaft	Kliniksektor	Gesamt-wirtschaft
1,66 %	3,1 %	6,8 %

Eine weitere Kennzahl, die Hinweise auf den Digitalisierungsgrad einer Organisation, bzw. ihrer IT-Durchdringung gibt, ist die Höhe des Budgets, das in die IT fließt. Eine Befragung der Bank für Sozialwirtschaft zu Digitalisierung im Jahr 2020 lässt darauf schließen, dass viele Organisationen gerne mehr in IT investieren würden, wenn sie könnten. 50,4 % der befragten Organisationen geben an, dass ihre Organisation eigentlich mehr in Prozesse und IT (z.B. Hard- und Softwareausstattung) investieren müsste (Klemm et al. 2020, 25). Als Gründe, warum Digitalisierungsinvestitionen – darunter die IT-Ausstattung – nicht erfolgt sind, nennen sie Personalmangel (79,0 % der Antwortenden), fehlende Refinanzierung durch die Kostenträger (49,1 %) und fehlende Eigenmittel (46,6 %) (ebd., 26). Dies deckt sich mit dem IT-Report für die Sozialwirtschaft 2024: Über 70 % der Organisationen sehen mangelnde Wirtschaftlichkeit und Refinanzierbarkeit von Investitionen als sehr hohes oder hohes Risiko bezogen auf Digitalisierung an (Kreidenweis und Wolff 2024, 33).

Ein Blick auf die IT-Kostenquote[2] zeigt, dass die Sozialwirtschaft deutlich weniger in IT investiert als andere Branchen. Kreidenweis und Wolff ermitteln für 2022, dass eine sozialwirtschaftliche Organisation im Mittel 1,66 % ihres Gesamtbudgets für IT aufwendet[3] (Kreidenweis und Wolff 2022, 17ff). Die Spanne reicht dabei von 0,36 % bis 4,45 %; die Tendenz ist seit 2007 stetig steigend (ebd., siehe *Abbildung 7*). Damit gibt die Sozialwirtschaft deutlich weniger für IT aus als die Gesamtwirtschaft: Der Bundesverband für IT-Anwender ermittelt für 2022 ein durchschnittliches IT-Budget von 6,8 % (VOICE - Bundesverband der IT-Anwender e. V. und metrics 2022, 5), weist jedoch darauf hin, dass dieser Wert stark zwischen verschiedenen Branchen variiert[4]. Helmut Kreidenweis zufolge eignet sich für eine Einordnung noch am ehesten der Vergleich mit dem Kliniksektor (Kreidenweis 2023, 818), für den Curacon für 2022 eine durchschnittliche IT-Kostenquote von 3,1 % errechnet (Redmann und Dessel 2022, 13).

IT-Personal

Dem Branchenverband bitkom zufolge können 2024 in Deutschland knapp 153.000 IT-Stellen nicht besetzt werden. Er prognostiziert, dass diese Lücke aufgrund des steigenden IT-Bedarfs bei gleichzeitigem Renteneintritt vieler Fachkräfte der Babyboomer-Generation bis 2040 auf knapp 663.000 wachsen wird (bitkom 2024). Diesen IT-Fachkräftemangel spüren sozialwirtschaftliche Organisationen besonders stark, da ihr limitiertes IT-Budget sie in Bezug auf Gehalt und Ausstattung weniger attraktiv für IT-Spezialist:innen macht als andere Arbeitgeber (vgl. Klemm et al. 2020, 26). 2022 empfanden von den Organisationen, die im vergangenen Jahr nach neuem IT-Personal gesucht hatten, 72 % die Suche als schwierig und nur 28 % gaben an, dass sie sich problemlos gestaltet hätte (Kreidenweis und Wolff 2022, 30). Die Probleme in der IT-Personalgewinnung hat auch Auswirkungen auf das bestehende IT-Personal: Immer weniger Mitarbeitende betreuen tendenziell immer mehr IT-Arbeitsplätze[5]:

---

[2] Die IT-Kostenquote bezeichnet den Anteil der IT-Kosten am Gesamtumsatz einer Organisation.

[3] Die durchschnittliche IT-Quote in der Sozialwirtschaft für 2023 beträgt 1,8 % (Kreidenweis und Wolff 2023, 14). Da für 2022 Vergleichswerte aus der Gesamtwirtschaft sowie dem Klinikbereich vorliegen, wird im Text der Wert von 2022 verwendet.

[4] Zudem sinken die Werte nach Ende der Coronapandemie sowie nach Ausbruch des Ukrainekriegs auf 4,2 % in 2022 und auf 3,62 % in 2024 (VOICE - Bundesverband der IT-Anwender e. V. und metrics 2023, 9; VOICE - Bundesverband der IT-Anwender e. V. und metrics 2024, 6).

[5] Kreidenweis und Wolff beobachten einen langjährigen, stetigen Trend. Den rasanten Anstieg im Jahr 2019 und entsprechend den Abfall im Jahr 2022 schreiben sie Ausreißern im Datensatz von 2019 zu.

Kennzahlen IT-Personal	2022	2019	2016	2013
Prozentsatz IT-Mitarbeitende an Gesamt-Mitarbeitendenzahl	0,6 %	0,5 %	0,7 %	0,8 %
Klassische IT-Arbeitsplätze pro IT-Mitarbeitendem (Mittelwert)	147	182	122	115
Registrierte Accounts pro IT-Mitarbeitendem (Mittelwert)	226	298	180	266

Abbildung 8: Kennzahlen IT-Personal in der Sozialwirtschaft 2022.

Quelle: Kreidenweis und Wolff 2022, 28.

Eine weiteres Indiz für die besondere Schwere des IT-Fachkräftemangels in der Sozialwirtschaft ist die Anzahl der IT-Anwender:innen, die eine IT-Fachkraft betreut. Hier liegen Vergleichswerte zur Krankenhaus-Branche vor: Während in der Sozialwirtschaft auf eine IT-Fachkraft durchschnittlich 206 (regelmäßige) IT-Anwender:innen kommen (Kreidenweis und Wolff 2022, 28), sind es in Krankenhäusern nur 135,6 Anwender:innen pro IT-Mitarbeiter:in (Redmann und Dessel 2022, 7). Interessant ist hier die Aufschlüsselung nach Trägertyp, die die Studie zusätzlich vornimmt: Bei privaten Trägern beträgt die Quote von Krankenhausmitarbeiter:innen pro IT-Mitarbeiterin 91,3 – bei freigemeinnützigen Trägern hingegen 121,7 (ebd.). Da nicht davon ausgegangen werden kann, dass private Träger über weniger IT-Nutzende (gemessen an der Gesamtbelegschaft) oder weniger IT-Personal verfügen als freie Träger, ist dies ein weiterer Hinweis sowohl auf eine verschärfte Wirkung des IT-Fachkräftemangels in der freien Wohlfahrt als auch auf die defizitären IT-Finanzierungsstrukturen.

4. Die Caritas in Deutschland als Fallbeispiel

Als Fallbeispiel für IT-Sicherheit in der freien Wohlfahrt dient in dieser Arbeit die Caritas. Mit knapp 696.000 hauptamtlichen Mitarbeitenden ist die Caritas der größte der deutschen Wohlfahrtsverbände und stellt somit einen repräsentativen Fall dar. Zudem hat die Autorin dieser Arbeit von Oktober 2021 bis September 2023 für den Diözesancaritasverband der Erzdiözese München und Freising e. V. gearbeitet und den Cyberangriff auf den Verband im September 2022 miterlebt. Zum Entstehungszeitpunkt dieser Arbeit ist sie für den Caritas-Netzwerk IT e. V. tätig, ein Verein, in dem etwa 150 Caritasorganisationen Mitglied sind (Stand: März 2025). Damit bietet sich die Caritas auch deswegen als Untersuchungsobjekt an, weil die Autorin auf ein persönliches Netzwerk an

Interviewpartner:innen zugreifen kann, die für andere Wissenschaftler:innen schwerer zu erreichen wären.

4.1 Struktur der Caritas

Unter der Caritas in Deutschland wird in dieser Arbeit die Gesamtheit aller Einrichtungen, Dienste, Unternehmen, Vereinigungen, und Verbände verstanden, die unter dem Dach des Deutschen Caritasverbandes (DCV) zusammengeschlossen sind. Insgesamt gehören knapp 6.200 eigenständige Rechtsträger zur Caritas (Panjas 2020), die 24.952 Einrichtungen mit 1.068.243 Betten und Plätzen betreiben (Deutscher Caritasverband 2023b). 71 % der Rechtsträger beschäftigen weniger als 50 Mitarbeitende (siehe *Tabelle 2*). Dagegen haben nur 0,4% der Rechtsträger mehr als 3.000 Mitarbeitende – diese machen jedoch fast 13 Prozent aller Caritasmitarbeitenden aus.

Tabelle 2: Größenstruktur der Caritas-Rechtsträger

Anzahl Mitarbeitende	Anteil Träger	Anteil Mitarbeitende (Köpfe)
bis 50	71,2 %	9 %
51 bis 250	19,8 %	18 %
251 bis 1.000	6,3 %	27 %
1.001 bis 3.000	2,2 %	29 %
Ab 3.001	0,4 %	17 %

Quelle: Auf Anfrage vom Referat „Sozialwirtschaft und Klimaneutralität“ des DCV erhalten; Stichtag der Erhebung: 31.12.2022.

Bezüglich IT-Sicherheit hat die Größe der Rechtsträger mehrere Auswirkungen. Zum einen gibt es einen statistisch signifikanten Zusammenhang zwischen der Unternehmensgröße und der Prävalenzrate von Cyberangriffen: Unternehmen unter 50 Mitarbeitenden haben signifikant kleinere Prävalenzraten als größere, und Unternehmen mit mehr als 500 Mitarbeitende eine signifikant größere Prävalenzrate (vgl. Dreißigacker et al. 2020, 31f, 102). Gleichzeitig haben Organisationen abhängig von ihrer Größe verschiedene Möglichkeiten sowie Herausforderungen, was ihre Verhandlungsstärke gegenüber Dienstleistern, die Komplexität ihrer Systemlandschaften und den Spezialisierungsgrad ihrer Mitarbeitenden betrifft. So investieren kleinere Träger anteilig an ihrem Umsatz

weniger in Digitalisierung und damit auch weniger in den Ausbau ihrer IT-Infrastruktur (Klemm et al. 2020, 35–37). Eine schlechter ausgebaute IT-Infrastruktur ist wiederum anfälliger für IT-Sicherheitsvorfälle. Zudem sind IT-Mitarbeitende in kleinen Organisationen weniger spezialisiert als in großen (Kreidenweis und Wolff 2022, 29f), was die Vermutung nahelegt, dass größere Träger eher eine IT-Sicherheitsfachkraft haben als kleinere.

Organisiert ist die Caritas in Diözesanverbände, Fachverbände, Vereinigungen und karitative Ordensgemeinschaften (siehe *Abbildung 9*). Durch die sogenannte „weitergereichte Mitgliedschaft" sind Mitglieder eines Mitgliedverbands automatisch auch Mitglied im DCV (Deutscher Caritasverband o.D.d).

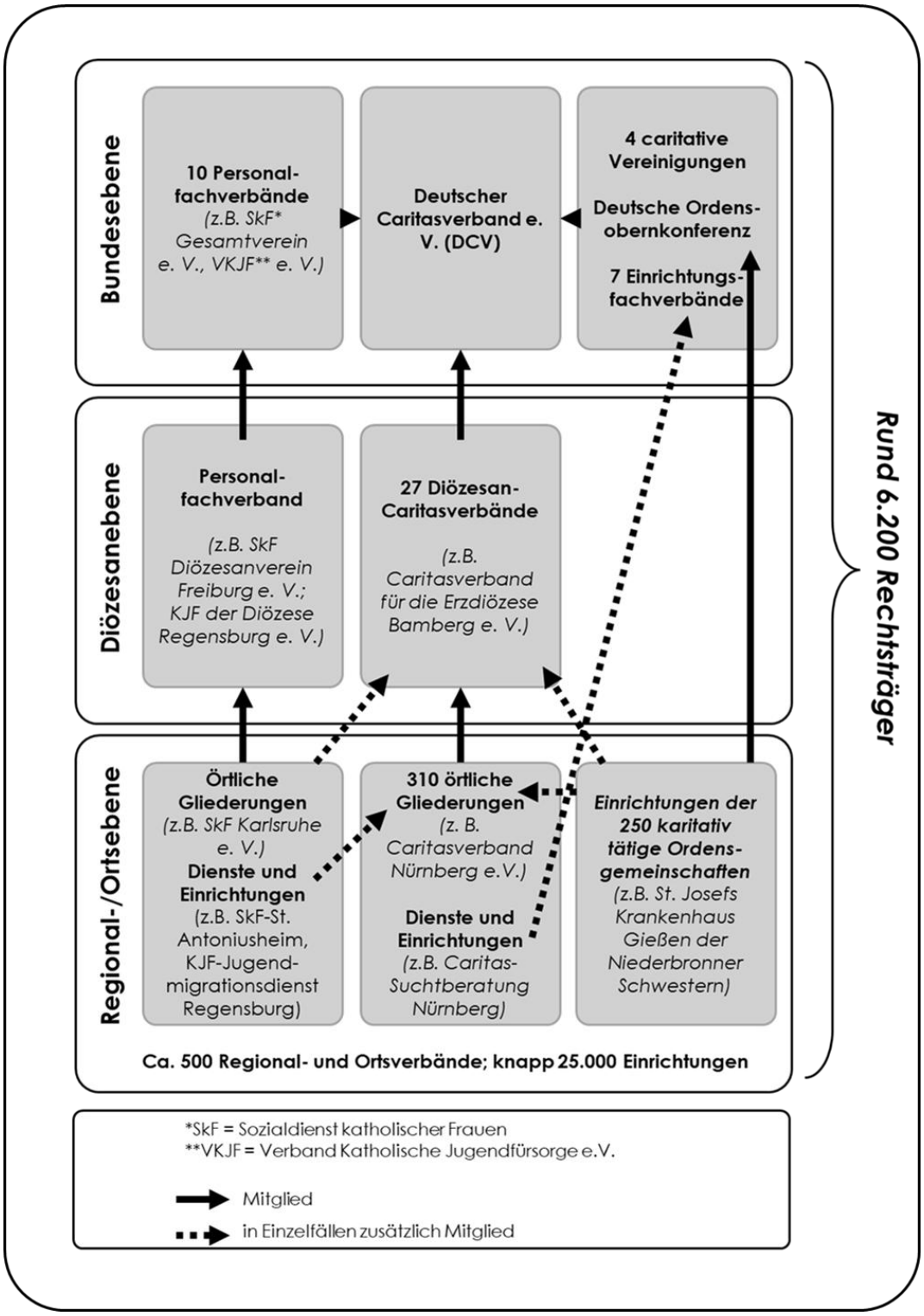

Abbildung 9: Struktur der Caritas in Deutschland

Eigene Abbildung, angelehnt an Deutscher Caritasverband 2023b, 25.

Diözesan-Caritasverbände

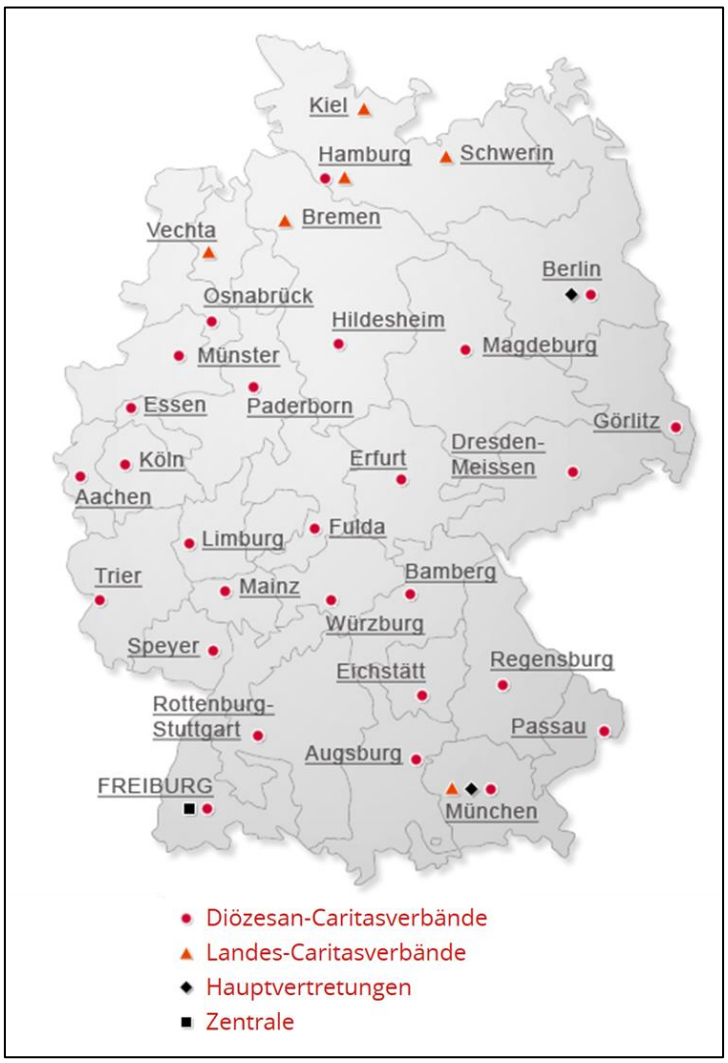

Abbildung 10: Karte der Diözesan-Caritasverbände

Quelle: Deutscher Caritasverband o.D.b.

Die Diözesan-Caritasverbände (DiCV) sind territorial den 27 Diözesen (auch: Bistümern) der katholischem Kirche in Deutschland zugeordnet (siehe *Abbildung 10*) (Schroeder 2017, 52; Deutscher Caritasverband o.D.a). Diese sind größtenteils nicht deckungsgleich mit den Grenzen der Bundesländer, sondern ihr Zuschnitt entspringt historischen Grenzen. Sie können in Dekanats-, Bezirks- Kreis- oder Ortscaritasverbände untergliedert sein, die wiederum nicht zwangsläufig mit den Grenzen von Landkreisen und Kommunen übereinstimmen (Deutscher Caritasverband o.D.a; Schmeja et al. 2023). Wie die einzelnen Diözesanverbände strukturiert sind und welche Aufgaben sie wahrnehmen, variiert von Verband zu Verband. So agiert beispielsweise der DiCV Münster als

Spitzenverband der 25 Dekanats-, Kreis- und Ortsverbände, sowie der Verbände des Sozialdiensts katholischer Frauen (SkF) und des Sozialdiensts Katholischer Männer (SKM) im Bistum Münster (Caritasverband für die Diözese Münster e. V. o.D.). Im DiCV München-Freising hingegen gibt es keine rechtlich eigenständigen Regional- oder Ortsverbände, sondern der Diözesanverband betreibt selbst als Einrichtungsträger über 350 Einrichtungen (Caritasverband der Erzdiözese München und Freising e.V. o.D.a). Gleichzeitig ist er Spitzenverband für etwa 100 katholische Fachverbände und angeschlossene Träger (Caritasverband der Erzdiözese München und Freising e.V. o.D.b). Im DiCV Stuttgart-Rottenburg wiederum gibt es neun rechtlich unselbständige Regionen, für deren Einrichtungen der DiCV als Träger fungiert, sowie den rechtlich eigenständigen Caritasverband für Stuttgart e. V., zahlreiche Fachverbände, karitative Ordensgemeinschaften und angeschlossene Träger (alles sogenannte ‚korporative Mitglieder'), die der DiCV spitzenverbandlich vertritt (Caritasverband der Diözese Rottenburg-Stuttgart e. V. o.D.a; Caritasverband der Diözese Rottenburg-Stuttgart e. V. o.D.b). Zu vielen der angeschlossenen Trägern gehören Einrichtungen, die der DiCV früher selbst betrieben und seit den frühen 2000er Jahren im Zuge einer Neustrukturierung an andere kirchliche Träger abgegeben hat (Caritasverband der Diözese Rottenburg-Stuttgart e. V. o.D.a).

Personalfachverbände

Personalfachverbände betreiben Sozialarbeit und stationäre Hilfen für bestimmte Personengruppen und Schwerpunktthemen (Deutscher Caritasverband o.D.c). Neben den Dachverbänden auf Bundesebene und den Gliederungen sowie Einrichtungen auf Ortsebene kann es Diözesanverbände geben. Verbände und Einrichtungen auf Ortsebene können sich zudem einem Diözesan-Caritasverband zur politischen Interessenvertretung anschließen. Insgesamt gibt es zehn Personalfachverbände:

- Caritaskonferenzen Deutschland (CKD)
- Familien-Ferien-Werk
- IN VIA – Verband für Mädchen- und Frauensozialarbeit - Deutschland
- Verband Katholische Jugendfürsorge e. V. (VKJF)
- Kreuzbund
- Malteser Hilfsdienst
- Raphaelswerk
- Sozialdienst katholischer Frauen (SkF)
- SKM Bundesverband
- Gemeinschaft der Vinzenz-Konferenzen Deutschlands (VKD)

Einrichtungsfachverbände

Die sieben Einrichtungsfachverbände betreiben für Einrichtungen gleicher Fachrichtung politische Lobbyarbeit auf Bundesebene (Deutscher Caritasverband o.D.c). Dabei spielt es keine Rolle, zu welchem Träger innerhalb der Caritas eine Einrichtung gehört und welchen anderen Spitzenverbänden sie bereits angeschlossen ist. Die Einrichtungsfachverbände sind:

- Bundesverband Caritas Kinder- und Jugendhilfe e. V. (BVkE)
- Bundesverband Caritas Behindertenhilfe und Psychiatrie (CBP)
- Caritas-Bundesverband Kinder- und Jugendreha (CKR)
- Katholischer Arbeitskreis für Familienerholung (KAFE)
- Katholischer Krankenhausverband Deutschland (KKVD)
- Verband Katholischer Tageseinrichtungen für Kinder (KTK)
- Verband katholischer Altenhilfe in Deutschland (VKAD)

Vereinigungen

Vereinigungen sind Interessensvertretungen natürlicher Personen aus katholischen, karitativ tätigen Organisationen (Deutscher Caritasverband o.D.f). Sie existieren lediglich auf Bundesebene und verfügen über keine regionalen Gliederungen. Folgende vier Vereinigungen gehören dem DCV an:

- Fraternität der Menschen mit Behinderung in Deutschland
- Katholischer Pflegeverband e. V.
- Katholische Arbeitsgemeinschaft für Soldatenbetreuung e. V. (KAS)
- "Selbsthilfe" Pensionskasse der Caritas VVaG

Ordensgemeinschaften

Zum Deutschen Caritasverband gehören etwa 250 karitativ tätige Ordensgemeinschaften, die überdiözesan tätig sind (Deutscher Caritasverband o.D.e). Auf Bundesebene werden sie durch die Deutsche Ordensobernkonferenz vertreten. Einzelne Ordensgemeinschaften, von ihnen betriebene Trägergesellschaften oder Einrichtungen können Diözesan-Caritasverbänden zur spitzenverbandlichen Interessensvertretung auf Orts- oder Diözesanebene, sowie Einrichtungsfachverbänden beitreten. So wird beispielsweise das *St. Josefs Krankenhaus Balserische Stiftung* in Gießen von einer Trägergesellschaft der *Kongregation der Schwestern vom Göttlichen Erlöser (Niederbronner Schwestern)* betrieben (Kongregation der Schwestern vom Göttlichen Erlöser o.D; gTrägergesellschaft mbH für die Einrichtungen der Schwestern vom Göttlichen Erlöser o.D.). Während die Trägergesellschaft ihren

Sitz im Bistum Eichstätt hat, ist die Ordensgemeinschaft im Bistum Bamberg angesiedelt. Das Krankenhaus selbst ist jedoch korporatives Mitglied beim Caritasverband Gießen e. V., der wiederum vom DiCV Mainz spitzenverbandlich vertreten wird (Caritasverband Gießen e.V. o.D; Caritasverband für die Diözese Mainz e. V. o.D.). Zudem ist es Mitglied im Einrichtungsfachverband *Katholischer Krankenhausverband Deutschland (KKVD*) (Katholischer Krankenhausverband Deutschland e. V. o. D.). Dieses Beispiel verdeutlicht: Adressaten für das Thema IT-Sicherheit im St. Josefs Krankenhaus können das Krankenhaus selbst, der Caritasverband Gießen, der Diözesancaritasverband Mainz, der Katholische Krankenhausverband Deutschland, die Deutsche Ordensobernkonferenz und der Deutsche Caritasverband sein. In diesem Fall könnten auch noch die Hessen-Caritas (i.e. die Arbeitsgemeinschaft der drei hessischen Diözesan-Caritasverbände, siehe *Tabelle 7* in *Anhang 2: Zusammenschlüsse von DiCVs auf Bundeslandebene*) miteinbezogen werden, sowie die überverbandlichen Arbeitsgemeinschaften der sechs Spitzenverbände, also die BAGFW auf Bundesebene und die Liga der freien Wohlfahrtspflege in Hessen e.V. auf Landesebene.

4.2 Politische Interessensvertretung auf Landesebene

Dadurch, dass die Diözesangrenzen nicht mit politischen Grenzen übereinstimmen, haben die Verbände auf DiCV-Ebene mit unterschiedlichen Landesgesetzgebungen und politischen Ansprechpartner:innen zu tun (Schmeja et al. 2023, 116). Andersherum können sich auch innerhalb eines Bundeslandes mehrere Diözesen befinden. Beispielsweise erstreckt sich das Erzbistum Köln über die beiden Bundesländer Nordrhein-Westfalen und Rheinland-Pfalz. In letzterem befinden sich wiederum gleich fünf Bistümer: Köln, Limburg, Mainz, Speyer und Trier. Für die überverbandliche Interessensvertretung gegenüber den Landesregierungen existieren – wie bereits angesprochen – die Landesarbeitsgemeinschaften der sechs Spitzenverbände der freien Wohlfahrt (siehe *Anhang 1: Liste der Landesarbeitsgemeinschaften der freien Wohlfahrt* inklusive einer Auflistung der jeweiligen Caritas-Mitglieder). Zusätzlich schließen sich Caritasverbände in vielen Bundesländern auch untereinander zu Verbänden und Arbeitsgemeinschaften zusammen. Wie diese ausgestaltet sind, d.h. welche Rechte und Aufgaben sie haben, ist von Zusammenschluss zu Zusammenschluss unterschiedlich (siehe *Anhang 2: Zusammenschlüsse von DiCVs auf Bundeslandebene*).

5. IT-Sicherheit

5.1 Definitionen

IT-Sicherheit bezeichnet die Sicherheit von Daten und Informationen, die von elektronischen Systemen verarbeitet werden, sowie die Sicherheit der Systeme, die diese Verarbeitung durchführen (Faber 2021, 15). Damit hat sie zum Ziel, die Werte (englisch: assets) einer Organisation zu schützen. Unter Werten wird alles zusammengefasst, was für das Überleben einer Organisation essentiell ist, etwa die Gesundheit der Mitarbeitenden und Klient:innen, Wissen, Gegenstände und Vermögen (vgl. Eckert 2023, 1; Bundesamt für Sicherheit in der Informationstechnik 2023b, 43; Faber 2021, 10f). In der Literatur werden häufig drei **Schutzziele** genannt: Vertraulichkeit, Integrität und Verfügbarkeit von Daten bzw. Informationen. Wegen der Anfangsbuschstaben der englischen Begriffe für diese Ziele (confidentiality, integrity, availability) wird hier von der CIA-Triade gesprochen (Bundesamt für Sicherheit in der Informationstechnik 2023b, 37; Eckert 2023, 8; Faber 2021, 12 und 16). Vertraulichkeit bedeutet, dass Unbefugte keinen Zugriff auf Daten und Informationen haben. Integrität heißt, dass Daten und Informationen nicht unberechtigt oder unbemerkt geändert oder manipuliert werden können. Verfügbarkeit bezieht sich darauf, dass Personen oder Systeme auf Informationen und Anwendungen unbeeinträchtigt zugreifen können, sofern sie über die entsprechenden Berechtigungen verfügen (vgl. Bundesamt für Sicherheit in der Informationstechnik 2023b, 38 und 42; Eckert 2023, 9, 10 und 12; Faber 2021, 11). Während sich der Begriff IT-Sicherheit auf die Systeme einer Organisation beschränkt, nimmt **Cyber-Sicherheit** den gesamten Cyber-Raum in den Blick, also das Internet und alle miteinander vernetzten Systeme (vgl. Bundesamt für Sicherheit in der Informationstechnik 2023b, 36; Faber 2021, 16; Eckert 2023, VI).

Bedrohungen (englisch: threats) im Kontext von IT- und Cybersicherheit zielen darauf ab, die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten oder Informationen zu beeinträchtigen, indem sie Schwachstellen in IT-Systemen ausnutzen (vgl. Bundesamt für Sicherheit in der Informationstechnik 2023b, 36; Eckert 2023, 18; Faber 2021, 13). Als Beispiele für Bedrohungen listet das Bundesamt für Sicherheit in der Informationstechnik (BSI) im IT-Grundschutzkompendium „höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen" (Bundesamt für Sicherheit in der Informationstechnik 2013, 36). Diese Arbeit fokussiert auf vorsätzliche Handlungen, die auch als **(Cyber-)Angriffe oder (Cyber**-)Attacken bezeichnet werden (ebd. 35). Als besonders prominente Angriffsarten nennt das BSI unter anderem Ransomware,

Advanced Persistent Threats (APT), Distributed Denial of Service (DDoS) und Phishing (Bundesamt für Sicherheit in der Informationstechnik 2023a, 14). Bei Ransomware-Angriffen wird Schadsoftware (englisch: malware) auf die IT-Systeme eingeschleust, die dann die Daten verschlüsselt. Für die Herausgabe des Entschlüsselungscodes versuchen die Angreifer ein Lösegeld (ransom) zu erpressen, meist in Kryptowährung (vgl. z.B. Eckert 2023, 25f). Oft drohen die Erpresser zugleich mit der Veröffentlichung von gestohlenen Daten, was als ‚double extortion' bezeichnet wird (Bundesamt für Sicherheit in der Informationstechnik 2023a, 14). Advanced Persistent Threats (APT) finden nicht wahllos auf Organisationen statt, bei denen sich zufällig gerade Sicherheitslücken auftun, sondern werden von einem gut ausgerüsteten, häufig staatlich gesteuerten Akteur auf ein bewusst ausgewähltes Ziel ausgeführt (Bundesamt für Sicherheit in der Informationstechnik 2023a, 25; Bundesamt für Sicherheit in der Informationstechnik o.D.). Sie werden aufwändig und langfristig geplant und dienen nicht – oder nicht nur – der Erpressung von Geld, sondern dem Erlangen von Informationen (Spionage) und der Sabotage von kritischen Infrastrukturen sowie von Informationssystemen (Buzatu 2022). Bei einem Distributed Denial-of-Service-Angriff (DDoS) wird eine große Anzahl von Anfragen gleichzeitig von mehreren, oft weltweit verteilten Computern an einen Server gesendet. Durch die Flut an Anfragen ist der Server überlastet und Websites oder andere Internetdienste, die auf dem Server gehostet werden, sind nicht mehr erreichbar (Bundesamt für Sicherheit in der Informationstechnik 2023a, 28). Bei Phishing zielen Kriminelle darauf ab, Personen dazu zu bringen, sensible Daten wie Zugangsdaten zu organisationsinternen IT-Systemen oder Bankzugangsdaten preiszugeben. Dies geschieht meistens über gefälschte E-Mails oder Webseiten, kann aber auch über SMS oder andere Kurznachrichtendienste und Telefonanrufe geschehen (vgl. Bundesamt für Sicherheit in der Informationstechnik 2023a, 31; National Institute of Standards and Technology o.D.).

5.2 Aktuelle Gesetzeslage

Informationssicherheit ist in Deutschland nicht in einem einzigen Gesetz geregelt sondert verteilt sich auf mehrere informationssicherheitsspezifische sowie wie sektorspezifische Gesetze. Das wichtigste Gesetz ist das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG), das die Aufgaben, Rechte und Pflichten des BSI sowie die informationssicherheitstechnischen Pflichten der betroffenen Einrichtungen festlegt. Das BSI-Gesetz wurde seit seinem Inkrafttreten im August 2009 mehrfach geändert, insbesondere 2015 durch das IT-

Sicherheitsgesetz 1.0[6], 2017 durch das NIS-RL-Umsetzungsgesetz[7] und 2021 durch das IT-Sicherheitsgesetz 2.0[8]. Die jüngste und bisher größte Änderung war für Anfange 2025 durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)[9] geplant, das die NIS-2-Richtlinie der EU[10] in deutsches Recht umsetzt. Aufgrund der vorgezogenen Neuwahlen im Februar 2025 wurde es jedoch zum Zeitpunkt dieser Arbeit noch nicht verabschiedet. Im Kern weitet NIS2 den bisherigen Anwendungsbereich der IT-Sicherheitsvorgaben signifikant aus, und verschärft sowie erweitert die Pflichten der betroffenen Einrichtungen (vgl. Voigt und Schmalenberger 2023, 717). Bisher galten diese vor allem für sogenannte kritische Infrastrukturen (Kritis), i.e. Einrichtungen und Anlagen der Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung, die eine hohe Bedeutung für das Funktionieren des Gemeinwesens haben (§ 2 Abs. 10 BSIG in der Fassung vom 23.6.2021). Ab wann eine Einrichtung oder Anlage zu Kritis zählte, ist in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) mit branchenspezifischen Schwellwerten geregelt. Krankenhäuser etwa fielen ab 30.000 vollstationären Fällen pro Jahr darunter (§ 6 Abs. 1 S. 1 BSI-KritisV und Anhang 5 Teil 3 BSI-KritisV).

Mit dem NIS2UmsuCG wird nicht mehr von kritischen Infrastrukturen, sondern von ‚kritischen Anlagen' und ‚kritischen Dienstleistungen' gesprochen (§ 2 Abs. 22 und 24 im geplanten BSIG laut Referentenentwurf; im Folgenden als „BSGI Neu" bezeichnet). Kritische Dienstleistungen werden hierbei neben den bereits genannten Sektoren auch in den Sektoren ‚Weltraum' und ‚Sozialversicherungsträgern sowie der Grundsicherung für Arbeitssuchende' erbracht (§ 2 Abs. 24 BSIG Neu). NIS2 führt außerdem neue grundlegende Kategorien für betroffene Einrichtungen ein: Es unterscheidet zwischen *besonders wichtigen* und *wichtigen Einrichtungen*. Besonders wichtige Einrichtungen

[6] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

[7] 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

[8] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

[9] NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

[10] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

sind unter anderem Betreiber kritische Anlagen, sowie Unternehmen aus in Anlage 1 BSIG Neu aufgeführten Sektoren, die mindestens 250 Mitarbeitende beschäftigen oder einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen ausweisen (§ 28 Abs. 1 BSIG Neu). Wichtige Einrichtungen sind unter anderem Unternehmen, die Sektoren angehören, die in Anlage 1 und 2 BSIG Neu gelistet sind, und die mindestens 50 Mitarbeitende beschäftigen oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro erbringen (§ 28 Abs. 2 BSIG Neu).

Diese Unternehmen sind verpflichtet, „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen […] zu ergreifen", die dem „Stand der Technik" entsprechen (§ 30 Abs. 1 und 2 BSIG Neu). Diese Risikomanagementmaßnahmen umfassen zum Beispiel Konzepte zur Risikoanalyse und Notfallmanagement, den Einsatz von Multifaktor-Authentifizierung und IT-Sicherheitsschulungen (§ 30 Abs. 2 BSIG Neu). Die Einrichtungen sind außerdem verpflichtet, sich bei einer gemeinsamen Meldestelle des BSI und des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe zu registrieren. Zudem müssen sie bei ‚erheblichen' Sicherheitsvorfällen mehrere Meldungen an ebendiese Meldestelle abgeben (§ 32 Abs. 2 BSIG Neu).

Eine weitere große Neuerung, die NIS2 einführt, ist die Geschäftsleitungshaftung. Verantwortlich für die Umsetzung der Risikomanagementmaßnahmen sowie deren Überwachung sind die Geschäftsleitungen. Diese haften bei schuldhaft verursachtem Schaden und sind verpflichtet, regelmäßig an Schulungen teilzunehmen (§ 39 Abs. 2 BSIG Neu). Zudem gelten nun deutlich höhere Bußgelder. Je nach Ordnungswidrigkeit, Jahresumsatz sowie danach, ob eine Einrichtung wichtig oder besonders wichtig ist, können diese bis zu 10 Millionen Euro, oder bei einem Jahresumsatz von mehr als 500 Millionen Euro bis zu 2 % des Jahresumsatzes betragen (§ 65 Abs. 2 BSIG Neu).

In der freien Wohlfahrt betrifft NIS2 – wie schon die vorherige Rechtsprechung – vor allem Krankenhäuser, mit den neuen Regelungen jedoch mehrere als zuvor und mit umfassenderen Pflichten. Pflegeeinrichtungen fallen nach § Anlage 1, Nr. 4.1.1. BSIG Neu mit Bezugnahme auf Art. 1 Abs. 3 lit. A RL 2011/24/EU[11] weiterhin nicht unter die Regelungen. Prinzipiell können auch Einrichtungen betroffen sein, in denen Dienstleistungen in anerkannten Heilberufen erbracht werden,

[11] Richtlinie (EU) 2011/24 des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45)

etwa Reha-Einrichtungen oder interdisziplinäre Frühförderzentren. Für die Schwellenwerte gelten jedoch nur die konkreten Mitarbeitenden und Umsätze, die dem entsprechenden Geschäftsbereich einer Einrichtung zuzuordnen sind und nicht die Gesamtwerte eines Trägers. Ein fiktives Beispiel: Beschäftigt ein Komplexträger mit 1.000 Mitarbeitenden und einer Jahresbilanz von 20 Millionen Euro als einzige Angehörige eines Heilberufs fünf Logopäd:innen und drei Physiotherapeut:innen in einem Frühförderzentrum, fällt nicht automatisch der ganze Träger unter NIS2, sondern es wird nur das spezifische Frühförderzentrum betrachtet, das in diesem Beispiel unter den Schwellwerten bleibt (vgl. Paritätischer Gesamtverband 2024, 5f).

Vor dem Hintergrund der bereits dargestellten Probleme mit der IT-Infrastruktur und der Finanzierung der freien Wohlfahrt hätten viele Organisationen große Schwierigkeiten, den umfangreichen Pflichten zum Risikomanagement nachzukommen, wenn die IT-Sicherheitsgesetze für sie griffen. Ebenso würden aufgrund der ohnehin schwierigen Finanzsituation die hohen Bußgelder zu einem Problem. Auch die Geschäftsführerhaftung hätte negative Konsequenzen, da es bereits jetzt vielen Verbänden zunehmend schwerfällt, Vorstands- und Geschäftsführungsposten nachzubesetzen.

5.3 Allgemeiner Anstieg an Cyberbedrohungen

Das im Januar 2024 veröffentliche Risikobarometer der Allianz zeigt, dass deutsche Unternehmen Cybervorfälle wie Cyberkriminalität, IT-Unterbrechungen, Ransomware-Angriffe oder Datenlecks als größtes Geschäftsrisiko ansehen (Allianz Commercial 2024). Die Einschätzung der Unternehmen ist nicht unbegründet: Laut dem IT-Branchenverband bitkom entstand der deutschen Wirtschaft 2023 durch Cyberattacken ein Schaden von 148 Milliarden Euro – ein Anstieg von 15,6 % verglichen mit 2022 (bitkom 2023). Auch die entsprechenden Behörden auf europäischer und Bundesebene attestieren die steigende Gefahr im Cyberraum. Die Agentur der Europäischen Union für Cybersicherheit ENISA verzeichnet für Juli 2022, dem Beginn der Berichtsperiode des Berichts für 2023, etwa 120 Vorfälle – zum Ende des beobachteten Zeitraums im Juni 2023 waren es bereits über 600 (European Union Agency for Cybersecurity 2023, 12). Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Zeitraum vom 1. Juni 2022 bis 30. Juni 2023 für Deutschland fest, dass „die Bedrohung im Cyberraum […] so hoch [ist] wie nie zuvor“ (Bundesamt für Sicherheit in der Informationstechnik 2023a, 11). Insbesondere dokumentiert das BSI einen Anstieg von rund 24 % an Schwachstellen im Vergleich zum vorherigen Berichtszeitraum: Pro Tag

wurden 2022/23 durchschnittlich 68 neue Software-Schwachstellen registriert, rund 15 % davon waren kritisch (ebd., 11f). Durchschnittlich wurden täglich 250.000 neue Schadsoftware-Varianten bekannt und pro Tag 21.000 durch Botnetze infizierte Systeme vom BSI an die betroffenen Provider gemeldet (ebd., 13). Die größte Gefahr geht sowohl auf europäischer als auch auf deutscher Ebene von Ransomware aus. ENISA schlüsselt dabei auf, dass 13 % dieser Angriffe auf den Gesundheitssektor und 11 % auf die öffentliche Verwaltung entfallen sind (European Union Agency for Cybersecurity 2023, 14). Das BSI stellt heraus, dass von 118 Angriffen 27 auf Kommunalverwaltungen und kommunale Betriebe und zwölf auf Bildungs- und Forschungseinrichtungen getätigt wurden (Bundesamt für Sicherheit in der Informationstechnik 2023a, 49). Diese Zahlen zeigen, dass es längst nicht mehr nur große Wirtschaftsunternehmen sind, die Opfer von Cyberkriminalität werden, sondern eben auch Einrichtungen, die öffentliche Güter bereitstellen. Angreifer scheinen erkannt zu haben, dass es durchaus lukrativ sein und weniger Aufwand bedeuten kann, anstatt ein großes Unternehmen mit guter IT-Infrastruktur anzugreifen, zahlreiche kleine mit schlechten Sicherheitsmaßnahmen ins Visier zu nehmen:

> Cyberkriminelle Angreifer gingen im Berichtszeitraum zunehmend den Weg des geringsten Widerstands und wählten verstärkt solche Opfer aus, die ihnen leicht angreifbar erscheinen. Nicht mehr die Maximierung des potenziellen Lösegelds stand im Vordergrund, sondern das rationale Kosten-Nutzen-Kalkül. So wurden vermehrt kleine und mittlere Unternehmen sowie Behörden der Landes- und Kommunalverwaltungen, wissenschaftliche Einrichtungen sowie Schulen und Hochschulen Opfer von Ransomware-Angriffen. (Bundesamt für Sicherheit in der Informationstechnik 2023a, 11)

Insbesondere schlecht gegen Cybergefahren gerüstete Organisationen sehen sich zwei weiteren Trends gegenüber, die sie noch angreifbarer machen: Die Professionalisierung der cyberkriminellen Schattenwirtschaft sowie der zunehmende Einsatz von künstlicher Intelligenz. Beide Behörden, ENISA wie das BSI, beobachten eine deutliche Professionalisierung des Cybercrime-Sektors durch Cyber-Crime-as-a-Service-Modelle (CCaaS). Dabei spezialisieren sich kriminelle Akteure auf bestimmte Angriffswerkzeuge, die sie entweder als Produkt (in Form von Code) oder als Dienstleistung im Darknet anbieten. Durch die Spezialisierung der Werkzeuge steigert sich deren Effektivität und dadurch, dass sie von vielen Angreifern gleichzeitig genutzt werden können, deren Verbreitung. Zudem senkt es die Bandbreite und Tiefe an Fähigkeiten, die ein:e Angreifer:in mitbringen muss – er oder sie kann sich diese Fähigkeiten einfach einkaufen. Dies führt wiederum zu einem Anstieg an Akteur:innen (vgl. Bundesamt für Sicherheit in der Informationstechnik 2023a, 16–18).

Dieses Phänomen wird durch die rasante Weiterentwicklung großer KI-Sprachmodelle (Large Language Models, LLMs) noch weiter befeuert (vgl. ebd., 41-44). LLMs können Spam- und Phishing-Mails schreiben, die keine sprachlichen Fehler mehr enthalten und folglich schlechter erkannt werden. Zudem können sie im Internet und in Code nach Schwachstellen suchen und eine entsprechende Strategie zur Ausnutzung (Exploit) entwickeln. Auch deshalb wird es künftig immer einfacher werden, Cyberangriffe zu starten:

> Insbesondere die Codegenerierung dürfte die Zugangsvoraussetzungen zu cyberkriminellen Aktivitäten wie zumindest rudimentäre Programmier- und Systemkenntnisse deutlich senken. Die Zahl der Personen mit krimineller Energie, die zum Erzeugen von Schadprogrammen fähig sind, wird durch diese geringeren fachlichen Anforderungen vermutlich steigen. (Bundesamt für Sicherheit in der Informationstechnik 2023a, 44)

5.4 Anstieg an Cyberbedrohungen auf die Sozialwirtschaft

Wie in Kapitel 5.1 dargestellt, unterliegen weite Teile der freien Wohlfahrt in Deutschland keiner Meldepflicht bei IT-Sicherheitsvorfällen. Entsprechend ist die Datenlage außerhalb des Krankenhaussektors ausgesprochen dünn. Eine Befragung unter 381 sozialwirtschaftlichen Organisationen in der Schweiz im Juni 2022 hat ergeben, dass 62,2 % von ihnen in den zurückliegenden zwölf Monaten mindestens einmal einen Cyberangriff erlebt hatten und damit einem ähnlich hohen Risiko ausgesetzt waren wie Wirtschaftsunternehmen (Baier et al. 2022). Für die Sozialwirtschaft in Deutschland liegt bisher keine ähnliche Befragung vor. Jedoch listet der Fachverband Informationstechnologie in Sozialwirtschaft und Sozialverwaltung e. V. (FINSOZ) 2022 in einem Lagebericht zu Cyberkriminalität im Sozialbereich acht anonyme Fälle von Datenschutz- und Sicherheitsvorfällen aus dem Kreis ihrer Mitglieder sowie sieben öffentlich bekannte Vorfälle im Gesundheits- und Sozialwesen (FINSOZ e. V. - Fachgruppe IT-Compliance 2022). Eine eigene Internetrecherche[12] nach öffentlich bekanntgewordenen Fällen deutet darauf hin, dass die Sozialwirtschaft demselben Trend unterliegt, den ENISA und das BSI für die Gesamtwirtschaft beobachten, nämlich dass Cyberangriffe ab 2022 deutlich zugenommen haben:

[12] Durchgeführt zwischen dem 22.02.2024 und dem 20.03.2025. Aus der Suche ausgeschlossen waren reine Krankenhausträger.

Tabelle 3: Cyberangriffe auf sozialwirtschaftliche Organisationen

Datum	Opfer	Details	Fundstelle
2016[13]	Caritas Paderborn	Einschleusung eines Verschlüsselungstrojaners über eine Massen-Phishing-Mail; einige wenige Stunden kein Zugriff auf Pflegedokumentation; Selektive Rücksicherung von einzelnen Dateien innerhalb von zwölf Stunden.	Fehler melden, statt zu vertuschen (caritas-nrw.de)
Februar 2018	Diakonie Mark-Ruhr	Unbefugter Zugriff auf Server; durch Unterbrechung des Zugriffs auf die Server kam es zu Beeinträchtigungen in der ambulanten Pflege.	Cyberangriff auf Diakonie Mark-Ruhr | Diakonie Mark-Ruhr (diakonie-mark-ruhr.de)
Juli 2019	DRK Rheinland-Pfalz	Verschlüsselung von Servern durch Schadsoftware; elf Krankenhäuser und vier Altenpflegeheime betroffen; Pflegedokumentation nur noch auf Papier möglich.	Rheinland-Pfalz und Saarland: Hackerangriff auf Krankenhäuser - DER SPIEGEL
September 2021	Olchinger Sozialdienst	Ransomware-Angriff; Lösegeldforderung von 10.000 USD, ambulante Pflege und Kindertagestätten betroffen.	Cyber-Attacke auf Sozialdienst: Hacker sperren Daten und fordern Lösegeld - Auswirkungen dramatisch (merkur.de), Cyberkriminalität - Sozialdienst verweigert Lösegeld - Fürstenfeldbruck - SZ.de (sueddeutsche.de), Cyberangriff trifft Sozialdienst Olching e.V. - Sozialdienst Olching e.V. (sozialdienst-olching.de)
Januar 2022	CRPS Netzwerk gemeinsam stark e.V.	Angriff auf die Server; Website und E-Mail-Adressen nicht mehr erreichbar; Einrichtung einer neuen Domain notwendig.	Totalausfall unserer Systeme - CRPS Netzwerk gemeinsam stark. e.V.
März 2022	Diakonie Stiftung Salem	Ransomware-Angriff; 2.800 Mitarbeitende in 89 Einrichtungen betroffen.	Cyberkriminalität: Systemverschlüsselung durch Hackerangriff – AZ-TEKA Consulting GmbH
Juni 2022	Ambulanter Pflegedienst in Berlin	Ransomware-Angriff; 60 Mitarbeitende betroffen.	Hackerangriffe auf Kliniken: "Nur eine Frage der Zeit" | tagesschau.de
September 2022	Caritasverband München/ Freising	Gezielter Ransomware-Angriff; 10.000 Mitarbeitende in 380 Einrichtungen betroffen; Wiederaufbau der IT-Infrastruktur und Wiederherstellung der Daten auch ein Jahr später noch nicht vollständig abgeschlossen (Quelle: eigene Erfahrung).	Cyber-Kriminelle fordern Lösegeld für Caritas-Daten - katholisch.de
September 2022	SKM Düsseldorf	Abfluss und Verschlüsselung von Daten.	Hackerangriff auf katholischen Sozialdienstleister SKM - katholisch.de
Oktober 2022	Caritas-Behindertenwerk in Eschweiler	Meldung auf Rechnern, dass die Organisation gehackt worden sei; Systeme vom Netz genommen und Betrieb eingestellt; Ermittlungen durch das LKA.	Cyber-Attacke legt die IT der CBW in Eschweiler lahm | Aachener Zeitung (aachener-zeitung.de), Aachener Zeitung vom 05.11.2022, Seite 13
November 2022	Caritasverband Eifel	Ransomware-Angriff; 500 Mitarbeitende und 1000 Pflegebedürftige betroffen.	Cyber-Attacke auf Caritas – Betrieb in der Eifel läuft weiter nur analog - Nachrichten - WDR

[13] Jahreszahl nicht in der Fundstelle enthalten, sondern auf Anfrage direkt vom CV Paderborn erhalten.

November 2022	Die Zieglerschen	Dank frühzeitiger Warnung durch die Polizei wurden die Systeme rechtzeitig heruntergefahren und Normalbetrieb konnte nach zehn Tagen wieder aufgenommen werden.	01_jahresbericht_zie_2022_end_es.pdf (zieglersche.de)
März 2023	DRK Baden-Württemberg	DDoS-Attacke auf die Webseiten mehrerer Kreisverbände.	https://www.swp.de/baden-wuerttemberg/hackerangriff-auf-drk-internetseiten-hacker-legen-teile-der-webseiten-des-roten-kreuzes-im-suedwesten-lahm-69981231.html
Mai 2023	Erzbistum Köln, darunter Caritasverbände	Angriff auf die Server eines IT-Dienstleisters, bei dem sich das Erzbistum Köln unter den Kunden befand; Caritasverbände im Gebiet des Erzbistums mitbetroffen; Websites der betroffenen Einrichtungen drei Wochen lang nicht erreichbar.	Internetseiten des Erzbistums Köln gehen wieder online (erzbistum-koeln.de)
September 2023	Caritasverband Rhein-Erft-Kreis	1.600 Mitarbeitende in 70 Einrichtungen betroffen.	Caritasverband für den Rhein Erft Kreis e.V. | Caritas Rhein-Erft ist Opfer einer Cyberattacke (caritas-rhein-erft.de)
Oktober 2023	CURA Unternehmensgruppe	Aufgrund eines Hacker-Angriffs mussten alle Systeme vom Netz genommen und konnten erst im Januar 2024 wieder hochgefahren werden. Betroffen waren u.a. über 40 Pflegeeinrichtungen und über 5.000 Mitarbeitende.	089 - Jana Förste (CURA) | Hacker-Angriff | Turbo-Digitalisierung | Cloud ~ Pflege Digital Podcast
Januar 2024	Evangelische Stiftung Neinstedt	Ausfall der zentralen IT-Systeme ab 30.01.2024; Stand 22.04.2024 waren immer noch nicht alle Mitarbeitenden wieder mit einer funktionierenden E-Mailadresse ausgestattet	4331-Cyberangriff-auf-Evangelische-Stiftung-Neinstedt.png (1309×694) (security-incidents.de)
Februar 2024	Gesundheits- und Pflegeeinrichtungen Lindenbrunn	Vier Pflegeheime und ein Krankenhaus betroffen; Server und Datenbanken vom Netz genommen.	Pflegeeinrichtungen nach Cyberangriff seit Samstag offline | Care Inside (carevor9.de)
Februar 2024	DRK Mannheim	Erreichbarkeit per Telefon und E-Mail eingeschränkt; 490 Hauptamtliche und 1.900 Ehrenamtliche betroffen	Deutsches Rotes Kreuz im Visier: DRK-Kreisverband Mannheim bestätigt Cyberangriff - Golem.de
April 2024	St. Elisabeth Stiftung, Bad Waldsee	Stiftungsnetzwerk wurde vom Internet getrennt.	St. Elisabeth-Stiftung, Bad Waldsee - Detail (st-elisabeth-stiftung.de)
April 2024	AWO Münsterland-Recklinghausen	Phishing-Welle führt zum Abgreifen von E-Mail-Passwörtern. Nach Abschalten des Mailservers sind ambulante Pflegedienste, Kitas und der Offene Ganztag an Grundschulen nicht mehr per Mail erreichbar.	Hackerangriff auf AWO im Kreis Recklinghausen und Münsterland - Ruhrgebiet - Nachrichten - WDR
April 2024	Katholische Jugendfürsorge der Diözese Augsburg e.V.	Hacker erbeuten Personaldaten und Finanzdaten, Patientendaten und Gesundheitsdaten von mehr als 20 Kliniken, Berufsschulen und sozialen Einrichtungen.	Cyberangriff auf KJF Augsburg (kjf-augsburg.de)

September 2024	Caritas-Betriebsführungs- und Trägergesellschaft mbH (CBT)	Eine Ransomwaregruppe verschlüsselt Teile des IT-Systeme und veröffentlicht erbeutete Daten im Darknet.	Ransomware-Angriff: Caritas-Betriebsführungs- und Trägergesellschaft mbH (CBT) | Sicherheitsvorfalls-Datenbank (dsgvo-portal.de) CBT ist Opfer eines Cyberangriffs - CBT GmbH (cbt-gmbh.de)
September 2024	Haus des Stiftens	Ransomwareangriff mit Datenabfluss in erheblichem Umfang. Zur Verhinderung weitern Schadens mussten IT-Systeme vom Netz genommen werden, u.a. die Systeme zur Abwicklung des Zahlungsverkehrs.	Infos zum Cyberangriff - Haus des Stiftens
Oktober 2024	Gaggenauer Altenhilfe	Ransomwareangriff; Pflegeeinrichtungen und ambulanter Pflegedienst mussten auf Papierdokumentation umstellen und die Telefonanalgen fielen zwischenzeitlich aus.	Gaggenauer Altenhilfe ist Ziel eines Cyber-Angriffs geworden - Gaggenauer Altenhilfe
Oktober 2024	Johannesstift Diakonie	Ransomwareangriff, von dem Krankenhäuser, Pflegeeinrichtungen und soziale Dienste mit rund 11.000 Beschäftigten in sechs Bundesländern betroffen waren. Notaufnahmen waren zwischenzeitlich nicht anfahrbar, der Zugriff auf die Pflegedokumentation war nicht möglich und die Einrichtungen waren nicht per E-Mail erreichbar.	Cyberangriff - Johannesstift Diakonie; Johannesstift-Diakonie Berlin: Cyber-Angriff legt Rettungsstellen lahm - erste Hinweise auf Täter - erste Hinweise auf Täter | rbb24
Oktober /November 2024	DRK Wolfenbüttel	Störung der IT-Infrastruktur, Spähprogramme auf Tablets entdeckt, Erpressungsversuche (kleinere Geldbeträge, sowie die Forderung, zwei Führungskräfte zu entlassen), gefälschte E-Mails an abgegriffene Mailadressen.	Cyberattacke auf DRK: Verdächtigte Mitarbeiterin ist unschuldig, Wolfenbütteler Zeitung - Wolfenbüttel-Braunschweig vom 13.02.2025 Seite 22
März 2025	Sozial-Holding der Stadt Mönchen-gladbach	Ransomware-Angriff; sechs Altenheime betroffen, sowie Schulen, die die Sozial-Holding mit Essen versorgt.	Cyberangriff gegen Altenheim-Verwaltung in Mönchengladbach
Plus drei weitere Vorfälle, die nicht öffentlich gemacht wurden, der Autorin aber bekannt sind. Die Dunkelziffer dürfte weitaus höher sein.			

Obwohl das Fehlen einer systematischen Erhebung eine konkrete Einschätzung der Bedrohungslage in der Sozialwirtschaft erschwert, lassen Trends aus der allgemeinen Bedrohungslage darauf schließen, dass in Zukunft immer mehr soziale Einrichtungen Opfer von Cyberangriffen werden könnten:

> Noch sind die Angriffe auf Unternehmen, Einrichtungen und Institutionen aus dem Sozial- und Gesundheitssektor überschaubar. […] Doch gerade die immer häufiger auftretenden Angriffe auf Universitäten und Gemeinden lassen Schlimmes befürchten. (Niedung 2023, 14)

5.5 Forschung zu IT-Sicherheit in angrenzenden Bereichen: KMU, Gesundheitswesen, NPOs und NGOs

Zu IT-Sicherheit in kleinen und mittlere Unternehmen (KMU) sowie zum Gesundheitssektor existiert eine Vielzahl an Literatur, die von Behörden, Wissenschaft und wirtschaftlichen Akteuren erstellt wird. Neben technischen Beiträgen aus der Informationstechnik befasst sich die Literatur größtenteils mit der Bedrohungslage im jeweiligen Sektor (zum Beispiel: Europäische Kommission 2022; Bundesamt für Sicherheit in der Informationstechnik 2022), mit der Gefährdungslage und dem Gewappnetsein des Sektors (etwa Kappe et al. 2023; European Union Agency for Cybersecurity 2021) und mit konkreten Maßnahmen zur Erhöhung von IT-Sicherheit (beispielsweise Deistler 2023; Darms et al. 2019). Mit der Sozialwirtschaft haben viele kleinen und mittlere Unternehmen gemein, dass sie mit veralteten Systemen und geringen IT-Ressourcen ausgestattet sind. Das Gesundheitswesen wiederum arbeitet mit höchst sensiblen personenbezogenen Daten und gehört zudem in Teilen zur Sozialwirtschaft.

Auch wenn sicher einige Erkenntnisse aus der Literatur zu KMU und dem Gesundheitssektor für die Sozialwirtschaft relevant sein können, ist unklar, wie groß diese Schnittmenge tatsächlich ist (vgl. Baier et al. 2022, 3). Mehr Ähnlichkeiten zu sozialwirtschaftlichen Organisationen in Deutschland – insbesondere der freien Wohlfahrt – gibt es mit Non-Profit-Organisationen (NPOs) und Non-Governmental-Organisationen (NGOs). Im internationalen Kontext wird die Sozialwirtschaft mit dem Nonprofit-Bereich gleichgesetzt und auch die EU folgt diesem Verständnis (Zimmer und Paul 2024, 87). Bezogen auf IT-Sicherheit gibt es für NPOs und NGOs deutlich weniger Literatur. Einer der frühsten Beiträge stammt von Mierzwa und Scott aus dem Jahr 2017 (Mierzwa und Scott 2017), in dem die Autoren eine anonyme, knappe Umfrage unter 53 NPOs/NGOs in den USA durchführen. Ermicoi und Liu werten 2020 eine ausführlichere Umfrage unter 65 kleinen und mittelgroßen NPOs in Washington DC, Maryland und Virginia aus (Ermicioi und Liu 2022). Das Sample für die Umfrage von Hassan et al 2022 umfasst 168 NGOs in Saudi-Arabien, wovon etwa drei Viertel Mikro- oder kleine Unternehmen sind. (Hassan et al. 2023) Das CyberPeace Institute, selbst eine NGO, die andere NGOs bei IT-Sicherheit unterstützt, befragt 27 NGOs in Genf, also im Umfeld der Vereinten Nationen (CyberPeace Institute 2023). Nyonzigira beschäftigt sich abermals mit den USA, führt jedoch keine Umfrage, sondern semi-strukturierte Interviews mit IT-Leitern von zwölf NPOs durch (Nyonzigira 2023). All diese Studien kommen zu dem Ergebnis, dass der NPO/NGO-Sektor schlecht gegen Cyberangriffe gerüstet ist. Als Gründe arbeiten sie

heraus, was auch für die Sozialwirtschaft in Deutschland gilt: Fehlende Erfahrung, fehlendes Fachpersonal und fehlendes Budget. Hassan et al. und Nyonzigira stellen zudem fest, dass fehlende Bereitschaft seitens des Managements, IT-Sicherheit Priorität einzuräumen, Teil des Problems ist.

Während sich alle Beiträge vor allem mit der Gefährdungslage und dem Gewappnetsein befassen, geben Mierzwa und Scott und das CyberPeace Institute darüber hinaus Empfehlungen zu konkreten Maßnahmen, wie NPOs/NGOs ihre IT-Sicherheit steigern können. Das CyberPeace Institute geht sogar noch weiter: Es sieht die Unterstützung der IT-Sicherheit in NGOs als eine gesamtgesellschaftliche und damit auch politische Aufgabe. Es fordert: „NGOs sollten als Stakeholder mit spezifischen, eigenen Bedürfnissen anerkannt werden, auf die die Behörden gezielt eingehen" (CyberPeace Institute 2023, 14, eigene Übersetzung). Zudem sollen Behörden die transparente Erfassung von und Berichterstattung über Cyberangriffe gegen NGOs fördern, damit die Politik sich des Problems bewusstwerde und Maßnahmen einleiten könne (ebd.). Des Weiteren plädiert das Institut für Partnerschaften und Netzwerke mit Wissenschaft und Privatwirtschaft, um Wissen sowie Technologie mit NGOs zu teilen.

5.6 Forschungsstand zu Cyberbedrohungen in der Sozialwirtschaft

Mangel an Forschungsliteratur

Ist internationale Literatur zu IT-Sicherheit in NGOs und NPOs dünn gestreut, so ist sie im deutschsprachigen Raum so gut wie gar nicht existent. Tatsächlich gibt es nur eine Handvoll Publikationen, die sich dezidiert mit IT-Sicherheit in der Sozialwirtschaft auseinandersetzen:

Der Bericht von FINSOZ beschreibt anhand von Fallbeispielen die Bedrohungslage und bietet einen Leitfaden für praktische Maßnahmen (siehe FINSOZ e. V. - Fachgruppe IT-Compliance 2022). Baier et al. tragen eine sehr detailliere quantitative Erhebung zu Bedrohungs- und Gefährdungslage bei, aber eben nicht für Deutschland sondern für den Kanton Zürich in der Schweiz (siehe Baier et al. 2022).

Interessant für Deutschland ist der Report zu IT in der Sozialwirtschaft, den Helmut Kreidenweis und Dietmar Wolf von der katholischen Universität Eichstätt-Ingolstadt jährlich herausbringen und aus dem in dieser Arbeit bereits mehrfach zitiert wurde. Alle drei Jahre enthält der Bericht ein Kapitel zu IT-Sicherheit und Datenschutz (z.B. Kreidenweis und Wolff 2022). Eine Erkenntnis aus dem Report von 2022 ist, dass ein Drittel aller befragten sozialen Organisationen über kein IT-

Sicherheitskonzept verfügt (Kreidenweis und Wolff 2022, 39). Weiter bewerten sie die Qualität dieser Konzepte, indem sie danach fragen, ob das Konzept eine Identifikation und Bewertung von Bedrohungen der IT, präventive Schutzmaßnahmen und Notfall- bzw. Wiederanlaufpläne (reaktive Maßnahmen) vorsieht. Sie stellen fest:

> Setzt man als Maßstab das Vorhandensein aller drei Bestandteile an, womit man ein gutes Stück von Standards, wie etwa dem des BSI-Grundschutzkatalogs, entfernt ist, so fällt nach wie vor ein Viertel bis ein Fünftel der Einrichtungen durchs Raster (ebd.)

Außerhalb der Wissenschaft ist Expertise zu IT-Sicherheit in der Sozialwirtschaft in der Wirtschaft zu finden, nämlich in IT-Unternehmen, die Organisationen der Sozialwirtschaft als Kunden erkannt und sich teilweise auf sie spezialisiert haben. Diese thematisieren die Spezifika der Branche vereinzelt in Blogbeiträgen und Artikel, die zwar Marketinginstrumente der Unternehmen sein mögen, aber dennoch interessante Praxiseinblicke bieten. So ist beispielsweise Matthias Niedung, der Autor des oben zitierte Artikels aus der Branchenzeitschrift *Sozialwirtschaft,* Berater bei Althammer&Kill, einer Consulting-Firma mit Fokus auf Datenschutz und Informationssicherheit insbesondere in Kirche, Wohlfahrt und Krankenhäusern (vgl. Niedung 2023). Ebenfalls auf Datenschutz und Informationssicherheit spezialisiert ist DataGuard, das in ihrem Unternehmensblog erklärt, warum gerade Wohltätigkeitsorganisationen attraktive Ziele für Hacker sind (Whitmore 2023).

Sowohl Wissenschaft als auch IT-Unternehmen haben herausgearbeitet, welche strukturellen Schwächen dafür sorgen, dass Organisationen der freien Wohlfahrt leichte Ziele für Cyberattacken sind. Diese Schwachstellen sind im Folgenden dargestellt.

Organisationen der freien Wohlfahrt als leichtes Ziel für Cyberattacken

Die Einschätzung Niedungs, dass sich Cyberangriffe auf die Sozialwirtschaft in Zukunft mehren könnten, ist im Einklang mit den Beobachtungen des BSI und ENISAs, dass Cyberkriminelle sich vermehrt auf leichte Opfer fokussieren. Einrichtungen der freien Wohlfahrt sind aus mehreren Gründen sowohl attraktive als auch leichte Ziele (vgl. FINSOZ e. V. - Fachgruppe IT-Compliance 2022; Niedung 2023; Whitmore 2023):

Attraktivität für Angreifer

Soziale Organisationen arbeiten mit hochsensiblen, personenbezogenen Daten und sind für ihre Arbeit in besonderem Maß auf die Verfügbarkeit dieser Daten angewiesen. Das Bestreben, diese Daten vor Veröffentlichung zu schützen, die Abhängigkeit von ihnen zur Aufrechterhaltung des

Betriebs und mögliche negative Auswirkungen einer Nichtverfügbarkeit auf die Gesundheit von Menschen (z.B. Medikationspläne in der stationären Pflege oder Routenpläne in der ambulanten Pflege) führen zu einer hohen Erpressbarkeit.

Schlechte technische Absicherung

Viele Organisationen haben veraltete IT-Systeme, die leichte Einfallstore für Angreifende bieten. So erhebt etwa der IT-Report für die Sozialwirtschaft 2022, dass auf 17 % der klassischen Endgeräte in den befragten Organisationen Windows 7 oder noch ältere Windowsversionen laufen, für die es keinen Support und damit auch keine Sicherheitsupdates mehr gibt (Kreidenweis und Wolff 2022, 23). Zudem sind die IT-Landschaften oft weit verzweigt an vielen Standorten und mit einer Vielzahl an Partnern und Zulieferern vernetzt. Hinzu kommt eine weit verbreitete Schatten-IT, das heißt der Einsatz von Programmen und Geräten, die von der zuständigen IT-Abteilung nicht genehmigt wurden und von denen die IT in der Regel noch nicht einmal weiß.

Ressourcenmangel

Was für die IT in der Sozialwirtschaft allgemein gilt (siehe *3.5 IT und Digitalisierung in der freien Wohlfahrt* ab S. 26), gilt auch – oder sogar insbesondere – für IT-Sicherheit: Es fehlt an IT-Ressourcen, sowohl bezogen auf Fachkräfte als auch auf Budget. Zusätzlich zu dem insgesamt niedrigen IT-Budget ist gerade der Anteil der Ausgaben für IT-Sicherheit an den Gesamtaufwendungen für IT gering. Kreidenweis und Wolff zufolge geben 76 % der sozialen Organisationen anteilig an ihrem IT-Budget zehn Prozent oder weniger für IT-Sicherheit aus (Kreidenweis und Wolff 2022, 42). Das ist weit weg von den 20 %, die das BSI als Anteil am IT-Budget empfiehlt (Pawlowska und Scherer, 8)[14].

Fehlende Kompetenzen

Mitarbeitende in der Sozialwirtschaft verfügen über eine geringe IT-Literacy im Allgemeinen, was mit einem mangelnden Bewusstsein für IT-Sicherheit im Speziellen einhergeht. Schulungen finden aufgrund von einem ebenfalls niedrigen Risikobewusstsein seitens des Managements sowie Zeit-

[14] Zum Vergleich: Auch andere Bereiche der Wirtschaft erfüllen diese Empfehlung nicht, schneiden aber immer noch besser ab als die Sozialwirtschaft. In der Gesamtwirtschaft sind es 55 % der Unternehmen, die nur 10 % ihres IT-Budgets oder weniger für IT-Sicherheit aufwenden (Pawlowska und Scherer, 13), und unter KRITIS-Unternehmen ist der der Wert erschreckenderweise mit 58 % sogar noch höher (Bundesamt für Sicherheit in der Informationstechnik 2023c, 17) Letztere geben durchschnittlich 14 % ihres IT-Budgets für Cybersecurity aus.

und Geldmangel nicht oder nicht häufig genug statt. Kreidenweis und Wolff ermitteln, dass nur 49 % der befragten Organisationen ihre Mitarbeitenden jährlich zu IT-Sicherheit schulen, wohingegen 43 % weniger als einmal im Jahr, nur bei Einstellung oder nie schulen (ebd.). Die Ergebnisse der Befragung im Kanton Zürich fallen sogar noch niedriger aus: Hier geben nur 33,9 % der Organisationen an, mindestens jährlich IT-Sicherheitsschulungen durchzuführen (Baier et al. 2022, 24).

Mangelnde Aufmerksamkeit für IT-Sicherheit

Hinzu kommt, dass die Sozialwirtschaft in puncto Cyberbedrohungen auf mehreren Ebenen unter dem Radar läuft:

Politisch: Wie bereits angesprochen, findet die Sozialwirtschaft (von Krankenhäusern abgesehen) keine besondere Beachtung in der Gesetzgebung, was sich auch durch die NIS2-Richtlinie der EU nicht ändert. Auch in den Berichten von Enisa und BSI gibt es keine gesonderten Angaben zur Sozialwirtschaft und die Bemühungen beider Behörden, schlecht abgesicherte, kleinere Akteure praktisch zu unterstützen, richten sich lediglich an KMUs[15].

Kommerzielles Threat Reporting: Kommerzielles Threat Reporting stellt eine wichtige Informationsquelle zu Cyberattacken dar, sowohl für betroffene Branchen als auch für Sicherheitsforscher und politische Entscheidungsträger. Dabei analysieren kommerzielle Cybersecurityfirmen detailliert Cyberattacken und stellen die Berichte frei im Netz zur Verfügung. Für sie ist es ein Marketingtool, mit dem sie ihre Produkte bewerben. Durch dieses kommerzielles Interesse fokussieren sie ihre Berichterstattung vor allem auf bekannte Opfer aus zahlungskräftigen Branchen. Maschmeyer et al. untersuchen einen Datensatz von 629 kommerziellen Threat Reports darauf, wie häufig Angriffe auf die Zivilgesellschaft analysiert werden (Maschmeyer et al. 2021). Sie kommen zu dem Ergebnis, dass zivilgesellschaftliche Opfer in nur 13 % thematisiert werden – einen primären Fokus auf die Zivilgesellschaft haben sogar nur 4 %. Sie warnen davor, dass die mangelnde Berichterstattung dazu führe, dass zivilgesellschaftliche Organisationen nicht genügend Informationen zu den Bedrohungen hätten, denen sie ausgesetzt sind. Außerdem resultiere daraus, dass Politik und Geldgeber die Abwehr von Cybergefahren in diesem Bereich nicht priorisierten (vgl. Maschmeyer et al.

[15] Siehe die entsprechenden Toolboxen: SecureSME — ENISA (europa.eu), BSI - Kleine- und Mittlere Unternehmen (bund.de)

2021, 5, 17). Obwohl die Studie von Maschmeyer et al. zivilgesellschaftliche Organisationen betrachtet, dürften die Erkenntnisse auch auf die freie Wohlfahrt übertragbar sein.

Verbände: Es ist nicht so, dass die Spitzenverbände der freien Wohlfahrt die Augen vor den Gefahren aus dem Cyberraum und den daraus resultierenden Bedürfnissen ihrer Mitglieder komplett verschließen würden. So haben beispielsweise der Paritätische Wohlfahrtsverband und das Deutsche Rote Kreuz Rahmenverträge mit IT-Security-Dienstleistern geschlossen, sodass ihre Mitgliedseinrichtungen diese Dienstleistungen und Produkte (Software, Beratung, etc.) vergünstigt beziehen können (siehe Deutscher Paritätischer Wohlfahrtsverband o.D; DRK-Service GmbH o.D.). Als ein weiteres Beispiel organisierte die Diakonie Deutschland im Rahmen einer Digitalkonferenz für Führungskräfte und Digitalisierungsbeauftragte einen Workshop zu Cyber-Security in der Sozialwirtschaft (Diakonie Deutschland 2023a). Die Caritas widmet Ausgabe 20/2024 ihres alle zwei Wochen erscheinenden Magazins *Neue Caritas* dem Themenschwerpunkt Cybersicherheit (Deutscher Caritasverband 2024). Eine herausragende Stellung nimmt die Zentralwohlfahrtsstelle der Juden in Deutschland ein: Die ZwSt betreibt ein Wissensportal zur digitalen Transformation für jüdische Gemeinden und Organisationen mit einer eigenen Rubrik zu IT-Sicherheit und bietet regelmäßig Trainings an (Zentralwohlfahrtsstelle der Juden in Deutschland o.D.b; Zentralwohlfahrtsstelle der Juden in Deutschland o.D.a)[16].

Über Einzelmaßnahmen hinaus scheinen die Spitzenverbände jedoch nicht zu gehen. Weder die Bundesarbeitsgemeinschaft noch die einzelnen Spitzenverbände stellen politischen Forderungen, die sich ausdrücklich auf IT-Sicherheit beziehen. Ihre digitalpolitischen Forderungen konzentrieren sich stattdessen auf digitale Teilhabe insbesondere marginalisierter Gruppen, sowie die Förderung und Refinanzierung der digitalen Transformation der Träger der freien Wohlfahrt (vgl. Arbeiterwohlfahrt 2023; Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege 2020; Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege 2021; Deutsches Rotes Kreuz 2023; Deutscher Paritätischer Wohlfahrtsverband 2022). Letztere Forderung betrifft zwar auch IT-Sicherheit, benennt sie aber nicht explizit. Lediglich der Deutsche Caritasverband fordert in seinem Digitalpolitischen Positionspapier „staatliche Finanzierungsmöglichkeiten für die Ausstattung sozialer Einrichtungen und Dienste mit Hard- und Software sowie zur Gewährleistung ihrer IT-Sicherheit“ (Deutscher

[16] Die ZWSt ist allerdings der kleinste Spitzenverband der freien Wohlfahrt in Deutschland. Seine Bemühungen dürften auf den gesamten Bereich betrachtet daher leider geringe Auswirkungen haben.

Caritasverband 2023a, 8) – wahrscheinlich vor dem Hintergrund der Cyberangriffe auf mehrere Caritasorganisationen in den Jahren 2022 und 2023 (siehe *Tabelle 3*).

Die gelisteten Fallbeispiele und die Erhebungen im IT-Report für die Sozialwirtschaft zeigen, dass diese bisherigen Bemühungen nicht ausreichend sind. Kreidenweis und Wolff fordern daher mehr Engagement seitens der Verbände:

> Es wird höchste Zeit, dass die Verbände der freien Wohlfahrtspflege endlich insbesondere gegenüber ihren kleinen Mitgliedern Verantwortung übernehmen, sie für die Gefahren sensibilisieren und ihnen Beratung und Begleitung bei der Einführung von IT-Sicherheitsmaßnahmen anbieten. Warum gibt es für alle möglichen Themen dort Referate und Fachberatung, nur nicht zu IT-Sicherheit? Selbstverständlich kann man dazu auch externe Beratung einkaufen, doch diese ist vor allem für kleine Träger eben nur schwer finanzierbar. (Kreidenweis und Wolff 2022, 39)

6. Zwischenfazit

Die Ergebnisse der Recherche zur freien Wohlfahrt, Caritas und IT-Sicherheit in der Sozialwirtschaft können in organisationsinterne und organisationsexterne Faktoren zusammengefasst werden, die den Stand der IT-Sicherheit in der freien Wohlfahrt beeinflussen.

Faktoren innerhalb der Einrichtungsträger begründen unmittelbar, wie es um IT-Sicherheit in der konkreten Organisation bestellt ist. Die IT-Infrastruktur vieler sozialer Einrichtungen befindet sich in einem schlechten Zustand, was sie anfällig für Cyberangriffe macht. Kleine IT-Budgets im Allgemeinen und kleine IT-Sicherheitsbudgets im Speziellen sowie fehlendes IT-Fachpersonal führen dazu, dass dieser Ist-Zustand kaum verbessert werden kann. Des Weiteren verfügen Mitarbeitende in der Sozialwirtschaft über geringere IT-Kompetenzen als in anderen Branchen und den Organisationen fehlt es an Aufmerksamkeit für das Thema IT-Sicherheit.

Diese internen Faktoren hängen häufig von externen Faktoren ab, die in politischen und wirtschaftlichen Strukturen sowie den Organisationsstrukturen der Branche zu finden sind. Die freie Wohlfahrt zeichnet sich durch eine enorme Heterogenität der Rechtsträger bezüglich ihrer Arbeitsbereiche, Größe und Finanzierungsquellen aus. Ein weiteres Merkmal sind unübersichtliche Zuständigkeiten in der politischen Interessensvertretung. Diese spielen auch bei einem weiteren wichtigen externen Faktor eine Rolle: der mangelnden IT-Refinanzierung. Hinzu kommt der allgemeine IT-Fachkräftemangel, der sich durch den demografischen Wandel noch weiter verschärfen wird.

Zudem gibt es seitens Politik und Behörden keine besondere Aufmerksamkeit für IT-Sicherheit in der freien Wohlfahrt bzw. Sozialwirtschaft außerhalb des Gesundheitssektors.

7. Methodik

Die Gütekriterien der quantitativen Sozialforschung – Reliabilität, Validität und Objektivität – sind nur schwer auf die qualitative Sozialforschung übertragbar (vgl. Flick 2014). Stattdessen gilt es, intersubjektive Nachvollziehbarkeit zu gewährleisten, das heißt, die Wahl der Methoden und die Prozesse der Datenerhebung, Analyse und Interpretation so zu begründen und darzustellen, dass Außenstehende die Schritte des Forschungsprojekts nachvollziehen und die Qualität von Vorgehen und Ergebnissen bewerten können (Flick 2014, 422; Kaiser 2021, 10; Mayring 2020, 4). Neben der Begründung des Forschungsdesigns im Allgemeinen bedeutet das für leitfadengestützte Experteninterviews im Speziellen, die Kriterien für die Expertenauswahl offenzulegen, den Leitfaden zugänglich zu machen, die Interviewsituation zu dokumentieren und die Auswertungsmethode zu beschreiben. Dies geschieht in diesem und dem folgenden Kapitel. Ein weiteres Gütekriterium bei Experteninterviews sind Neutralität und Offenheit der Forscherin / des Forschers gegenüber neuen Erkenntnissen und anderen Denkmustern (Kaiser 2021, 10f). Für die Befragten bedeutet das, dass sie in der Interviewsituation auszudrücken können, was und wie sie es gerne sagen möchten (ebd., und Helfferich 2014, 562). Dies wird dadurch sichergestellt, dass der Interviewleitfaden so offen wie möglich und so strukturierend wie nötig gestaltet wird, wobei Experteninterviews zu den stärker strukturierten Interviewformen zählen (ebd. 560 und 571f). Zudem müssen die Interviewfragen möglichst neutral ausgewählt und formuliert werden (Kaiser 2021, 11f). Die bereits erwähnte Veröffentlichung des Leitfadens sowie Dokumentation der Interviewsituation dient dazu, dass Dritte die Einhaltung auch dieses Gütekriteriums einschätzen können.

7.1 Forschungsdesign

Allgemeines Design: Deskriptive Fallstudie

Bei der vorliegenden Arbeit handelt es sich um eine deskriptive Fallstudie. Ähnlich wie bei explorativen Designs ist bei deskriptiven Studien noch zu wenig über den Forschungsgegenstand bekannt, als dass man präzise Hypothesen formulieren könnte. Es liegen allerdings bereits Beschreibungsdimensionen vor, anhand derer man den Forschungsgegenstand möglichst genau und umfassend beschreiben kann (vgl. Mayring 2020, 10–13). Wie in den vorherigen Kapiteln dargestellt,

ist der Forschungsstand zu IT-Sicherheit in der freien Wohlfahrt bzw. Sozialwirtschaft noch rudimentär. Zur Sozialwirtschaft an sich, zu IT-Sicherheit im Allgemeinen und zu IT in der Sozialwirtschaft ist jedoch durchaus Literatur vorhanden, aus der sich Beschreibungsdimensionen ableiten lassen, nämlich die internen und externen Faktoren aus Kapitel 6. Das Ziel von deskriptiven Studien – die genaue und umfassende Beschreibung – deckt sich mit dem Ziel von Einzelfallanalysen: ein Tiefenverständnis über den vorliegenden Fall zu erlangen (vgl. Hering und Schmidt 2014, 529). Auch wenn deskriptive Forschungsdesigns nicht zwingend mit Fallstudien umgesetzt werden müssen, so wird Robert Yin zufolge die Fallstudie als Methode am besten auf deskriptive Fragestellungen angewandt (Yin 2006, 112). Die Wahl einer Einzelfallanalyse zur Beantwortung der vorliegenden Frage ist damit aus der Forschungspraxis heraus gerechtfertigt. Die Caritas wurde als Fallbeispiel ausgesucht, da sie gemessen an der Mitarbeitendenzahl der größte Wohlfahrtsverband in Deutschland ist (vgl. *4. Die Caritas in Deutschland als Fallbeispiel*) und damit einen repräsentativen Fall darstellt. Wie bereits in *2. Fragestellung* erläutert, hat die Autorin zudem aufgrund ihrer aktuellen Tätigkeit beim Caritas-Netzwerk IT e. V. einen guten Zugang zu Akteur:innen in der Caritas.

Erhebungsmethode: Leitfadengestützte Experteninterviews

Zur Datenerhebung werden leitfadengestützte Experteninterviews geführt. Diese eignen sich dann als Erhebungsmethode, wenn Informationen gewonnen werden sollen, die sich aus anderen Quellen nicht oder nur eingeschränkt ermitteln lassen (Kaiser 2021, 21). Da es zu der vorliegenden Fragestellung kaum spezifische Literatur, Statistiken oder andere Primärquellen gibt, trifft dies hier zu. Bogner et al. bezeichnen Interviews, die die hauptsächliche Datenquelle eines Forschungsprojekts darstellen und systematisches, möglichst vollständiges Betriebs- und Kontextwissen erheben, als „systematisierende" Interviews (Bogner et al. 2018, 659). Kontextwissen besteht dabei aus Kenntnissen über institutionelle und sozioökonomische Rahmenbedingungen eines Phänomens (hier: IT-Sicherheit in der Sozialwirtschaft) (Kaiser 2021, 8; siehe auch Bogner et al. 2018, 657). Diese Art von Wissen ist für folgende in den Experteninterviews zu beantwortende Unterfrage relevant: *Gibt es Herausforderungen für die Branche bezüglich IT-Sicherheit, die von bisheriger Literatur noch nicht erfasst wurden?* Betriebswissen wiederum bezieht sich auf Kenntnisse über organisatorische Prozesse bei der Bewältigung von Problemen und basiert auf den praktischen Erfahrungen des Experten / der Expertin (Kaiser 2021, 8; Bogner et al. 2018, 657) Auf Betriebswissen zielen die dritte und vierte Unterfrage ab: *Wie begegnet die Branche den Herausforderungen aktuell? Welche Handlungsoptionen sieht sie, beziehungsweise welche Forderungen stellt sie, um die Rahmenbedingungen für IT-Sicherheit zu verbessern?*

Die dritte Art von Wissen, Deutungswissen, das subjektive Interpretationen umfasst (Kaiser 2021, 8; Bogner et al. 2018, 659), spielt bei systematisierenden Interviews, und damit für diese Arbeit, keine Rolle. Die Reflexion der Wissensarten, die ein Experteninterview erheben soll, ist insofern relevant, als verschiedene Wissensarten verschiedener Fragen im Leitfaden bedürfen und unterschiedliche Anforderungen an die Interviewsituation mit sich bringen (vgl. Kaiser 2021, 151–154). Während Kontextwissen theoretisch auch aus anderen Quellen gewonnen werden könnte, kann Betriebswissen sensibler Natur sein, sodass Expert:innen ihr Wissen oft nur dann offen preisgeben, wenn ein gewisses Maß an Vertraulichkeit gegeben ist. Die konkreten Maßnahmen, die im Rahmen dieser Arbeit getroffen werden, sind weiter unten unter *Ethische Überlegungen und Datenschutz* beschrieben.

Expert:innen sind nach Aglaja Przyborski und Monika Wohlrab-Sahr Personen, die „über ein spezifisches Rollenwissen verfügen, solches zugeschrieben bekommen und diese besondere Kompetenz für sich in Anspruch nehmen" (Przyborski und Wohlrab-Sahr 2021, 155; siehe auch Helfferich 2014, 571). Die zu befragenden Personen müssen also aufgrund ihrer (beruflichen) Rolle über Praxiswissen zu IT-Sicherheit in der Caritas verfügen. Damit bieten sich drei Personengruppen an: IT-Leiter:innen oder IT-Administrator:innen in Caritasorganisationen oder bei für die Caritas tätigen IT-Dienstleistern, Organisationsentwickler:innen in Caritasorganisationen mit einem Fokus auf IT(-Sicherheit), und sozialpolitisch für die jeweilige Caritasorganisation verantwortliche Personen mit einem Fokus auf IT-Sicherheit. Da sich diese Arbeit mit politischen und wirtschaftlichen Rahmenbedingungen befasst und weder mit konkreten IT-sicherheitstechnischen Maßnahmen noch mit organisatorischen Maßnahmen, kommt nur der dritte Personenkreis in Frage. Für die sozialpolitische Interessensvertretung der jeweiligen Organisation sind entweder die Vorständ:innen / Geschäftsführer:innen selbst oder in größeren Organisationen auch spezialisierte Referent:innen zuständig, die meist direkt an den Vorstand / die Geschäftsleitung berichten. Im Caritas-Netzwerk IT e. V. sind in der Regel die Vorständ:innen / die Geschäftsleitung die rechtlichen Vertreter:innen ihrer Organisation im Verein. Entsprechend liegen der Autorin dieser Arbeit die Kontaktdaten der jeweiligen Vorständ:innen vor. Aus diesem Grund wurden die Interviewanfragen direkt an die Vorstandsebene gestellt.

Ethische Überlegungen und Datenschutz

Die in den Experteninterviews abgefragten Informationen sind in zweierlei Hinsicht sensibel: Erstens sprechen die Expert:innen über die IT-Infrastruktur und die IT-Sicherheitsarchitektur ihrer

Organisationen. Sollten Details aus diesem Themenbereich in die Hände von kriminellen Akteur:innen gelangen, könnten sie zum Schaden der Organisationen ausgenutzt werden. Sofern es sich um eine negative Bewertung der IT-(Sicherheits-)Infrastruktur handelt, könnte ein Öffentlichwerden dieser Informationen außerdem zu einem Vertrauens- und Ansehensverlust bei Klient:innen, Mitarbeitenden und Geschäftspartner:innen führen.

Zweitens sind kritische Aussagen zu Spitzenverbänden, politischen Institutionen und Entscheider:innen, anderen karitativ tätigen Organisationen, usw. ebenfalls sensibel. Sollten sie ungewollt an die Öffentlichkeit geraten, könnte dies die Position der betroffenen Organisation in politischen Aushandlungsprozessen schwächen. Auch die Reputation der Expertin / des Experten selbst könnte dadurch beschädigt werden.

Um die Expert:innen und ihre Organisationen zu schützen und um zu gewährleisten, dass die Befragten überhaupt bereit sind, sensible Informationen preiszugeben, bleiben die Namen der Interviewpartner:innen sowie ihrer Organisationen anonym. Zudem werden die Transkripte der Interviews nicht veröffentlicht, sondern es wird nur in Ausschnitten aus ihnen zitiert. Die vollständigen Daten liegen neben der Autorin ausschließlich der Betreuerin dieser Arbeit sowie der Lehrstuhlinhaberin vor.

Alle Interviewpartner:innen haben ihre informierte Zustimmung zur Durchführung des Interviews und der Verwendung der generierten Informationen und Daten gegeben. Dazu wurden die Expert:innen im Zuge der Vereinbarung des Interviewtermins schriftlich, und zusätzlich zu Beginn des Interviews mündlich über Zweck und Inhalt der Arbeit, Art der Veröffentlichung, Umfang der Anonymisierung und Einsatz der verwendeten technischen Hilfsmittel informiert. Zudem wurden sie darauf hingewiesen, dass sie ihre Zustimmung auch jederzeit nachträglich noch zurückziehen können. Zusätzlich haben die Expert:innen einer Datenschutzerklärung zur Verarbeitung ihrer personenbezogenen Daten durch die Autorin sowie durch die Anbieter der eingesetzten elektronischen Hilfsmittel zugestimmt. Die Vorlage für die Einverständniserklärung befindet sich in *Anhang 3: Vorlage Einverständniserklärung für die Interviews*. Von der Autorin wurden als personenbezogene Daten Name, die berufliche E-Mail-Adresse sowie die berufliche Telefonnummer der Expert:innen erhoben und nach Vorgaben der DSGVO verarbeitet.

7.2 Datenerhebung

Auswahl der befragten Organisationen

Die Interviewpartner:innen wurden größtenteils aus den Mitgliedern des Caritas-Netzwerk IT e. V. angefragt. Bei diesem Vorgehen wurden folgende Risiken und Vorteile miteinander abgewogen: Einerseits bedeutet die Mitgliedschaft im Verein, dass die Befragten kein repräsentatives Sample darstellen, da sie ähnliche Einstellungen zu IT-Sicherheit haben könnten, ausgedrückt in ihrer Mitgliedschaft im Verein. Zudem könnten sie die Autorin weniger in ihrer Rolle als neutrale Forscherin und mehr in ihrer Rolle als Mitarbeiterin des Vereins wahrnehmen und daher ihre Ansichten zurückhalten oder Antworten geben, von denen sie denken, dass sie im Sinne des Vereins sind (Problem der sozialen Erwünschtheit). Ersterem Risiko kann nur durch eine entsprechende kritische Einordnung in der Analyse der Ergebnisse begegnet werden. Zweiteres soll dadurch minimiert werden, dass die Autorin zu Beginn des Interviews ihre Rolle als Forscherin klarstellt und zusichert, Informationen aus dem Interview rein für die Forschungsarbeit und nicht für Vereinszwecke zu verwenden, sowie die Anonymität der Befragten und ihrer Organisationen zu wahren. Ein Vorteil der Expert:innen-Gewinnung über den Caritas-Netzwerk-IT e. V. liegt in einem erleichterten Feldzugang. Darüber hinaus kann bei den Mitgliedern davon ausgegangen werden, dass sie sich für das Thema IT und IT-Sicherheit in ihren Organisationen interessieren. Die Mitgliedschaft dient dadurch als eine Art Filter, der dabei hilft, gezielt Vorständ:innen anzusprechen, die über die benötigte Expertise verfügen. Da die benannten Risiken mitigiert werden können, überwiegen die Vorteile und die Akquise der Expert:innen über den Caritas-Netzwerk IT e. V. ist vertretbar.

Insgesamt stammen so fünf von acht Interviewpartner:innen direkt aus Mitgliedsorganisationen des Caritas-Netzwerk IT e. V. Zwei weitere Expert:innen sind Kontakte von Kontakten aus dem Netzwerk und eine Person war bis wenige Monate vor dem Interview bei einer Mitgliedsorganisation tätig.

Bei der Auswahl der Organisationen wurde darauf geachtet, ein Sample zu generieren, das eine Streuung entlang folgender Kriterien sicherstellt: Trägerart (Caritasverband / Fachverband und Spitzenverband / Einrichtungsträger), Betroffenheit (bereits Opfer einer Cyberattacke gewesen / bisher kein Cyberangriff auf die Organisation), Größe der Organisation (Mitarbeitendenzahl),

Geschlecht (weiblich/männlich[17]) und Bundesland. Da die Caritas stärker in West- und Süddeutschland vertreten ist, stammen auch in diesem Sample mehr Organisationen aus diesen Regionen. Obwohl knapp über 80 % der Mitarbeitenden weiblich sind, sind nur knapp unter 25 % in oberen Führungspositionen tätig[18] (Dihle 2021). Das Sample ist daher repräsentativ für den Anteil an Frauen in der Grundgesamtheit. Die Merkmale verteilen sich folgendermaßen über das Sample:

Tabelle 4: Merkmale der interviewten Organisationen

Merkmal	Ausprägung /Verteilung im Sample	Gesamt
Trägerart	• 3 Ortscaritasverbände • 2 Diözesancaritasverbände, die sowohl als Spitzenverbände als auch operativ als Einrichtungsträger agieren • 3 Spitzenverbände, davon 1 Personalfachverband, 1 Einrichtungsfachverband, 1 sonst. Spitzenverband; einer davon auch operativ als Einrichtungsträger tätig	8
Betroffenheit	• 3 noch von keinem Cyberangriff betroffen • 5 schon einmal von einem Cyberangriff betroffen gewesen; davon: 2 schwer (Arbeitsfähigkeit über längeren Zeitraum massiv eingeschränkt), 2 mittel (Arbeitsfähigkeit über kürzeren Zeitraum eingeschränkt), 1 leicht (Vorfall gegeben, aber Arbeitsfähigkeit nicht eingeschränkt)[19]	
Größe	• OCVs und DiCVs: zwischen 165 und 10.000 Mitarbeitende; Median: 1.000 • Spitzenverbände: o Eigene MA: zwischen 10 und 25; Median: 15 o MA in den Mitgliedsorganisationen: zwischen 4.000 und 185.000; Median: 100.000	
Bundesland	- Bayern: 2 - Baden-Württemberg: 1 - Hessen: 1 - NRW: 1 - Sachsen: 1 - Bundesweit: 2	
Geschlecht	2 Frauen, 6 Männer	
Funktion / Rolle	- 4 Vorständ:innen - 2 Geschäftsführer:innen - 1 Fachreferent:in - 1 Unternehmensberater:in mit Fokus auf die Sozialwirtschaft[20]	

[17] Der Autorin ist bewusst, dass Geschlecht weder auf das biologische Geschlecht noch auf Binarität zu reduzieren ist. Da genderwissenschaftliche Betrachtungen jedoch nicht Fokus dieser Arbeit sind, wird das Merkmal „Geschlecht" auf die Ausprägungen „männlich" und „weiblich" reduziert.

[18] Beide weiblichen Expertinnen haben in den Interviews von sich aus den Mangel an Frauen in den obersten Führungsetagen thematisiert. Dies ist nicht der Fokus dieser Arbeit. Als Denkanstoß sind jedoch Zitate der beiden Expertinnen in *Anhang 15: Zitate zur Unterrepräsentation von Frauen in den obersten Führungsebenen in Caritas-Organisationen* zu finden.

[19] Skala: Eigene Skala; Einschätzung auf Grundlage der Erzählungen der Expert:innen. Nicht alle der Angriffe wurden in der Presse öffentlich gemacht.

[20] Die Person ist seit vielen Jahren als Strategieberater:in in der freien Wohlfahrt tätig, darunter auch für zahlreiche Caritasorganisationen. Für die Sample-Statistik wurden die Merkmale der letzte Caritasorganisation verwendet, die er:sie bis kurz vor dem Interview über mehrere Jahre betreut hatte.

Die Expert:innengewinnung gestaltete sich größtenteils problemlos. Die Interviewpartner:innen wurden alle per E-Mail angefragt; in einem Fall ging der Mail ein Gespräch mit der Vorstandsassistentin voraus und in einem anderen Fall wurde die Kontaktaufnahme zunächst telefonisch durch einen der Vorstände des Caritas-Netzwerk IT e. V. angekündigt. Alle Zusagen durch die Expert:innen erfolgten innerhalb von 24 Stunden. Zwei angefragte Personen reagierten auch auf Nachfrage nicht auf die E-Mail. Entsprechend wurde ein:e andere:r Expert:in kontaktiert sowie die Entscheidung getroffen, den Pretest in die Analyse einfließen zu lassen.

Leitfaden

Der Interviewleitfaden (siehe *Anhang 4: Interviewleitfaden für rein operative Träger* und *Anhang 5: Interviewleitfaden für Spitzenverbände*) orientiert sich an den internen und externen Faktoren, die in *6. Zwischenfazit* aus der Literatur herausgearbeitet wurde. Um den Interviewverlauf für die Befragten nachvollziehbar zu machen, wurden die Faktoren in folgende Themenblöcke zusammengefasst:

- Awareness:
    - Intern: Aufmerksamkeit von Vorständen
    - Intern: Aufmerksamkeit und Fähigkeiten von Mitarbeitenden
    - Extern: Aufmerksamkeit von Verbänden
- Politische Rahmenbedingungen:
    - Extern: Politische Interessensvertretung
    - Extern: Politische Aufmerksamkeit
- Finanzierung:
    - Extern: IT-Refinanzierung
- Fachkräfte
    - Intern und extern: Fachkräftemangel

Die Entwicklung des Fragebogens ist auf Grundlage von Kaiser 2021 erfolgt. Dort wird explizit darauf hingewiesen, dass eine Abweichung vom Leitfaden bei Experteninterviews ausdrücklich möglich sein muss. Entsprechend ist der Leitfaden in *Anhang 4: Interviewleitfaden für rein operative Träger* und *Anhang 5: Interviewleitfaden für Spitzenverbände* lediglich eine Vorlage. Die Reihenfolge der Fragen variierte von Interview zu Interview stark und oftmals mussten Fragen auch gar nicht gestellt werden, weil der Experte / die Expert:in das Thema von selbst angesprochen hatte. Dies lag

vor allem an der Einstiegfrage („Was sind Ihrer Meinung nach die größten Herausforderungen für eine Caritas-Organisation, um IT-Sicherheit in einer Caritas-Organisation herzustellen?“), die der/dem Interviewten bewusst die Möglichkeit gab, ein längeres Statement abzugeben und eigene Schwerpunkte zu setzen, sowie als Anknüpfungspunkt für spätere Fragen diente. In einigen Fällen war auch die Abschlussfrage („Gibt es etwas, das Ihnen zu diesem Thema noch wichtig und bisher zu kurz gekommen ist?“) nochmal besonders ergiebig.

Pre-Test

Anhand eines Pre-Tests wurde der Fragebogen auf folgende Kriterien überprüft (nach Kaiser 2021, 82f):

- Verständlichkeit
- Interesse des Befragten an den Fragen
- Kontinuität des Interviewverlaufs
- Dauer des Interviews

Das Interview wurde zudem mit der Pre-Test-Interviewpartnerin/ dem Pre-Test-Interviewpartner reflektiert. Aufgrund des reibungslosen Verlaufs des Interviews, des positiven Feedbacks des Experten/ der Expertin und des informationsreichen Materials, das aus dem Interview entstanden ist, musste der Leitfaden nur leicht angepasst, das heißt um zwei Fragen erweitert werden. In Absprache mit der Betreuerin dieser Arbeit sowie mit der Expertin/des Experten wurde das Interview in den Hauptcorpus aufgenommen. Dies ist möglich, da der Fragekatalog in Folge des Pre-Tests kaum verändert wurde (siehe ebd., S. 83).

Durchführung der Interviews

Die Interviews fanden größtenteils zwischen dem 30. Oktober 2024 und dem 20. Dezember 2024 statt; nur eines wurde deutlich später abgehalten, nämlich am 28. Februar 2025. Sie wurden per TUM-Conf, der Zoom-Instanz der Technischen Universität München (Zoom Video Communications 2022), durchgeführt und aufgezeichnet. Insgesamt wurden 11 h 54 min Audiomaterial aufgezeichnet, mit einer durchschnittlichen Interviewdauer von 1 h 29 min. Das kürzeste Interview dauerte 1 h 9 min, das längste 2 h 8 min.

Bei dem Führen von Experteninterviews können sogenannte Interaktionseffekte auftreten, die das Produzieren brauchbaren Materials erschweren (siehe Kaiser 2021, 95ff). Dazu zählt, wenn der/die

Expert:in das Interview zur Selbstdarstellung nutzt (Katharsiseffekt), mehr Fragen an den/ die Interviewer:in stellt als selbst Fragen zu beantworten (Rückkopplungseffekt), aus Misstrauen Informationen zurückhält (Eisbergeffekt) oder versucht, dem Forscher/der Forscherin vorzuschreiben, in welche Richtung die Forschung gehen soll (Paternalismuseffekt). Gerade die letzten beiden Effekte betreffen insbesondere jüngere und weibliche Forscher:innen, da diesen weniger Expertise zugetraut wird (Helfferich 2014, 573) und hätten potentiell auch bei dieser Arbeit zum Problem werden können.

Um beim Auswerten des Materials dessen Qualität einschätzen zu können und die Rahmenbedingungen des Interviews nachvollziehbar zu machen, wurde die Gesprächssituation nach jedem Interview in einem Gesprächsprotokoll festgehalten (die verwendete Vorlage befindet sich in *Anhang 6: Vorlage für die Protokollierung der Interviewsituation*). Dort wurden wahrgenommene Interaktionseffekte, der Gesprächsmodus (Frage-Antwort-Schema oder offenes Fachgespräch) und die allgemeine Gesprächsatmosphäre notiert. Die Gesprächsatmosphäre war in allen Interviews angenehm und offen. Nur in einem Fall war es für die Interviewerin nicht immer ganz einfach, die Stimmung des Interviewpartners / der Interviewpartnerin einzuschätzen, weil sie mit dessen/deren Dialekt nicht vertraut war. Ein:e Expert:in wirkte – mutmaßlich aufgrund der späten Uhrzeit – etwas müde und gestresst, ein:e andere:r schien ob des Themas frustriert zu sein. Die Qualität der Antworten ist jedoch in keinem der Fälle beeinträchtigt: Die Expert:innen schienen sich Mühe zu geben, wohlüberlegt und nach besten Wissen und Gewissen zu antworten, auch wenn ihre Formulierungen teilweise etwas knapper ausfielen als die besser ausgeruhter / weniger frustrierter/ anderer Dialekte sprechender Personen.

Interaktionseffekte waren bis auf einen leichten Paternalismuseffekt in einem Fall nicht wahrnehmbar („Das ist ein Dilemma, das in Ihrer Arbeit herauszuarbeiten, finde ich total wichtig."). Es ist anzunehmen, dass dies mitunter dem Umstand zu verdanken ist, dass die Interviewten die Forscherin bereits persönlich kannten oder der Kontakt durch Personen zustande gekommen war, die die Expert:innen respektierten. Zudem zeigten alle großes Interesse an dem Forschungsthema und schienen bemüht zu sein, bestmöglich einen Beitrag zu seiner Bearbeitung zu leisten.

Aufbereitung der Daten

Der Pre-Test wurde dazu genutzt, eine Transkriptionssoftware auszuwählen. Das Material wurde mit f4 Audiotranskription (Pehl und Dresing 2024) und MAXQDA Transcription (VERBI

Software 2024) transkribiert; die Transkriptionsergebnisse waren bei beiden Programmen qualitativ gleich gut, die Transkriptionsgeschwindigkeit fiel bei f4 jedoch schneller aus (zwölf Minten pro eine Stunde Audiomaterial vs. 23 Minuten pro eine Stunde bei MAXQDA). Daher wurden alle folgenden Interviews mit f4 Audiotranskription transkribiert.

Die von der Software generierten Transkripte wurden anschließend mittels Anhören der Audiodateien bei gleichzeitiger Bearbeitung der Textdateien manuell verbessert. Da der Fokus der Analyse auf dem Inhalt des Materials und nicht auf sprachlichen Merkmalen liegt, wurden zur besseren Verständlichkeit sprachliche Glättungen vorgenommen, etwa das Löschen von Füllwörtern (z.B. „ähm", „genau", „also", „ja", usw.) oder grammatikalische Korrekturen (z.B. Verschieben des Verbs an die grammatikalisch korrekte Stelle). Dabei wurde darauf geachtet, dass durch die Veränderungen am Text keine Veränderung am Sinn der Aussagen entstanden. Zudem wurden Textpassagen gelöscht, die weder Bedeutung für das Forschungsthema haben noch für das Verständnis des Textkontexts relevant sind, in der Regel Small-Talk zu Beginn oder Ende des Interviews. Diese Auslassungen sind im Transkript gekennzeichnet. Der Betreuerin dieser Arbeit liegen zur Nachvollziehbarkeit sowohl die bearbeiteten Transkripte als auch die Rohversionen vor.

7.3. Analysemethode

Für die Analyse des Datenmaterials wird die qualitative Inhaltsanalyse nach Philipp Mayring angewandt. Sie ist eine Auswertungs- und Erhebungsmethode, die auf dem Grundprinzip der Reduktion basiert und sich daher dazu eignet, große Mengen an Textmaterial zu strukturieren. Sie zeichnet sich dadurch aus, dass das Material in den Kommunikationszusammenhang eingebettet wird, das Vorgehen systematisch und regelgeleitet ist, die Kategorien im Zentrum der Analyse stehen, das Verfahren dem jeweiligen Forschungsgegenstand angepasst und durch mehrere Probedurchläufe überprüft und verfeinert wird, quantitative Analyseschritte miteinbezogen werden und sie bestimmten Gütekriterien genügen muss (vgl. Mayring 2022, 49–52).

Analysemethode: Kategoriensystemerweiterung

Konkret wird eine Kategoriensystemerweiterung durchgeführt, bei der sowohl Techniken der Strukturierung als auch der Zusammenfassung zum Einsatz kommen, die Kategorien also sowohl deduktiv als auch induktiv gebildet werden (ebd., S. 107). Ziel der deduktiven Kategorienbildung (Strukturierung) ist es, „bestimmte Aspekte aus dem Material herausfiltern, unter vorher festgelegten Ordnungskriterien einen Querschnitt durch das Material zu legen oder das Material aufgrund

bestimmter Kriterien einzuschätzen“ (ebd., S. 66). Die Kategorien werden deduktiv aus der Theorie abgeleitet und an das Material herangetragen. Dazu wird ein Kodierleitfaden erstellt, in dem definiert ist, welche Textbestandteile unter eine Kategorie fallen, was anhand von Ankerbeispielen (repräsentativen Textbeispielen) und gegebenenfalls erläuternden Kodierregeln geschieht. Die detaillierten Schritte einer deduktiven Textauswertung nach Mayring, nach denen in dieser Arbeit vorgegangen wird, befinden sich in *Anhang 7: Regeln der deduktiven Kategorienbildung nach Philipp Mayring.*

Der induktive Teil der Kategoriensystemerweiterung besteht darin, dass der Kodierleitfaden um neue Kategorien erweitert wird, die nicht aus der Theorie abgeleitet wurden, sondern sich aus dem Text selbst ergeben (ebd., S. 107). Dabei werden die Regeln der Zusammenfassung angewandt, die in *Anhang 8: Regeln der Zusammenfassung nach Philipp Mayring* gelistet sind.

In dieser Analyse wurde zunächst ein Viertel des Materials durchgegangen (also zwei Interviews), anhand dessen der Kodierleitfaden deduktiv und induktiv erstellt wurde. Dazu wurden je ein Interview mit einem Spitzenverband und eines mit einem Ortscaritasverband ausgewählt. Anschließend wurde das restliche Material bearbeitet. Entstanden daraus weitere induktive Kategorien, wurde das bereits kodierte Material noch einmal durchgegangen, um die neuen Kategorien auch darauf anzuwenden.

Die Kategoriensystemerweiterung wurde als Analysemethode gewählt, weil mit dem Material mehrere Forschungsfragen beantwortet werden sollen, die sowohl induktive als auch deduktive Ansätze erfordern:

Tabelle 5: Analyseansatz je Forschungsfrage

Forschungsfrage	Ansatz	Begründung
1) Welche politischen, wirtschaftlichen und organisationalen Rahmenbedingungen lassen sich in der Literatur finden?	Deduktiv	Am Material wird überprüft, ob sich die Rahmenbedingungen, die die Literaturrecherche ergeben hat, auch in den Expert:innen-Aussagen wiederfinden. Die Literatur gibt deduktiv die Kategorien für die Analyse der Expert:innen-Aussagen vor.
2) Gibt es Herausforderungen für die Branche bezüglich IT-Sicherheit, die von bisheriger Literatur noch nicht erfasst wurden?	Induktiv	Da diese Herausforderungen nicht aus der Literatur übernommen werden können, müssen sie induktiv aus dem Material herausgearbeitet werden
3) Wie begegnet die Branche den Herausforderungen aktuell?	Deduktiv und induktiv	Die Maßnahme können (teilweise) den bereits in der Literatur beschriebenen Herausforderungen zugeordnet werden, d.h. auf der höchsten Abstraktionsebene entspringen sie einem deduktiven Ansatz (z.B.: Rahmenbedingung „Geringe Awareness der Mitarbeitenden“ → Maßnahme „Schulungen für Mitarbeitende“).

		Maßnahmen gegen nicht in der Literatur beschriebenen Herausforderungen sowie Unterkategorien werden induktiv gebildet (z.B. Maßnahme „Schulungen für Mitarbeitende“ → Konkretisierungen „Online-Schulungen“, „Newsletter“)
4) Welche Handlungsoptionen sieht sie, beziehungsweise welche Forderungen stellt sie, um die Rahmenbedingungen für IT-Sicherheit zu verbessern?	Deduktiv und induktiv	Siehe Forschungsfrage 3. Zum Beispiel (deduktiv): Rahmenbedingung „geringe Awareness der Mitarbeitenden“ → Forderung „Verankerung von IT-Sicherheit in den Lehrplänen der Schulen“

Richtung der Analyse und Analyseeinheiten

Für beide Analyseformen müssen Richtung und Einheiten der Analyse festgelegt werden. Die Richtung der Analyse bestimmt, welche Aspekte der festgehaltenen Kommunikation betrachtet werden sollen, etwa was der Text über den Kommunikator aussagt, welche Wirkung bei den Rezipienten erzielt werden soll, oder über den Gegenstand des Textes (vgl. ebd., S. 57f). In dieser Arbeit ist letzteres von Interesse. Die Auswertungseinheit gibt an, welche Materialteile jeweils nacheinander bearbeitet werden (ebd., S. 60), hier Interview für Interview. Die Kodiereinheit ist der kleinste Textbestandteil, der unter eine Kategorie fallen kann (ebd.). In dieser Analyse sind das Sätze oder bedeutungstragende Satzteile. Die Kontexteinheit ist der größte Materialbestandteil, der einer Kategorie zugeordnet werden kann, hier die Antwort eines einer Expertin/ eines Experten auf eine Frage.

Gütekriterien

Wie bereits eingangs in diesem Methodenkapitel dargelegt, lassen sich die klassischen Gütekriterien der quantitativen Sozialforschung nur schwer auf qualitative Ansätze übertragen. Dies gilt auch für die qualitative Inhaltsanalyse (vgl. ebd. S. 119). Stattdessen wird intersubjektive Nachvollziehbarkeit durch eine genaue Dokumentation des Forschungsablaufs (siehe nächster Absatz zum Ablaufmodell) und des Kodierleitfadens (siehe *Anhang 9: Kodierleitfaden)* hergestellt. Zudem gibt es spezifische inhaltsanalytische Gütekriterien, die die Zuverlässigkeit der Kategorienkonstruktion sowie der Anwendung der Kategorien auf das Textmaterial sicherstellen sollen und sich so den klassischen Kriterien Validität und Reliabilität annähern (ebd., S. 121). Eine Validierung durch ein externes Kriterium ist nur bedingt möglich: Da der Ausgangspunkt der Analyse deduktive Kategorien sind, die aus der Theorie abgeleitet wurden, können diese nicht zur externen Validierung herangezogen werden. Stattdessen wird die semantische Gültigkeit überprüft, also die Angemessenheit der Kategoriendefinition (ebd.). Dazu werden im Laufe des Kodierprozesses regelmäßig alle bisherigen

Textstellen einer Kategorie durchgegangen und auf Homogenität verglichen. Ist diese nicht gegeben, werden Textstellen umkodiert oder die Kategorie angepasst, etwa durch Aufsplittung in neue (Unter-)Kategorien. Der Erfüllung von Reliabilität wird sich durch die Kriterien der Reproduzierbarkeit und Stabilität (ebd., S.122) angenähert. Reproduzierbarkeit ist in diesem Fall mit intersubjektiver Nachvollziehbarkeit gleichzusetzen, die bereits beschrieben wurde. Die Stabilität der Analyse bezieht sich in dieser Arbeit vor allem auf die Intracoderreliabilität, das heißt, dass die Forscherin die Kategorien durchgängig gleich auf das Material anwendet. Diese wird dadurch erreicht, dass nach einem ersten Durchlauf von 25 % des Materials dieses noch einmal durchgearbeitet wird.

Ablaufmodell

Die qualitative Inhaltsanalyse zeichnet sich nach Mayring durch einen hohen Gegenstandsbezug des Analyseinstruments aus, ergo das Ablaufmodell muss für jede Inhaltsanalyse individuell entwickelt werden (vgl. ebd., S. 51). Aus den oben beschriebenen Überlegungen sowie unter Berücksichtigung der allgemeinen Ablaufmodelle in Mayring 2022 ergibt sich folgendes Modell:

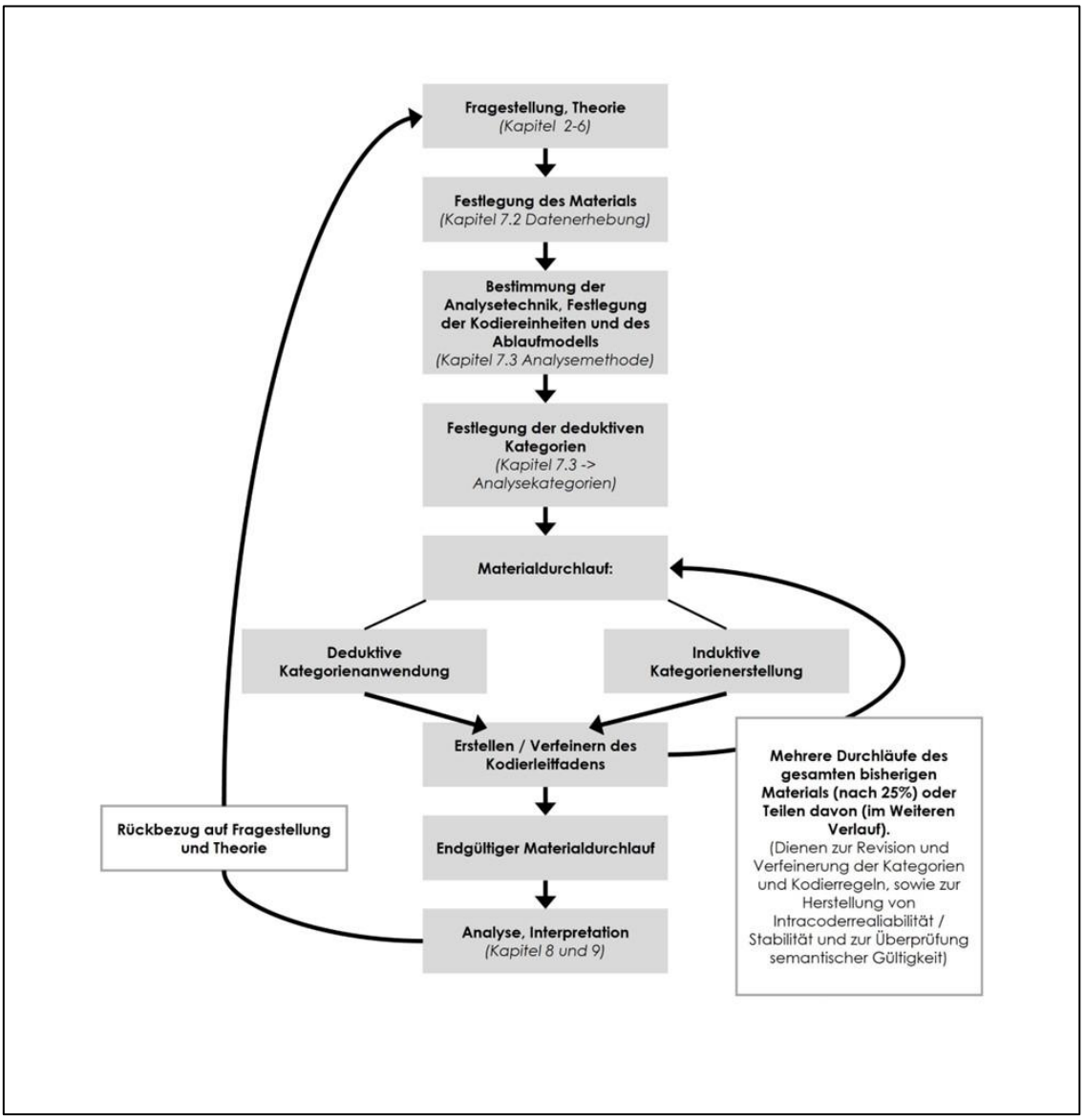

Abbildung 11: Ablaufmodell der Inhaltsanalyse. Eigene Darstellung.

Analysesoftware

Für die Kodierung wurde die Software MAXQDA Plus 24 in der Version 24.7.0 verwendet.

Analysekategorien

Die inhaltlichen Kategorien der obersten Ebene lassen sich – bis auf eine – alle deduktiv aus der Literatur ableiten und entsprechen in etwa den Themenblöcken des Interviewleitfadens. Lediglich eine Oberkategorie wurde induktiv aus dem Textmaterial gebildet, nämlich *Datenschutz*. Dieses Thema wurde in der Literaturrecherche nicht berücksichtigt und folglich wurde in den Interviews auch nicht danach gefragt. Dennoch stellen sechs von acht Expert:innen einen Bezug zwischen

Datenschutz und IT-Sicherheit her; in einem Interview beziehen sich sogar 15 % des Gesamttextes auf Datenschutz. Auf die Rolle der *Struktur* der freien Wohlfahrt und der Caritas für den Umgang mit IT-Sicherheit wurde im Literaturteil intensiv eingegangen. In den Interviews wurden allerdings keine dedizierten Fragen danach gestellt, um den zeitlichen Rahmen begrenzt zu halten. Nichtsdestotrotz sprachen alle Interviewpartner:innen Strukturmerkmale an. Die Unterkategorien zu den Oberthemen wurden teils deduktiv gebildet, sofern sie bereits aus der Literatur bekannte Aspekten besprachen, teils induktiv, wenn sie neue Gedanken darstellten. Auf der obersten Ebene befinden sich neun Kategorien (z.B. *6. Awareness Politik*), auf der zweiten Ebene 61 (z.B. 6.*4 Lobby*), auf der dritten 72 (z.B. *6.4.2 Lobby – Herausforderungen*) und auf der vierten 14 (z.B. *6.4.2.2. Mangelnde Zusammenarbeit in der freien Wohlfahrt*). Insgesamt wurden 928 inhaltliche Kodierungen vorgenommen.

Zusätzlich zu den inhaltlichen Kategorien wurden alle kodierten Segmente einer *Aussageart* zugeordnet, die den Forschungsfragen entsprechen: *Probleme* (Forschungsfrage 1: Rahmenbedingungen der Literatur entsprechend; Forschungsfrage 2: Bisher nicht erfasste Herausforderungen), *Maßnahmen* (Forschungsfrage 3: aktuelle Maßnahmen) und *Wünsche* (Forschungsfrage 4: Handlungsoptionen und Forderungen). Um die entsprechenden Textstellen schneller wiederfinden und besser vergleichen zu können, wurden außerdem bestimmte Interviewteile mit einem entsprechenden zusätzlichen Code versehen: *Beschreibung eines Cyberangriffs*, *Definition von IT-Sicherheit*, *Größte Herausforderungen*, *Sonst noch wichtig.*

Der vollständige Kodierleitfaden mit allen Unterkategorien sowie Kodieranweisungen, Ankerbeispielen, Code-Art (deduktiv / induktiv) befindet sich in *Anhang 9: Kodierleitfaden.* Auf der obersten Ebene sieht das Kategoriensystem folgendermaßen aus:

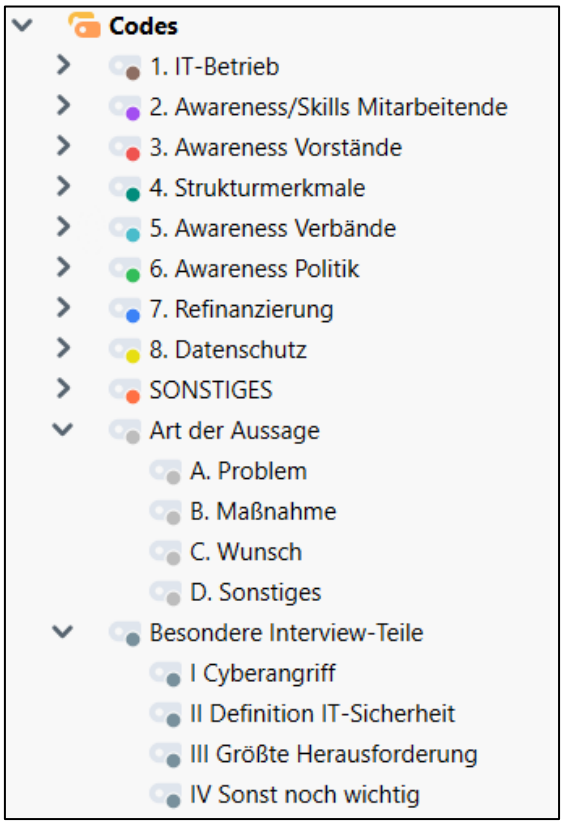

Abbildung 12: Codesystem

Quelle: Screenshot aus MAXQDA

8. Analyse

Die Auswertung der Interviews ergibt: Die Expert:innen bestätigen die Literatur. Sie berichten von schlechter IT-Infrastruktur, fehlendem IT-Fachpersonal, geringen IT-Kompetenzen der Mitarbeitenden, einer geringen Aufmerksamkeit unter Vorständ:innen für das Thema IT-Sicherheit, der Heterogenität und damit einhergehenden Komplexität der Caritas, Schwierigkeiten bei der Interessensvertretung und vor allem von Problemen bei der Refinanzierung. In den Details offenbaren die Interviews auch neue Aspekte und Nuancen.

Zu Beginn eines jeden Interviews wurde gefragt, was in den Augen des:der Expert:in die größten Herausforderungen bei der Herstellung von IT-Sicherheit für eine Caritasorganisation seien. Dies diente vorrangig dazu, einen leichteren Gesprächseinstieg und Anknüpfungspunkte für spätere Fragen zu schaffen. Gleichzeitig ist dadurch feststellbar, welche Herausforderungen von mehreren Gesprächspartner:innen als besonders wichtig identifiziert werden. Die Antwort ist eindeutig: In

ihrem Eingangsstatement benennen alle Expert:innen die Refinanzierung von IT-Ausgaben als größtes Problem. Zudem geht die Hälfe auf die fehlende Sensibilität ihrer Mitarbeitenden für IT-Sicherheit ein. Drei von acht führen Schwierigkeiten bei der IT-Infrastruktur / technischen Ausstattung an.

Ebenfalls zu Anfang der Interviews wurden die Expert:innen gebeten zu erklären, was sie unter IT-Sicherheit beziehungsweise Cybersecurity verstehen. In allen Definitionen kommt der Schutz von IT-Infrastruktur zum Erhalt der Arbeitsfähigkeit vor, was in der CIA-Triade der Dimension *availability* entspricht. Fünf Gesprächspartner:innen betonen, dass IT-Sicherheit dem Schutz von Daten dient (*confidentiality*)[21]. Für 50 % bedeutet IT-Sicherheit außerdem die Sensibilisierung von Mitarbeitenden. Zwei Personen gaben an, dass es bei Cybersecurity auch um Prozesse innerhalb der eigenen Organisation gehe, um jene zu gewährleisten. Damit zeigt sich, dass die Expert:innen durchaus ein gutes Verständnis davon haben, was IT-Sicherheit beinhaltet. Im weiteren Verlauf der Interviews fällt jedoch auf, dass der Fokus vieler Interviewpartner:innen mehr auf den Mitarbeitenden und Datenschutz liegt als auf dem Erhalt der Arbeitsfähigkeit. Insgesamt ist Datenschutz ein Thema, das sechs von acht Personen mehrfach ansprechen. Ein:e Expert:in setzt Datenschutz sogar mehr oder weniger mit IT-Sicherheit gleich. Da der Fokus dieser Arbeit nicht auf Datenschutz liegt, wird in diesem Kapitel nicht weiter darauf eingegangen. Stattdessen sind in *Anhang 10: Interviewausschnitte zur kirchlichen Datenschutzaufsicht* einige Schilderungen aufgeführt, inwiefern die Expert:innen kirchliche Datenschutzaufsichtsbehörden als wenig hilfreich empfinden, insbesondere im Umgang mit Cybervorfällen. Eine interessante Einschätzung sei an dieser Stelle geteilt: Die schlechten Erfahrungen mit dem (kirchlichen) Datenschutz verhinderten eine Auseinandersetzung mit IT-Sicherheit. In den Worten des Experten / der Expert:in:

> Das zahlt ein – oder eigentlich nimmt eher raus aus der Kasse – bei dem Thema Unternehmenskultur, die du ja brauchst, um eine entsprechende IT-Security umsetzen zu können. Also wenn der Datenschutz immer negativ konnotiert ist, dann dringst du auch mit dem Thema Cybersecurity schlecht durch. Ich habe ja vorhin erläutert, Cybersecurity ist nach meinem Verständnis Schutz der Infrastruktur und der physische Schutz der Daten, aber es ist zum anderen natürlich auch der Schutz schützenswerter Daten vor dem Zugriff Dritter, und da ist Cybersecurity ein Aspekt und Datenschutz im Sinne der Datenschutzgrundverordnung bzw. des KDG ein zweiter. So, und wenn

[21] *Integrity* wurde von niemandem angesprochen, was wahrscheinlich darauf zurückzuführen ist, dass bewusste Datenmanipulation in den Arbeitsfeldern der Sozialwirtschaft eher selten vorkommen dürfte.

> natürlich von diesen beiden Teilen der eine von echt schlechtem Ansehen ist, dann hat es auch der andere schwer.

Neben dem wiederkehrenden Thema des Datenschutzes sticht hervor, dass alle Expert:innen bisweilen ihren Gesprächsfokus von IT-Sicherheit auf IT im Allgemeinen oder Digitalisierung verschieben. Rückblickend hätte dies durch eine eingreifendere Interviewführung vermieden werden können. Allerdings wurden bewusst Vorständ:innen und nicht IT-Administrator:innen oder IT-Sicherheitsexpert:innen befragt – diese hätten sich gezielter zu IT-Sicherheit äußern können. Stattdessen geht es in dieser Arbeit um die strukturellen Rahmenbedingungen für IT-Sicherheit. Hier zeigen die Expert:innen klar auf, wie IT, IT-Sicherheit und Digitalisierung zusammenhängen: Wem Digitalisierung nicht wichtig ist, der versteht nicht, warum er:sie in IT-Infrastruktur investieren sollte, und dann ist auch keine IT-Sicherheit gegeben. Ein:e Expert:in macht dies explizit:

> Und so glaube ich, ist es auch, was IT und Digitalisierung betrifft. Aber wir sind noch gar nicht so weit, dass wir uns sozusagen als Vorreiter von Digitalisierung definieren, und deswegen ist auch die IT-Sicherheit, die dann in der Folge ist, auch nicht so im Blickpunkt. Und da glaube ich, dass wir als ganze Gesellschaft, als Volkswirtschaft und ergänzend als Wohlfahrtsverbände, dort einen erheblichen Schub brauchen, sonst werden wir das auch im internationalen Vergleich etc. nicht aufholen und nicht halten können. Und dann ist meine Hoffnung, dass Huckepack auch die IT-Sicherheit mitkommt.

Daher werden in der Analyse auch Textstellen, in denen die Interviewpartner:innen von IT und Digitalisierung sprechen, auf IT-Sicherheit mitbezogen.

Ein weiterer Aspekt, der sich durch alle Interviews zieht, ist, dass die Expert:innen deutlich öfter Probleme benennen als Maßnahmen oder Vorschläge: 63 % des kodierten Textes beschreiben Probleme, 21 % beinhalten Maßnahmen zur (systemischen) Verbesserung der IT-Sicherheit, die die Organisationen aktuell ergreifen, und 17 % sind Wünsche, Vorschläge oder Forderungen, wie die Probleme gelöst werden könnten[22]. Auch hier muss kritisch gesagt werden, dass eine andere Gesprächsführung möglichweise andere Ergebnisse erzielt hätte: Die Fragen waren mehr auf Probleme als auf Lösungen ausgerichtet. In den Beschreibungen der Schwierigkeiten sind allerdings häufig Maßnahmen und Wünsche impliziert, die in der nun folgenden Analyse entsprechend herausgearbeitet werden.

---

[22] Manche Textstellen fallen unter mehrere Kategorien; zudem gab es eine Kategorie „Sonstiges". Daher ergeben die Prozentangaben addiert nicht 100 %.

8.1 Organisationsinterne Faktoren

8.1.1 IT-Betrieb: Infrastruktur und IT-Fachkräfte

In Bezug auf ihren IT-Betrieb bestätigen die Expert:innen, dass karitative Einrichtungen oft mit veralteten Geräten und Programmen arbeiten, Privatgeräte nutzen und sich keine Fachkräfte mit einer Spezialisierung auf IT-Sicherheit leisten können. Textbeispiele zur IT-Ausstattung finden sich in *Anhang 11: Interviewausschnitte zur IT-Ausstattung*. Auffällig ist, dass beinahe allen Interviewpartner:innen – egal ob Vorständ:in eines kleinen operativen Trägers, eines größeren Trägers oder spitzenverbandlich tätig – bewusst ist, dass die Situation bei den kleineren Trägern deutlich schwieriger ist als bei den Großen:

> Der zweite Punkt ist, wenn ich auf die interne Struktur schaue, da ist schon die Frage: Sind vor allem die kleinen Träger, wo zuweilen noch Turnschuh-Administration geschieht, strukturell und prozessual darauf vorbereitet, einen Angriff abzuwehren bzw. ihn, wenn er kommt, überhaupt bewältigen zu können?

Den großen Trägern (das Zitat bezieht sich auf einige konkrete Träger zwischen 2.500 und 8.500 Mitarbeitenden) wird eine bessere Ausstattung zugeschrieben:

> Da gibt es tatsächlich auch ausgesprochen professionelle IT-Strukturen; entweder Partner, externe Partner oder Kooperationen nach innen, oder auch in eigenen Abteilungen. Ich sag mal, da würde ich jetzt von Weitem sagen, die sind alle zeitgemäß unterwegs.

Vier der fünf befragten Organisationen, die operativ in der sozialen Arbeit tätig sind, betreiben ihre IT nicht selbst, sondern haben sie an Dienstleister abgegeben, zwei von ihnen erst kürzlich. Dies ist nicht repräsentativ für die Sozialwirtschaft: Laut Kreidenweis und Wolff waren 2022 nur 19 % aller IT-Aufwendungen ausgelagert (Kreidenweis und Wolff 2022, 19). Interessant sind die Begründungen, weswegen die Organisationen ins Outsourcing gegangen sind. Der:die Vorständ:in eines kleineren Ortscaritasverband gibt an, dass seine:ihre Organisation schlicht zu klein sei, als dass es sich lohnen würde, eigenes IT-Personal anzustellen. Eine Abteilung, die groß genug ist, auch im Urlaubs- und Krankheitsfall den Träger lückenlos zu betreuen, könne er:sie sich nicht leisten. Die beiden größeren Verbände haben sich dagegen weniger aus finanziellen Gründen für Outsourcing entschieden, sondern aus der Einsicht heraus, langfristig kein qualifiziertes IT-Fachpersonal für die steigende IT-Komplexität zu finden. IT-Fachkräfte fänden in reinen IT-Unternehmen bessere Technik, Fortbildungsmaßnahmen und Gehälter vor als in der internen IT-Abteilung

eines Caritasträgers. Für diese großen Träger ist Outsourcing an einen größeren Dienstleister mehr als eine individuelle Entscheidung; es ist ein Desiderat für die Caritaswelt an sich:

> IT-Mitarbeitende brauche ich im Grunde in der Caritas nicht mehr. Das ist jetzt ein bisschen eine Zuspitzung, aber wir müssen uns konzentrieren auf das, was wir können. Und wir brauchen professionelle Partner und wir müssen die Partner steuern. […]Ich brauche als Vorstand einen Sicherheitsberater, einen CISO[23], der mich in diesen Fragen unterstützt, berät, begleitet und der mir drei Szenarien vorstellt, damit ich mich entscheiden kann. Aber ich brauche keinen, der mir das nach innen selber aufbaut und umsetzt und sicherstellt. Und das ist schon noch ein Entwicklungsschritt, den die Caritas gehen muss, glaube ich.

Doch auch die Dienstleistersteuerung gestaltet sich für die kleinen Träger schwierig: Dies müssen Mitarbeitende aus der Geschäftsführung, Verwaltungsleitung, dem Datenschutz oder der Öffentlichkeitsarbeit zusätzlich zu ihren eigentlichen Aufgaben übernehmen. In einem Fall war der:die Vorständ:in übergangsweise sogar monatelang persönlich für den Austausch von Rechnern und Telefonen und das Zurücksetzen von Passwörtern zuständig. Alle betroffenen Organisationen bemühen sich daher, bei der Nachbesetzung solcher Stellen auf IT-Affinität zu achten. Das nächste Kapitel zu IT-Fähigkeiten von Mitarbeitenden in der freien Wohlfahrt lässt jedoch darauf schließen, dass es nicht ganz einfach ist, solche Mitarbeitenden zu finden.

Hinzu kommt, dass Dienstleister nicht gleich Dienstleister ist. Die beiden Vorständ:innen der kleineren Organisationen betonen beide, dass sie zufrieden mit ihren lokalen Dienstleistern sind, schon lange mit ihnen zusammenarbeiten und daher ein enges, gutes Verhältnis hätten. Auch die drei Expert:innen aus Spitzenverbänden verstehen, dass für kleine Träger der persönliche Kontakt zu Dienstleistern und spezifisch auf sie zugeschnittene Lösungen wichtig sind. Gleichzeitig problematisieren sie und auch der der:die Gesprächspartner:in, der:die zahlreiche kleine Verbände als Unternehmensberater:in betreut hat, kleine lokale Dienstleister:

> In den Mitgliedsvereinen, da ist es immer das Risiko von den One-Man-Shows. Kleine Vereine haben kleine IT-Dienstleister, oft Einzelunternehmer, die das dann eben machen. Die machen oft einen guten Job, es sei denn, die sind an einem Punkt stehen geblieben und haben sich selber nicht weitergebildet. Dann ist die IT natürlich sozusagen auf dem Stand, wo diejenigen aufgehört haben, sich weiterzuentwickeln. So, und das sehe ich als schwierig an.

[23] Chief Information Security Officer

Große Dienstleister sind wiederum teuer und ihr Angebot schlicht zu groß für die Bedürfnisse kleiner Träger, wie ein:e Vertreter:in eines Spitzenverbandes erklärt. Dies unterstreicht auch ein:e Expert:in aus eigener Erfahrung: Der Versuch, von einem lokalen Anbieter zu einem größeren, zumal auf die Sozialwirtschaft spezialisierten, Anbieter zu wechseln, scheiterte an den Preisen.

8.1.2 Mitarbeitende

Wie bereits erwähnt, ist die Sensibilisierung von Mitarbeitenden für IT-Sicherheit ein Thema, das die Expert:innen besonders umtreibt. Teilweise sehen sie im mangelnden Sicherheitsbewusstsein der Mitarbeitenden ein größeres Problem als in der Umsetzung technischer Anforderungen. Sie betonen, dass es wichtig sei, Mitarbeitende zu schulen und dies kontinuierlich zu tun. Sie geben aber auch zu, dass sie an der Umsetzung scheiterten, aus Geld-, Zeit- und Personalmangel:

> Ich stelle den Mitarbeiter frei, ich bezahle den und in der Zeit erarbeitet er mir aber ja auch nichts. Eine doppelte Investition, das kostet alles Geld und Ressourcen – und die haben ja auch in den letzten Jahren abgenommen. Wenn sich jemand aus der Pflege schulen will, dann fehlt er mir nicht nur finanziell, sondern ja auch tatsächlich als Kopf am Bett.

Zudem bestätigen die Interviewpartner:innen, dass in ihrer Erfahrung Mitarbeitende im sozialen Bereich über ein gering ausgeprägtes Interesse an IT und damit auch geringe Kompetenzen verfügen. Pflegekräfte, Sozialarbeiter:innen, Pädagog:innen usw. hätten ihren Beruf gewählt, weil sie mit Menschen arbeiten wollen, nicht mit Technik. Einen weiteren wichtigen Faktor sehen sie in der fehlenden digitalen Bildung in Schulen, Berufsschulen und Studiengängen:

> Fangen wir da noch tiefer an: Schule. Also eigentlich gehört das in die Schule rein, dass unterrichtet wird: Immer wenn ihr solche Sachen hier benutzt, dann müsst ihr euch auch immer Gedanken zum Thema Sicherheit machen. Also dass da so Grundsachen mitvermittelt werden. Das ist jetzt eigentlich eine unserer Kulturtechniken geworden, die IT-Nutzung, und dann muss man die auch vermitteln, damit man zumindest Grundverständnisse von Dingen hat. Das gehört eigentlich in sämtliche Ausbildungsberufe mit hinein.

Damit müssten sie als Arbeitgeber „ein Defizit [nachholen], das durch die Bildung in der Bundesrepublik passiert […], weil das nicht im Bildungskanon auf den normalen Bildungswegen erfolgt." Selbst diejenigen, die Berufsschulen vertreten oder sogar selbst betreiben, sehen dort wenig eigenen Handlungsspielraum, weil die Lehrpläne Sache der Bundesländer sind.

8.1.3 Vorständ:innen

Gefragt, wie sie das Bewusstsein von Vorständ:innen in anderen Caritasorganisationen einschätzen, fällt das Bild gemischt aus: Vier Expert:innen nehmen bei ihren Peers bzw. Mitgliedsorganisationen eine Awareness für IT-Sicherheit wahr, vier sehen eher eine fehlende Beschäftigung mit dem Thema[24]. Doch auch diejenigen, die IT-Sicherheit als im Bewusstsein ihrer Kolleg:innen angekommen bewerten, tun dies mit Einschränkungen: Es sei stärker in der Diskussion als früher, habe aber keine hohe Priorität. Hier hätten andere Themen Vorrang: Fachkräftemangel, die Refinanzierung von Immobilien, sinkende Sozialausgaben seitens des Staates, das Alltagsgeschäft in Form von Verwaltungsaufgaben. Zudem müssten Vorständ:innen das Thema IT-Sicherheit aufgrund von Geldmangel bewusst depriorisieren (mehr dazu in *8.2.4 Refinanzierung*):

> Also, um es sehr zugespitzt zu formulieren, könnte man sagen: Stecke ich das Geld in die IT-Sicherheit oder berate ich dafür 50 Leute mehr? Was ist mein eigentlicher Auftrag? Für IT-Sicherheit zu sorgen oder die 50 Menschen zu versorgen?

Als Gründe für ein mangelndes Bewusstsein werden vor allem fehlendes Wissen und Überforderungen angeführt: Das Thema sei „angstbesetzt und fremd", „völlig unverständlich und schwierig" und „wenig greifbar für die Menschen." Zudem bedeute eine ernsthafte Beschäftigung mit IT-Sicherheit, sich grundlegend mit den Defiziten und Prozessen in der eigenen Organisation auseinandersetzen zu müssen, und dazu fehle die Bereitschaft. Diese Unwissenheit und Überforderung führten letztlich zu einer falschen Einschätzung bezüglich der Gefährdung der Organisation durch Cybervorfälle:

> Und da glaube ich, haben wir tatsächlich auch in der verbandlichen Caritas ein Thema, weil diese Fragestellungen hochvirulent sind, von den Führungskräften und von den Vorständen in der Verantwortung aber nicht gesehen werden. Oder sie werden negiert oder sie werden relativiert und im Sinne eines Risikomanagements als ‚tritt bei mir nicht ein' abgetan. Also das heißt, die Einschätzung für das eigene Unternehmen, was das Risiko angeht, ist fehlgeleitet.

Wie schon bei der Ausstattung und Organisation des IT-Betriebs scheint auch bei der Awareness der Vorstände die Größe des Trägers eine Rolle zu spielen. Während der:die Vorständ:in eines kleinen OCVs klar formuliert, dass die anderen Vorständ:innen in seiner:ihrer Region sich nicht

[24] Ein:e Expert:in sieht eine geringe Awareness in der Sozialwirtschaft an sich, aber eine hohe bei den größeren unter den eigenen Mitgliedern. Ein:e andere:r spricht vor allem über das Interesse benachbarter Organisationen nach einem Cyberangriff in der Region, macht aber keine Aussagen über eine grundlegende Awareness.

mit IT-Sicherheit beschäftigten, betont ein:e Vertreter:in eines Spitzenverbandes, große Träger mit einer hoch professionalisierten Unternehmenssteuerung verfügten über eine hohe Sensibilität.

Als einen weiteren Faktor nennen zwei Gesprächspartner:innen das Alter von Vorständ:innen: Wer kurz vor dem Ruhestand stehe, fasse Themen wie Digitalisierung, IT und IT-Sicherheit nicht mehr grundlegend an. Dies bestätigt eine Person aus eigener Erfahrung: Er:sie hatte von seinem:ihrem Vorgänger, der sein Amt bis zur Rente innehatte, eine marode IT-Infrastruktur übernommen. In diesem Fall wurde der Vorstandswechsel als Chance genutzt, IT und IT-Sicherheit in der Organisation neu zu denken.

Hauptgrund für vorhandene bzw. gestiegene Sensibilität von Vorständ:innen für IT-Sicherheit sind ganz klar Cyberangriffe auf die Sozialwirtschaft, insbesondere auf andere Caritasorganisationen[25]. Vorständ:innen, deren Verband selbst Opfer geworden war, zeigen ein tiefes Verständnis von technischen Zusammenhängen, scheinen IT-Sicherheit und IT an sich eine besondere Bedeutung für das Wohlergehen ihrer Organisation beizumessen, teilen ihre Erkenntnisse in verschiedenen Formaten und erleben wiederum Interesse seitens anderer Vorständ:innen an ihren Erfahrungen. Auch Gesprächspartner:innen, die selbst von keinen Cyberangriff betroffen waren, betonen, wie insbesondere der Angriff auf den DiCV München das Thema IT-Sicherheit in ihren Fokus und in den Fokus anderer gerückt habe. Sogar innerorganisatorisch sei dies hilfreich:

> Und dabei hat uns die Konstellation, dass München so lahmgelegt war, schon geholfen, dass es eine hohe Anerkennung und Anerkenntnis und eine Sensibilität für die Themen gab und wir die auch organisational signifikant einfacher durchsetzen konnten als vorher. Das ist bitterbös, wenn man das ehrlich anguckt.

Dass München als „Warnschuss" wahrgenommen wird, mag am Ausmaß des Vorfalls liegen, sicher aber auch daran, dass Thomas Schwarz, Finanzvorstand im DiCV München/Freising, auf zahlreichen Veranstaltungen[26] von dem Angriff berichtete, und entsprechend auch von mehreren Expert:innen namentlich erwähnt wurde. Solche Formate werden von den Expert:innen als wichtig und hilfreich eingeschätzt. Wie effektiv sie langfristig sind, wird aber zumindest von einem:einer

---

[25] Eine Zitatsammlung zu dem Thema befindet sich in *Anhang 12: Interviewausschnitte zur Sensibilisierung für IT-Sicherheit durch Cyberattacken auf die Sozialwirtschaft.*

[26] Öffentlich verfügbare Beiträge: Webinar zur Cybersicherheit in der Gesundheits- und Sozialbranche | Bayerische IHK am 22.11.2024; Nichts geht mehr | Neue Caritas 20/2024

Gesprächspartner:in kritisch gesehen: Kurz nach einem Angriff gebe es einen Aufschrei, doch zu einer systematischen Bearbeitung des Themas führe das nicht.

Wie wichtig Awareness für IT-Sicherheit von Vorständ:innen und Geschäftsführer:innen ist, darin sind sich die Interviewpartner:innen einig: Sieben von acht thematisieren, dass IT-Sicherheit Managementaufgabe sein müsse. Eine Person aus dem Vorstand einer attackierten Organisation beschreibt, dass IT für ihn:sie vor dem Angriff nur ein Randthema gewesen sei, das sei „wie eine Versicherung, die muss laufen, da kümmert man sich nicht wirklich drum", beziehungsweise, das sei „Tagesgeschäft, wie dass irgendeiner sich drum kümmern muss, dass Klopapier da ist." Inzwischen sei IT für ihn:sie nicht mehr nur irgendein „Orga-Thema", sondern gleichwertig mit Personal und Finanzen. Andere nehmen mit Sorge wahr, dass ihrem Eindruck nach andere Organisationen IT und IT-Sicherheit nicht als Führungsaufgabe definieren, sondern sich auf ihre IT- oder Verwaltungsleitungen verlassen, wodurch das Thema aber nicht strategisch und systemisch durchdacht werde. Dies zeige sich auch daran, dass zu Gremien / Arbeitskreisen / etc. zu IT und Digitalisierung in der Regel IT-Administrator:innen und Digitalbeauftragte geschickt würden, anstatt dass die erste Führungsebene selbst teilnehme. Einen Unterschied zwischen kleinen und großen Trägern, der an anderen Stellen deutlich sichtbar ist, gibt es hier interessanterweise nicht. So macht der:die Vorständ:in eines Ortscaritasverbands deutlich:

> Aus meiner Sicht ist es eine Führungsaufgabe. Also nur, wenn der Geschäftsführer oder der Vorstand dahintersteht und das Thema treibt, nehmen es auch alle mit. Also für mich ist immer die Frage, wie kann man das als Stabsstelle – die ist ja eine Querabteilung – wie will die das in die Leitungsebenen und nach unten bringen? Das funktioniert aus meiner Sicht nicht.

Damit ist seine:ihre Aussage fast identisch mit der eines: einer Vorständ:in eines großen Diözesanverbandes, der:die sie um ein strategisches Element ergänzt:

> Was, glaube ich, noch mal eine relevante Botschaft ist, ist die Frage, wie gelingt es in der Sozialwirtschaft und in der Caritaswelt insgesamt, das IT-Thema und damit auch das Securitythema als Managementthema zu verstehen? Das finde ich hochrelevant. Und immer dann, wenn ich das nicht tue, wird es die notwendige Bedeutung nicht bekommen. Also wenn die IT-Security und alle vorgelagerten und / oder damit verbundenen IT-Fragen System der IT-Abteilung sind, werden wir nicht ausreichend auf die Risiken vorbereitet sein als Caritasverband oder Stiftung oder GmbH oder was auch immer, und werden auch die Entwicklung nicht gehen können. […] Also meine These, und das wäre mir tatsächlich auch ein Anliegen als Kernaussage: Wenn das nicht als Managementaufgabe verstanden wird, dann wird es nicht gelingen, die relevanten

> Zukunftsfragen der IT und der IT-Security vernünftig in die Zukunft zu führen. Davon bin ich überzeugt, tatsächlich.

8.2 Organisationsexterne Faktoren

8.2.1 Strukturmerkmale

In den Interviews wurde nicht direkt nach Strukturmerkmalen der freien Wohlfahrt und der Caritas gefragt; nichtsdestotrotz sprechen alle Expert:innen diese Ebene an, teils sogar ganz explizit: „Eines der großen Probleme, die die Caritas hat, mutmaßlich auch bei dem Thema IT-Security, liegt in der Struktur begründet." Bevor auf die organisationsexternen Strukturen eingegangen wird, sollen zunächst noch zwei organisationsintere strukturelle Faktoren erwähnt werden, die bereits im vorherigen Kapitel angeklungen sind. Zum einen erwähnen die Gesprächspartner:innen wiederholt, welche Rolle die Größe einer Organisation spielt: Kleine Träger haben es besonders schwer. Das soll nicht heißen, dass mittlere und große Organisationen problemlos einen hohen Standard an IT und IT-Sicherheit herstellen könnten – sie stehen häufig vor genau den gleichen Herausforderungen wie die kleinen – die kleinen haben nur *noch* weniger Ressourcen, diese Probleme zu lösen. Sie verfügen über eine schlechtere IT-Ausstattung und finden schwerer qualifiziertes IT-Fachkräfte. Außerdem sind sie finanziell schlechter aufgestellt (siehe *8.2.4 Refinanzierung*) und haben nicht das Personal, um sich zu einem weiteren Thema zu informieren, zu vernetzen und ihre Interessen zu vertreten (siehe *8.2.2 Verbände*). Ein zweiter Faktor, der sich unmittelbar in den Organisationen selbst manifestiert, gleichzeitig aber ein Merkmal der freien Wohlfahrt an sich zu sein scheint, ist eine „Hemdsärmeligkeit", wie es ein:e Expert:in bezeichnet, also mangelnde Kompetenz in der Unternehmensführung. Dies zeige sich in fehlendem Krisen- und Risikomanagement sowie mangelhafter Prozess- und Finanzsteuerung („Ich sage jetzt mal, die Finanzsteuerung ist jetzt nicht unbedingt die Stärke der Sozialwirtschaft, in Summe, meines Erachtens"). Ohne diese Kompetenzen ist es schwierig, IT-Vorfällen vorzubeugen, sie im Ernstfall schnell zu bearbeiten und den Schaden zu begrenzen.

Bei den organisationsexternen Strukturmerkmalen heben die Expert:innen die bereits in der Literatur beschriebene Heterogenität der Organisationen hervor, bezogen auf ihre Unternehmens-, Finanzierungs- und IT-Infrastrukturen. Das behinderte die Träger dabei, mit anderen Trägern zu kooperieren und die Spitzenverbände, Koordinationsarbeit zu leisten:

> Das große Problem, warum wir uns auch als Verband da sehr schwertun, irgendwie einen Fuß in die Tür zu kriegen – übrigens bei dem Thema Digitalisierung überhaupt

> und insgesamt – ist, dass es eine sehr, sehr heterogene Landschaft an Systemen gibt, auch an Infrastruktur. […] Das ist sehr heterogen und auch die Prozesse sind wenig vergleichbar – nein, anders: Die Prozesse sind zwar vergleichbar, aber auch nur vergleichbar. Sie sind nicht gleich und das macht es schwierig. Noch nicht mal der Input und der Output sind das Gleiche. Da ist es dann halt echt schwierig, koordinierend tätig zu sein.

Eng verbunden mit der Heterogenität ist das Subsidiaritätsprinzip, zu dem die Gesprächspartner:innen ein ambivalentes Verhältnis haben: Sie sehen in ihm die Quelle von Ineffizienz, aber auch das Ermöglichen von maßgeschneiderten Lösungen, Taubheit gegenüber den Erfahrungen anderer und zugleich kurze Reaktionszeiten vor Ort, Chaos und Kreativpotential, eine Gefahrenquelle und gleichzeitig die Essenz von karitativem Handeln. Oder wie es eine Person auf den Punkt bringt: „Unsere Freiheit ist unsere Strafe: Dass wir eben nicht durchgreifen können." Drei Gesprächspartner:innen identifizieren es als problematisch, dass es prinzipiell eine Angst gebe, Macht, Einfluss und Verantwortung zu verlieren, gleichzeitig bewerten zwei derselben Personen es als positiv, dass Verantwortung lokal übernommen wird:

> Aber wie gesagt, dieses Thema der Handhabbarkeit unternehmerischer Risiken, für die ich Verantwortung trage als Führungskraft – als oberste Führungskraft –, das ist etwas, was die Einrichtungen und die Verbände zu Recht nicht abgeben wollen, und auch nicht abgeben können, wenn sie verantwortungsbewusst sind.

Konkret geht es hier auch darum, bei einem IT-Problem schnell handlungsfähig und nicht abhängig von einer weit entfernten Instanz zu sein. Dies bestätigt ein kleiner Ortscaritasverband: Das Angebot des zuständigen Diözesancaritasverbandes, die IT-Infrastruktur des OCVs in die IT-Abteilung des DiCVs einzugliedern, lehnte der kleine Träger vehement ab, weil er zufrieden mit dem lokalen IT-Dienstleister sei. Denn: „Wie gesagt, wir wählen da aus, was für uns passt."

Die Folge aus dieser Heterogenität und diesem ambivalenten Verhältnis zum Subsidiaritätsprinzip ist fehlende Kooperation, die sich einige der Interviewpartner:innen explizit wünschen würden. Wenn es darum geht, Lobbyarbeit zu betreiben (mehr dazu in *8.2.3 Politik*), erschweren es die Vielfältigkeit und das Beharren auf dem eigenen Standpunkt, gemeinsame Forderungen zu formulieren. Bei der Zusammenarbeit zwischen den sechs Spitzenverbänden der freien Wohlfahrt käme laut einer Person hinzu, dass die Kürzungen von Sozialausgaben in öffentlichen Haushalten eine Konkurrenzsituation kreieren würden, bei der die Verbände ihre individuellen Interessen an den begrenzten Ressourcen über die ohnehin nur schwer formulierbaren gemeinsamen Interessen stellten.

Kooperation unter den Einrichtungsträgern, einhergehend mit einer Standardisierung und Konsolidierung von IT-Infrastruktur, wird ebenfalls durch die Unterschiedlichkeit der IT-Systeme und Unternehmensstrukturen sowie Angst vor Kontrollverlust behindert. Dadurch werden mögliche Skalierungseffekte nicht genutzt:

> Grundsätzlich ist es doch völlig absurd, wenn ich als Ortscaritasverband oder als Stiftung XY […] eine Finanzsoftware einführen will und bei null anfange. Ich beschäftige mich mit X Anbietern, mache ein Riesen-Auswahlverfahren […]; da sind dann monatelang Ressourcen beschäftigt und [ich] komme hinten zu dem Ergebnis, zu dem ein anderer Verband mit einem ähnlichen Prozess auch gekommen ist. Und wenn ich es dann einführe, dann bin ich nicht in der Lage, Standardprozesse zu denken, also Kostenstellenstandards zu definieren. Da gibt es zwar dann im Buchhaltungsbereich einen Kontenrahmenplan für die Sozialwirtschaft, das ist ja schon mal was, sage ich mal, aber dann fängt es schon an und so könnte ich alle möglichen Prozesse durchgehen.

8.2.2 Verbände

Bezogen auf die Spitzenverbände, die für die befragten Organisationen zuständig sind, ist das Bild, inwiefern sie für IT-Sicherheitsthemen sensibilisiert sind, sehr gemischt. Dabei muss Folgendes bedacht werden: Aussagen von Ortscaritasverbänden zu ihren Diözesancaritasverbänden beziehen sich auf spezifische DiCVs, Schlussfolgerungen zu „den" DiCVs zu ziehen, ist also nicht möglich. Da unter den Befragten zwei DiCV-Vorständ:innen sind, kann diese Art von Spitzenverband sowohl von der Innen- als auch Außenperspektive betrachtet werden. Die Einschätzung des Deutschen Caritasverbandes und der Bundesarbeitsgemeinschaft der freien Wohlfahrtspflege findet wiederum von verschiedenen Entfernungen heraus statt: Während die OCVs kaum Kontakt zu dieser Ebene haben[27], sind die beiden DiCV-Vertreter:innen Mitglied in Kommissionen des DCVs und die Fachverbände sprechen in manchen Themengebieten sogar stellvertretend für den DCV.

Bei der Frage, ob IT-Sicherheit eine spitzenverbandliche Aufgabe sei, zeigt sich, dass zwar Erwartungen an die jeweils höhere Ebene existieren, die Spitzenverbände IT-Sicherheit jedoch nicht als expliziten Auftrag interpretieren. So äußert ein:e OCV-Vorständ:in, dass sie es als Aufgabe von Spitzenverbänden ansehe, die Rahmenbedingung für Digitalisierung (und damit implizit auch IT-Sicherheit) zu schaffen, indem sie Einfluss auf Sozialgesetzgebung und Refinanzierungs-Rahmenvereinbarungen nehmen. Vertreter:innen eines DiCVs und eines Fachverbands erklären, dass sie

[27] Ein:e OCV-Vertreter:in ist ebenfalls Mitglied einer DCV-Kommission, thematisiert dies aber nicht.

von ihren Mitgliedern keinen Auftrag für das Thema hätten, sondern Angebote zu IT-Sicherheit aus eigener Motivation heraus, „on top" anböten. Derselbe DiCV sieht aber wiederum Verantwortung beim DCV und den anderen Spitzenverbänden der freien Wohlfahrt: „Also ich glaube tatsächlich, dass es von den Spitzenverbänden eine derer Aufgaben ist. Die wird halt an dem Punkt nicht wahrgenommen."

Während die beiden DiCVs deutlich äußern, dass sie weder beim DCV noch bei der BAGFW wahrnehmen, dass diese IT-Sicherheit als Thema für sich annehmen, schätzen die Fachverbände die Sensibilität beider Akteure als definitiv gegeben oder zumindest beim Thema Telematikinfratruktur[28] vorhanden an. Von den OCVs sagen zwei aus, dass sie seitens des DCVs und der BAGWF keine Impulse zu IT-Sicherheit erhalten würden:

> Klar, wir bekommen grundsätzlich [Informationen], aber jetzt konkret zu IT-Sicherheit? Nein. Also ich kriege auch LAG[29]-Infos etc., aber auch was vom DCV kommt, klar. Die Caritas aktuell[30], mehr kommt da ja eh nicht.

Dieselbe Person stellte allerdings auch klar, dass bei ihren spitzenverbandlichen Kontakten „die Decke drauf" sei beim DiCV, d.h. die Vertretung auf höheren Ebenen für sie durch den DiCV geschehe – wie föderales Spitzenverbandswesen nun einmal funktioniert.

Ein Format, das zwei OCVs erwähnen, ist die Bundeskonferenz der hauptamtlichen Vorstände und Geschäftsführungen der Ortscaritasverbände (Buko), die einmal im Jahr stattfindet und von der Fortbildungsakademie des DCVs organisiert wird. Bei einer der Konferenzen sei IT-Sicherheit ein Thema gewesen, insbesondere der Cyberangriff auf den DiCV München. Was zudem von den meisten Akteur:innen (positiv) wahrgenommen wird, sind die Bemühungen der DCV-Geschäftsstelle, Digitalisierungsprojekte in der Caritaswelt voranzubringen. Hier werden vor allem die Stabstelle Digitale Transformation, die Vorstandskommission Digitale Agenda und der Digitalfond

28 Die Telematikinfrastruktur (TI) ist ein digitales Netzwerk, das Akteure im Gesundheitswesen wie Ärzte, Apotheken und Krankenkassen miteinander verbindet, um den schnellen und sicheren Austausch von Gesundheitsdaten zu ermöglichen. Ab dem 1. Juli 2025 müssen auch Pflegeeinrichtungen an die TI angeschlossen sein.

29 Landesarbeitsgemeinschaft der freien Wohlfahrt

30 Gemeint ist die *Neue Caritas*. Ausgabe 2024/20 der *Neuen Caritas*, die drei Artikel zu IT-Sicherheit erhält, war kurz vor dem Interview erschienen. Der:Die Gesprächspartner:in hatte sie jedoch zu diesem Zeitpunkt noch nicht gelesen.

erwähnt, über den das Projekt *caritas.next*[31] aufgesetzt wurde. Diese Digitalvorhaben fokussierten jedoch auf Digitalisierung der Klient:innenarbeit, z.B. ein KI-Chatbot, der bei der Beantragung von Bürgergeld unterstützt, und nicht auf IT-Infrastruktur und IT-Sicherheit. Bei der Kooperation zu Digitalisierung mit anderen Spitzenverbänden der freien Wohlfahrt auf Landesebene berichten Expert:innen aus Bayern und Hessen, dass es in den entsprechenden LAGs keine Arbeitsgruppe zu Digitalisierung gibt; in Baden-Württemberg hingegen gibt es seit Anfang 2024 einen Arbeitskreis Digitalisierung. Dass die Expert:innen so ausführlich über Digitalisierung sprechen, obwohl sie wissen, dass IT-Sicherheit in den entsprechenden Digitalisierungsgremien nicht behandelt wird, scheint die Hoffnung zu implizieren, dass Digitalisierung als Hebel für insgesamt bessere IT und damit auch IT-Sicherheit dienen könnte.

Die Erfahrungen der Ortsebene mit ihren Diözesancaritasverbänden fallen verschieden aus: Eine Person merkt an, dass ihrer Erfahrung nach DiCVs digital selbst schlecht aufgestellt seien und daher keine Vorreiterrolle übernehmen könnten. Das bereits zitierte Beispiel eines DiCVs, das dem OCV die Eingliederung dessen IT-Betriebs in die IT-Abteilung des DiCVs vorschlägt, zeigt, dass es hier zwar ein Angebot gibt, dieses aber von der Ortsebene als nicht passend angesehen wird. Die digitale Datenschutzschulung, die derselbe DiCV zur Verfügung stellt, betrachtet der OCV dagegen mit Interesse und prüft, ob sie sich für seine Einrichtungen eignet. Der dritte OCV ist wiederum voll des Lobes für seinen Diözesancaritasverband: Der DiCV frage sehr genau nach, was die Ortsebene brauche, sei sich der Problematik von IT-Sicherheit bewusst und bemühe sich, sie in die Rahmenverhandlungen für Leistungsentgelte einzubringen. Zudem gibt es dort eine sehr aktive Digitalisierungsbeauftragte, die einen Arbeitskreis für IT-Verantwortliche ins Leben gerufen hat, in dem sich die Mitgliedsverbände zu IT-Fragen, darunter auch IT-Sicherheit, austauschen. Bei den interviewten Diözesanverbänden existieren ähnliche Angebote: Lobbyarbeit zu Digitalisierung auf Landesebene, der Versuch, in Rahmenvertragsverhandlungen IT-Refinanzierung zu thematisieren, eine Arbeitsgruppe zu IT mit einem der größeren Mitglieder, einen Arbeitskreis zu

[31] caritas.next ist ein auf vier Jahre angelegtes Projekt, bei dem Digitalprojekte in der Caritaswelt identifiziert werden, die Skalierungspotential haben. Die Projekte haben ihre Schwerpunkte auf Klient:innenarbeit, insbesondere Menschen in finanzieller Not, Eltern und Senior:innen. Die Finanzierung erfolgt zunächst über Eigenmittel der DCV-Zentrale und nicht über gesonderte Mitgliedsbeiträge. Mehr dazu siehe unter: https://www.caritas-digital.de/projekte/next/

Verwaltungssynergien, Vermittlung eines Dienstleisters zu Cybersecurity-Awareness-Schulungen und Penetration Testing[32] und die Möglichkeit, sich gemeinsam einem IT-Dienstleister anzuschließen.

Die drei weiteren Spitzenverbände berichten ebenfalls von ihren Bemühungen bei Rahmenvertragsverhandlungen, politischem Lobbying und außerdem davon, dass sie auf Konferenzen IT-Sicherheit auf die Agenda setzen. Tatsächlich erwähnen fast alle Expert:innen auch das Caritas-Netzwerk IT: Sich dort zu engagieren wird von den Spitzenverbänden als Engagement für die eigenen Mitglieder verstanden. Sie hoffen, dass dort Angebote entwickelt werden, die für ihre Mitglieder nutzbar sind, wie der Incident&Response-Vertrag[33]. Sie bewerben den Verein entsprechend bei ihren Mitgliedern, auch als Angebot, sich dort zu IT-Fragen zu informieren und auszutauschen[34]. Gleichzeitig drücken zwei Gesprächspartner:innen ihre Enttäuschung darüber aus, dass aus dem Netzwerk über Incident&Response und Austausch hinaus bisher noch keine tiefere Kooperation zwischen den Vereinsmitgliedern entstanden ist.

Es gibt also durchaus konkrete Aktivitäten, die Diözesan- und andere Spitzenverbände betreiben, um das Thema IT-Sicherheit für ihre Mitglieder zu bedienen. Dabei benennen sie aber auch Herausforderungen, etwa fehlende technische Expertise, wie ein Spitzenverband selbstkritisch anmerkt:

> Es gibt Einrichtungen, Dienste und DiCVs, die haben mehr Mitarbeiter in ihrer IT-Abteilung als wir hier beim Verband insgesamt und insofern haben wir wenig beizutragen zu den sehr konkreten Anfragen, die die haben. Also wie mache ich Connext-Vivendi[35] sicher? Wie kriege ich die Leitungen sicher? Wo stelle ich meine Server hin und wie machen wir das mit dem Backup? Da haben wir einfach operativ genau nichts beizutragen.

---

[32] Penetration Testing (kurz: Pentesting) ist ein gezielter Sicherheitstest, bei dem ethische Hacker IT-Systeme auf Schwachstellen überprüfen, indem sie Angriffe simulieren, um Sicherheitslücken zu identifizieren und zu beheben.

[33] Hierbei handelt es sich um einen Vertrag zwischen dem Netzwerk und einem IT-Sicherheitsdienstleister, dem CNIT-Mitglieder für einen Monatsbeitrag pro Mitarbeitendem (in Vollzeitäquivalenten) beitreten können. Bei einem Cybervorfall steht ihnen Hilfe seitens des Dienstleisters bei der Eindämmung, Aufklärung, Behebung und dem Wiederanlauf zur Verfügung. Siehe: https://www.caritas-netzwerk-it.de/leistungen

[34] Der Verein betreibt monatlich stattfindende Erfahrungsaustauschgruppen zu den Themen IT-Sicherheit/Notfallmanagement Microsoft 365 und der Fachsoftware Vivendi.

[35] Vivendi ist eine Fachsoftware der Firma Connext. Sie wird für die Pflegedokumentation, Kliente:innenverwaltung und Leistungsabrechnung eingesetzt.

Die Stärke von Spitzenverbänden liegt naturgemäß eher in Information und Koordination, was durch die Heterogenität und Subsidiarität der Träger erschwert wird. Hinzu kommt, dass Spitzenverbände nicht zu allen Mitgliedern engen Kontakt haben:

> Keine Ahnung, wie die ganz kleinen [Träger] aufgestellt sind. Was ich tatsächlich gar nicht einschätzen kann, sind Sozialstationen mit, sagen wir mal, 20 oder 30 Mitarbeitern und die haben wir auch noch bei uns als Mitglieder; da habe ich kein Gefühl für, ehrlich gesagt.

Hier scheint sich neben einem Angebotsproblem auch ein Nachfrageproblem aufzutun. Ein DiCV und ein Spitzenverband zeigen sich ernüchtert darüber, dass ihre konkreten Angebote zu IT-Sicherheit auf wenig Resonanz stoßen, das sei „jetzt eher mal ein bisschen frustrierend." Dies ist kein spezifisches Problem für IT-Sicherheit, eher eines von spitzenverbandlicher Arbeit an sich:

> Die [Mitglieder] haben das noch nicht gelernt, wie sie ihren Verband eigentlich wirklich nutzen könnten, welche Wirkmacht wir dann hätten. Also wir müssen alles immer nachfragen, dann kriegen wir auch Antworten, dann vernetzen wir auch, dann sind die auch ganz dankbar. Wir sollen denen von den Lippen ablesen, was denn wohl interessante Themen sein könnten. So, das ist schon ein bisschen schwierig diese Verbandsarbeit. Also wir sollen die machen, aber dass sich dann mit viel Engagement reingekniet wird von den Mitgliedern, das ist auch eher weniger.

Warum das Interesse an spitzenverbandlichen Aktivitäten so gering ist, darauf gibt ein:e Vertreter:in eines Ortscaritasverbandes Antwort: mangelnde personelle und zeitliche Ressourcen. Er:sie habe schlicht niemanden in der ersten und zweiten Führungsebene, den:die er:sie für entsprechende Arbeitskreise, hier konkret IT, mandatieren könne. Entsprechend könne er:sie auch keine Erwartungen an den zuständigen Diözesanverband formulieren:

> Ich glaube, wenn wir mehr wollten, würde sie [die Digitalisierungsbeauftragte des DiCVs] mehr tun. Unser limitierender Faktor sind wir selber. […] Wir halten es einfach nicht nach. Das ist bei so vielen Themen so, Nachhaltigkeit zum Beispiel ist auch so ein Thema, wo wir uns viel auf die Agenda geschrieben haben. Aber dann im Alltag rutscht uns das weg und ich glaube, das ist dann eher das Problem. Also wenn ich da eine Erwartung hätte, müsste ich dieselbe auch erfüllen und das leisten wir gerade nicht.

8.2.3 Politik und Lobbying

Eine der wichtigsten Aufgaben, die Spitzenverbände erfüllen, ist Lobbyarbeit auf verschiedenen Ebenen. Auf kommunaler Ebene haben auch Ortsverbände Kontakt zu politischen Akteur:innen. Doch egal, ob Kommunen, Länder oder Bund: Ein Bewusstsein für IT-Sicherheit ist nach Empfinden der Expert:innen auf keiner Ebene vorhanden. Darüber hinaus machen sie die Erfahrung,

dass politisch insgesamt wenig Aufmerksamkeit und Verständnis für die freie Wohlfahrt existiert: „Ich glaube, das ist nicht so ganz weit hergeholt, dass da immer mehr Politiker wenig Kernwissen haben, wie die Mechanismen sind und was Gemeinnützigkeitsrecht ist." Insbesondere monieren sie, dass nicht bekannt sei, wie groß und wirtschaftlich bedeutend die Branche ist (siehe dazu *3.2 Wirtschaftliche Bedeutung der freien Wohlfahrt)*, dass sie nicht als Teil der Wirtschaft, sondern als Kostenfaktor wahrgenommen werde. Darüber hinaus sei die deutsche freie Wohlfahrt in Europa ein einzigartiges Konstrukt und somit den politischen Akteur:innen der Europäischen Union fremd. Dabei betonen die meisten Interviewpartner:innen, dass sie die EU prinzipiell positiv sehen – einheitliche europäische Standards, gerade auch im Bereich IT-Sicherheit, seien wichtig – bei der Umsetzung ins nationale Recht gelinge aber die Übersetzungsleistung, das heißt die Berücksichtigung der Besonderheiten der freien Wohlfahrt, nicht. Im Ergebnis werde seitens der Politik verkannt, dass Organisationen der freien Wohlfahrt unternehmerische Interessen und Herausforderungen haben. Folglich würden sich die politischen Ressorts, die unternehmerische Themen adressieren, für die freie Wohlfahrt nicht zuständig fühlen. In der Konsequenz haben die Träger keinen Zugriff auf Fördertöpfe, sei es der EU, des Bundes oder der Länder, beispielsweise für Digitalisierungsmaßnahmen, mit denen sie auch ihre IT-Sicherheit erhöhen könnten. Einige Interviewausschnitte sind hierzu in *Anhang 13: Interviewausschnitte zum fehlenden Verständnis für die freie Wohlfahrts seitens politischer Akteur:innen* zusammengestellt. Besonders eindrücklich wird das Problem in diesem Bericht illustriert:

> Der [*Name des Trägers*] hat mal versucht, einen Zuschuss für IT nach den Förderprogrammen zu organisieren und also auch auf diesen Digitalbonus Bayern zuzugreifen. Dann haben sie als erstes beim Sozialministerium angerufen. Die haben gesagt: ‚Was, nee … Digitalisierung? Wir machen nur Soziales. Digitalisierung? Ruft mal bitte bei der Gerlach[36] an'. Dann haben sie sich also an das Digitalministerium gewendet. Die haben gesagt: ‚Wir haben kein Budget. Da müsst ihr beim Wirtschaftsministerium nachfragen'. Und das Wirtschaftsministerium hat dann gesagt: ‚Na ja, ihr seid kein Wirtschaftsunternehmen, ihr seid Soziales, also geht bitte zum Sozialministerium'. Ja, und dann stehst du da. Das heißt, für IT und Digitalisierung in der Sozialwirtschaft fühlt sich zunächst mal niemand so richtig verantwortlich.

Entsprechend bemühen sich die Verbände, Lobbyarbeit zu leisten: bei der EU über das Brüsseler Büro des DCVs, beim Bundesfamilienministerium, Bundesgesundheitsministerium,

[36] Judith Gerlach war von 2018 bis 2023 bayerische Staatsministerin für Digitales.

Bundeswirtschaftsministerium, Bundesfinanzministerium, den entsprechenden Pendants auf Landesebene sowie den thematisch zugehörigen Parlamentsausschüssen auf beiden Ebenen, dem Spitzenverband der gesetzlichen Krankenkassen (GKV) und bei Verhandlungspartnern auf Landes-, Bezirks-, Kreis- und Ortsebene. Ein:e Expert:in sucht zudem den Kontakt zur Wirtschaft, etwa den Industrie- und Handelskammern, Start-Ups oder auf der re:publica[37], um dort das Potential und die Anliegen der freien Wohlfahrt bekannter zu machen und Kooperationen zu starten. Bei der politischen Lobbyarbeit geht es um die Sichtbarkeit der freien Wohlfahrt an sich, um Förderprogramme für Digitalisierung und um die Refinanzierung von IT-Kosten, zu denen Kosten für IT-Sicherheitsmaßnahmen zählen (siehe *8.2.4 Refinanzierung*). Aus diesen Bemühungen ziehen die Expert:innen, die aktiv Lobbyarbeit betreiben, eine ernüchternde Bilanz: „Aber ich sage mal, das Thema Wirkung und politischer Einfluss, da darf man zumindest mal Fragezeichen dransetzen." Oder sogar: „Sie sehen ja, wie erfolgreich das ist: null. Passiert ja nichts."

Ein Grund für die geringe Effektivität von Lobbying seitens der Caritas seien fehlende Ressourcen: Die Lobby-Abteilung des DCV habe nicht genügend Mitarbeiter:innen und zudem sei es problematisch, dass der Hauptsitz der DCV-Zentrale noch in Freiburg und nicht in Berlin sei. Damit habe die Caritas weniger direkte Nähe zu Entscheidungsträger:innen auf Bundesebene[38]. Was Digitalisierung und IT betreffe, gebe es außerdem ein Kompetenzproblem: Das Hauptthema der Caritas seien nun einmal Menschen, weswegen es wenige Personen gebe, die sich strukturell mit Digitalisierung auseinandersetzen und fachlich überhaupt Einflussnahme betreiben könnten. Die DiCVs hätten auch zeitlich und finanziell keine Ressourcen für Lobbyarbeit zu dem Thema: Sie müssten sich erst einmal um die IT-Infrastruktur und Digitalisierung im eigenen Haus kümmern. Hinzu käme, dass diejenigen, für die die Lobbyarbeit im Endeffekt betrieben wird, das heißt Klient:innen, Patient:innen und deren Angehörige, im Gegensatz zu anderen Interessensgruppen bei ihrer Interessensvertretung kaum mitwirken können: Landwirt:innen und Arbeiter:innen der

[37] Die re:publica ist eine jährliche Konferenz in Berlin zu Themen rund um digitale Gesellschaft, Medien, Netzpolitik und Technologie.

[38] Die deutschen Bundesgeschäftsstellen des DCVs befinden sich in Freiburg und Berlin, wobei in Freiburg etwa 380, in Berlin etwa 50 Mitarbeitende beschäftigt sind. Im April 2024 kündigte der DCV an, den Standort Berlin zu stärken: Bis 2020 soll die Hälfte der Stellen in Berlin angesiedelt sein. Mehr dazu: Freiburg soll nicht länger Hauptsitz der Caritas sein - SWR Aktuell am 27.04.2024

Automobilindustrie gingen für ihre Anliegen auf die Straße – Pflegebedürftige können nicht demonstrieren gehen.

Darüber hinaus werden die einzelnen Lobbybemühungen zu IT und IT-Sicherheit als eben das bewertet: als einzeln. Eine gemeinsame, strategische Bearbeitung des Themas finde nicht statt:

> Das Problem ist tatsächlich: Für das Platzieren braucht es konzertierte Aktionen der Sozialanbieter. Und ich sage mal, die BAGFW ist an dem Punkt so zersplittert, dass ein konzertiertes Platzieren dieses Anliegens überhaupt gar nicht passiert. Wir sind als Wohlfahrtsverbände, auch als Spitzenverbände, nicht in der Lage, das Thema strukturiert an den Mann zu bringen und an die Frau oder an den Abgeordneten, die Abgeordnete. Das ist eigentlich, das ist fatal.

Dies sei – wie bereits angesprochen – in einem Verteilungskampf um begrenzte finanzielle Ressourcen begründet. Die BAGFW habe noch nicht verstanden, dass man nicht einfach nur mehr Geld fordern könne – welches immer weniger vorhanden ist – sondern gemeinsam Lösungsangebote erarbeiten müsse.

Diese deutliche Kritik an der mangelnden Zusammenarbeit zwischen den großen Wohlfahrtsverbänden, die insbesondere von einer Expertin / einem Experten geäußert wird, scheint im Grunde einer Sehnsucht nach bzw. der Erkenntnis der Notwendigkeit von mehr Einigkeit zu entstammen:

> Das wäre auch vielleicht ein bisschen die Lösung für das Thema Cybersecurity. Also ich glaube, es ist tatsächlich gut, wenn man sich zusammenschließt und die Themen tatsächlich konzertiert bearbeitet und nicht solitär. Da sehe ich schon einen nicht ganz unwichtigen Schlüssel.

8.2.4 Refinanzierung

Das größte Problem für das Herstellen von IT-Sicherheit in der freien Wohlfahrt ist allen Expert:innen zufolge, dass Kostenträger keine Finanzmittel für IT-Sicherheit bereitstellen. Dieses Problem betrifft nicht nur IT-Sicherheit im Speziellen, sondern IT und Digitalisierung an sich: „Wenn es schon nicht gelingt, für normale Digitalaktivitäten, -prozesse, -themen, Geld einzuwerben, also warum soll dann die Sicherheit noch eine besondere Rolle spielen?“ In den Leistungsentgelt- und Pflegesatzverhandlungen müssen die Träger plausibel machen, wie hoch ihre Kosten sind, um eine soziale Dienstleistung zu erbringen. Dies schlüsselt sich auf in Sachkosten (direkte Kosten für Material- und Verbrauchsgüter), Gemeinkosten (indirekte Kosten, zu denen Verwaltungs- und

Betriebskosten zählen) und gegebenenfalls Investitionskosten[39] (langfristige Investitionen für Anschaffung, Bau, Abschreibung und Finanzierung von Gebäuden, Anlagen und langlebigen Gütern). Dort IT abzubilden sei jedoch extrem schwierig, weil die Kostenträger reale IT-Ausgaben nicht einpreisen; stattdessen verweisen sie auf Gemein- und Sachkostenpauschalen, über die der Träger eben auch seine IT abdecken müsse. Die Verhandlungen verliefen dabei wie ein „türkischer Basar" oder „Kuhhandel", bei dem im Endergebnis nicht mehr transparent sei, wie Sach- und Gemeinkosten zustande kommen. Selbst wenn IT-Kosten es in die Verhandlungen schaffen, werden sie nicht ausreichend anerkannt: „Es gelingt von Zeit zu Zeit schon, das Thema IT ins Bewusstsein zu rufen. Das heißt aber nicht, dass man das dann hinterher auskömmlich finanziert bekommt. Das auf gar keinen Fall." Ausführliche Interviewausschnitte, wie solche Kostenverhandlungen ablaufen, befinden sich in *Anhang 14: Interviewausschnitte zu Refinanzierungsverhandlungen.*

Dem gegenüber stehen steigende technische und gesetzliche Anforderungen, etwa durch die Datenschutzgrundverordnung, NIS-2 oder IT-Sicherheitsstandards in der Telematikinfrastruktur (TI):

> Beim Anschluss an die TI, da wird einfach gesagt ‚Ja, das ist doch das Problem der Pflege, was das dann nachher kostet'. Die GKV[40] will da immens hohe Sicherheitsprotokolle rein haben, was das ganze System verteuert. Und dann sagen die ‚Ja, das müssen die Einrichtungen bezahlen'. Wovon bitte? Wohlfahrtspflege-Unternehmen dürfen keine Gewinne machen. Also wo soll ich denn bitte das Geld hernehmen? In die Pflegesätze kriege ich es noch nicht rein, weil es heißt: ‚wirtschaftlich nicht notwendig'. [41]

[39] Ob, von wem und in welcher Höhe Investitionskosten vom Kostenträger übernommen werden, hängt vom Hilfefeld und Bundesland ab.

[40] Spitzenverband der gesetzlichen Kranken- und Pflegekassen

[41] Nach § 106b SGB XI und § 380 SGB V zahlen die Kranken- und Pflegekassen TI-Pauschalen für die TI-Anbindung und den elektronischen Heilberufeausweis (eHBA). Erste Erhebungen des FINSOZ e.V. ergeben jedoch, dass die Kosten der Einrichtungen damit nicht gedeckt sind, sondern Eigenanteile zwischen niedrigen und sehr hohen vierstelligen Beträgen übernehmen müssen. Siehe: Wolff und Stock 2024 (https://www.altenheim.net/telematikinfrastruktur-wie-hoch-sind-die-pauschalen/).

Während eine Regelfinanzierung fehlt, gibt es zumindest hin- und wieder Förderprogramme. Genannt werden hier Tandem 4.0[42], das Pflegepersonalstärkungsgesetz (PpSG)[43], sowie Sonderprogramme der Länder. Problematisch an diesen Förderprogrammen ist, dass sie nur punktuell wirken, nicht auskömmlich und letztlich nicht nachhaltig sind, da einmal angeschaffte Technik ja langfristig betrieben und irgendwann erneuert werden muss. Wie in *8.2.3 Politik und Lobbying* beschrieben, hat die freie Wohlfahrt auf viele Förderprogramme überhaupt keinen Zugriff.

Für eine echte Refinanzierung fehlen die rechtlichen Grundlagen, das heißt sie ist in den Leistungs- und Vergütungsvereinbarungen nicht vorgesehen:

> Wenn es für irgendwas keine gesetzliche Grundlage, keine Verwaltungsvorschrift gibt, dann macht deutsche Verwaltung gar nichts. Bloß weil etwas Sinn macht, heißt das noch lange nicht, dass die Verwaltung dafür empfänglich wäre und schon gleich gar nicht, dass Kostenträger Kosten für irgendwas übernehmen würden, was Sinn macht.

Zusätzlich fokussiert die Logik von Refinanzierung auf Personal: Dass Digitalisierung als Kompensationsmittel für den Fachkräftemangel eingesetzt werden kann, sei nicht angedacht. Werde durch digitale Hilfsmittel Personal entlastet, sodass dieses mehr Menschen betreuen könne[44], würden nicht etwa diese Hilfsmittel erstattet, sondern der Träger laufe Gefahr, weniger Personalkosten bewilligt zu bekommen.

Wo sich in Bezug auf Regelungen tatsächlich eine positive Entwicklung feststellen lässt, ist die Eingliederungshilfe, in der im Zuge des Inkrafttretens des Bundesteilhabegesetzes (BTHG)[45] die Landesrahmenverträge zwischen Kosten- und Leistungsträgern neu verhandelt werden mussten. So weist ein:e Expert:in darauf hin, dass in NRW nun im Bereich der sozialen Teilhabe für

---

[42] Siehe: https://www.caritas-digital.de/projekte/tandem-4-0/, Tandem 4.0 war ein Programm des Deutschen Caritasverbandes zur Digitalisierung von Caritasverbänden in Ostdeutschland. Es lief von 2018 bis 2021 und wurde durch EU-Mittel (ESF rückenwind+) finanziert.

[43] Über das PpSG können einmalige Investitionen in die Digitalisierung von Pflegeeinrichtungen zu 40% kofinanziert werden mit maximal 12.000 € pro Maßnahme und 30.000 € pro Einrichtung. Ein:e Expert:in rechnet jedoch vor, dass die Ausstattung eines Pflegeheims mit WLAN auch schnell 100.000 € kosten könne.

[44] Der:die entsprechende Interviewpartner:in betont, dass es nicht darum geht, Stellen abzubauen, sondern durch digitale Hilfsmittel Personal zu kompensieren, das aufgrund des Fachkräftemangels schon gar nicht mehr vorhanden ist.

[45] Das BTHG wurde 2016 erlassen und trat in vier Stufen in Kraft: 25. Juli 2017 (Stufe 1), 2018 (Stufe 2), 2020 (Stufe 3) und 2023 (Stufe 4).

Leitungs- und Verwaltungskräfte IT-Arbeitsplatzkosten in Anlehnung an die KGSt[46]-Systematik pauschaliert sind: 3.450 € pro Jahr für Leitungs- und 3.000 € für Verwaltungsmitarbeitende. Für Betreuungspersonal außerhalb besonderer Wohnformen wird der IT-Aufwand auf 4.159,32 € angesetzt (Rahmenvertrag nach § 131 SGB IX Nordrhein-Westfalen vom 19.06.2024, Anlage B, Abs. 3.1 und 3.2).

Im Rahmenvertrag nach § 131 SGB IX Bayern ist seit Juni 2023 geregelt, dass in Werkstätten für behinderte Menschen IT-Administration und die Wartung von EDV-Anlagen Inhalt der Leistungserbringung sind (Rahmenvertrag nach § 131 SGB IX in Bayern vom 30.06.2023, Anlage B3.1, Abs. 4.2, Nr. 3, Buchst. c). Der Basisstellenplan für WfbMs sieht daher mindestens eine Stelle für IT-Administration bei einem Stellenschlüssel von 1:240[47] vor (Rahmenvertrag nach § 131 SGB IX in Bayern vom 30.06.2023, Anlage B3.1.1, Nr. 10.2). Die Stellenanzahl ist auf maximal zwei gedeckelt. Bei den Verhandlungen haben die Leistungsträger angebracht, dass der Rahmenvertrag das letzte Mal in den 1990er Jahren angefasst wurde und sich IT-technisch seitdem einiges getan habe; IT-Betrieb sei inzwischen notwendig, um den Betrieb einer Werkstätte aufrecht zu erhalten. Zudem werde IT inzwischen direkt zu Rehabilitationszwecken für die Leistungsempfänger:innen eingesetzt. Die IT-Administrationsstellen hätten es vor allem deswegen in die Vereinbarung geschafft, um gezielt diese IT-Ausstattung für Klient:innen betreuen zu können. Ausreichend seien diese Regelungen im Rahmenvertrag jedoch nicht und IT-Sicherheit sei als Argument und Kostenpunkt nicht angenommen worden:

> IT-Security, da haben sie gesagt ‚Ihr habt Computer dastehen, die Datenschutzgrundverordnung gilt, also bitte'. Dass IT-Security mehr ist als nur das Erfüllen der Datenschutzgrundverordnung oder in unserem Fall vom KDG, das zieht nicht.

Damit ist ein Grund für die Nicht-Finanzierung von IT-Sicherheit mangelndes Bewusstsein seitens der Kostenträger. Dieses schätzen die Expert:innen als „nicht vorhanden", „gar nicht" und „gegen null gehend" ein. Dies käme auch daher, dass die Behörden, insbesondere die Kommunen, selbst digital schlecht ausgestattet und ausgebildet seien:

---

[46] Die Kommunale Gemeinschaftsstelle für Verwaltungsmanagement (KGSt) ist ein Fachverband von Städten, Gemeinden und Landkreisen Sie gibt eine Leitlinie für die Kosten von Arbeitsplätzen im kommunalen Dienst heraus: https://kgst.de/dokumentdetails?path=/documents/20181/11022390/B-09-2024_Kosten-eines-Arbeitsplatzes.pdf/f9b7e928-ceaf-037c-f6f8-e6a09431f254?t=1736780350833.

[47] 1 IT-Stelle pro 240 Betreuungsplätze.

> Sie haben ja im Amt selber gar nicht so eine Technik, und wenn wir dann sagen, wir schicken nur noch Personalnummern oder nur noch verschlüsselte Unterlagen ans Jugendamt, dann maulen die schon sehr rum, weil sie sagen, sie können das dann nicht öffnen. Mittlerweile gibt es auch gesicherte Laufwerke, die versuchen die Mitarbeiter zu umgehen, weil sie nicht wissen, wie es funktioniert, weil sie sich dann Passwörter besorgen müssen, weil es sie einfach nervt. Und wir sagen aber, wir schicken es nicht [unverschlüsselt]. Dann stecken wir es eben wieder in Briefumschläge.

Gleichzeitig spielt Geldmangel eine entscheidende Rolle: Die Gesprächspartner:innen sind sich durchaus bewusst, dass die Kommunen aufgrund der Kürzungen von Sozialmitteln im Bundes- und in Landeshaushalten und der allgemein hohen kommunalen Verschuldung in einer schwierigen Situation sind. Das gehe laut dreier Expert:innen sogar so weit, dass Leistungsberechtigte sowie Träger Ansprüche einklagen müssten:

> Ich habe schon Kämmerer sagen hören, von nicht-kleinen Kommunen: ‚Es mag ja sein, dass das eine Pflichtleistung ist. Dann müssen Sie uns eben verklagen. Und wenn Sie uns verklagt haben und das Gericht Ihnen zuspricht, dass wir das finanzieren müssen, dann kriegen Sie das Geld auch. Aber freiwillig können wir es nicht bezahlen und wollen es nicht bezahlen'.

Hier zeigt sich am Beispiel von IT-Sicherheit ein ganz grundsätzliches Problem, nämlich dass die „sozialstaatlichen Finanzierungsmöglichkeiten an die Grenzen stoßen." In der Konsequenz müssten soziale Angebote eingestellt und/oder die Qualität dieser Angebote gesenkt werden. Im schlimmsten Fall verschwinden Organisationen der freien Wohlfahrt sogar ganz:

> Von daher glaube ich tatsächlich, dass es zu einem tiefergehenden grundlegenden Wandel der Daseinsfürsorge in der Bundesrepublik kommen wird: Dass nämlich die freigemeinnützigen Träger sich in der Perspektive aus den Angeboten zurückziehen oder zurückziehen müssen oder auch in die Insolvenz getrieben werden; und dass die Angebote der Daseinsfürsorge dann durch kommunale Anbieter, wo ja auch die Verpflichtung dazu besteht, wahrgenommen werden. Und natürlich von Marktbegleitern, die aber nicht gemeinnützig sind, sondern tatsächlich profitorientiert und das dann definitiv zulasten der Anspruchsgruppen kommt.

8.3 Maßnahmen und Forderungen

Tritt man einen Schritt zurück, lassen sich die Herausforderungen für IT-Sicherheit in der freien Wohlfahrt auf vier Dimensionen zusammenfassen: Mangelndes Problembewusstsein für IT-Sicherheit, mangelnde politische Sichtbarkeit der freien Wohlfahrt, mangelnde Koordination innerhalb der Branche und fehlende Finanzmittel.

Um diese Probleme zu adressieren, berichten die Expert:innen von verschiedenen Maßnahmen, die schon jetzt ergriffen werden und formulieren Wünsche, Ideen und Forderungen. Auch diese lassen sich in vier Dimensionen clustern: Information und Vernetzung, Standardisierung und Kooperation, Gesetzesanpassungen, grundlegende politische und gesellschaftliche Forderungen.

Information und Vernetzung

Information und Vernetzung – sowohl innerhalb der freien Wohlfahrt als auch nach außen – sehen die Gesprächspartner:innen als notwendig an, um gegen das mangelnde Problembewusstsein anzukämpfen und die Sichtbarkeit der Branche zu erhöhen. Wie in *8.1.3 Vorständ* dargelegt, betonen sie, dass IT-Sicherheit Management-Aufgabe ist, also explizit Vorständ:innen und Geschäftsführer:innen für IT-Sicherheit sensibilisiert werden müssen. Dafür müsse man „Management-Orte" schaffen. Als solche Orte, an denen dies bereits versucht wird, werden die Bundeskonferenz der hauptamtlichen Vorstände und Geschäftsführungen der Ortscaritasverbände (Buko), das Caritas-Netzwerk IT, die Mitgliederversammlungen der Fachverbände und Austauschformate der Diözesanverbände für und mit ihren Mitgliedern genannt. Besonders wichtig sei es zudem, über Cyberangriffe auf die Branche zu sprechen. Da beides schon geschieht, gleichzeitig die Awareness von Vorständ:innen als noch zu gering eingeschätzt wird, scheint es hier eine Intensivierung der Bemühungen zu brauchen oder eine Anpassung der Formate.

Vernetzung und Information nach Außen zielt auf politisches Lobbying für die freie Wohlfahrt an sich und für Digitalisierung, also auch IT-Sicherheit, im Speziellen. Hier wünschen sich die Expert:innen einen engeren Schulterschluss mit den anderen Spitzenverbänden der freien Wohlfahrt und mehr Fokussierung auf die gemeinsame Erarbeitung von Lösungsvorschlägen anstatt Konkurrieren um Finanzmittel. Zudem sprechen sie an, dass mehr Personal für Lobbyarbeit und darunter mehr Spezialist:innen für Digitalisierung erforderlich sind. Eine Person berichtet hier von Maßnahmen, die im entsprechenden DiCV bereits getroffen werden: Eine Lobby-Stelle für Digitalisierung, ein Arbeitskreis der Landes-Liga zu Digitalisierung und Lobby-Stellen, die sich der DiCV mit einem anderen DiCV im selben Bundesland teilt. Darüber hinaus schlägt ein:e Expert:in vor, stärker in der freien Wirtschaft Verbündete zu suchen: Diese sei darauf angewiesen, dass Kinder betreut, Pflegebedürftige versorgt und Menschen in den Arbeitsmarkt integriert werden, und müsse daher ein Interesse an einer starken Wohlfahrt haben. Wirtschaftlichen Akteuren die Strukturen, Herausforderungen und Werte der Wohlfahrt näherzubringen, sei außerdem nötig, damit

soziale Organisationen bei der Entwicklung von (digitalen) Produkten und Dienstleistungen mitberücksichtigt werden.

Standardisierung und Kooperation

Die Heterogenität der Caritaslandschaft beinhaltet, dass es keine technischen Standards oder einheitliche Prozesse gibt. Dies bedeutet, dass keine Synergie- und Skalierungseffekte genutzt werden und letztlich mehr Aufwand betrieben wird und höhere IT-Kosten anfallen als notwendig. Hier haben die Interviewpartner:innen drei Vorschläge, die sich in ihrem Grad an Zentralisierung unterscheiden: Den höchsten Zentralisierungsgrad hat die Idee einer Konsolidierung der IT der gesamten Caritas, d.h. ein IT-Dienstleister wird ausgewählt oder aufgebaut, der mehrheitlich Caritasorganisationen gehört und Haupt-IT-Dienstleister der verbandlichen Caritas ist. Einen dahingehenden Versuch sieht ein:e Expert:in als gescheitert an. Am anderen Ende stehen Einkaufsgenossenschaften, Verhandlungspartnerschaften und Rahmenverträge, etwa der Incident&Response-Vertrag des Caritas-Netzwerk-IT e. V.s oder eine ähnliche Initiative eines DiCVs bezüglich einer Software zur Nachhaltigkeitsberichtserstattung. Dazwischen liegt die Idee eines zentralen Dienstleistungszentrum, das zwar zentral gesteuert wird und Standards vorgibt, aber eine gewissen Auswahl an Tools je Anwendungsbereich und Individualisierungsmöglichkeiten zulässt. Was diese Vorschläge eint, ist, dass es hier um mehr als Erfahrungsaustausch und Projektzusammenarbeit geht, sondern um wirtschaftliche Kooperation. Bei dieser werden Risiken gemeinsam getragen, aber auch ein Stück weit Kompetenzen abgegeben. Bedenkt man, dass bisherige Konsolidierungsvorhaben gescheitert sind, wie tief das Subsidiaritätsprinzip in der DNA der Caritas verankert ist und dass auch die hier zitierten OCVs auf die Unabhängigkeit in ihrer Dienstleisterwahl pochen, ist anzunehmen, dass Lösungen, bei denen vergleichsweise wenig Kompetenzen abgegeben werden, leichter zu vermitteln wären.

Gesetzesanpassungen

Die Wünsche, die die Expert:innen an den Gesetzgeber richten, zielen alle auf die Finanzierung von Digitalisierung, IT und IT-Sicherheit ab. Ein Hebel wären Richtlinien und Verordnungen, z.B. durch das BSI, die verpflichtende IT-Sicherheitsstandards für die Sozialwirtschaft vorschreiben. Damit hätte man den Kostenträgern gegenüber Argumente für die Kostenübernahme. Dieser Ansatz birgt jedoch die Gefahr von bürokratischen Hürden und das Entstehen von zusätzlichen Kosten aufgrund von Nachweispflichten. Zudem befürchtet ein:e der wenigen Expert:innen, der:die

eine tiefere Kenntnis von NIS-2 zeigt, dass bereits die Teile des Sozialwesen, die von NIS-2 betroffen sind, zu dessen Erfüllung keine zusätzlichen Mittel erhalten werden.

Eine weitere Forderung sind Gesetze, die die Förderung von Digitalinvestitionen ermöglichen. Hierzu sollten Organisationen der freien Wohlfahrt als Wirtschaftsunternehmen anerkannt werden (ohne dabei ihre Gemeinnützigkeit zu verlieren), um Zugang zu allgemeinen Fördertöpfen zu erhalten. Tatsächlich fordert die BAGFW bereits, eine Klausel in alle Förderprogrammen des Bundes aufzunehmen, die gemeinnützige Träger, Dienste und Einrichtungen in öffentlichen Förderprogrammen prioritär bedenkt (Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege 2022, 5). Der Paritätische Wohlfahrtverband Niedersachsen ruft außerdem die Bundesregierung und die Länder auf, sich bei der EU dafür starkzumachen, freigemeinnützige Unternehmen in die KMU-Definition aufzunehmen (Paritätischer Wohlfahrtsverband Niedersachsen e. V. 2024, 4f). Ein alternativer Vorschlag sind breite, branchenspezifische Förderprogramme, wie ein Pflegezukunftsgesetz, analog zum Krankenhauszukunftsgesetz (KHZG)[48].

Die Anpassung der Sozialgesetzbücher, Rahmenverträge, Leistungs- und Vergütungsvereinbarungen sind eine dritte Option und die von den Interviewpartner:innen am häufigsten vorgebrachte Forderung. Das Vorhalten einer funktionierenden und sicheren IT-Infrastruktur müsste als essenziell für die Leistungserbringung anerkannt werden. In den Vergütungsvereinbarungen müssten realistische IT-Kostenaufschläge pro Person enthalten sein; dies ließe sich über eine Orientierung an der KGSt-Systematik umsetzen, wie es bereits in Teilbereichen der Eingliederungshilfe in Nordrhein-Westfalen geschieht. Auch wenn eine Aufschlüsselung der tatsächlichen Kosten aktuell schwierig ist, weil die meisten Träger keine exakte Übersicht darüber hätten, wäre es laut einem:einer Expert:in wünschenswert zu ermitteln, wie viel ein IT-Arbeitsplatz in der freien Wohlfahrt durchschnittlich kostet und langfristig diesen Wert zu verwenden. Zusätzlich sollen sozialen Organisationen als Wirtschaftsunternehmen anerkannt und ihnen darüber ein Wagniszuschlag gewährt werden, damit sie Rücklagen bilden und diese für Notfälle und Investitionen verwenden können. Zudem müssten digitale Hilfsmittel gleichwertig zu Personal anerkannt werden, damit

[48] Das KHZG stellte ein Gesamtfördervolumen von 4,3 Milliarden Euro für Digitalisierungsprojekte in Krankenhäusern bereit (Bundesministerium für Gesundheit 2024). 15 % einer bewilligten Fördersumme muss in IT-Sicherheitsmaßnahmen investiert werden (Gesetz für ein Zukunftsprogramm Krankenhäuser vom 23.10.2020, § 14 Abs. 3).

Personalaufwände, die durch Digitalisierung eingespart werden, beim Träger verbleiben und zweckgebunden für IT-Infrastruktur, Schulungen, IT-Sicherheit und Weiterentwicklung digitaler Tools und Prozesse verwendet werden können.

Grundlegende politische und gesellschaftliche Forderungen

An vielen Stellen wird in den Interviews deutlich, dass die beschriebenen Probleme der freien Wohlfahrt mit IT-Sicherheit weder auf die freie Wohlfahrt noch auf IT-Sicherheit beschränkt sind. Die Gesprächspartner:innen stellen fest, dass Deutschland insgesamt in der Digitalisierung hinterherhinkt. Sie wünschen sich mehr Investitionen in digitale Bildung sowie die Sensibilisierung für IT-Sicherheit in allgemeinbildenden Schulen, Berufsschulen und Universitäten, damit Mitarbeitende über grundlegende digitale Fähigkeiten verfügen. Zudem wäre das Vorantreiben der Verwaltungsdigitalisierung – in Prozessen, Ausstattung und Mitarbeiterbefähigung – hilfreich, um bei den Kostenträgern ein Verständnis für die Notwendigkeit von IT-Ausstattung in sozialen Organisationen zu schaffen. Auch eine politische Priorisierung von IT-Sicherheitsfragen und ein damit einhergehendes höheres IT-Sicherheitsbewusstsein in der Bevölkerung würde sich positiv auf Bewusstsein für und Handhabung von IT-Sicherheit im sozialen Bereich auswirken.

Insgesamt kämpft die freie Wohlfahrt jedoch nicht nur damit, IT und IT-Sicherheit refinanziert zu bekommen, sondern insgesamt mit dem Aufrechterhalten von Leistungen. Schon jetzt gibt es zahlreiche Insolvenzen, insbesondere von kleineren Trägern. In der Folge verschwinden freigemeinnützige Unternehmen vom Markt; die Lücke wird von gewinnorientierten Akteuren gefüllt – oder gar nicht. Verbleibende Organisationen müssen ebenfalls heute schon ihr Angebot einschränken und die Qualität absenken[49]. Neben der demographischen Entwicklung in Deutschland, sehen die Expert:innen als grundlegende Ursachen einen gesellschaftlichen Wertewandel: Immer mehr Individualisierung und sinkende Solidarität hätten dazu geführt, dass die freie Wohlfahrt gesellschaftlich und politisch nicht mehr gesehen oder nicht mehr als wichtig angesehen. Daraus abgeleitet

[49] Persönliche Anmerkung: Die Situation ist im Bereich der Pflege besonders prekär. Hier treffen eine wachsende Anspruchsgruppe, schrumpfendes Personal, eine sinkende Anzahl an Beitragszahler:innen, steigende Kosten und damit steigende Eigenbeteiligungen aufeinander. Innerhalb der Branche kursiert der Spruch, dass mehr als ein rudimentäres „sauber, satt, trocken" zukünftig nicht mehr möglich sein werde. Eine mir bekannte Ärztin, die regelmäßig Patient:innen in Pflegeheimen versorgt, äußerte mir gegenüber, dass dies häufig heute schon nicht mehr der Fall sei. Aus meiner beruflichen Erfahrung weiß ich außerdem, dass Akteure der freien Wohlfahrt hinter hervorgehaltener Hand befürchten, dass es zukünftig zu mehr Suiziden unter älteren Menschen kommen könnte: weil sie ihren Lebensabend nicht unter diesen Bedingungen beschließen möchten und weil sie ihren Familien finanziell nicht zur Last fallen wollen.

rufen die Interviewpartner:innen zu einen gesellschaftlichen Rückbesinnung auf Solidarität mit den Schwächeren und einer politischen Priorisierung von wohlfahrtstaatlichen Aktivitäten auf – sowohl aus moralischen Gründen als auch zum Erhalt der Wirtschaftsleistung in Deutschland.

9. Diskussion

9.1 Einordnung der Ergebnisse in die Literatur

Insgesamt verifizieren die Expert:innen die in der Literaturrecherche zusammengetragenen Rahmenbedingungen für IT-Sicherheit in der freien Wohlfahrt. Bei der IT-Infrastruktur bestätigen sie, dass viele Organisationen mangelhaft ausgestattet sind; sie machen aber auch deutlich, dass die Größe der Träger eine Rolle spielt: Unter den ganz großen Trägern gibt es durchaus professionelle IT-Strukturen, während die ganz kleinen besonders schlecht aufgestellt sind. Den IT-Fachkräftemangel erkennen die Gesprächspartner:innen als Problem an, die meisten von ihnen sind davon aber nicht direkt betroffen, weil sie ihren IT-Betrieb an Dienstleister ausgelagert haben, wo IT-Personal attraktivere Bedingungen vorfindet. Die geringen IT-Kompetenzen der Mitarbeitenden sehen sie als eines der Hauptprobleme für IT-Sicherheitsrisiken im eigenen Haus an, verweisen allerdings auch auf allgemein mangelnde digitale Bildung in Deutschland. Was das Bewusstsein für IT-Sicherheit von Vorständ:innen und Verbänden betrifft, ist das Bild deutlich gemischter, als die Literatur es zunächst erscheinen lässt. Die Ortscaritasverbände nehmen bei ihren Peers ein geringes Bewusstsein wahr; dasselbe gilt für die Diözesanverbände in Bezug auf ihre kleineren Mitglieder. Bei großen Trägern scheint das Bewusstsein ausgeprägter, IT-Sicherheit aber kein priorisiertes Thema zu sein. Inwiefern Diözesanverbände, der Deutsche Caritasverband und die Bundesarbeitsgemeinschaft der freien Wohlfahrt IT-Sicherheit bedenken, ist unklar – die Einschätzungen reichen von „gar nicht“ zu „unbedingt.“ Einig sind sich die Interviewpartner:innen darin, dass IT-Sicherheit eine spitzenverbandliche Aufgabe und innerhalb der Organisationen selbst auf der obersten Managementebene angesiedelt sein sollte.

Die Heterogenität der Caritas wird als Hindernis für eine gemeinschaftliche Bearbeitung des Problems bestätigt. Gleichzeitig halten die Expert:innen am Subsidiaritätsprinzip fest. Bei der politischen Interessensvertretung problematisieren sie mangelnde Kooperation zwischen den Spitzenverbänden, mangelnde Ressourcen, und dass IT-Sicherheit bisher bei Lobbyarbeit nicht auf der Agenda steht. Wie schwierig die Finanzierungsstrukturen sind, die in der Literatur ausführlich

erläutert werden, wird von den Interviewpartner:innen ausdrücklich untermauert. Die nicht vorhandene Refinanzierung ist ihrer Meinung nach die größte Hürde für IT-Sicherheit in der freien Wohlfahrt. Sie stimmen mit der Literatur überein, dass ein Grund dafür das fehlende Verständnis für IT-Sicherheit in sozialen Organisationen seitens politischer Entscheidungsträger sowie seitens der Kostenträger ist. Darüber hinaus stellen sie klar, dass dies in einer niedrig ausgeprägten Wahrnehmung für die freie Wohlfahrt an sich begründet ist.

9.2 Ableitungen

Aus der Analyse der Interviews geht hervor, dass die freie Wohlfahrt im Kern mit einem Ressourcen- und mit einem Kooperationsproblem zu kämpfen hat. Selbst die mangelnde Awareness für IT-Sicherheit seitens der Branche und seitens der Politik sind darauf zurückzuführen: Es fehlen Geld, Zeit und Personal, sodass keine effektive Aufklärungsarbeit geleistet werden kann, und es gibt keine ausreichende Bereitschaft, diesen Mangel durch Kooperation zu kompensieren.

Als Maßnahme, um eine ausreichende Refinanzierung zu erreichen, wird Lobbyarbeit genannt; für eine Sensibilisierung von Führungskräften wird auf Kommunikations- und Netzwerkarbeit verwiesen. Zur Verbesserung der IT-Angebote sollen konkrete Dienstleistungen wie Rahmenverträge oder andere unternehmerische Kooperationen entwickelt werden. Hier stellt sich die Frage, ob das angesichts der knappen Ressourcen alles gleichzeitig leistbar ist. Es deutet auf eine Überforderung hin, dass es in allen drei Bereichen bereits Bemühungen gibt – und zwar häufig seitens der immer selben Akteur:innen –, die IT- und IT-Sicherheitssituation in der Caritas aber nach wie vor prekär ist. Daraus lassen sich drei Handlungsoptionen ableiten: Zusammenarbeit, Priorisierung und Arbeitsteilung.

Über Zusammenarbeit / Kooperationen lassen sich Ressourcen sparen, wie etwa bei den beiden DiCVs, die sich eine Lobbystelle teilen. Gleichzeitig muss man bedenken, dass Zusammenarbeit gewisse Reibungsverluste mit sich bringt: Die Ergebnisse sind Kompromisse, und Abstimmungen erfordern ebenfalls personelle und zeitliche Ressourcen. Entsprechend sind Kooperationen nicht in unendlichem Ausmaß möglich.

Die Option der Priorisierung zieht tatsächlich einer der befragten Spitzenverbände in Betracht: Zum Zeitpunkt des Interviews wurden dort Mitglieder befragt, ob sie sich mehr Lobbyarbeit, mehr Serviceleistungen oder weiterhin eine Mischung aus beidem wünschen. Sollte es einen Ausschlag für einen der beiden Arbeitsschwerpunkte geben, plant der Verband, sich danach zu richten.

Natürlich werden in einem solchen Fall wichtige Themen nicht bedient. Die Hoffnung ist aber, dass am Ende wenigstens eine Sache gut funktioniert, anstatt Vieles nur mäßig.

Die dritte Option, Arbeitsteilung, ist eine Mischung aus Kooperation und Priorisierung. Arbeitsteilung bedeutet, dass sich nicht alle um alles kümmern und dennoch alle Arbeitsfelder abgedeckt sind. Dafür müsste klar definiert werden, welcher Akteur welche Zuständigkeit hat und es müssten entsprechend Mandate vergeben werden. Welche Rolle für das Herstellen von IT-Sicherheit bzw. der allgemeinen Verbesserung von IT-Infrastruktur wollen die Mitglieder, dass der Deutsche Caritasverband spielt? Wo sehen sie das Caritas-Netzwerk IT? Welche Aufgaben sollte die BAGFW übernehmen? Wo können Fachverbände, DiCVs oder auch andere Spitzenverbände der freien Wohlfahrt Aufgaben stellvertretend für alle übernehmen? Die Option der Arbeitsteilung erfordert eine Menge Vertrauen und die Bereitschaft, Einfluss abzugeben. Außerdem müssen Organisationen Ergebnisse akzeptieren, die für sie nicht die Optimallösung darstellen, aber für die Branche als Ganzes funktionieren.

Die Frage nach Priorisierung drängt sich noch bei einem weiteren Aspekt auf, nämlich der Größenstruktur der Caritas. Aus den Interviews geht hervor, dass das Ausmaß des IT-(Sicherheits-)Problems von der Größe des Trägers abhängen kann. Nun haben 71, 2 % der Träger weniger als 51 Mitarbeitende – dabei machen sie aber nur 9 % aller Mitarbeitenden der Caritas aus. Gleichzeitig sind nur 2,6 % der Träger größer als 1001 Mitarbeitende, stellen damit aber 46 % der Gesamtmitarbeitendenschaft (siehe *Tabelle 2: Größenstruktur der Caritas-Rechtsträger* in *4.1 Struktur der Caritas*). Provokativ kann man hier fragen: Ergibt es bei begrenzten Ressourcen Sinn, nach Lösungen für alle zu suchen? Oder sollte man Lösungen auf diejenigen zuschneiden, die die meisten Mitarbeitenden und damit die meisten Klient:innen haben? Solche Betrachtungen stellt niemand gerne an, und sie müssten auch weiter nach Arbeitsfeldern und regionalen Besonderheiten differenziert werden. So würden Hilfefelder und/oder Regionen mit besonders vielen kleinen Organisationen nicht benachteiligt.

Die schmerzhafte Erkenntnis, dass nicht allen Organisationen gleichermaßen geholfen werden kann, betrifft auch die Thematik der Insolvenzen. In den Gesprächen schien es manchmal, als gäbe es zwei Elefanten im Raum: Einem werden durchaus sorgenvolle Blicke zugeworfen, während man sich bei dem anderen nicht traut, seine Existenz offen anzusprechen. Worum es geht: Insolvenzen und die damit verbundene Frage nach Fusionen und Zentralisierung. Es sind nicht nur kleine Träger, die in wirtschaftliche Schieflage geraten, sie sind aber die ersten, die von Insolvenzwellen

betroffen sind. Um Insolvenzen vorzubeugen, entscheiden sich daher vermehrt Träger zu Fusionen. Im Jahr 2024 haben sich zum Beispiel die Caritasverbände Hochtaunus (ehemals knapp über 250 Mitarbeitende) und Main-Taunus (ebenfalls knapp über 250 Mitarbeitende) zum Caritasverband Taunus (dann mit 550 Mitarbeitenden) zusammengeschlossen. Im selben Jahr haben die Caritasverbände Siegen-Wittgenstein (ca. 200 MA) und Olpe (ca. 2.000 MA) ihre Fusion zu einem 2.200-Mitarbeitenden-starken Träger verkündet (Schulz 18.07.2024; Schulz 12.11.2024). Die Diskussion um den Erhalt lokaler Unabhängigkeit verschweigt also, dass manche kleinere Träger längst dazu gezwungen sind, sich zu größeren Strukturen zusammenzuschließen. IT spielt dabei eine nicht unbedeutende Rolle: Je standardisierter die Struktur und Prozesse, desto leichter und kostengünstiger der Zusammenschluss. Dies gilt insbesondere, wenn beide Organisationen ohnehin beim selben Dienstleister sind oder ihre IT bereits vor der Fusion anderweitig gemeinsam betreiben. Zudem wird sich gerade ein deutlich größerer Fusionspartner genau überlegen, ob die IT-Struktur eines kleineren Partners in einem Zustand ist, in dem er sie übernehmen kann und möchte. Eine vollkommen marode IT-Infrastruktur ist ein Kostenrisiko, an dem Fusionen und damit möglicherweise der Erhalt von Einrichtungen und Diensten scheitern können.

Hinzu kommt, dass ein Träger vielleicht heute wirtschaftlich und IT-technisch solide dasteht – aber was ist mit morgen? Es ist verständlich, dass gerade Organisationen, die lokal Lösungen gefunden haben, die gut funktionieren, keine Kompetenzen abgeben möchten. Hier gilt es jedoch, Risiken miteinzukalkulieren und für die Zukunft zu planen: Ist die IT anschlussfähig, wenn der Träger einmal wirtschaftlich in eine Schieflage gerät und sich mit einer anderen Organisation zusammenschließen muss? Was passiert, wenn die interne IT-Abteilung, die heute gute Arbeit leistet, keinen Nachwuchs mehr findet? Können die Prozesse dann noch nach extern überführt werden, oder sind sie so handgestrickt, dass Außenstehende sie nicht verstehen? Diese Fragen müssen sich auch mittlere und große Träger stellen. Auch sie wollen gegebenenfalls anschlussfähig sein für andere, und auch sie sind betroffen vom demographischen Wandel und Fachkräftemangel.

Eine letzte Ableitung aus dem Interviewmaterial betrifft politische Forderungen. Einerseits sagt zumindest einer der Expert:innen, dass die Zeiten vorbei seien, in der man als freie Wohlfahrt einfach nur mehr Geld fordern konnte; stattdessen müsse man Lösungsvorschläge machen. Eine ähnliche Aussage tätigte eine der befragten Personen außerhalb des Interviews im Rahmen eines anderen Termins. Andererseits zielen die meisten in den Interviews geäußerten Forderungen gegenüber dem Gesetzgeber lediglich auf höhere Finanzmittel ab. Diese mögen nötig und ethisch-

gesellschaftlich geboten sein. Das ändert aber nichts daran, dass man mit reinen Forderungen angesichts der wirtschaftlichen Lage und politischen Stimmung nichts erreichen zu können scheint. Ein Angebot, dass die freie Wohlfahrt der Politik machen könnte, um im Gegenzug höhere Mittel für die eigentliche Leistungserbringung, Digitalisierung und Investitionen zu erhalten, sind Einsparungen durch Verwaltungskonsolidierung und eben auch IT-Konsolidierung. Hier geht es nicht darum, Finanzlücken durch Einsparungen im Verwaltungsbereich selbst zu stopfen – das ist gar nicht möglich – sondern zu signalisieren, dass die freie Wohlfahrt gewillt ist, Mehrfachstrukturen abzubauen und Effizienzen zu erhöhen. Wie ein Gesprächspartner sagte: Verhandlungen sind ein Kuhhandel. Es mag sein, dass durch die Zentralisierung von Verwaltungsaufgaben und IT-Infrastruktur auf lokale Bedürfnisse schlechter eingegangen werden kann – allen Beteiligten ist klar, dass „Vereinheitlichung und Standardisierung nicht immer Gold [ist], nur weil es glänzt", aber letztendlich geht es darum, überhaupt für Klient:innen da sein zu können. Sie sind es, wofür IT-Sicherheit gut ist: Ihre Versorgung muss sichergestellt und ihre sensiblen personenbezogenen Daten müssen geschützt werden. Wenn Träger ihren Betrieb einstellen müssen – sei es wegen Fachkräftemangel, wegen fehlender Finanzierung oder weil sie die Folgen eines Cyberangriffs wirtschaftlich nicht bewältigen können – dann braucht man im Anschluss keine IT-Sicherheit mehr. Daher gilt für IT-Sicherheit das, was für die freie Wohlfahrt im Ganzen gilt: Es ist mehr Kooperationsbereitschaft innerhalb der Branche nötig und eine höhere Priorisierung seitens der Politik.

9.3 Methodische Einschränkungen

Unter dem Dach des Deutschen Caritasverbandes sind etwa 6.200 eigenständige Rechtsträger vereint. In den Interviews wurden davon acht befragt – entsprechend kann diese Masterarbeit nur einen Einblick in die Caritas und einen Überblick über das Problem der IT-Sicherheit in derselben geben. Sie kann keine Aussagen treffen, die alle Organisationen zu hundert Prozent unterschreiben würden. Die Expert:innen wurden allerdings so ausgewählt, dass sie in ihrer Gesamtheit ein möglichst umfassendes Bild zeichnen. Aus dem Versuch, viele Organisationstypen abzudecken, folgt aber auch, dass die einzelnen Typen nicht bis ins Details beleuchtet werden können. Diese Arbeit kann also keine Aussagen machen über „die" OCVs, „die" DiCVs oder „die" Spitzenverbände.

Zudem gibt es Träger, die gar nicht berücksichtigt wurden, etwa lokale Dienste und Einrichtungen von Fachverbänden oder angeschlossene Träger. Dazu kommt, dass eine Definition dessen, was kleine, mittlere und große Organisationen eigentlich sind, bewusst unterlassen wurde. Eine

einheitliche Definition gibt nicht, weil die Expert:innen unterschiedlich einschätzen, in welche Größenkategorie sie selbst oder andere fallen. Nichtsdestotrotz muss angemerkt werden, dass ein größeres Sample auch eine bessere Berücksichtigung der Organisationsgröße ermöglicht hätte. Darüber hinaus wurden weder der DCV noch die BAGFW befragt. Dies geschah aus der Sorge heraus, dass die Anonymität dieser Organisationen nicht gewährleistet und ihre Vertreter:innen in den Interviews nicht vollständig offen hätten sprechen können. Damit fehlen die Perspektiven des DCV und der BAGFW in dieser Arbeit.

Zusätzlich sind einige Ergebnisse spezifisch für die Caritas und würden für Organisationen anderer Wohlfahrtsverbände anders ausfallen. Zum Beispiel sind die Mitglieder des Paritätischen Wohlfahrtsverbands noch heterogener und erhalten keine Kirchensteuer, ebenso wenig wie das DRK und die AWO. Unter der Trägerschaft des DRKs befinden sich außerdem besonders viele Einrichtungen, die zu kritischer Infrastruktur zählen und damit unter IT-Sicherheitsgesetze fallen.

Hinzu kommt, dass die Interviewfragen thematisch sehr breit waren. Zu jedem Themenblock ließe sich eine eigene Arbeit schreiben, die die Feinheiten einzelner Aspekte besser herausarbeiten würden. Zudem lag der Fokus der Fragen mehr auf den Herausforderungen als auf den Maßnahmen.

9.4 Zukünftige Forschung

Aus diesen methodischen Einschränkungen ergeben sich Desiderate für weitere Forschung: Träger und Akteure, die hier nicht beleuchtet werden konnten, sollten Gegenstand zukünftiger Forschung sein. Da in dieser Arbeit die systemischen Probleme für die Herstellung von IT-Sicherheit in der freien Wohlfahrt ausgiebig beschrieben wurden, ist es nötig, sich in weiteren Schritten nun Maßnahmen zuzuwenden. Man könnte zum Beispiel die Rahmenverträge in der Eingliederungshilfe vergleichen und erforschen, warum IT-Kosten in einigen Bundesländern dort Einzug gefunden haben und andere nicht. Auch die verschiedenen Herangehensweisen und die Wirksamkeit von Lobbyarbeit zu Digitalisierung in der freien Wohlfahrt kann verglichen werden. Was den IT-Betrieb betrifft, wäre es hilfreich für die Praxis, verschiedene IT-Betriebsformen in sozialen Organisationen zu beleuchten. Von besonderem Interesse wären hierbei Kooperationen zwischen Trägern und Dienstleistern, die sich auf die Sozialwirtschaft spezialisiert haben im Vergleich zum klassischen Eigenbetrieb und branchenfernen Dienstleistern. Ziel wäre es, Handlungsempfehlungen zu geben, welche Betriebsform sich für welche Akteure unter welchen Bedingungen eignen. Ein besonderes Augenmerk könnte hier auf die Bedeutung und Umsetzung von IT-

Sicherheitsmaßnahmen gelegt werden. Ebenfalls wertvoll für die Praxis wäre eine wissenschaftliche Begleitung von IT-Übergängen (Wechsel der Betriebsform) und Fusionen. Auf politischer Ebene wäre es interessant, Politiker:innen und Ministerialbeamt:innen zu Themen außerhalb ihres eigentlichen Ressorts zu befragen: Sozialpolitiker:innen zu Digitalisierung und IT-Sicherheit, und Digital-, Wirtschafts- und Finanzpolitiker:innen zur freien Wohlfahrt. Die daraus gewonnenen Erkenntnisse könnten dazu genutzt werden, Strategien zu erarbeiten, die Sichtbarkeit der freien Wohlfahrt und ihrer Bedürfnisse bezogen auf Digitalisierung, IT und IT-Sicherheit zu erhöhen.

10. Fazit

Diese Arbeit hat sich zur Aufgabe gemacht, die politischen, wirtschaftlichen und organisationalen Rahmenbedingungen für IT-Sicherheit in der freien Wohlfahrt zu beleuchten. Dazu wurden eine ausführliche Literaturrecherche durchgeführt und acht Expert:innen befragt. Die Berichte decken sich: Die freie Wohlfahrt leidet unter schlechter IT-Infrastruktur; fehlendem IT-Fachpersonal und geringen IT-Kompetenzen der Mitarbeitenden. Es besteht tendenziell eine geringe Aufmerksamkeit unter Vorständ:innen und Spitzenverbänden für das Thema IT-Sicherheit. Die Heterogenität der Caritas behindert Koordination und Kooperation. Es gibt Hürden bei der Interessensvertretung, keine Refinanzierung von IT-Ausgaben und mangelndes politischen Interesse. Aus den Interviews geht zusätzlich hervor, dass die hohen bürokratischen Anforderungen beim Datenschutz das Durchsetzen von IT-Sicherheitsmaßnahmen erschweren. Die Expert:innen betonen außerdem, dass aufgrund des fehlenden politischen Verständnisses für die Bedeutung der Wohlfahrt Digitalisierung und damit auch IT-Sicherheitsmaßnahmen im Speziellen und klassische soziale Dienstleistungen im Allgemeinen nicht auskömmlich finanziert werden. In Folge müssen Träger Angebote einschränken oder ihre Arbeit ganz einstellen. Fehlende IT-Sicherheit ist damit nur einer von vielen Faktoren, die zur Insolvenzgefährdung von sozialen Organisationen beitragen. Die Probleme mit IT-Sicherheit sind letztlich symptomatisch für das System der freien Wohlfahrt an sich.

Die Herausforderungen für IT-Sicherheit in der Branche lassen sich in vier Kategorien einteilen: Mangelndes Problembewusstsein für IT-Sicherheit, mangelnde politische Sichtbarkeit der freien Wohlfahrt, mangelnde Koordination innerhalb der Branche und fehlende Finanzmittel. Es gibt vier Arten an Maßnahmen und Ideen, um diesen Problemen zu begegnen:

- Information und Vernetzung innerhalb der freien Wohlfahrt und in Richtung Politik und Wirtschaft,
- Standardisierung und Kooperation in Bezug auf IT-Betrieb,
- Gesetzesanpassungen zur auskömmlichen Refinanzierung, und
- grundlegende politische und gesellschaftliche Forderungen nach einer Priorisierung der Unterstützung für Wohlfahrtsarbeit.

Immer mehr freigemeinnützige Träger sind insolvenzbedroht. Finanzressourcenbegrenzt sind begrenzt und das politische Problembewusstsein nicht gegeben. Daher muss sich die freie Wohlfahrt und in diesem Fall insbesondere die Caritas überlegen, ob sie ihre bisherige heterogene, komplexe Struktur aufrechterhalten kann. Alternativ müssten Träger Kompetenzen abgeben und sich zu größeren Strukturen zusammenschließen. Dadurch könnten Synergieeffekte genutzt werden, auch bei IT-Infrastruktur. Dies könnte einen Beitrag dazu leisten, IT-Sicherheit in sozialen Organisationen zu verbessern.

Danksagung

An dieser Stelle möchte ich all jenen meinen Dank aussprechen, die mich auf dem Weg zu dieser Masterarbeit begleitet und unterstützt haben.

Mein besonderer Dank gilt den Expert:innen, dass Sie sich die Zeit genommen haben, meine Fragen zu beantworten. Ohne Ihre Offenheit und Expertise wäre diese Arbeit nicht möglich gewesen.

Ebenso danke ich meinen ehemaligen Kolleg:innen vom Caritas-Netzwerk IT e.V. für die Türen, die ihr mir geöffnet habt, die Flexibilität in meiner Arbeitszeitgestaltung und die inspirierenden Gespräche.

Mein Dank gilt auch dem Chaos Computer Club e. V. für das Chaotische Catalysator Stipendium und dem damit verbundenen Interesse der Community der ethischen Hacker an der freien Wohlfahrt.

Von Herzen danke ich meiner Familie und meinen Freund:innen dafür, dass ihr mich nach dem Cyberangriff auf den DiCV München in meiner Arbeit so sehr unterstützt habt. Auch danach habt ihr in eurer Unterstützung nicht nachgelassen, als ihr euch weitere eineinhalb Jahre lang im Rahmen dieser Masterarbeit von mir zu IT-Sicherheit und der freien Wohlfahrt aufklären lassen musstet. Danke!

Literaturverzeichnis

Allianz Commercial (2024). Allianz Risk Barometer Results appendix 2024. München.

Arbeiterwohlfahrt (2023). Digitalpolitische Eckpfeiler der Arbeiterwohlfahrt. Berlin. Online verfügbar unter https://digital.awo.org/wp-content/uploads/2023/10/Digitalpolitische-Eckpfeiler-der-AWO.pdf (abgerufen am 26.02.2024).

Backhaus-Maul, Holger (2019). Zentrifugalkräfte in der Freien Wohlfahrtspflege: Wohlfahrtsverbände als traditionsreiche und ressourcenstarke Akteure. In: Matthias Freise/Annette Zimmer (Hg.). Zivilgesellschaft und Wohlfahrtsstaat im Wandel. Wiesbaden, Springer Fachmedien Wiesbaden, 83–100.

Baier, Dirk/Biberstein, Lorenz/Girschik, Katja/Wardak, Sabera (2022). Cyberkriminalität gegen Organisationen im Sozialbereich: Ergebnisse einer Onlinebefragung im Kanton Zürich. Zürich. https://doi.org/10.21256/zhaw-25678.

Betzer, André/Doumet, Markus/Doumet, Sylvie/Herbrand, Marc (2025). Die volkswirtschaftliche Bedeutung der freien Wohlfahrtspflege im Bergischen Städtedreieck. Wuppertal. https://doi.org/10.25926/BUW/0-815.

Bieker, Rudolf (2022). Einrichtungsträger. Online verfügbar unter https://www.socialnet.de/lexikon/Einrichtungstraeger (abgerufen am 16.05.2024).

Bingener, Reinhard (2024). Stille Pleite im Sozialsystem. Frankfurter Allgemeine Zeitung (Online) vom 01.11.2024. Online verfügbar unter https://www.faz.net/aktuell/politik/inland/caritas-und-diakonie-stille-pleitewelle-im-sozialsystem-110079788.html (abgerufen am 20.03.2025).

bitkom (2023). Organisierte Kriminalität greift verstärkt die deutsche Wirtschaft an. Online verfügbar unter https://www.bitkom.org/Presse/Presseinformation/Organisierte-Kriminalitaet-greift-verstaerkt-deutsche-Wirtschaft-an (abgerufen am 24.02.2024).

bitkom (2024). Mangel an IT-Fachkräften droht sich dramatisch zu verschärfen. Online verfügbar unter https://www.bitkom.org/Presse/Presseinformation/Mangel-an-IT-Fachkraeften-droht-sich-zu-verschaerfen#_ (abgerufen am 01.07.2024).

Boeßenecker, Karl-Heinz (2018). Spitzenverbände der Wohlfahrtspflege im Transformationsprozess zu sozialwirtschaftlichen Organisationen. In: Klaus Grunwald/Andreas Langer (Hg.). Sozialwirtschaft. Handbuch für Wissenschaft und Praxis. Baden-Baden, Nomos, 288–302.

Bogner, Alexander/Littig, Beate/Menz, Wolfgang (2018). Generating Qualitative Date with Experts and Elites. In: Uwe Flick (Hg.). The SAGE Handbook of Qualitative Data Collection. London, SAGE Publications Ltd, 652–667.

Brinkmann, Volker (2009). Sozialökonomie. Grundlagen - Modelle - Übungen. Wiesbaden, Betriebswirtschaftlicher Verlag Gabler.

Bundesamt für Sicherheit in der Informationstechnik (2013). Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. Leitfaden. Bonn. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Themen-Downloads/Gesundheit/risikoanalyse_krankenhaus-it_langfassung.pdf?__blob=publicationFile&v=4.

Bundesamt für Sicherheit in der Informationstechnik (2022). Lagebild Gesundheit. Cyber-Sicherheit im Gesundheitswesen 2022. Bonn. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Lagebild_Gesundheit_2022.pdf?__blob=publicationFile&v=6 (abgerufen am 27.02.2024).

Bundesamt für Sicherheit in der Informationstechnik (2023a). Die Lage der IT-Sicherheit in Deutschland 2023. Bonn.

Bundesamt für Sicherheit in der Informationstechnik (2023b). IT-Grundschutz-Kompendium. Köln, Bundesanzeiger-Verl.

Bundesamt für Sicherheit in der Informationstechnik (2023c). Untersuchung zur Wirksamkeit der IT-Sicherheitsgesetze unter Betreibern Kritischer Infrastrukturen. Ergebnisbericht. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/evaluierung-itsig2-ergebnisbericht.pdf?__blob=publicationFile&v=3 (abgerufen am 04.07.2024).

Bundesamt für Sicherheit in der Informationstechnik (o.D.). Advanced Persistent Threat. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/apt.html (abgerufen am 26.09.2024).

Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege (2020). Digitale Transformation und gesellschaftlicher Zusammenhalt. Gemeinsame Erklärung von BMFSFJ und BAGFW zur

Wohlfahrtspflege in der Digitalen Gesellschaft. Berlin. Online verfügbar unter https://www.bagfw.de/fileadmin/user_upload/Veroeffentlichungen/Stellungnahmen/2020/GemeinsameErkl%C3%A4rung_BMFSFJ_und_BAGFW.pdf.

Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege (2021). Erwartungen der BAGFW an die Bundespolitik der 20. Legislaturperiode. Teilhabe durch gemeinwohlorientierte Digitalisierung. Berlin. Online verfügbar unter https://www.bagfw.de/fileadmin/user_upload/Veroeffentlichungen/Publikationen/Forderungspapiere_2021/BT-Wahl_Digitalisierung.pdf (abgerufen am 26.02.2024).

Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege (2022). Für Teilhabe und gesellschaftlichen Zusammenhalt. Vorrang der #Gemeinnützigkeit - Anregung für ein Reformpaket. Online verfügbar unter https://www.bagfw.de/fileadmin/user_upload/Veroeffentlichungen/Stellungnahmen/2022/neu_2022-06-22_BAGFW-Papier_Vorrang_f%C3%BCr_Gemeinn%C3%BCtzigkeit.pdf (abgerufen am 19.03.2025).

Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege (2023). Gesamtstatistik 2020. Einrichtungen und Dienste der Freien Wohlfahrtspflege. Berlin. Online verfügbar unter https://www.bagfw.de/fileadmin/user_upload/Veroeffentlichungen/Publikationen/Statistik_2020/Einzelseiten/BAGFW_Gesamtstatistik_2020_2023-12-14_ES.pdf (abgerufen am 23.04.2024).

Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege (2024). Sozialkürzungen verhindern - In Zusammenhalt investieren. Umfrage zur finanziellen Lage der freien Wohlfahrt. Online verfügbar unter https://www.bagfw.de/fileadmin/user_upload/Veroeffentlichungen/Pressemeldungen/PM_2024/Sozialk%C3%BCrzungen_verhindern_in_Zusammenhalt_investieren_190624.pdf (abgerufen am 22.08.2024).

Bundesarbeitsgemeinschaft der überörtlichen Träger der Sozialhilfe und der Eingliederungshilfe (2024). Unsere Mitglieder. Online verfügbar unter https://www.bagues.de/de/mitglieder/ (abgerufen am 20.07.2024).

Bundesarbeitsgemeinschaft Werkstätten für behinderte Menschen e. V./Katholische Universität Eichstätt/xit GmbH (Hg.) (2015). Bundesweite SROI-Studie der BAG WfbM 2013/2014. Berlin / Eichstätt / Nürnberg. Online verfügbar unter https://www.bagwfbm.de/file/950 (abgerufen am 15.03.2025).

Bundesministerium für Wirtschaft und Klimaschutz (o.D.). Automobilindustrie. Online verfügbar unter https://www.bmwk.de/Redaktion/DE/Textsammlungen/Branchenfokus/Industrie/branchenfokus-automobilindustrie.html#:~:text=Zur%20deutschen%20Automobilindustrie%20z%C3%A4hlen%20die,23.000%20weniger%20als%20im%20Vorjahr. (abgerufen am 25.02.2024).

Buzatu, Anne-Marie (2022). Advanced Persistent Threat Groups Increasingly Destabilize Peace and Security in Cyberspace. In: Scott J. Shackelford/Frederick Douzet/Christopher Ankersen (Hg.). Cyber Peace. Cambridge University Press, 236–242.

Caritas-Netzwerk IT e. V. (2024). Willkommen beim Caritas Netzwerk IT e. V. Online verfügbar unter https://www.caritas-netzwerk-it.de/ (abgerufen am 27.08.2024).

Caritasverband der Diözese Rottenburg-Stuttgart e. V. (o.D.a). Die Geschichte des Caritasverbandes der Diözese Rottenburg-Stuttgart. Online verfügbar unter https://www.caritas-rottenburg-stuttgart.de/wer-wir-sind/wissenswertes/geschichte/geschichte (abgerufen am 21.05.2024).

Caritasverband der Diözese Rottenburg-Stuttgart e. V. (o.D.b). Korporative Mitglieder. Online verfügbar unter https://www.caritas-rottenburg-stuttgart.de/wer-wir-sind/mitglieder/korporative-mitglieder/korporative-mitglieder (abgerufen am 21.05.2024).

Caritasverband der Erzdiözese München und Freising e.V. (o.D.a). Caritas ist sozialer Dienstleister. Online verfügbar unter https://der-caritasverband.caritas-nah-am-naechsten.de/de/caritas-ist-sozialer-dienstleister (abgerufen am 21.05.2024).

Caritasverband der Erzdiözese München und Freising e.V. (o.D.b). Caritas ist Spitzenverband. Online verfügbar unter https://der-caritasverband.caritas-nah-am-naechsten.de/de/caritas-ist-spitzenverband (abgerufen am 21.05.2024).

Caritasverband für die Diözese Mainz e. V. (o.D.). Caritasverbände im hessischen Teil des Bistums. Online verfügbar unter https://www.caritas-bistum-mainz.de/ueberuns/caritasverbandfurdiedioezesemainz/mitglieder/caritasverbaendeimhessischenteildesbistums (abgerufen am 21.05.2024).

Caritasverband für die Diözese Münster e. V. (o.D.). Aufbau, Organe und Gremien. Online verfügbar unter https://www.caritas-bistum-muenster.de/verband/caritas-fuer-das-bistum-

muenster/aufbau-organe-und-gremien/aufbau-organe-und-gremien (abgerufen am 21.05.2024).

Caritasverband Gießen e.V. (o.D.). Mitglieder unMitglieder und Fachverbänded Fachverbände. Online verfügbar unter https://www.caritas-giessen.de/caritas-giessen/mitglieder-und-fachverbaende/mitglieder-und-fachverbaende (abgerufen am 21.05.2024).

CyberPeace Institute (2023). NGOs serving humanity at risk: Cyber threats affecting international Geneva. Genf. Online verfügbar unter https://cyberpeaceinstitute.org/publications/cyber-peace-analytical-reportngos-serving-humanity-at-risk-cyber-threats-affecting-international-geneva/.

Darms, Martin/Haßfeld, Stefan/Fedtke, Stephen (2019). IT-Sicherheit und Datenschutz im Gesundheitswesen. Wiesbaden, Springer Fachmedien Wiesbaden.

Deistler, Nico (2023). IT-Compliance in KMU – Eine Methode zum angepassten Einsatz von Rahmenwerken. HMD Praxis der Wirtschaftsinformatik. https://doi.org/10.1365/s40702-023-00974-0.

Deutscher Caritasverband (2019). Angebote für alte Menschen. Online verfügbar unter https://www.caritas.de/diecaritas/wir-ueber-uns/transparenz/finanzierung/altenhilfe (abgerufen am 11.08.2024).

Deutscher Caritasverband (2023a). Digitale Zukunft gestalten: Mehr Teilhabe für alle. Digitalpolitische Positionen des Deutschen Caritasverbandes. Berlin/Brüssel/Freiburg.

Deutscher Caritasverband (2023b). Einblicke in die Arbeit des Deutschen Caritasverbandes im Jahr 2022. Geschäftsbericht. Freiburg. Online verfügbar unter https://www.caritas.de/geschaeftsbericht (abgerufen am 23.04.2024).

Deutscher Caritasverband (2024). Neue Caritas - Ausgabe 20/2024. Online verfügbar unter https://www.caritas.de/neue-caritas/heftarchiv/jahrgang-2024/ausgabe-20 (abgerufen am 14.03.2025).

Deutscher Caritasverband (o.D.a). Diözesancaritasverbände (DiCV). Online verfügbar unter https://www.caritas.de/glossare/dioezesancaritasverbaende-dicv (abgerufen am 21.05.2024).

Deutscher Caritasverband (o.D.b). Diözesanverbände der Caritas. Online verfügbar unter https://www.caritas.de/diecaritas/deutschercaritasverband/dioezesanverbaende/dioezesanverbaende (abgerufen am 23.04.2024).

Deutscher Caritasverband (o.D.c). Fachverbände. Online verfügbar unter https://www.caritas.de/diecaritas/deutschercaritasverband/fachverbaende/fachverbaende.aspx (abgerufen am 23.04.2024).

Deutscher Caritasverband (o.D.d). Mitglieder des Deutschen Caritasverbandes. Online verfügbar unter https://www.caritas.de/glossare/mitglieder-des-deutschen-caritasverbande (abgerufen am 23.04.2024).

Deutscher Caritasverband (o.D.e). Ordensgemeinschaften. Online verfügbar unter https://www.caritas.de/glossare/ordensgemeinschaften (abgerufen am 23.04.2024).

Deutscher Caritasverband (o.D.f). Vereinigungen. Online verfügbar unter https://www.caritas.de/glossare/vereinigungen (abgerufen am 23.04.2024).

Deutscher Paritätischer Wohlfahrtsverband (2022). Digitalisierung fördern, Zivilgesellschaft stärken, digitale Teilhabe für alle ermöglichen. Kassel. Online verfügbar unter https://www.der-paritaetische.de/fileadmin/user_upload/Schwerpunkte/Digitalisierung/doc/Positionspapier_Parita%CC%88tischer_Digitale_Teilhabe.pdf (abgerufen am 26.0.2.2024).

Deutscher Paritätischer Wohlfahrtsverband (o.D.). Einkaufsportal: Hardware Software. Online verfügbar unter https://www.der-paritaetische.de/leistungen-angebote/ihr-verband-ihre-einkaufsvorteile/einkaufsportal/hardware-software/ (abgerufen am 26.02.2024).

Deutsches Rotes Kreuz (2023). Digitale Transformation - Digitale Teilhabe für Alle. Online verfügbar unter https://www.drk.de/presse/pressemitteilungen/meldung/digitale-transformation-drk-digitale-teilhabe-fuer-alle/ (abgerufen am 16.02.2024).

Diakonie Deutschland (2023a). Digitalkonferenz. Einladung zur digitalen Veranstaltung über Zoom am 25. Januar 2023. Online verfügbar unter https://bildung.diakonie-baden.de/documents/158203/0/2023-01-25_Digitalkonferenz_VS221024.pdf/552f9d41-1a9f-4484-957a-a8714e7a8a24 (abgerufen am 26.02.2024).

Diakonie Deutschland (2023b). Einrichtungsstatistik 2022. Statistik der Diakonie Deutschland, Stand 01.01.2022. Berlin.

Dihle, Hanno (2021). Caritas denkt Führung neu. Deutscher Caritasverband. Online verfügbar unter https://www.caritas.de/fuerprofis/fachthemen/caritas/geschlechtergerechtigkeit/caritas-denkt-fuehrung-neu (abgerufen am 21.02.2025).

Dreißigacker, Arne/Skarczinski, Bennet von/Wollinger, Gina Rosa (2020). Cyberangriffe gegen Unternehmen in Deutschland: Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019. https://doi.org/10.15496/publikation-64243.

DRK-Service GmbH (o.D.). Rahmenverträge: Sofware & Service. Online verfügbar unter https://www.drkservice.de/rahmenvertraege/it/software-service/ (abgerufen am 26.02.2024).

Eckert, Claudia (2023). IT-Sicherheit. Konzepte - Verfahren - Protokolle. 11. Aufl. Berlin/Boston, De Gruyter.

Ermicioi, Natalia/Liu, Michelle Xiang (2022). Cybersecurity In Nonprofits: Factors Affecting Security Readiness During Covid-19. SAIS 2022 Proceedings (18). Online verfügbar unter https://aisel.aisnet.org/sais2022/18.

Europäische Kommission (2022). Flash Eurobarometer 496: SMEs and Cybercrime. Report. Brüssel. https://doi.org/10.2837/14988.

European Union Agency for Cybersecurity (2021). CSIRT Capabilities in Healthcare Sector. Status and Development. Athen/Heriaklon. https://doi.org/10.2824/201143.

European Union Agency for Cybersecurity (2023). Enisa threat landscape 2023. July 2022 to June 2023. Athen/Heriaklon.

Faber, Eberhard von (2021). IT und IT-Sicherheit in Begriffen und Zusammenhängen. Thematisch sortiertes Lexikon mit alphabetischem Register zum Nachschlagen. Wiesbaden, Springer Vieweg.

Falter, Alexander (2010). Wirtschaftsfaktor Wohlfahrtsverbände. Deutsche Bank Research. Frankfurt am Main. Online verfügbar unter https://www.dbresearch.de/PROD/RPS_DEPROD/PROD0000000000474515/Wirtschaftsfaktor_Wohlfahrtsverb%C3%A4nde.pdf (abgerufen am 25.02.204).

FINSOZ e. V. - Fachgruppe IT-Compliance (2022). IT-Sicherheit in der Sozialwirtschaft. Lagebericht & Leitfaden. Berlin.

Flick, Uwe (2014). Gütekriterien qualitativer Sozialforschung. In: Nina Baur/Jörg Blasius (Hg.). Handbuch Methoden der empirischen Sozialforschung. Wiesbaden, Springer Fachmedien Wiesbaden, 411–423.

Freie Wohlfahrtspflege Bayern (2024). Wohlfahrtsverbände warnen vor Versorgungskrise. Online verfügbar unter https://www.freie-wohlfahrtspflege-bayern.de/informationen/pressemitteilungen/presseartikel/news/wohlfahrtsverbaende-warnen-vor-versorgungskrise/?tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=f2adb08213ab6bc136bb0fde5273190a (abgerufen am 22.08.2024).

Gerlach, Florian/Hinrichs, Knut (2018). Leistungserbringungsrecht in der Sozialwirtschaft. In: Klaus Grunwald/Andreas Langer (Hg.). Sozialwirtschaft. Handbuch für Wissenschaft und Praxis. Baden-Baden, Nomos, 168–194.

Grunwald, Klaus/Langer, Andreas (2018). Sozialwirtschaft - eine Einführung in das Handbuch. In: Klaus Grunwald/Andreas Langer (Hg.). Sozialwirtschaft. Handbuch für Wissenschaft und Praxis. Baden-Baden, Nomos, 45–64.

gTrägergesellschaft mbH für die Einrichtungen der Schwestern vom Göttlichen Erlöser (o.D.). Der TGE-Einrichtungsverband. Online verfügbar unter https://www.tge-online.de/ueber-uns/tge-einrichtungsverbund/ (abgerufen am 21.05.2024).

Hassan, Mariyam/Saeedi, Kawther/Almagwashi, Haya/Alarifi, Suaad (2023). Information Security Risk Awareness Survey of Non-governmental Organization in Saudi Arabia. In: Anna Visvizi/Orlando Troisi/Mara Grimaldi (Hg.). Research and Innovation Forum 2022. Cham, Springer International Publishing, 39–71.

Heidrich, Christian (2021). Gewaltiger Finanzierungsmix. Caritas in NRW - Zeitschrift der Diözesan-Caritasverbände Aachen, Köln, Münster und Paderborn. Online verfügbar unter https://www.caritas-nrw.de/magazin/2021/artikel/gewaltiger-finanzierungsmix-d88fc0b7-009d-48f2-8d30-989fe8765ec3 (abgerufen am 16.07.2024).

Helfferich, Cornelia (2014). Leitfaden- und Experteninterviews. In: Nina Baur/Jörg Blasius (Hg.). Handbuch Methoden der empirischen Sozialforschung. Wiesbaden, Springer Fachmedien Wiesbaden, 559–574.

Hering, Linda/Schmidt, Robert J. (2014). Einzelfallanalyse. In: Nina Baur/Jörg Blasius (Hg.). Handbuch Methoden der empirischen Sozialforschung. Wiesbaden, Springer Fachmedien Wiesbaden, 529–541.

Kaiser, Robert (2021). Qualitative Experteninterviews. Wiesbaden, Springer Fachmedien.

Kappe, Miriam/Härting, Ralf-Christian/Karg, Christoph/Deffner, Demian (2023). Cybersecurity in SMEs – Drivers of Cybercrime, Insufficient Equipment and Prevention. Procedia Computer Science 225, 3631–3640. https://doi.org/10.1016/j.procs.2023.10.358.

Katholischer Krankenhausverband Deutschland e. V. (o. D.). Übersicher Standorte. Online verfügbar unter https://die-katholischen-krankenhaeuser.de/uebersicht/#uebersicht-standorte (abgerufen am 22.08.2024).

Kehl, Konstantin/Then, Volker (2024). Soziale Investitionen, Wirkungsorientierung und 'Social Return'. In: Klaus Grunwald/Andreas Langer/Monika Sagmeister (Hg.). Sozialwirtschaft. Handbuch für Wissenschaft, Studium und Praxis. Baden-Baden, Nomos, 925–939.

Klauß, Thomas (2014). Verbände digital. Berlin, Heidelberg, Springer Berlin Heidelberg.

Klemm, Britta/Sobottke, Markus/Leuschen, Sabrina/Klein, Florian/Möller, Desdemona (2020). Erfolgsfaktor Digitalisierung. Auf dem Weg zur Sozialwirtschaft 4.0. Bank für Sozialwirtschaft AG. Köln. Online verfügbar unter https://www.sozialbank.de/fileadmin/2015/flipbook/BFS_Erfolgsfaktor_Digitalisierung (abgerufen am 02.07.2024).

Koglin, Erika (2023). Gemeinnützigkeit - Zusammenalt für das Gemeinwohl. Online verfügbar unter https://www.wir-sind-paritaet.de/wir-berichten/blog/gemeinnuetzigkeit-zusammenhalt-fuer-das-gemeinwohl (abgerufen am 10.07.2024).

Kolhoff, Ludger (2019). Öffentliche Finanzierung der Sozialwirtschaft. In: Ludger Kolhoff (Hg.). Aktuelle Diskurse in der Sozialwirtschaft II. Wiesbaden, Springer Fachmedien Wiesbaden, 155–170.

Kongregation der Schwestern vom Göttlichen Erlöser (o.D.). Krankenhäuser. Online verfügbar unter https://www.schwestern-vom-goettlichen-erloeser.de/einrichtungen/krankenhaeuser (abgerufen am 21.05.2024).

Kopf, Hartmut (2020). Zwischen Tradition und Innovation Wie Digitalisierung die Organisationskultur sozialer Unternehmen verändert: Ein Impuls zu mehr digitaler Fitness. In: Michael

Vilain (Hg.). Wege in die digitale Zukunft. Nomos Verlagsgesellschaft mbH & Co. KG, 49–68.

Kreidenweis, Helmut (2023). Stand, neuere Entwicklungen und Zukunft der Digitalisierung in der Sozialwirtschaft. Sozialer Fortschritt 72 (11), 811–828. https://doi.org/10.3790/sfo.72.11.811.

Kreidenweis, Helmut/Wolff, Dietmar (2022). IT-Report für die Sozialwirtschaft 2022. Eichstätt, Katholische Universität Eichstätt-Ingolstadt.

Kreidenweis, Helmut/Wolff, Dietmar (2023). IT-Report für die Sozialwirtschaft 2023. Eichstätt, Katholische Universität Eichstätt-Ingolstadt.

Kreidenweis, Helmut/Wolff, Dietmar (2024). IT-Report für die Sozialwirtschaft 2024. Eichstätt, Katholische Universität Eichstätt-Ingolstadt.

Maschmeyer, Lennart/Deibert, Ronald J./Lindsay, Jon R. (2021). A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. Journal of Information Technology & Politics 18 (1), 1–20. https://doi.org/10.1080/19331681.2020.1776658.

Mayring, Philipp (2020). Qualitative Forschungsdesigns. In: Günter Mey/Katja Mruck (Hg.). Handbuch Qualitative Forschung in der Psychologie. Wiesbaden, Springer Fachmedien Wiesbaden, 3–17.

Mayring, Philipp (2022). Qualitative Inhaltsanalyse. Grundlagen und Techniken. 13. Aufl. Weinheim/Basel, Beltz.

Mierzwa, Stan/Scott, James (2017). Cybersecurity in Non-Profit and Non-Governmental Organizations. Institute for Critical Infrastructure Technology. Online verfügbar unter https://www.researchgate.net/publication/314096686_Cybersecurity_in_Non-Profit_and_Non-Governmental_Organizations.

National Institute of Standards and Technology (o.D.). phishing. U.S. Department of Commerce. Online verfügbar unter https://csrc.nist.gov/glossary/term/phishing (abgerufen am 26.09.2024).

Niedung, Matthias (2023). Wie kann sich die Sozialwirtschaft schützen? Sozialwirtschaft 33 (3), 14–15. https://doi.org/10.5771/1613-0707-2023-3-14.

Nyonzigira, Fidele (2023). Exploring Nonprofit Organizations' Successful Compliance Strategies Against Cyber Threats: A Qualitative Study Inquiry. Dissertation. Minneapolis, Capella University. Online verfügbar unter https://www.proquest.com/openview/3d26b932db8a1e2d45a057c31a99aff5/1?pq-origsite=gscholar&cbl=18750&diss=y.

Ottnad, Adrian/Wahl, Stefanie/Miegel, Meinhard (2000). Zwischen Markt und Mildtätigkeit. Die Bedeutung der Freien Wohlfahrtspflege für Gesellschaft, Wirtschaft und Beschäftigung. München, Olzog Verlag.

Panjas, Jennifer (2020). Zumeist kleine Träger - doch tendenziell nimmt ihre Größe zu. Neue Caritas 121 (15), 31. Online verfügbar unter https://www.caritas.de/neue-caritas/heftarchiv/jahrgang2020/artikel/zumeist-kleine-traeger--doch-tendenziell-nimmt-ihre-groesse- (abgerufen am 21.05.2024).

Paritätischer Gesamtverband (2024). Anlage zur PARITÄTISCHEN Fachinformation vom 26. Juli 2024 (Regierungsentwurf für NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz beschlossen). Online verfügbar unter https://www.der-paritaetische.de/fileadmin/user_upload/Fachinfos/2024-7-26_Anlage_NIS2-UmsuCG_Paritaet_barrierefrei.pdf (abgerufen am 29.10.2024).

Paritätischer Wohlfahrtsverband Niedersachsen e. V. (2024). Ein wirtschaftlich und sozial starker Partner. Die freigemeinnützige Sozialwirtschaft als Wirtschaftsfaktor. Online verfügbar unter https://www.paritaetischer.de/fileadmin/Aktuelles/Verbandspositionen/2024-03-12_Positionspapier-Sozialwirtschaft.pdf (abgerufen am 18.03.2025).

Patjens, Rainer (2017). Förderrechtsverhältnisse im Kinder- und Jugendhilferecht. Wiesbaden, Springer VS.

Pawlowska, Agnieszka/Scherer, Benedikt. IT-Sicherheit im Home-Office. Unter besonderer Berücksichtigung der Covid-19 Situation. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Umfrage-Home-Office/umfrage_home-office-2020.pdf?__blob=publicationFile&v=3 (abgerufen am 04.07.2024).

Pehl, Thorsten/Dresing, Thorsten (2024). f4 Audiotranskription. Marburg, dr. dresing & pehl GmbH. Online verfügbar unter https://f4x.audiotranskription.de/ (abgerufen am 21.02.2025).

Pfahler, Johannes/Packmohr, Katharina (2021). Suchtberatung wirksam und effizient! Studie zum „Social Return on Investment“ am Beispiel der Sozialteam-PsBB Görlitz. Nürnberg. Online verfügbar unter https://www.slsev.de/fileadmin/dokumente/veranstaltungen/SLS_VortragPhaler.pdf (abgerufen am 15.03.2025).

Przyborski, Aglaja/Wohlrab-Sahr, Monika (2021). Qualitative Sozialforschung. Ein Arbeitsbuch. 5. Aufl. Berlin/Boston, De Gruyter Oldenbourg.

Rada, Alejandro/Stahlmann, Anne (2016). Sozialwirtschaftsstudie Hessen. Frankfurt am Main. Online verfügbar unter https://www.liga-hessen.de/securedl/sdl-eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE3NDIwNTc3NDQsImV4cCI6MTc0MjA4MzIwMCwidXNlciI6MCwiZ3JvdXBzIjpbMCwtMV0sImZpbGUiOiJmaWxlYWRtaW4vdXNlcl91cGxvYWQvRG9rdW1lbnRlL1ByZXNzZS8yMDE3LzIwMTctMDItMDZfR2VzYW10YmVyaWNodF9maW4ucGRmIiwicGFnZSI6ODV9.clccHh0AKa23Mo0TPBwyGc-Y5ICmMWcVQZ-y2BYcU3E/2017-02-06_Gesamtbericht_fin.pdf (abgerufen am 15.03.2025).

Rahmenvertrag nach § 131 SGB IX in Bayern vom 30.06.2023.

Rahmenvertrag nach § 131 SGB IX Nordrhein-Westfalen vom 19.06.2024.

Redmann, Jörg/Dessel, Christoph (2022). Studie Benchmark Krankenhaus IT. Curacon. Berlin u.a. Online verfügbar unter https://www.curacon.de/index.php?eID=dumpFile&t=r&r=519359&token=aec66c8305293ff5466fe436f1ae1267ec1bebc8 (abgerufen am 26.06.2024).

Schellberg, Klaus (2018). Bericht Sozialwirtschaft Bayern 2018. Evangelische Hochschule Nürnberg; xit GmbH. Nürnberg. Online verfügbar unter https://www.lagoefw.de/wp-content/uploads/2024/10/Bericht_Sozialwirtschaft_Bayern_2018.pdf.

Schellberg, Klaus (2024). Finanzierung in der Sozialwirtschaft. In: Klaus Grunwald/Andreas Langer/Monika Sagmeister (Hg.). Sozialwirtschaft. Handbuch für Wissenschaft, Studium und Praxis. Baden-Baden, Nomos, 525–540.

Schick, Stefan (2024). Grundlagen des Gemeinnützigkeitsrechts. In: Klaus Grunwald/Andreas Langer/Monika Sagmeister (Hg.). Sozialwirtschaft. Handbuch für Wissenschaft, Studium und Praxis. Baden-Baden, Nomos, 587–604.

Schmeja, Brigitte/Albrecht, Peter-Georg/Skalitz, Klaus (2023). Transformation der Caritas-Sozialarbeit in Ostdeutschland. In: Mandy Schulze/Julia Hille/Peter-Georg Albrecht (Hg.). Genese Ost: Transformationen der Sozialen Arbeit in Deutschland. Verlag Barbara Budrich, 115–126.

Schmid, Josef (2018). Schwankende Riesen? Riesige Schwankungen? Die unklare Stellung der Wohlfahrtsverbände im deutschen Modell. In: Rolf G. Heinze/Joachim Lange/Werner Sesselmeier (Hg.). Neue Governancestrukturen in der Wohlfahrtspflege. Nomos Verlagsgesellschaft mbH & Co. KG, 39–54.

Schmid, Josef/Mansour, Julia I. (2007). Wohlfahrtsverbände. Interesse und Dienstleistung. In: Thomas von Winter/Ulrich Willems (Hg.). Interessenverbände in Deutschland. Wiesbaden, VS Verlag für Sozialwissenschaften, 244–270.

Schneiders, Katrin (2021). Sozialwirtschaft. Online verfügbar unter https://www.socialnet.de/lexikon/Sozialwirtschaft (abgerufen am 16.05.2021).

Schroeder, Wolfgang (2017). Konfessionelle Wohlfahrtsverbände im Umbruch. Wiesbaden, Springer Fachmedien Wiesbaden.

Schulz, Oliver (2024). Caritas Siegen-Wittgenstein/Caritas Olpe: Südwestfälische Verbände planen Zusammenschluss. Wohlfahrt Intern (Online) vom 12.11.2024. Online verfügbar unter https://www.wohlfahrtintern.de/newsdetails/article/suedwestfaelische-verbaende-planen-zusammenschluss (abgerufen am 20.03.2025).

Schulz, Oliver (2024). Caritasverband Taunus: Zwei katholische Träger in Hessen gehen zusammen. Wohlfahrt Intern (Online) vom 18.07.2024. Online verfügbar unter https://www.wohlfahrtintern.de/newsdetails/article/zwei-katholische-traeger-in-hessen-gehen-zusammen (abgerufen am 20.03.2025).

Statistisches Bundesamt (2023). Betriebe, tätige Personen und Umsatz im Baugewerbe. Online verfügbar unter https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Bauen/Tabellen/betriebe.html (abgerufen am 25.02.2024).

Then, Volker/Schober, Christian (2015). Was ist eine SROI-Analyse? Wie verhält sie sich zu anderen Analyseformen? Warum sind Wirkungen zentral? Die Einleitung. In: Christian Schober/Volker Then (Hg.). Praxishandbuch Social Return on Investment. Wirkung sozialer investitionen messen. Stuttgart, Schäffer-Poeschel Verlag, 1–22.

Ver.di (o.D.). Ver.di in kirchlichen Betrieben. Online verfügbar unter https://gesundheit-soziales-bildung.verdi.de/mein-arbeitsplatz/kirchliche-betriebe#:~:text=Die%20gr%C3%B6%C3%9Ften%20Arbeitgeber%20in%20Deutschland,dem%20Dach%20der%20beiden%20Wohlfahrtsverb%C3%A4nde. (abgerufen am 25.02.2024).

VERBI Software (2024). MAXQDA Transcription. Berlin, VERBI GmbH. Online verfügbar unter https://www.maxqda.com/de/automatische-transkription (abgerufen am 21.02.2025).

VOICE - Bundesverband der IT-Anwender e. V./metrics (2022). IT-Agenda 2022. Online verfügbar unter https://voice-ev.org/it-agenda-2022-mehr-it-selbstbewusstsein-mehr-budget-kampf-um-mehr-sicherheit/.

VOICE - Bundesverband der IT-Anwender e. V./metrics (2023). IT-Agenda 2023. Online verfügbar unter https://www.metrics.biz/de/studie/it-agenda-2023.html.

VOICE - Bundesverband der IT-Anwender e. V./metrics (2024). IT-Agenda 2024. Online verfügbar unter https://www.metrics.biz/de/studie/it-agenda-2024.html.

Voigt, Paul/Schmalenberger, Alexander (2023). Die Gesetzesentwürfe zur Umsetzung von NIS2 und CER im Überblick — Deutschland verschärft (IT-)Sicherheitsanforderungen: Ein Blick auf die geplanten Änderungen. Computer und Recht 39 (11), 717–724. https://doi.org/10.9785/cr-2023-391108.

Weber, Tobias/Bertschek, Irene/Ohnemus, Jörg/Ebert, Martin (2018). Monitoring-Report Wirtschaft DIGITAL 2018. Kurzfassung. Bundeministerium für Wirtschaft und Energie. Online verfügbar unter https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/monitoring-report-wirtschaft-digital-2018-langfassung.html (abgerufen am 02.07.2024).

Whitmore, Andrew (2023). Erste Hilfe benötigt? Warum ausgerechnet soziale Einrichtungen gehackt werden. DataGuard. Online verfügbar unter https://www.dataguard.de/blog/erste-hilfe-benoetigt-warum-ausgerechnet-soziale-einrichtungen-gehackt-werden (abgerufen am 24.02.2024).

Wolff, Dietmar (2020). Chancen und Risiken der Digitalisierung in der Sozialwirtschaft. In: Sandra Ückert/Hasan Sürgit/Gerd Diesel (Hg.). Digitalisierung als Erfolgsfaktor für das Sozial- und Wohlfahrtswesen. Baden-Baden, Nomos Verlagsgesellschaft, 77–86.

Wolff, Dietmar/Stock, Nele (2024). Telematikinfrastruktur: Wie hoch sind die Pauschalen? Online verfügbar unter https://www.altenheim.net/telematikinfrastruktur-wie-hoch-sind-die-pauschalen/ (abgerufen am 19.03.2025).

Yin, Robert (2006). Case Study Methods. In: Judith L. Green/Gregory Camilli/Patricia B. Elmore et al. (Hg.). Handbook of complementary methods in education research. Mahwah, NJ/Washington, DC, Lawrence Erlbaum Associates; American Educational Research Association, 111–122.

Zentralstatistik des Deutschen Caritasverbandes e.V. (2022). Erhebung: 31.12.2020. Einrichtungsstatistik -Gesamtübersicht. Freiburg.

Zentralwohlfahrtsstelle der Juden in Deutschland (o.D.a). Digitale Trainings. Online verfügbar unter https://zwst.org/de/angebote/digitale-transformation/digitale-trainings (abgerufen am 26.02.2024).

Zentralwohlfahrtsstelle der Juden in Deutschland (o.D.b). Wissensportal Mabat. Einblicke in die digitale Transformation und ihre Bedeutung für jüdische Gemeinden und Organisationen. Online verfügbar unter https://padlet.com/zwst/wissensportal-mabat-uoxgwanm3xvgpgkh (abgerufen am 26.02.2024).

Zimmer, Annette/Paul, Franziska (2024). Zur volkswirtschaftlichen Bedeutung der Sozialwirtschaft. In: Klaus Grunwald/Andreas Langer/Monika Sagmeister (Hg.). Sozialwirtschaft. Handbuch für Wissenschaft, Studium und Praxis. Baden-Baden, Nomos, 87–100.

Zoom Video Communications (2022). TUM-Conf / Zoom. San Jose (California), Zoom Video Communications, Inc. Online verfügbar unter https://collab.dvb.bayern/spaces/TUM-zoom/pages/67398005/Impressum (abgerufen am 21.02.2025).

Anhang

Anhang 1: Liste der Landesarbeitsgemeinschaften der freien Wohlfahrt

Tabelle 6: Liste der Landesarbeitsgemeinschaften der freien Wohlfahrt

Bundesland	Name und Website	Caritas-Mitglieder
Baden-Württemberg	Liga der freien Wohlfahrtspflege in Baden-Württemberg e.V. https://liga-bw.de	DiCV Rottenburg-Stuttgart DiCV Freiburg Die Liga Baden-Württemberg e.V. ist gemeinsam mit dem Städtetag, dem Landkreistag, dem Gemeindeverband und dem Kommunalverband für Jugend und Soziales Mitglied in der Landesarbeitsgemeinschaft der freien und öffentlichen Wohlfahrtsverbände in Baden-Württemberg (LAGÖFW; https://lag-oeffentliche-und-freie-wohlfahrtspflege-bw.de/)
Bayern	Freie Wohlfahrtspflege Landesarbeitsgemeinschaft Bayern https://www.freie-wohlfahrtspflege-bayern.de	Landesverband Bayern e.V. (Mitglieder im Landesverband Bayern: siehe *Tabelle 7: Zusammenschlüsse von DiCVs auf Bundeslandebene* auf S.122)
Berlin	LIGA der Spitzenverbände der Freien Wohlfahrtspflege in Berlin (LIGA Berlin) https://www.ligaberlin.de	DiCV Berlin
Brandenburg	LIGA der freien Wohlfahrtspflege - Spitzenverbände im Land Brandenburg https://www.liga-brandenburg.de	DiCV Berlin DiCV Görlitz
Bremen	LandesArbeitsGemeinschaft (LAG) der Freien Wohlfahrtspflege Bremen e.V. https://www.sozialag.de	Caritasverband Bremen
Hamburg	Arbeitsgemeinschaft der freien Wohlfahrtspflege Hamburg e.V. https://www.agfw-hamburg.de	DiCV Hamburg
Hessen	Liga der freien Wohlfahrtspflege in Hessen e.V. https://www.liga-hessen.de	DiCV Fulda DiCV Limburg DiCV Mainz

Mecklenburg-Vorpommern	LIGA der spitzenverbände der Freien Wohlfahrtspflege in Mecklenburg-Vorpommern e. V. http://www.liga-mv.de	DiCV Berlin (Region Caritas Vorpommern)
Niedersachsen	LAG der Freien Wohlfahrtspflege in Niedersachsen e. V.: https://lag-fw-nds.de	DiCV Hildesheim DiCV Osnabrück Landescaritasverband für Oldenburg
NRW	Arbeitsgemeinschaft der Spitzenverbände der Freien Wohlfahrtspflege des Landes Nordrhein-Westfalen https://www.freiewohlfahrtspflege-nrw.de	DiCV Aachen DiCV Essen DiCV Köln DiCV Münster DiCV Paderborn
Rheinland-Pfalz	LIGA der Freien Wohlfahrtspflege Rheinland-Pfalz e. V. https://www.liga-rlp.de	DiCV Köln DiCV Limburg DiCV Mainz DiCV Speyer DiCV Trier Arbeitsgemeinschaft der Caritasverbände in Rheinland-Pfalz (= Arbeitsgemeinschaft aus den genannten vier DiCVs)
Saarland	LIGA der freien Wohlfahrtspflege Saar https://www.liga-saar.de	Arbeitsgemeinschaft der Diözesan-Caritasverbände im Saarland (besteht aus dem DiCV Trier und dem DiCV Speyer)
Sachsen	Liga der Freien Wohlfahrtspflege in Sachsen https://liga-sachsen.de	DiCV Dresden-Meißen DiCV Görlitz
Sachsen-Anhalt	LIGA der Freien Wohlfahrtspflege im Land Sachsen-Anhalt e.V.: https://www.liga-fw-lsa.de	DiCV Magdeburg
Schleswig-Holstein	Landes-Arbeitsgemeinschaft der freien Wohlfahrtsverbände Schleswig-Holstein e. V. https://www.lag-sh.de	Caritasverband für Schleswig-Holstein (seit 2018 rechtlich nicht selbstständiger Teil von „Caritas im Norden“, i.e. dem DiCV Hamburg)
Thüringen	LIGA der Freien Wohlfahrtspflege in Thüringen e. V. https://liga-thueringen.de	DiCV Erfurt

Anhang 2: Zusammenschlüsse von DiCVs auf Bundeslandebene

Die folgende Tabelle gibt einen Überblick über Zusammenschlüsse von Diözesanverbänden. Personalfachverbände werden hier nicht betrachtet. Wo keine Zusammenschlüsse gelistet sind, bedeutet das nicht, dass die betroffenen Diözesanverbände nicht miteinander zu landespolitischen Anliegen im Austausch stünden. Es kann durchaus informelle Kooperationen zwischen ihnen geben – zu diesen existieren jedoch keine öffentlich zugänglichen Informationen.

Tabelle 7: Zusammenschlüsse von DiCVs auf Bundeslandebene

Bundesland	Caritas-Zusammenschluss	Mitgliedsverbände	Anmerkungen
Baden-Württemberg	/		Die in Baden-Württemberg gelegenen DiCVs **Rottenburg-Stuttgart** und **Freiburg** haben keine formale Arbeitsgemeinschaft auf Landesebene. Es existieren aber gemeinsame, themenspezifische Arbeitskreise und Projekte, z.B. der Caritas-Journalistenpreis: https://www.caritas-rottenburg-stuttgart.de/wer-wir-sind/unsere-partner/caritas-baden-wuerttemberg/caritas-in-baden-wuerttemberg
Bayern	Deutscher Caritasverband Landesverband Bayern e. V., https://www.caritas-bayern.de	DiCV Augsburg DiCV Bamberg DiCV Eichstätt DiCV München/Freising DiCV Passau DiCV Regensburg DiCV Würzburg Sowie diverse Fachverbände.	Der Landesverband Bayern stellt einen Sonderweg unter den Caritas-Zusammenschlüssen dar: Er ist ähnlich strukturiert wie der DCV, ist höchst institutionalisiert und hat ein weitreichenderes Mandat als andere Landeszusammenschlüsse. So vertritt er seine Mitglieder gegenüber der Bayerischen Staatsregierung und verhandelt Verträge und Vereinbarungen mit den Kostenträgern sozialer Leistungen.
Berlin	/		Im Land Berlin ist nur der **DiCV Berlin** tätig.
Brandenburg	/		Die Diözesancaritasverbände **Görlitz** und **Berlin** betreiben neben ihren eigenen Websites eine Website namens „Caritas in Brandenburg“ (https://www.caritas-brandenburg.de/), auf der sich Hilfesuchende über Angebote der Caritas im Bundesland Brandenburg Diözesen-übergreifend informieren können.
Bremen	/		Der größte Teil des Bundeslands Freie Hansestadt Bremen gehört zum Dekanat Bremen

			im Bistum Osnabrück mit dem Caritasverband Bremen e.V., der dem **DiCV Osnabrück** angehört. Der nördliche Teil der Stadt Bremen liegt mit dem Dekanat Bremen Nord im Bistum Hildesheim, wie auch die Stadt Bremerhaven. Für die Caritas in diesen beiden Teilen der Hansestadt ist damit der **DiCV Hildesheim** zuständig.
Hamburg	/		In der Freien und Hansestadt Hamburg ist allein der **DiCV Hamburg** („Caritas im Norden“) tätig.
Hessen	Hessen-Caritas, https://www.hessen-caritas.de/	DiCV Fulda DiCV Limburg DiCV Mainz	Die Hessen-Caritas betreibt sechs fachspezifische Caritas-Landesarbeitsgemeinschaften (CLAG), um die fachpolitischen Interessen der Einrichtungen und Dienste gegenüber u.a. dem Land Hessen, den Sozialleistungsträgern auf Landesebene und der Öffentlichkeit zu vertreten. Der DiCV Limburg und der DiCV Mainz sind gleichzeitig auch in der Arbeitsgemeinschaft der Caritasverbände in Rheinland-Pfalz.
Mecklenburg-Vorpommern	/		Im Bundesland Mecklenburg-Vorpommern sind zwei Diözesancaritasverbände tätig: Im größeren, westlichen Teil, operiert der **DiCV Hamburg** („Caritas im Norden“) mit den Regionen Neubrandenburg, Rostock und Schwerin. Das östliche Drittel gehört zum **DiCV Berlin** mit der „Caritas in Vorpommern“, die in die Regionen Anklam, Bergen, Greifswald, Heringsdorf, Pasewalk und Stralsund unterteilt ist.
Niedersachsen	Caritas in Niedersachsen, https://www.caritas-nds.de	LCV Oldenburg DiCV Osnabrück DiCV Hildesheim	Die Caritas in Niedersachsen bezeichnet sich als die „ständige Vertretung“ der Arbeitsgemeinschaft der Caritasverbände in Niedersachsen. Sie vertritt ihre gemeinsame landespolitischen Interessen. Der Landes-Caritasverband Oldenburg e.V. liegt zwar im Bistum Münster, der Offizialatsbezirk Oldenburg ist jedoch kirchenrechtlich weitestgehend eigenständig. Der LCV Oldenburg wird daher nicht vom DiCV Münster vertreten.
NRW	Caritas NRW, https://www.caritas-nrw.de	DiCV Aachen DiCV Essen DiCV Köln	Die Caritas NRW hat kein Mandat zur gemeinsamen politischen Interessensvertretung, sondern betont auf ihrer Website, dass die

		DiCV Münster DiCV Paderborn	fünf DiCVs rechtlich selbstständige Spitzenverbände sind. Sie kooperieren jedoch in der Caritas NRW bei verschiedenen Projekten und Initiativen, etwa bei der bereits seit 1972 bestehenden Zeitschrift, „Caritas in NRW“, einer Landes-Arbeitsgemeinschaft für Werkstätten für Menschen mit Behinderung oder einer gemeinsamen EU-Fördermittelberatung. Der DiCV Köln ist zugleich Mitglied in der Arbeitsgemeinschaft der Caritasverbände in Rheinland-Pfalz.
Rheinland-Pfalz	Arbeitsgemeinschaft der Caritasverbände in Rheinland-Pfalz, https://www.caritas-rheinland-pfalz.de	DiCV Speyer DiCV Mainz DiCV Trier DiCV Köln DiCV Limburg	Die Arbeitsgemeinschaft hat die gemeinsame politische Interessensvertretung zum Zweck. Dazu betreibt sie einige Caritas-Arbeitsgemeinschaften auf Landesebene, meist unter Einbezug des **Saarlandes**, zu dem Teile der Bistümer Trier und Speyer gehören. DiCV Limburg und DiCV Mainz sind zudem Teil der Hessen Caritas. Der DiCV Köln ist gleichzeitig in der Caritas NRW.
Saarland	Arbeitsgemeinschaft der Diözesancaritasverbände im Saarland, Kein Webauftritt	DiCV Trier DiCV Speyer	In der Arbeitsgemeinschaft der Diözesancaritasverbände im Saarland (AG CV Saar) koordinieren der DiCV Trier und der DiCV Speyer ihre gemeinsamen spitzenverbandlichen, politischen Interessen. Die Arbeitsgemeinschaft hat keinen Webauftritt, wird aber auf den Seiten des DiCV Trier (https://www.caritas-trier.de/ueber-uns/arbeitsgemeinschaften/caritasverbaende-saarland/caritasverbaende-saarland) und der Liga Saar (https://www.liga-saar.de/) erwähnt. Für den Bereich der Kinder- und Jugendhilfe gibt es eine Landesarbeitsgemeinschaft: https://www.caritas-trier.de/ueber-uns/arbeitsgemeinschaften/kinder-jugendhilfe/kiju-sl/kiju-sl. Zudem ist das Saarland in einige AGs der Caritasverbände in Rheinland-Pfalz eingebunden.
Sachsen	/		In Sachsen sind folgende Diözesancaritasverbände tätig, ohne sich formal auf Landesebene zur politischen Interessensvertretung zusammengeschlossen zu haben: **DiCV Dresden-Meißen**, **DiCV Görlitz** und **DiCV Magdeburg**.
Sachsen-Anhalt	/		In Sachsen-Anhalt ist allein der **DiCV Magdeburg** tätig.

Schleswig-Holstein	/		In Schleswig-Holstein ist ausschließlich der **DiCV Hamburg** („Caritas im Norden“) mit der Landesstelle Schleswig-Holstein tätig.
Thüringen	/		Der größte Teil Thüringens gehört zum Bistum Erfurt mit dem **DiCV Erfurt.** Im Osten und Westen des Bundeslandes liegen kleinere Teile in den Bistümern **Dresden-Meißen** und **Fulda**.

Anhang 3: Vorlage Einverständniserklärung für die Interviews

Titel des Projekts: Masterarbeit zu Rahmenbedingungen der IT-Sicherheit in der freien Wohlfahrt am Beispiel der Caritas

Studienleiterin: Katharina Schlotthauer

1. Zweck der Studie:

Dieses Interview wird im Rahmen meiner Masterarbeit im Studiengang „Politics and Technology" an der Hochschule für Politik an der Technischen Universität München durchgeführt. Meine Arbeit soll die Frage beantworten, welche politischen, wirtschaftlichen und organisationalen Rahmenbedingungen die Fähigkeit der freien Wohlfahrt in Deutschland beeinflussen, gegen Cyberangriffe gerüstet zu sein und wie diese Rahmenbedingungen verbessert werden können. Als Fallbeispiel dient die Caritas, also Organisationen, die Mitglied im Deutschen Caritasverband sind.

Bei einigen meiner Fragen werden wir möglicherweise auf sensible Informationen zu sprechen kommen. Bitte denken Sie daran, dass Sie jede Frage unbeantwortet lassen können.

2. Freiwillige Teilnahme:

Ihre Entscheidung, an diesem Interview teilzunehmen, ist freiwillig. Sie können jederzeit aufhören. Sie müssen keine Fragen beantworten, die Sie nicht beantworten möchten.

3. Vertraulichkeit:

Ihre Teilnahme an dieser Untersuchung ist vertraulich. Ihr Name sowie der Name Ihrer Organisation bleiben anonym, d.h. sie werden in der Arbeit nicht genannt. Zudem wird das Transkript des Interviews nicht veröffentlicht, sondern ich werde nur in Ausschnitten daraus zitieren. Die vollständigen Daten liegen neben mir selbst ausschließlich der wissenschaftlichen Betreuerin meiner Masterarbeit sowie der Lehrstuhlinhaberin vor.

4. Förderung und Veröffentlichung:

Diese Masterarbeit wird durch ein Stipendium des Chaos Computer Club Flensburg e. V. gefördert. Der Chaos Computer Club nimmt keinerlei Einfluss auf den Inhalt der Arbeit. Voraussetzung für die Förderung ist die Zugänglichkeit der Arbeit nach Fertigstellung. Entsprechend wir die Arbeit auf den Seiten des CCC Flensburg und der Hochschule für Politik frei verfügbar sein.

5. Dauer/Zeit:

Das Gespräch wird etwa 2 Stunden dauern. Sie werden die Fragen mündlich beantworten und Ihre Antworten werden aufgezeichnet.

6. Technische Durchführung, Aufzeichnung und Transkription des Gesprächs:

Das Gespräch wird über TUM-Conf stattfinden und aufgezeichnet werden, einer Videokonferenzplattform der Technischen Universität München, die auf Zoom basiert. Außerdem wird das Interview mit dem Transkriptionsprogramm f4 transkribiert werden. Der Anbieter nutzt DIN-ISO/IEC-27001-zertifizierte Server in Deutschland und arbeitet gemäß der Europäischen Datenschutzverordnung (DSGVO). Die Aufzeichnung des Interviews wird nach der Transkription dauerhaft gelöscht. Wenn Sie möchten, dass ich die Daten, die Sie mir mitgeteilt haben, lösche, können Sie mir eine E-Mail an katharina.schlotthauer@tum.de senden.

Hier finden Sie Näheres zum Datenschutz der genannten Dienste:

- Datenschutz TUM-Conf/Zoom
- Datenschutz f4

7. Daten und Rechte: Personenbezogene Daten werden gemäß der Europäischen Datenschutzverordnung (DSGVO) verarbeitet (siehe: https://dsgvo-gesetz.de).

8. Das Recht, Fragen zu stellen:

Bitte wenden Sie sich an mich (katharina.schlotthauer@tum.de), wenn Sie Fragen, Beschwerden oder Bedenken zu dieser Studienarbeit haben.

_____	_____
Unterschrift des/der Teilnehmenden	Datum
_____	_____
Unterschrift der Durchführerin	Datum

Anhang 4: Interviewleitfaden für rein operative Träger

Tabelle 8: Interviewleitfaden für operative Träger

Interviewabschnitt	Themenkomplex	Forschungsfrage	Analysedimension	Wissensart	Frage	Anmerkungen für die Vorbereitung
Eröffnung - Einwilligungserklärung					**Thema der Arbeit:** Rahmenbedingungen für IT-Sicherheit in der freien Wohlfahrt am Beispiel der Caritas **Bedeutung der konkreten Befragung:** Begründung, warum genau diese Organisation und diese:r Expert:in befragt wird (*individuell*) **Veröffentlichung:** Diese Arbeit wird durch ein Stipendium des Chaos Computer Clubs Flensburg gefördert und daher auf deren Website veröffentlicht. Inhaltlich nimmt der CCC keinen Einfluss auf die Arbeit. Die Arbeit wird außerdem auf den Seiten der TUM veröffentlicht **Anonymisierung:** Name und Organisation des Interviewpartners der Interviewpartnerin werden nicht veröffentlich und lediglich der Betreuerin und der Lehrstuhlinhaberin vorgelegt. Auch das Transkript des Interviews wird nicht veröffentlicht sondern es wird nur in Ausschnitten daraus zitiert. **Vertraulichkeit:** Auch wenn ich für den Caritas-Netzwerk IT e. V. arbeite und der Kontakt zu Ihnen über den Verein zustande gekommen ist, bin ich hier als neutrale Forscherin. Alles, was Sie mir erzählen bleibt selbstverständlich unter uns und werde ich nicht an den Vorstand des Vereins, die Mitarbeitenden oder andere Mitglieder weitergeben. **Aufzeichnung:** Das Interview wird per Zoom/Diktiergerät aufgezeichnet. Die Aufzeichnung dient lediglich der Transkription des Interviews und wird nicht veröffentlicht. **Widerruf:** Sie haben auch nach dem Interview jederzeit die Möglichkeit, Ihre Einwilligung zur Teilnahme an dieser Forschungsarbeit zu widerrufen. **Einwilligung:** Haben Sie hierzu noch Fragen? Sind Sie mit diesen Rahmenbedingungen einverstanden und möchten Sie mit dem Interview fortfahren? Dann werde ich nun die Aufzeichnung starten.	

Eröffnung - Daten zur Organisation					**Größe:** Zunächst möchte ich gerne sicherstellen, dass die Informationen, die ich über Ihre Organisation habe, korrekt sind. Laut XXX haben Sie etwa XXX Mitarbeitende. Ist das in etwa noch aktuell? **Arbeitsfelder:** Sie sind in XXX *(Altenhilfe, Eingliederungshilfe, Soziale Dienste, etc.)* tätig - stimmt das so oder fehlt hier ein Arbeitsfeld? **Betroffenheit**: War Ihre Organisation schon einmal Opfer einer Cyberattacke? Wenn ja, können Sie bitte beschreiben, was passiert ist?	*Betroffenheit nur abfragen, sofern kein Angriff öffentlich gemacht wurde.*
Eröffnung - Vorstellung des Experten / der Expertin					Könnten Sie mir bitte kurz etwas zu Ihrem Werdegang und Ihren Aufgaben in Ihrer Organisation erzählen? Das wird nicht in die Auswertung des Interviews einfließen, hilft mir aber, Ihre Ausführungen besser einzuordnen.	
Hauptteil - Definition					Der Einfachheit und Einheitlichkeit halber spreche ich meistens von IT-Sicherheit. Ich differenziere dabei allerdings nicht zwischen IT-Sicherheit und Cybersicherheit bzw. Cybersecurity. Bitte beschreiben Sie kurz, was Sie unter IT-Sicherheit verstehen. Ich möchte sicherstellen, dass wir nicht aneinander vorbeireden.	

Hauptteil - Eröffnungs-statement		2)	/	Betriebs- und Kontextwissen	Sie haben sicher mitbekommen, dass in den vergangenen Jahren Caritasorganisationen Opfer von Cyberattacken geworden sind, zum Beispiel der DiCV München und der Caritasverband Eifel 2022 oder der Caritasverband Rhein-Erft-Kreis 2023. / Sie haben ja leider am eigenen Leib erfahren müssen, dass auch Organisationen der freien Wohlfahrt Opfer von Cyberattacken werden können. Gleichzeitig ist IT-Sicherheit ein komplexes Thema, gerade für Organisationen der freien Wohlfahrt. Was sind Ihrer Meinung nach die größten Herausforderungen für eine Caritas-Organisation, um IT-Sicherheit in einer Caritas-Organisation herzustellen?	*Beispiele so wählen, dass der/die Befragte sie kennen kann, also z.B. nach örtlicher Nähe.* *Gesprächspartner soll die Möglichkeit haben, ein längeres Statement zu geben ---> leichterer Einstieg in die Interviewsituation; Sehr offene Frage, die Facetten produzieren soll, die die Literatur / die die Forscherin noch nicht erfasst hat; Informationen aus dem Eröffnungsstatement bieten Anknüpfungspunkte für spätere Fragen*
Hauptteil - Fragen	Awareness	Spezifizierung zu 1) und 2)	Intern: Aufmerksamkeit von Vorständen	Betriebswissen	Welche Rolle spielt IT-Sicherheit für Sie in Ihrer Rolle als Vorstand, auch im Vergleich zu anderen Themen?	
Hauptteil - Fragen	Awareness	Spezifizierung zu 1) und 2)	Intern: Aufmerksamkeit von Vorständen	Betriebswissen	Sie stehen auf lokaler Ebene und über verschiedene Gremien im Austausch mit Vorständen anderer Einrichtungsträger. Ihrer Einschätzung nach, welche Aufmerksamkeit schenken diese dem Thema IT-Sicherheit?	
Hauptteil - Fragen	Awareness	Spezifizierung zu 1) und 2)	Extern: Aufmerksamkeit von Verbänden	Betriebswissen	Spitzenverbandlich werden Sie von XXX, XXX und XXX vertreten und überverbandlich kooperieren Sie mit XXX. Habe ich das richtig im Kopf oder habe ich jemanden vergessen? Welche Rolle spielt IT-Sicherheit als Thema für die Spitzenverbände, mit denen Sie zusammenarbeiten?	*Im Vorhinein zusammenschreiben, wer die entsprechenden Spitzenverbände und Ligen auf lokaler, Diözesan-, Landes- und Bundesebene sind*

Hauptteil - Fragen	Awareness	Spezifizierung zu 1) und 2)	Intern: Aufmerksamkeit von Vorständen	Betriebswissen	Ihre Organisation ist selbst als Spitzenverband für andere Organisationen tätig. Welche Rolle spielt das Thema IT-Sicherheit in Ihrer Arbeit für Ihre Mitglieder? Welche Anfragen erreichen Sie in Bezug auf das Thema von Ihren Mitgliedern?	*Nur für spitzenverbandlich tätige Organisationen*
Hauptteil - Fragen	Awareness	Spezifizierung zu 1) und 2)	Intern: Aufmerksamkeit / Fähigkeiten von Mitarbeitenden	Betriebswissen	Welche spezifischen Herausforderungen haben Ihrer Meinung nach die Mitarbeitenden in sozialen Organisationen bezogen auf IT-Sicherheit? Wie begegnen Sie den Herausforderungen?	
Hauptteil - Fragen	Politik	3) und 4)	Extern: politische Interessensvertretung	Betriebswissen	Wer ist außerhalb Ihrer eigenen Organisation für politische Interessensvertretung bzgl. IT-Sicherheit zuständig oder wer sollte Ihrer Meinung nach dafür zuständig sein?	
Hauptteil - Fragen	Politik	3) und 4)	Extern: politische Interessensvertretung und politische Aufmerksamkeit	Kontext- und Betriebswissen	Welche politischen Stellen/Akteure müssen erreicht werden, um die Rahmenbedingungen für IT-Sicherheit in der Sozialwirtschaft zu verbessern?	
Hauptteil - Fragen	Politik	3) und 4)	Extern: politische Aufmerksamkeit	Betriebswissen	Wie kann man die relevanten Stellen/Akteure erreichen?	
Hauptteil - Fragen	Politik	4)	Extern: politische Aufmerksamkeit	Betriebswissen	Welche Wünsche bzw. Forderungen haben Sie an diese Stellen und Akteure? Welche Maßnahmen seitens des Gesetzgebers wären Ihrer Meinung nach sinnvoll?	

Hauptteil - Fragen	Politik	2)	Extern: politische Aufmerk-samkeit	Kontext- und Betriebswis-sen	Welchen Einfluss hat ihrer Meinung nach die EU-Ebene auf die Rahmenbedin-gungen für IT-Sicherheit in der freien Wohlfahrt in Deutschland?	
		Spezifizierung zu 2)	Intern: Aufmerk-samkeit von Vorständen	Betriebswis-sen	Inwieweit kennen Sie sich mit der aktuellen Gesetzeslage zu IT-Sicherheit aus?	
Hauptteil - Fragen	Politik	4)	Extern: politische Aufmerk-samkeit	Betriebswis-sen	Was würden Sie an der Gesetzeslage ändern, um die IT-Sicherheit in der freien Wohlfahrt zu verbessern?	
Hauptteil - Fragen	Finanzierung	Spezifizierung zu 1) und 2)	Extern: IT-Refinanzie-rung	Betriebswis-sen	Ein Großteil der Finanzmittel für soziale Dienstleistungen kommt ja über Leis-tungsentgelte und Pflegesätze. Welche Rolle spielen IT-Kosten im Allgemeinen und IT-Sicherheitskosten bei diesen Verhandlungen?	
Hauptteil - Fragen	Finanzierung	Spezifizierung zu 1) und 2)	Extern: IT-Refinanzie-rung	Betriebswis-sen	Wie schätzen Sie das Bewusstsein der Kostenträger für die Relevanz und die Kosten von IT-Sicherheitsmaßnahmen ein?	
Hauptteil - Fragen	Finanzierung	3)	Extern: IT-Refinanzie-rung	Betriebswis-sen	Versuchen Sie, IT-Sicherheit in die Entgelte mitreinzuverhandeln? Welche Argumente bringen Sie an? Mit welchen Argumenten begegnen Ihnen die Kostenträger?	
Hauptteil - Fragen	Finanzierung	4)	Extern: IT-Refinanzie-rung	Betriebswis-sen	Was wünschen Sie sich? Wie würden Sie das Finanzierungsmodell ändern?	
Hauptteil - Fragen	Fachkräfte	3) und 4)	Intern und Extern: Fachkräfte-mangel	Betriebswis-sen	Spüren Sie den IT-Fachkräftemangel in Ihrer Organisation? Welche Auswirkun-gen hat er?	
Hauptteil - Fragen	Fachkräfte	3) und 4)	Intern und Extern: Fachkräfte-mangel	Betriebswis-sen	Was tun sie dagegen? Was wünschen Sie sich von Spitzenverbänden und Politik?	

Abschluss					Wir sind mit unserer Zeit fast am Ende und auch ich habe mir keine weiteren Fragen mehr aufgeschrieben. Gibt es etwas, das Ihnen zu diesem Thema noch wichtig ist?	
Abschluss					Herzlichen Dank für Ihre Zeit und die wertvollen Einblicke. Wenn Ihnen im Nachhinein noch Rückfragen an mich einfallen, können Sie mich jederzeit kontaktieren. Wenn Sie möchten, schicke ich Ihnen außerdem nach Fertigstellung meiner Arbeit ein Exemplar als Pdf zu.	

Anhang 5: Interviewleitfaden für Spitzenverbände

Tabelle 9: Interviewleitfaden für Spitzenverbände

Interviewabschnitt	Themenkomplex	Forschungsfrage	Analysedimension	Wissensart	Frage	Anmerkungen für die Vorbereitung
Eröffnung - Einwilligungserklärung					**Thema der Arbeit:** Rahmenbedingungen für IT-Sicherheit in der freien Wohlfahrt am Beispiel der Caritas **Bedeutung der konkreten Befragung:** Begründung, warum genau diese Organisation und diese:r Expert:in befragt wird (*individuell*) **Veröffentlichung:** Diese Arbeit wird durch ein Stipendium des Chaos Computer Clubs Flensburg gefördert und daher auf deren Website veröffentlicht. Inhaltlich nimmt der CCC keinen Einfluss auf die Arbeit. Die Arbeit wird außerdem auf den Seiten der TUM veröffentlicht **Anonymisierung:** Name und Organisation des Interviewpartners der Interviewpartnerin werden nicht veröffentlich und lediglich der Betreuerin und der Lehrstuhlinhaberin vorgelegt. Auch das Transkript des Interviews wird nicht veröffentlicht sondern es wird nur in Ausschnitten daraus zitiert. **Vertraulichkeit:** Auch wenn ich für den Caritas-Netzwerk IT e. V. arbeite und der Kontakt zu Ihnen über den Verein zustande gekommen ist, bin ich hier als neutrale Forscherin. Alles, was Sie mir erzählen bleibt selbstverständlich unter uns und werde ich nicht an den Vorstand des Vereins, die Mitarbeitenden oder andere Mitglieder weitergeben. **Aufzeichnung:** Das Interview wird per Zoom aufgezeichnet. Die Aufzeichnung dient lediglich der Transkription des Interviews und wird nicht veröffentlicht. **Widerruf:** Sie haben auch nach dem Interview jederzeit die Möglichkeit, Ihre Einwilligung zur Teilnahme an dieser Forschungsarbeit zu widerrufen. **Einwilligung:** Haben Sie hierzu noch Fragen? Sind Sie mit diesen Rahmenbedingungen einverstanden und möchten Sie mit dem Interview fortfahren? Dann werde ich nun die Aufzeichnung starten.	

Eröffnung - Daten zur Organisation					**Größe:** Zunächst möchte ich gerne sicherstellen, dass die Informationen, die ich über Ihre Organisation habe, korrekt sind. Laut XXX vertreten Sie XXX Organisationen und damit XXX Mitarbeitende. Sie selbst haben etwa XXX Mitarbeitende. Ist das in etwa noch aktuell? **Betroffenheit**: War Ihre Organisation oder eines Ihrer Mitglieder schon einmal Opfer einer Cyberattacke? Wenn ja, können Sie bitte beschreiben, was passiert ist? Inwiefern hat ein Angriff auf eines Ihrer Mitglieder Sie betroffen?	*Betroffenheit nur abfragen, sofern kein Angriff öffentlich gemacht wurde.*
Eröffnung - Vorstellung des Experten / der Expertin					Könnten Sie mir bitte kurz etwas zu Ihrem Werdegang und Ihren Aufgaben in Ihrer Organisation erzählen? Das wird nicht in die Auswertung des Interviews einfließen, hilft mir aber, Ihre Ausführungen besser einzuordnen.	
Hauptteil - Definition					Der Einfachheit und Einheitlichkeit halber spreche ich meistens von IT-Sicherheit. Ich differenziere dabei allerdings nicht zwischen IT-Sicherheit und Cybersicherheit bzw. Cybersecurity. Bitte beschreiben Sie kurz, was Sie unter IT-Sicherheit verstehen. Ich möchte sicherstellen, dass wir nicht aneinander vorbeireden.	

Hauptteil - Eröffnungs-statement		2)	/	Betriebs- und Kontextwissen	Sie haben sicher mitbekommen, dass in den vergangenen Jahren Caritasorganisationen Opfer von Cyberattacken geworden sind, zum Beispiel der DiCV München und der Caritasverband Eifel 2022 oder der Caritasverband Rhein-Erft-Kreis 2023. / Sie haben ja leider am eigenen Leib erfahren müssen, dass auch Organisationen der freien Wohlfahrt Opfer von Cyberattacken werden können. Gleichzeitig ist IT-Sicherheit ein komplexes Thema, gerade für Organisationen der freien Wohlfahrt. Was sind Ihrer Meinung nach die größten Herausforderungen für eine Caritas-Organisation, um IT-Sicherheit in einer Caritas-Organisation herzustellen?	*Beispiele so wählen, dass der/die Befragte sie kennen kann, also z.B. nach örtlicher Nähe.* *Gesprächspartner soll die Möglichkeit haben, ein längeres Statement zu geben ---> leichterer Einstieg in die Interviewsituation; Sehr offene Frage, die Facetten produzieren soll, die die Literatur / die die Forscherin noch nicht erfasst hat; Informationen aus dem Eröffnungsstatement bieten Anknüpfungspunkte für spätere Fragen*
Hauptteil - Fragen	Awareness	Spezifizierung zu 1) und 2)	Intern: Aufmerksamkeit von Vorständen und Verbänden	Betriebswissen	Welche Rolle spielt IT-Sicherheit für Sie in Ihrer Rolle als Vorstand/Geschäftsführers/Mitarbeiter eines Spitzenverbandes, auch im Vergleich zu anderen Themen? Sehen Sie IT-Sicherheit als eine spitzenverbandliche Aufgabe gegenüber Ihren Mitgliedern?	
Hauptteil - Fragen	Awareness	Spezifizierung zu 1) und 2)	Intern: Aufmerksamkeit von Vorständen	Betriebswissen	Ihrer Einschätzung nach, welche Aufmerksamkeit schenken Ihre Mitglieder dem Thema IT-Sicherheit? Welche Anfragen erreichen Sie in Bezug auf das Thema von Ihren Mitgliedern?	

Hauptteil - Fragen	Awareness	Spezifizierung zu 1) und 2)	Extern: Aufmerksamkeit von Verbänden	Betriebswissen	Spitzenverbandlich werden Sie selbst von XXX, XXX und XXX vertreten und überverbandlich kooperieren Sie mit XXX. Habe ich das richtig im Kopf oder habe ich jemanden vergessen? Welche Rolle spielt IT-Sicherheit als Thema für die Spitzenverbände, mit denen Sie zusammenarbeiten?	*Im Vorhinein zusammenschreiben, wer die entsprechenden Spitzenverbände und Ligen auf lokaler, Diözesan-, Landes- und Bundesebene sind*
Hauptteil - Fragen	Awareness	Spezifizierung zu 1) und 2)	Intern: Aufmerksamkeit / Fähigkeiten von Mitarbeitenden	Betriebswissen	Welche spezifischen Herausforderungen haben Ihrer Meinung nach die Mitarbeitenden in sozialen Organisationen bezogen auf IT-Sicherheit? Wie begegnen Sie den Herausforderungen?	
Hauptteil - Fragen	Politik	3) und 4)	Extern: politische Interessensvertretung	Betriebswissen	Wer ist außerhalb Ihrer eigenen Organisation für politische Interessensvertretung bzgl. IT-Sicherheit zuständig oder wer sollte Ihrer Meinung nach dafür zuständig sein?	
Hauptteil - Fragen	Politik	3) und 4)	Extern: politische Interessensvertretung und politische Aufmerksamkeit	Kontext- und Betriebswissen	Welche politischen Stellen/Akteure müssen erreicht werden, um die Rahmenbedingungen für IT-Sicherheit in der Sozialwirtschaft zu verbessern?	
Hauptteil - Fragen	Politik	3) und 4)	Extern: politische Aufmerksamkeit	Betriebswissen	Wie kann man die relevanten Stellen/Akteure erreichen?	
Hauptteil - Fragen	Politik	4)	Extern: politische Aufmerksamkeit	Betriebswissen	Welche Wünsche bzw. Forderungen haben Sie an diese Stellen und Akteure? Welche Maßnahmen seitens des Gesetzgebers wären Ihrer Meinung nach sinnvoll?	

Hauptteil - Fragen	Politik	(2)	Extern: politische Autorenkategorie	Kontext- und Betriebswissen	Welchen Einfluss hat Ihrer Meinung nach die EU-Ebene auf die Rahmenbedingungen für IT-Sicherheit in der freien Wirtschaft in Deutschland?
Hauptteil - Fragen		Spezialisierung (2)	Intern: Autorenkategorie von sämtlich Verständen	Betriebswissen	Inwieweit kennen Sie sich mit der aktuellen Gesetzeslage zu IT-Sicherheit aus?
Hauptteil - Fragen		Spezialisierung zu 1) und 2)	Extern: politische Autorenkategorie sämtlich	Betriebswissen	Was würden Sie an der Gesetzeslage ändern, um die IT-Sicherheit in der freien Wirtschaft zu verbessern?
Hauptteil - Fragen	Finanzierung	Spezialisierung zu 1) und 2)	Extern: IT-Reifenanzierung	Betriebswissen	Ein Großteil der Finanzmittel für soziale Dienstleistungen kommt ja über Leistungsempfänger und Pflegesätze. Welche Rolle spielen IT-Kosten im Allgemeinen und IT-Sicherheitskosten bei diesen Verhandlungen?
Hauptteil - Fragen	Finanzierung	Spezialisierung zu 1) und 2)	Extern: IT-Reifenanzierung	Betriebswissen	Wie schätzen Sie das Bewusstsein der Kostenträger für die Relevanz und die Kosten von IT-Sicherheitsmaßnahmen ein?
Hauptteil - Fragen	Finanzierung	(3)	Extern: IT-Reifenanzierung	Betriebswissen	Verraschen Sie, IT-Sicherheit in die Entgelte mitreinzuverhandeln? Welche Argumente bringen Sie an? Mit welchen Argumenten begegnen Ihnen die Kostenträger?
Hauptteil - Fragen	Finanzierung	(4)	Extern: IT-Reifenanzierung	Betriebswissen	Was wünschen Sie sich? Wie würden Sie das Finanzierungsmodell ändern?
Hauptteil - Fragen	Technikäfte	3) und 4)	Intern und Extern: Fachkräfte-Mangel	Betriebswissen	Spüren Sie den IT-Fachkräftemangel in Ihrer eigenen Organisation und bei Ihren Mitgliedern? Welche Auswirkungen hat er? Was tun sie dagegen? Was wünschen Sie sich von der Politik?

Abschluss					Wir sind mit unserer Zeit fast am Ende und auch ich habe mir keine weiteren Fragen mehr aufgeschrieben. Gibt es etwas, das Ihnen zu diesem Thema noch wichtig ist?	
Abschluss					Herzlichen Dank für Ihre Zeit und die wertvollen Einblicke. Wenn Ihnen im Nachhinein noch Rückfragen an mich einfallen, können Sie mich jederzeit kontaktieren. Wenn Sie möchten, schicke ich Ihnen außerdem nach Fertigstellung meiner Arbeit ein Exemplar als Pdf zu.	

Anhang 6: Vorlage für die Protokollierung der Interviewsituation

		Erläuterungen
Ort	Zoom	
Datum, Uhrzeit		
Dauer		
Vertraulichkeit zugesichert?		
Auf Möglichkeit zum Widerruf hingewiesen?		
Biografischer Hintergrund		
Interviewsituation und Gesprächsatmosphäre		- Offenes Fachgespräch oder Frage-/Antwort-Modus? - Interaktionseffekte? (Eisberg, Paternalismus, Rückkopplung, Katharsis) - Allgemeine Atmosphäre? - Störfaktoren?
Hinweise auf weitere potenzielle Gesprächspartner:innen		
Fakten, die noch recherchiert werden müssen		
Besonders ertragreiche und besonders unergiebige Themenkomplexe		
Sonstiges		

(Übernommen aus: Mayring 2020, 103, Abb. 3.6)

Anhang 7: Regeln der deduktiven Kategorienbildung nach Philipp Mayring

D1	Fragestellung
D1.1	Formuliere eine klare Fragestellung, nicht nur ein Thema!
D1.2	Verknüpfe mit dem Stand der Forschung und formuliere die eigene theoretische Position!
D1.3	Lege das Textmaterial begründet fest!
D2	Kategoriensystemerstellung
D2.1	Leite aus der Fragestellung die Auswertungsaspekte ab und formuliere sie in Kategorien!
D2.2	Das Kategoriensystem kann Haupt- und Unterkategorien enthalten.
D2.3	Das Kategoriensystem kann nominal (einfache Kategorienliste) oder ordinal (Ordinalskala, z.B. positiv - neutral - negativ) konzipiert sein.
D3	Kodierleitfaden
D3.1	Formuliere vorab theoriegeleitet klare Definitionen zu allen Kategorien!
D3.2	Sammle während der Textarbeit exemplarische Textstellen als Ankerbeispiele für die Kategorien!
D3.3	Bei unklaren Textstellen formuliere theoriegeleitet Entscheidungsregeln für die Kategorisierung (Kodierregeln)!
D3.4	Stelle Definitionen, Ankerbeispiele und Kodierregeln zu einem Kodierleitfaden
D4	Überarbeitungsschleife
D4.1	Wenn sich die Kategorienzuordnung stabilisiert (wenig Abgrenzungsprobleme), unterziehe die Kategorien und den Kodierleitfaden einer Revision!
D5	Auswertung
D5.1	Die Zuordnung der deduktiv gebildeten Kategorien zum Textmaterial kann bereits das Ergebnis darstellen. Häufigkeiten der Kategorienzuordnung können aber auch quantitativ analysiert werden.

(Übernommen aus: Mayring 2022, 98)

Anhang 8: Regeln der Zusammenfassung nach Philipp Mayring

Z1	Paraphrasierung	
Z1.1	Streiche alle nicht (oder wenig) inhaltstragenden Textbestandteile wie ausschmückende, wiederholende, verdeutlichende Wendungen!	
Z1.2	Übersetze die inhaltstragenden Textstellen auf eine einheitliche Sprachebene!	
Z1.3	Transformiere sie auf eine grammatikalische Kurzform!	
Z2	Generalisierung auf das Abstraktionsniveau	
Z2.1	Generalisiere die Gegenstände der Paraphrasen auf die definierte Abstraktionsebene, sodass die alten Gegenstände in den neu formulierten impliziert sind!	
Z2.2	Generalisiere die Satzaussagen (Prädikate) auf die gleiche Weise!	
Z2.3	Belasse die Paraphrasen, die über dem angestrebten Abstraktionsniveau liegen!	
Z2.4	Nimm theoretische Vorannahmen bei Zweifelsfällen zu Hilfe!	
Z3	Erste Reduktion	In dieser Arbeit ein großer Schritt aufgrund der Materialmenge
Z3.1	Streiche bedeutungsgleiche Paraphrasen innerhalb der Auswertungseinheiten!	
Z3.2	Streiche Paraphrasen, die auf dem neuen Abstraktionsniveau nicht als wesentlich inhaltstragend erachtet werden!	
Z3.3	Übernehme die Paraphrasen, die weiterhin als zentral inhaltstragend erachtet werden (Selektion)!	
Z3.4	Nimm theoretische Vorannahmen bei Zweifelsfällen zu Hilfe!	
Z4	Zweite Reduktion	
Z4.1	Fasse Paraphrasen mit gleichem (ähnlichem) Gegenstand und ähnlicher Aussage zu einer Paraphrase (Bündelung) zusammen!	
Z4.2	Fasse Paraphrasen mit mehreren Aussagen zu einem Gegenstand zusammen (Konstruktion/Integration)!	
Z4.3	Fasse Paraphrasen mit gleichem (ähnlichem) Gegenstand und verschiedener Aussage zu einer Paraphrase zusammen (Konstruktion/Integration)!	
Z4.4	Nimm theoretische Vorannahmen bei Zweifelsfällen zu Hilfe!	

(Übernommen aus: Mayring 2022, 71)

Anhang 9: Kodierleitfaden

Code	Kodieranweisungen
1. IT-Betrieb	**Erklärung:** Textstellen, die sich damit befassen, wie der IT-Betrieb von Organisationen der freien Wohlfahrt aufgebaut und ausgestattet ist. **Art:** Deduktiv
1.1 IT-Infrastruktur, -Ausstattung, -Organisation	**Erklärung:** Textteile, die beschreiben, wie die IT von Caritas-Organisationen ausgestattet und organisiert sind und wie ihr Digitalisierungsgrad ist. **Ankerbeispiel:** „Die sind aber noch dabei – zum Teil in unterschiedlicher Geschwindigkeit – ihre IT Systeme auf das Jahr 2015 zu modernisieren." **Art:** Deduktiv
1.2 IT-Fachkräfte	**Erklärung:** Textstellen, in denen es um IT-Fachkräfte in der freien Wohlfahrt geht. **Ankerbeispiel:** „Also es ist ganz grundsätzlich für uns extrem schwierig, wirklich gute Leute zu finden. Zum einen, weil es da einfach wenig Leute gibt und zum anderen, weil wir natürlich mit einer Boombranche konkurrieren, wo Arbeitgeber Tagessätze aufrufen, die wir auf gar keinen Fall haben. Ich habe die Refinanzierungsproblematik angesprochen; diese Fachkräfte sind einfach unfassbar teuer, die kosten echt Geld und das ist über die AVR, unseren Tarifvertrag, nicht abzubilden. Insofern haben wir diese Leute bei uns einfach nicht in dem Maße, wie wir sie bräuchten im Regelbetrieb." **Art:** Deduktiv
1.3 Outsourcing	**Erklärung:** Textstellen, die Auslagerung von IT-Dienstleistungen thematisieren. **Ankerbeispiel:** „Aber es gibt auch kleine Träger, die sich anderen IT-Unternehmen anschließen und auch da ist natürlich schon mal deutlich mehr Know-how da, weil logischerweise dadurch, dass sie mehr bedienen, mehr Wissen, mehr Know-how da ist, oft Spezialisten auch innerhalb des Bereiches oder innerhalb der Dienstleistung da sind." **Art:** Induktiv
1.4 Technische Cybersecurity-Maßnahmen	**Erklärung:** Textstellen, in denen es um technische Maßnahmen zur Herstellung von Cybersicherheit geht. **Ankerbeispiel:** „Also das war zum Beispiel ein Thema, ein Learning hinten dran nach unserem Hackerangriff, dass wir eine standardisierte Passwortrichtlinie nach BSI-Standard eingeführt haben, was sozusagen schon circa 50 % des Hackerangriffs vermieden hätte bei uns." **Art:** Induktiv
1.5 IT-Betrieb Sonstiges	
2. Awareness/Skills Mitarbeitende	**Erklärung:** Textstellen, die Fähigkeiten und Awareness von Mitarbeitenden bzgl. IT-Sicherheit thematisieren. **Art:** Deduktiv
2.1 Mitarbeitende als Risiko	**Erklärung:** Textstellen, die besonders herausstreichen, wie wichtig Mitarbeiter-Awareness für IT-Sicherheit ist und/oder Mitarbeitende als Risiko für IT-Sicherheit bezeichnen. **Ankerbeispiel:** „Der Nutzer ist die größte Herausforderung. Da bin ich sehr eindeutig. Also sozusagen jeder, der ein IT-Endgerät in der Hand hat und im Einsatz hat, ist stark anfällig aufgrund seines Nutzerverhaltens und seiner Gewohnheiten, seiner Arbeitsweisen, usw."

	Art: Induktiv
2.2 Arbeit mit besonders sensiblen Daten	**Erklärung:** Textstellen, die betonen, dass Mitarbeitende der freien Wohlfahrt besonders achtsam bei IT-Sicherheit sein müssen, weil sie mit besonders sensiblen Daten arbeiten. **Ankerbeispiel:** „Na gut, es gibt vielleicht diesen Teil der datenschutzkonformen Beratung von Klienten, der anders ist. Das hilft mir aber eher. Habe ich sozusagen ein technologisches Angebot, wo das über meine Applikation in einer gesicherten Umgebung möglich ist? Das ist natürlich aber zugleich auch wiederum eine Angriffsfläche, wenn die Klientendaten elektronisch dokumentiert werden, abrufbar sind usw." **Art:** Deduktiv
2.3 Gründe für geringe Awareness/Skills	
2.3.1 wenig IT-affin wegen Berufsfeld	**Erklärung:** Textstellen, die beinhalten, dass Mitarbeitende sich mit Menschen beschäftigen wollen, nicht mit IT(-Sicherheit). **Ankerbeispiel:** „Na, ich denke, dass wir ja hauptsächlich mit Sozialpädagogen und Mitarbeitern in der Pflege zu tun haben, die einfach von ihrem Berufsbild und von ihrem Wirkenwollen und Tätigseinwollen nicht IT-Sicherheit als Erstes auf dem Schirm haben." **Art:** Induktiv
2.3.2 wenig IT-affin wegen Alter	**Erklärung:** Textstellen, die das Alter von Mitarbeitenden als Grund für geringe IT(-Sicherheits)-Literacy benennen. **Ankerbeispiel:** „Das andere ist, dass wir Mitarbeiter und Mitarbeiterinnen aller Altersgruppen, aller Bildungsstände haben und die mit diesem Thema zu befassen, damit sie auch sicher damit umgehen können und fehlerfrei damit umgehen können und auch für sich sicher. Also die haben auch sehr viel Angst: 'Ich habe das Internet gelöscht'. Das ist nicht immer nur eine Altersfrage, aber sicherlich, wenn Sie eine Pflegekraft haben mit 60, die ist top, aber wenn die dann mit dem iPad da rumlaufen muss, das ist dann schon eine große Herausforderung." **Art:** Induktiv
2.4 IT-Sicherheits-Schulungen	
2.4.1 Ausgestaltung Schulungsangebote	
2.4.1.1 Schulungsangebote Diverses	**Erklärung:** Textabschnitte, die darauf eingehen, welche Inhalte und Formate Schulungen zu IT-Sicherheit haben oder haben sollten. **Ankerbeispiel:** „Dazu kommt, dass natürlich die Schulungsinhalte für die Mitarbeitenden, dass da IT-Security, Digitalisierung und auch – ich mag das Wort Mindset nicht –, aber, dass da so eine gewisse Kultur des ‚Lasst-uns-mal-überlegen,-wie-man-das-anders-machen-kann', ‚Lasst-mal-schauen,-wie-man-das-besser-machen-kann', und tatsächlich schon auch sowas wie eine Digital Literacy - das ist ja immer da das Schlagwort -, dass man die Leute befähigt, auch selbst einzuschätzen: ‚Was ist denn das jetzt'? Also wenn ich eine E-Mail kriege, auch wenn die noch so vertrauenswürdig aussieht, aber ich gehe mit der Maus drüber und ich sehe, das geht auf irgendeinen Server in Afrika, dann weiß ich, ich klicke auf diesen Link auf gar keinen Fall drauf. Aber ich würde mal mutmaßen, wenn ein Viertel der Leute diese Funktion überhaupt kennt, dann ist das viel. Und das hat natürlich Implikationen." **Art:** Induktiv
2.4.1.2 Kontinuierlichkeit	**Erklärung:** Textstellen, in denen darauf hingewiesen wird, dass IT-Sicherheitsawareness immer wieder und regelmäßig geschult werden muss. **Ankerbeispiel:** „Na, ich denke, das ist die jahrelange Sensibilisierung. Ich denke, dass

	wir auch als wir gestartet haben, da schon viel Augenleiern auch von unseren Mitarbeitern hatten und auch von den leitenden Mitarbeitern. Aber mittlerweile ist es eben … alles braucht ja eine Gewohnheit. Wenn ich, ich sage mal, wenn ich meine Essgewohnheiten verändern will, brauche ich dafür ja auch eine lange Zeit, um das einzuüben. Und genauso ist es mit diesen Themen auch. Wir üben das schon eine ganz Zeit ein, sodass es eben doch bei allen präsent ist und bei allen Entscheidungen auch immer mitschwingt. Ich glaube, wir brauchen keine Checkliste mehr, wo wir es abhaken müssen, weil es ist einfach dabei." **Art:** Induktiv
2.4.1.3 Digitale Angebote	**Erklärung:** Textstellen, in denen digitale Schulungsangebote zu Cyber Security Awareness thematisiert werden. **Ankerbeispiel:** „Aktuell sind wir im Austausch. Der DiCV bietet eine digitale Datenschutzschulung an. Ob wir uns dort mit andocken können, also ob wir da Kontingente kaufen, das würde ich sozusagen gern mal ausprobieren, ob diese Onlineschulung genauso hilfreich ist wie dieses Eins-zu-Eins im Gegenüber." **Art:** Induktiv
2.4.2 Herausforderungen bzgl. Schulungen	
2.4.2.1 Zeit- und Personalmangel	**Erklärung:** Schulungen sind schwierig durchzuführen, weil die Mitarbeitenden währenddessen im Betrieb fehlen und es ohnehin nicht genügend Personal gibt. **Ankerbeispiele:** „Gleichzeitig ist es natürlich so, dass für diese Fortbildungsinhalte einfach keine Zeit ist. Die Leute haben fachlich was völlig anderes zu tun, auch da entwickelt sich die Zeit schnell." „Wenn jemand aus der Pflege schulen will, dann fehlt er mir nicht nur finanziell, sondern ja auch tatsächlich als Kopf am Bett, sag ich jetzt mal." **Art:** Induktiv
2.4.2.2 Geldmangel	**Erklärung:** IT-Sicherheits-Awareness-Schulungen sind teuer. **Ankerbeispiel:** „Das sind natürlich Dinge, die du nur mit sehr viel Fortbildung und Bildungsangeboten und Schaffung von Awareness bearbeiten kannst. Was wiederum sehr aufwendig und teuer ist." **Art:** Deduktiv
2.4.2.3 Herausforderungen Sonstiges	
2.5 Schule und Ausbildung	**Erklärung:** Kompetenzen zu IT und IT-Sicherheit sollten bereits in Schule, Ausbildung und Studium vermittelt werden. **Ankerbeispiel:** „Fangen wir da noch tiefer an: Schule. Also eigentlich gehört das in die Schule rein, dass unterrichtet wird: Immer wenn ihr solche Sachen hier benutzt, dann müsst ihr euch auch immer Gedanken zum Thema Sicherheit machen. Also dass da so Grundsachen mitvermittelt werden. Das ist jetzt eigentlich eine unserer Kulturtechniken geworden, die IT-Nutzung und dann muss man die auch vermitteln, damit man zumindest so Grundverständnisse von Dingen hat. Das gehört eigentlich in sämtliche Ausbildungsberufe mit hinein, mehr oder weniger, je nachdem, was ich jetzt gerade so mache." **Art:** Induktiv
2.6 Awareness Sonstiges	
3. Awareness Vorstände	**Erklärung:** Textstellen, die darauf eingehen, ob Vorstände und Vorständinnen sich mit dem Thema IT-Sicherheit (oder IT im Allgemeinen) befassen, warum sie das tun oder

	eben nicht und ggf. wie sie das tun. **Art:** Deduktiv
3.1 Awareness nein	
3.1.1 Awareness nein allg.	**Erklärung:** Textstellen, die allgemein aussagen, dass sich Vorstände nicht/kaum mit IT-Sicherheit befassen. **Ankerbeispiel:** „Also in diesen Gremien ist es tatsächlich leider nie Thema. Ich würde auch behaupten, dass wir hier mit unserem Verband weit voraus sind. Und ich denke, dass schon der eine oder andere noch dolle Schwachstellen hat in seinem Verband. Es wird nicht thematisiert. Also ich meine meine Kollegen, also, ich will nicht sagen, dass sie es nicht wichtig finden, aber sie beschäftigen sich so nicht damit und haben das Thema eventuell auch abgegeben. Es ist kein Thema." **Art:** Induktiv
3.1.2 Priorisierungs-problem	**Erklärung:** Textstellen, in denen es darum geht, welche Wichtigkeit IT-Sicherheit im Verhältnis zu anderen Themen hat. **Ankerbeispiel:** „Na ja, das ist eigentlich ein Thema, was permanent präsent ist, was aber nicht auf Priorität eins ist. Also da kommen ja die Prioritäten, also das sind ja die Krisen, die tagtäglich stattfinden, dann gibt es ja die betriebswirtschaftlichen Themen und IT-Sicherheit ist ähnlich wie Nachhaltigkeit. Es begleitet uns permanent und wir müssen es permanent in allen Entscheidungen, muss es mitschwingen." **Art:** Induktiv
3.1.3 Überforderung und fehlendes Wissen	**Erklärung:** Vorstände beschäftigen sich nicht mit IT-Sicherheit, weil sie das Thema überfordert, sei es, weil es ihnen fremd ist / ihnen Wissen fehlt, aufgrund seiner Neuheit oder seiner Komplexität oder weil es ihnen Angst macht. **Ankerbeispiel:** „[...] es wächst das Verständnis, aber es ist auch angstbesetzt und fremd. Also wenn ich mal meine Biografie angucke und die drei Schritte, die ich gemacht habe in meinen Rollen, dann war das immer von großem Respekt begleitet, diese ganzen IT Fragen." **Art:** Induktiv
3.1.4 Alter der Vorstände	**Erklärung:** Ältere Vorstände befassen sich nicht mehr mit IT(-Sicherheit), weil sie kurz vor der Rente stehen. **Ankerbeispiel:** „Damals, als ich angefangen habe, Digitalisierung und Sicherheit aufzubauen und anzufassen, da haben viele von meinen Kollegen gesagt: ‚Also ich habe jetzt hier noch 5, 6, 8 Jahre, dann gehe ich in Ruhestand, ich mache hier nichts mehr. Das überfordert mich vielleicht auch. Der Laden läuft jetzt so, wie er ist'. Also gar nicht abwertend oder gar nicht schuldzuweisend. Ich denke, auch ich werde so, bevor ich in den Ruhestand gehe. Man fasst halt bestimmte Themen wahrscheinlich einfach nicht mehr an, weil dann das Interesse fehlt." **Art:** Induktiv
3.2 Awareness ja	
3.2.1 Awareness ja allgemein	**Erklärung:** Textstellen, die lediglich aussagen, dass sich Vorstände mit IT-Sicherheit (und IT im Allgemeinen) befassen **Ankerbeispiel:** „Es gibt da inzwischen schon mindestens bei den großen Stiftungen und Trägern, die Verantwortung für eine Unternehmenssteuerung haben, eine hohe Sensibilität."

	Art: Induktiv
3.2.2 Sensibilisierung durch Angriffe auf Branche	**Erklärung:** Awareness der Vorstände für IT-Sicherheit entsteht dadurch, dass sie von Cyberangriffen auf andere Organisationen der freien Wohlfahrt erfahren. **Ankerbeispiel:** „Gleichzeitig merken wir schon, dass IT-Security insbesondere durch den Cyberangriff in München und Freising und auf die KJF in Augsburg erhöhte Aufmerksamkeit bekommt." **Art:** Induktiv
3.2.3 Weitere Gründe für Awareness	
3.3 IT-S als Managementaufgabe / Direkte Beschäftigung	**Erklärung:** Textstellen, die sich damit beschäftigen, ob IT-Sicherheit als Thema direkt vom Vorstand angenommen wird/werden muss. **Ankerbeispiel:** „Also wenn ich jetzt von mir ausgehe, und man schließt ja in der Regel immer von sich auf andere, würde ich sagen, das ist nicht gut, dass sie sich nicht damit beschäftigen und das abgeben, weil aus meiner Sicht ist es eine Führungsaufgabe. Also nur, wenn der Geschäftsführer oder der Vorstand auch dahintersteht und das Thema auch treibt, nehmen es auch alle mit. Also für mich ist immer die Frage, wie kann man das, ich sage mal als Stabsstelle, die ist ja eine Querabteilung, wie will die das in die Leitungsebenen bringen und nach unten bringen? Das funktioniert aus meiner Sicht nicht." **Art:** Induktiv
3.4 Awareness Sonstiges	
4. Strukturmerkmale	**Erklärung:** Textstellen, die darauf eingehen, dass und wie Strukturmerkmale der freien Wohlfahrt, der Caritas oder der Einrichtungsträger sich auf die Themen IT-Sicherheit und IT auswirkt. **Art:** Deduktiv (aus der Literaturrecherche herausgearbeitet, in den Interviews aber bewusst nicht nachgefragt, um den zeitlichen Rahmen nicht zu sprengen; die Expert:innen sprachen den Aspekt allerdings von sich aus an, daher ist er Teil des Kategoriensystems).
4.1 Heterogenität, Komplexität, Dezentralität	
4.1.1 Komplexität freie Wohlfahrt	**Erklärung:** Textstellen, die auf die Komplexität der freien Wohlfahrt eingehen. **Ankerbeispiel:** „Im Kontext von Zuschüssen, da werden in jeder Kommune andere Vereinbarungen getroffen und da sind Gemeinkosten durchaus auch manchmal flexibler anerkennungsfähig, also da kann ich auch schon mal eine IT-Pauschale mit reinrechnen, aber das kann man jetzt nicht flächendeckend oder grundsätzlich sagen, sondern das hängt an den Verhandlungstraditionen, manchmal an dem Sachverstand der Verhandler vor Ort, an der Durchsetzungsfähigkeit, an der Art, wie ein Landkreis, ein Jugendamt, ein Sozialamt unbedingt will, dass ich die Leistung durchführe usw. Also das ist total individualisiert." **Art:** Deduktiv
4.1.2 Heterogenität Caritas	**Erklärung:** Textstellen, die auf die Heterogenität der Caritas eingehen. **Ankerbeispiel:** „Das große Problem, warum wir uns auch als [Name des Spitzenverbands] da sehr schwer tun, irgendwie einen Fuß in die Tür zu kriegen bei übrigens dem Thema Digitalisierung überhaupt und insgesamt, ist, dass es eine sehr, sehr heterogene Landschaft an Systemen gibt, auch an Infrastruktur. [..] Das ist sehr heterogen und auch die Prozesse sind wenig vergleichbar – nein, anders: Die Prozesse sind zwar vergleichbar, aber auch nur vergleichbar. Sie sind nicht gleich und das macht es schwierig. Noch nicht mal der Input und der Output sind das Gleiche. Da ist es dann halt echt schwierig,

	da koordinierend tätig zu sein.“ **Art:** Deduktiv
4.1.3 Subsidiarität/Unabhängigkeit	**Erklärung:** Textstellen, die sich mit dem Subsidiaritätsprinzip und der damit einhergehende Souveränität der Caritas-Organisationen im Kontext von IT-Sicherheit befassen. **Ankerbeispiel:** „Wir sind ein Verband, wir sind kein Konzern. [...] Wir haben Ortsverbände, Kreisverbände, Diözesanverbände, die […] sehr unterschiedlich aufgestellt sind und alle mehr oder weniger rechtlich selbstständig, was dazu führt, [...] dass jeder selber meint zu wissen, was das Beste ist und wie das funktionieren muss.“ **Art:** Deduktiv
4.2 Unzureichende Kooperation	
4.2.1 (Mangelnde) Kooperation und Standardisierung	**Erklärung:** Textstellen, die Kooperation zwischen den Einrichtungsträgern, verbindliche Standards und Zentralisierung als Lösung für bessere Rahmenbedingungen für IT(-Sicherheit) beschreiben, bzw. ihr Fehlen als Problem. **Ankerbeispiel:** „Da fehlt der gemeinsame Wille, der führt jetzt aktuell nicht wirklich zu einer verbindlicheren Form der Zusammenarbeit, die trägerübergreifend nötig ist.“ **Art:** Induktiv
4.2.2 Fehlende Solidarität zwischen FW-Verbänden	**Erklärung:** Textstellen, die beschreiben, dass fehlende Solidarität innerhalb der freien Wohlfahrt sich negativ auf die Behandlung des Themas IT-Sicherheit auswirken. **Ankerbeispiel:** „Unsere Handlungsfelder sind tatsächlich eher dort, wo ich vorhin schon Defizite skizziert habe, also unternehmerisches Wagnis in die Verhandlungen miteinzubringen, IT-Kostenrefinanzierung in die Entgelte mit reinzubringen, Zugänglichkeit für unsere Verbände bei bestimmten Förderprogrammen zu schaffen. Das sind die Bretter, an denen wir bohren. Die sind sehr dick, die sind sehr hart, weil natürlich, da geht immer das Hauen und Stechen los und die, die es jetzt schon kriegen, wollen nicht, dass da auf jeden Fall noch weitere Anspruchsberechtigte mit drin wären. Aber das ist notwendig und da müssen wir tatsächlich aktiv sein und sind es auch.“ **Art:** Induktiv
4.3 Kompetenzen in der Unternehmensführung	**Erklärung:** Textstellen, die auf vorhandene und fehlende Kompetenzen in der Unternehmenssteuerung eingehen, etwa Finanzkompetenzen, Risikomanagement und Krisenmanagement. **Ankerbeispiel:** „Das eine hängt ein bisschen davon ab, wie der Träger selber sonst auch seine Dinge tut. Und das meine ich gar nicht abwertend, das hat auch was ganz Gesundes. Wenn das etwas hemdsärmelig betrieben wird, dann wird auch die IT hemdsärmelig betrieben, inklusive Datenschutz etc. Das hat was Charmantes, das hat auch was Gutes, weil wir aus meiner Sicht in vielen Dingen auch völlig überreguliert sind. Und da hat es was erfrischend Gutes, diese Hemdsärmeligkeit, weil es uns erlaubt, Dinge zu tun, die wir vielleicht sonst nicht tun können. Aber es ist natürlich an der Stelle auch ein Spiel mit dem Risiko.“ **Art:** Induktiv
4.4 Größe der Träger	**Erklärung:** Textstellen, die einen Zusammenhang herstellen zwischen der Größe einer Organisation und wie sie IT(-Sicherheit) angeht/angehen kann. **Ankerbeispiel:** „Gerade in diesen kleinen mittelständischen Verbänden – also jetzt meine ich eben nicht Frankfurt oder Mannheim mit 3000 Mitarbeitern, sondern ich meine die, die 500 und kleiner sind – die sich eben vielleicht auch diese Stelle dafür nicht leisten können, in denen ist es verpasst worden, dass es eben ein Führungsproblem ist.“

	Art: Deduktiv
4.4.1 Groß	**Erklärung**: Von dem:der Interviewpartner:in als „groß“ bezeichnet.
4.4.1 Klein	**Erklärung**: Von dem:der Interviewpartner:in als „klein“ bezeichnet.
5. Awareness Verbände	**Erklärung:** Textstellen, die darauf eingehen, ob und wie Spitzenverbände IT-Sicherheit als spitzenverbandliche Aufgabe ihren Mitgliedern gegenüber ansehen und wahrnehmen. **Art:** Deduktiv
5.1 Akteure	
5.1.1 DCV	
5.1.2 DiCV	
5.1.3 Sonstiger Spitzenverband	Personalfachverband, Einrichtungsfachverband, etc.
5.1.4 BAGFW, Ligen	
5.1.5 CNIT	
5.1.6 Weitere Gremien und Akteure	z.B. Landescaritaskonferenz Bayern, Bundeskonferenz der örtlichen Caritasverbände (Buko), Vediso, Vorstandskommission des Deutscher Caritasverbands ‚Digitale Transformation‘, Workshop für Fachverbände zu Verwaltungsdigitalisierung, Netzwerk Verwaltungsdigitalisierung, Vorstandskommission Ökonomie, Verbändebündnis zur Digitalisierung in der Pflege, Landesarbeitsgemeinschaften der Caritas Hessen
5.2 Awareness allgemein	
5.2.1 Awareness ja	**Erklärung:** Textstellen, aussagen, dass ein Spitzenverband Awareness bzgl. IT-Sicherheit besitzt. **Ankerbeispiel:** „Interviewerin: ‚Und wenn wir jetzt auch noch mal konkret auf die Spitzenverbände gucken, die für Sie zuständig sind, also vor allem der DiCV [Name des DICVs], wird sich da mit IT-Sicherheit auseinandergesetzt? Gibt es da Angebote an Sie?‘ Expert:in: ‚Also da wird sich damit auseinandergesetzt‘.“ **Art:** Induktiv
5.2.2 Awareness nein	**Erklärung:** Textstellen, die aussagen, dass ein Spitzenverband keine Awareness bzgl. IT-Sicherheit besitzt. **Ankerbeispiel:** „Interviewerin: ‚Welche Rolle spielt denn IT-Sicherheit, Cybersecurity für die DCV-Geschäftsstelle und die BAGFW?‘ - Expert:in: ‚Ich bin Vorstand eines Diözesancaritasverbandes und weiß das nicht. Schon spannend, nicht? Keine Ahnung. Also bis vor ein paar Jahren gar keine, würde ich jetzt sagen. Mit Frau Pauser entwickelt sich da eine gute Dynamik und die hat das sicherlich mindestens mal für ihre eigene Firma im Blick. Aber was das jetzt heißt, konkret, und was daraus für Konsequenzen zu ziehen sind: Ich nehme nichts wahr, zumindest mal.‘“ **Art:** Induktiv
5.2.3 Keine Awareness - Gründe	**Erklärung:** In einer Textstelle werden explizit Gründe genannt, warum Spitzenverbände keine Awareness für IT-Sicherheit haben. **Ankerbeispiel:** „Also ich glaube tatsächlich, dass es von den Spitzenverbänden eine derer Aufgaben ist. Die wird halt an dem Punkt nicht wahrgenommen. Weil insgesamt die Refinanzierung einfach immer prekärer wird. Wir sprechen ja über Cybersicherheit. Und wir haben insgesamt andere Themen, die das überlagern: Also die Frage nach der Refinanzierung von Immobilien, zum Beispiel, die Frage nach Fachkräften, die Frage nach dem weiteren Prinzip der Daseinsfürsorge, die aktuell gefährdet ist, die Finanzierung der Sicherungssysteme. Und da ist jetzt das Thema Cybersicherheit nur ein mini-mini Baustein und rutscht in der Prioritätenliste natürlich immer weiter nach hinten, weil tatsächlich gerade im Grundsatz Dinge in Frage gestellt werden.“ **Art:** Deduktiv

5.3 Angebote	
5.3.1 IT-S als spitzenverbandliche Aufgabe	**Erklärung:** Textstellen, in denen explizit darauf eingegangen wird, ob das Thema IT-Sicherheit als spitzenverbandliche Aufgabe verstanden wird. **Ankerbeispiel:** „Cybersicherheit ist kein spitzenverbandlicher Auftrag. Den haben wir uns an der Stelle als Lerneffekt quasi auf die Fahne geschrieben, weil wir gesagt haben, wir möchten, dass unsere Mitglieder von unseren Erfahrungen profitieren. (...) Andere Spitzenverbände machen das anders." **Art:** Induktiv
5.3.2 Refinanzierungsverhandlungen	**Erklärung:** Spitzenverbandliche Aufgabe ist, IT-Refinanzierung in Entgelt- und Rahmenverhandlungen zu adressieren. **Ankerbeispiel:** „Unsere Handlungsfelder sind tatsächlich eher dort, wo ich vorhin schon Defizite skizziert habe, also unternehmerisches Wagnis in die Verhandlungen miteinzubringen, IT-Kosten-Refinanzierung in die Entgelte mit reinzubringen, Zugänglichkeit für unsere Verbände bei bestimmten Förderprogrammen zu schaffen." **Art:** Induktiv.
5.3.3 Informationsweitergabe	**Erklärung:** Spitzenverbände geben Informationen zu IT-Sicherheit, zum Beispiel gesetzliche Regelungen zu IT-Sicherheit, an ihre Mitglieder weiter. **Ankerbeispiel:** „Ich gebe mir Mühe, Entwicklungen und Regelungen mitzubekommen. Also das kommt vielleicht dann auch über den DiCV oder über den DCV bei uns an, aber es ist jetzt nicht mein Steckenpferd." **Art:** Induktiv
5.3.4 Austausch, Vernetzung	**Erklärung:** Spitzenverbände bieten Plattformen, Netzwerke und Arbeitskreise an, über die sich Mitglieder zu IT und IT-Sicherheit austauschen können. **Ankerbeispiel:** „Es gibt über den Deutschen Caritasverband schon unterschiedliche Netzwerke, die sich mit dem Thema Digitalisierung befassen, die eng ineinandergreifen mit dem, was an innovativen Verbandsentwicklung auch zusammenhängt. Weil natürlich Innovation ohne Digitalisierung zu denken, ist jetzt ehrlicherweise wenig zielführend. Da baut der Deutsche Caritasverband zum Glück Strukturen auf, also sprich Personal, um das auch bearbeitbar zu machen. Also es gibt Caritas.Next, es gibt den IT e. V., es gibt ein Netzwerk Verwaltungsdigitalisierung, das sich aus einer Arbeitsgruppe gebildet hat, dieses Onlinezugangsgesetz eine Zeit lang begleitet hat und diese Sozialplattform, die in Nordrhein Westfalen am Start war." **Art:** Induktiv
5.3.5 Sensibilisierung durch Angriffe auf die Branche	**Erklärung:** Spitzenverbände bieten einen Rahmen, in denen Erfahrungen mit Cyberattacken geteilt werden und so Sensibilisierung für das Thema geschaffen werden kann. **Ankerbeispiel:** „Just gestern war eine große Konferenz mit den Chefs der Fachverbände und der Diözesanverbände. Und die haben tatsächlich auch darüber berichtet, dass immer wieder, also keine erfolgreichen Attacken, aber tatsächlich seltsame Anfragen an den Server vorkommen." **Art:** Induktiv
5.3.6 Konkrete Dienstleistungen	**Erklärung:** Textstellen zu konkreten Dienstleistungen (neben Vernetzung und Informationsweitergabe), die Spitzenverbände für ihre Mitglieder in Bezug auf IT und IT-Sicherheit anbieten, etwa konkrete Schulungsangebote. **Ankerbeispiel:** „Der DiCV bietet eine digitale Datenschutzschulung an. Ob wir uns dort mit andocken können, also ob wir da Kontingente kaufen, das würde ich sozusagen

	gern mal ausprobieren, ob diese Onlineschulung genauso hilfreich ist wie dieses Eins-zu-Eins im Gegenüber." **Art:** Induktiv
5.3.7 Weitere Angebote	**Erklärung:** Weitere spitzenverbandliche Angebote an ihre Mitglieder zu IT-Sicherheit und IT, die keinem der obigen Angebotstypen zugeordnet werden können.
5.3.8 Probleme mit Angeboten	
5.3.8.1 Angebotsprobleme	**Erklärung:** Textstellen, die beschreiben, was an den spitzenverbandlichen Angeboten zu IT-Sicherheit/IT fehlt / nicht funktioniert. **Ankerbeispiel:** „Also nachdem wir als Spitzenverband … also ich sage mal so: Es gibt Einrichtungen, Dienste und DiCVs, die haben mehr Mitarbeiter in ihrer IT-Abteilung als wir hier beim Landesverband insgesamt und insofern haben wir wenig beizutragen zu den sehr konkreten Anfragen, die haben. Also wie mache ich Connext-Vivendi sicher? Wie kriege ich die Leitungen sicher? Wo stelle ich meine Server hin und wie machen wir das mit dem Backup? Da haben wir einfach operativ genau nichts beizutragen." **Art:** Induktiv
5.3.8.2 Nachfrageprobleme	**Erklärung:** Textstellen, die darauf eingehen, dass die Mitglieder die existierenden Angebote zu IT-Sicherheit und IT ihrer Spitzenverbände nicht annehmen. **Ankerbeispiel:** „Wir haben Angebote vermittelt für das Thema Schulung für Mitarbeitende. Gerade, was so Pentesting zum Beispiel angeht. Aber auch da, sage ich mal, war die Resonanz jetzt nicht so, dass man sagen kann, das ist etwas, was Mitglieder tatsächlich nachfragen wollen, weil dann müsste ich mich ja mit der eigenen Organisation und meiner eigenen Beschränktheit auseinandersetzen." **Art:** Induktiv
5.4 Awareness Sonstiges	
6. Awareness Politik	**Erklärung:** Textstellen, die darauf eingehen, ob die Politik sich des Problems der IT- und IT-Sicherheit in der Freien Wohlfahrt und der Freien Wohlfahrt an sich bewusst ist. **Art:** Deduktiv
6.1 Awareness allg.	
6.1.1 Awareness ja	**Erklärung:** Textstellen, die aussagen, dass politische Akteur:innen Awareness bzgl. IT-Sicherheit in der freien Wohlfahrt besitzen. **Ankerbeispiel:** „Auch im politischen Raum ist das tatsächlich Thema gewesen, weil man das dann schon auch mitbekommt. Das stand ja auch hier in der Zeitung, es wurde ja auch veröffentlicht, es gab ja auch Presse dann dazu." **Art:** Induktiv
6.1.2 Awareness nein	**Erklärung:** Textstellen, die aussagen, dass politische Akteur:innen keine Awareness bzgl. IT-Sicherheit besitzen. **Ankerbeispiel:** „Und von daher kann dieses Thema IT-Sicherheit an und für sich nur durch die Legislative auf Bundesebene verändert werden. Und ein bisschen in der Ausgestaltung der Länderparlamente, indem sie zum Beispiel Sonderanpassungen, zum Beispiel der Landtag in Bayern, machen könnten. Dafür ist aber die Bewusstheit zum jetzigen Zeitpunkt überhaupt nicht gegeben." **Art:** Induktiv
6.2 Wahrnehmung der FW	
6.2.1 Kein Wissen über die FW	**Erklärung:** Textstellen, die aussagen, dass die Politik die freie Wohlfahrt nicht wahrnimmt.

	Ankerbeispiel: „Ich glaube, das ist nicht so ganz weit hergeholt, dass da immer mehr Politiker wenig Kernwissen haben, wie die Mechanismen sind und was Gemeinnützigkeitsrecht ist.“ **Art:** Induktiv
6.2.2 FW nicht als Teil der Wirtschaft	**Erklärung:** Die freie Wohlfahrt wird nicht als Wirtschaftszweig wahrgenommen und entsprechend werden ihre wirtschaftlichen Interessen verkannt. **Ankerbeispiel:** „Was da dazu kommt – erschwerend – ist, dass Sozialwirtschaft nicht als Wirtschaftszweig wahrgenommen wird und wir als Verbände die meisten Förderprogramme nicht nutzen können, die von vom Staat aufgelegt werden. " **Art:** Induktiv
6.2.3 FW als Kostenfaktor	**Erklärung:** Die Politik nimmt die Freie Wohlfahrt vor allem als Kostenfaktor wahr. **Ankerbeispiel:** „Ein Problem, was sich bei der Gelegenheit uns – und wir begegnen dem immer wieder – stellt, ist, dass wir in der Regel als Kostenfaktor wahrgenommen werden. Also man kann das in der aktuellen Diskussion immer wieder auch sehen: Da wird zwar sehr viel Wertschätzendes über die Arbeit der Wohlfahrtsverbände gesagt, aber am Schluss heißt es dann ‚Ja, aber die Haushaltslage ist angespannt und deswegen müssen wir beim Sozialen sparen‘“ **Art:** Induktiv
6.2.4 FW nicht systemrelevant	**Erklärung:** Textstellen, die besagen, dass die freie Wohlfahrt von der Politik nicht als systemrelevant eingeschätzt wird. **Ankerbeispiel:** „Da würde ich mir wünschen, dass wir da eben nicht nur als Unternehmen wahrgenommen werden, sondern auch als eine der … also als Verband tragen wir auch ein Stück Gesellschaft, Zivilgesellschaft und Staat mit. Und da auch in unserer Rolle noch mal wahrgenommen zu werden.“ **Art:** Induktiv
6.2.5 Ressort-Problem	**Erklärung:** Für die freie Wohlfahrt ist das Sozialministerium zuständig; das befasst sich aber nicht mit IT/IT-Sicherheit/Digitalisierung. Ressorts, diese Themen auf dem Schirm haben, fühlen sich nicht für die FW zuständig. **Ankerbeispiel:** „Das liegt auch an den Ressortzuschnitten, also bzw. am Ressortprinzip in den Ministerien. Also ein Wirtschaftsministerium ist für Wirtschaftsunternehmen zuständig und halt eben nicht für die Sozialunternehmen, weil die sind mit ihren Anliegen beim Sozialministerium angesiedelt oder beim Gesundheitsministerium und haben deswegen mit dem Wirtschaftsministerium eigentlich nichts zu tun. Und deswegen denken die im Wirtschaftsministerium uns als Sozialwirtschaft, als gemeinnützige Sozialwirtschaft nicht mit.“ **Art:** Induktiv
6.3 EU	
6.3.1 FW bei der EU nicht bekannt	**Erklärung**: Textstellen, die darauf eingehen, dass das deutsche System der freien Wohlfahrt der EU fremd ist. **Ankerbeispiel**: „Da die Europäische Union jetzt den Wohlfahrtsstaat, wie wir ihn in Deutschland haben, so nicht kennt, ist es sicherlich etwas, was nicht im Blick ist.“ **Art**: Induktiv
6.3.2 Regulierungen, Standards	**Erklärung**: Textstellen, die sich mit EU-Regulierungen befassen.

	Ankerbeispiel: „Also wir haben mit der DSGVO die Datenschutzbestimmungen von der EU. Das finden alle belastend." **Art**: Induktiv
6.3.3 Umsetzung von EU-Recht in Deutschland	**Erklärung**: Textstellen, die darauf eingehen, wie EU-Recht in Deutschland umgesetzt wird. **Ankerbeispiel**: „Wenn im Prinzip die Datenschutzüberlegungen eigentlich die Menschen schützen sollen, so kann ich dem auch viel abgewinnen, wenn daraus nicht wieder ein Bürokratiemonster wird. Da ist nicht die EU schuld, sondern in der Umsetzung die Nationalstaaten." **Art**: Induktiv
6.3.4 Lobbyarbeit bei der EU	**Erklärung**: Textstellen, die sich auf Lobbyarbeit der freien Wohlfahrt bei der EU beziehen. **Ankerbeispiel**: „Ich habe das Gefühl, dass auch wir versuchen, also wenn ich das Brüsseler Büro der Caritas sehe, auch Entwicklungen, die auf die Wohlfahrtspflege überschwappen, dort auch noch mal zu lobbyieren und zu sensibilisieren." **Art**: Induktiv
6.4 Lobby	
6.4.1 Adressaten	**Erklärung:** Textstellen, die benennen, welche Akteur:innen die freie Wohlfahrt mit ihrer Lobbyarbeit adressiert / adressieren sollte. **Ankerbeispiel:** „Also einmal gehen wir natürlich zum BMG und sagen da unsere Forderungen, wir gehen zu den pflegepolitischen Sprecher:innen und stellen unsere Forderungen da und es gibt auch Kontakt zum GKV, wo wir unsere Forderungen auch ausbreiten und erklären." **Art:** Induktiv **Auswertung**: Sozialausschüsse der Parlamente, Sozialministerien der Länder, Bundesfamilienministerium, Wirtschaftsministerium, Finanzministerium, Gesundheitsministerium Bezirksebene, Kreisebene; Wirtschaftsvertreter (z.B. IHK), Verhandlungspartner auf kommunaler und Landesebene, Spitzenverband der gesetzlichen Krankenkassen, Bundekanzler
6.4.2 Herausforderungen	**Erklärung**: Textstellen, in denen Herausforderungen und Probleme bei der Lobbyarbeit bezüglich IT-Sicherheit und IT beschrieben sind. **Art:** Induktiv
6.4.2.1 Mangelnde Ressourcen	**Erklärung:** Textstellen, die beschreiben, dass Lobbyarbeit aufgrund fehlender Ressourcen schwierig ist (finanziell, personell, zeitlich, räumlich, etc.) **Ankerbeispiel:** „Hat auch was mit Ressourcen zu tun: Also wenn ich mir anschaue, wie groß das Büro in Berlin ist des Deutschen Caritasverbandes, da fokussiert sich das auf zwei Personen. Das ist ein bisschen wenig." **Art:** Induktiv
6.4.2.2 Mangelnde Zusammenarbeit in der FW	**Erklärung:** Textstellen, die eine mangelnde Zusammenarbeit zwischen den Spitzenverbänden der freien Wohlfahrt als Hindernis für effektives Lobbying benennen. **Ankerbeispiel:** „Und das Problem ist tatsächlich: Für das Platzieren braucht es konzertierte Aktionen der Sozialanbieter. Und ich sage mal, die BAGFW ist an dem Punkt so zersplittert, dass ein konzertiertes Platzieren dieses Anliegens überhaupt gar nicht passiert. Wir sind als Wohlfahrtsverbände, auch als Spitzenverbände nicht in der Lage, das

	Thema strukturiert an den Mann zu bringen und an die Frau oder an den Abgeordneten, die Abgeordnete. Das ist eigentlich, das ist fatal." **Art:** Induktiv
6.4.3.3 Mangelnde Ergebnisse	**Erklärung:** Textstellen, die aussagen, dass existierende Lobbyaktivitäten keine Ergebnisse erzielen. **Ankerbeispiel:** „Also wenn das Land ein Digitalisierungspakt ausruft, dann sind wir da am Start und entwickeln mit und gehen in Modellprojekte und was auch immer. Das funktioniert auch gut. Aber ich sage mal das Thema Wirkung und politischer Einfluss, da darf man zumindest mal Fragezeichen dransetzen." **Art:** Induktiv
6.4.2.4 Weitere Herausforderungen / Probleme	**Erklärung:** Weitere Herausforderungen / Probleme mit Lobbyarbeit, die keiner der oben genannten Kategorien zugeordnet werden können.
6.4.3 Strategien, Formate, Argumente	**Erklärung:** Textstellen, die Strategien, Formate und Argumente beschreiben, mit denen die Freie Wohlfahrt Lobbyarbeit zu IT und IT-Sicherheit betreibt. **Ankerbeispiel:** „Wir machen jetzt eine Kooperation auch auf der Ebene von Diözesanverbänden mit dem [Name eines anderen DiCVs] und gründen einzelne gemeinsame Lobbystrukturen, wo auch Personal geshared wird." **Art:** Induktiv
6.5 Lobby Sonstiges	
6.5 Awareness Politik Sonstiges	
7. Refinanzierung	**Erklärung:** Textstellen, die sich mit der Refinanzierung von IT-Sicherheitskosten und IT-Kosten befassen. **Art:** Deduktiv
7.1 Fehlende Refinanzierung	
7.1.1 Fehlende Refinanzierung allgemein	**Erklärung:** Textstellen, die feststellen, dass die Refinanzierung von IT, IT-Sicherheit oder sozialem Dienstleistungen im Allgemeinen nicht gegeben sind, ohne konkreter zu werden. **Ankerbeispiel:** „Cybersecurity ist echt teuer und bringt zunächst mal keinen unmittelbaren Nutzen für die Arbeit vor Ort. […] Cybersecurity ist teuer, ist in der Regel nicht refinanziert und muss deshalb bezahlt werden aus der Portokasse, aus anderen Zuschüssen." **Art:** Deduktiv
7.1.2 Steigende Anforderungen ohne Finanzierung	**Erklärung:** Textstellen, in denen es darum geht, dass die gesetzlichen und technischen Anforderungen für IT-Sicherheit steigen ohne dass die Finanzierung dafür ebenfalls steigt. **Ankerbeispiel:** „Was aber passiert, und das ist ja ein bisschen abstrus: Über weitergehende Regulierung – zum Beispiel NIS und NIS-2 – versucht der Gesetzgeber quasi das Thema Cybersecurity als Voraussetzung für Dienstleistungserbringung festzulegen und schafft gleichzeitig nicht die dafür notwendigen Finanzierungsstrukturen." **Art:** Induktiv
7.1.3 Insolvenzrisiko	**Erklärung**: Textstellen, die aussagen, dass durch mangelnde Refinanzierung Träger insolvent werden.

	Ankerbeispiel: „Von daher glaube ich tatsächlich, dass das zu einem tiefergehenden grundlegenden Wandel der Daseinsfürsorge in der Bundesrepublik kommen wird: Dass nämlich die freigemeinnützigen Träger sich in der Perspektive aus den Angeboten zurückziehen oder zurückziehen müssen oder auch in die Insolvenz getrieben werden." **Art:** Induktiv
7.2 Gründe für fehlende Refinanzierung	
7.2.1 Refinanzierungslogik	**Erklärung:** Textstellen, in denen darauf eingegangen wird, dass die Refinanzierung von IT-Sicherheit, IT und Digitalisierung in der aktuellen Refinanzierungslogik nicht vorgesehen ist, oder wie diese Logik geändert werden müsste. **Ankerbeispiel:** „Dann kommt natürlich auch dazu, dass – und das ist ein bisschen größer, aber auch da wäre dann natürlich IT-Sicherheit ein mögliches Handlungsfeld – dass wir Innovationen nicht – und das habe ich vorhin ja schon erläutert – wir können Innovationen nicht monetarisieren, die haben für uns erstmal keinen Nutzen. Zumindest nicht, was die Refinanzierungssystematik anbelangt. Wie gesagt, wenn ich Dinge besser machen kann oder schneller machen kann und dadurch Ressourcen beim Personal schaffe, freischaufele, dann sagen die: ‚Dann könnt ihr das ja mit weniger Leuten machen. Und wenn ihr es dann mit weniger Leuten macht, dann ist es für uns billiger, das ist doch super.' Sie zahlen aber die Innovation nicht." **Art:** Induktiv
7.2.2 Fehlende rechtliche Grundlage	**Erklärung:** Es fehlen rechtliche Grundlagen und Standards, um die Voraussetzungen für IT-Sicherheit in der freien Wohlfahrt zu verbessern. **Ankerbeispiel:** „Aber wie gesagt, wir bräuchten Richtlinien, die handhabbar sind, die die Kostenträger uns gegenüber verpflichten, für die Security aufzukommen oder zumindest einen Beitrag so zu leisten, dass das für uns stemmbar ist." **Art:** Induktiv
7.2.3 Fehlende Awareness Kostenträger	**Erklärung:** Textstellen, die besagen, dass sich die Kostenträger der Wichtigkeit von und IT-Sicherheit und IT für die freie Wohlfahrt nicht bewusst sind. **Ankerbeispiel:** „IT-Security, da haben sie gesagt ‚Ihr habt Computer dastehen, Datenschutzgrundverordnung gilt, also bitte'. Dass IT Security mehr ist als nur das Erfüllen der Datenschutzgrundverordnung oder in unserem Fall vom KDG, das zieht nicht bei denen."
7.2.4 Verweigerungshaltung Kostenträger	**Erklärung:** Textstellen, die besagen, dass Kostenträger unabhängig davon, ob sie sich der Wichtigkeit von IT(-Sicherheit) bewusst sind, oder nicht, weigern, für Kosten aufzukommen, außer sie werden eingeklagt. **Ankerbeispiel:** „Also eine allgemeine Sozialberatung, die werden aus Kirchensteuermitteln bezahlt, nehmen aber eine enorm wichtige Funktion ein, weil die so eine Art Clearingstelle ins Fürsorgesystem sind, aber der Staat agiert da halt so, dass er sagt ‚Na ja, wenn die Leute Rechtsansprüche haben, dann sollen sie die halt geltend machen. Es ist nicht meine Aufgabe, dazu Zugänge zu ermöglichen, sondern zu prüfen, ob die wirklich einen Anspruch haben' und sind da eher so in einer Abwehrhaltung. Aber das ist eine völlig andere Diskussion, die abbiegt. Aber das kommt natürlich mit dazu." **Art:** Induktiv
7.2.5 Mangelnde Digitalisierung Kostenträger	**Erklärung:** Grund für die fehlende Awareness der Kostenträger ist, dass sie IT-technisch selbst schlecht ausgestattet sind. **Ankerbeispiel:** „Sie haben ja im Amt selber gar nicht so eine Technik und wenn wir dann sagen, wir schicken nur noch Personalnummern oder nur noch verschlüsselte Unterlagen ans Jugendamt, dann maulen die schon sehr rum, weil sie sagen, sie können das

	dann nicht öffnen. Mittlerweile gibt es auch gesicherte Laufwerke, die versuchen die Mitarbeiter zu umgehen, weil sie nicht wissen, wie es funktioniert, weil sie sich dann Passwörter besorgen müssen, weil es sie einfach nervt. Und wir sagen aber, wir schicken es nicht. Dann stecken wir es wieder in Briefumschläge." **Art:** Induktiv
7.2.6 Geldmangel Kostenträger	**Erklärung:** Textstellen, die darauf eingehen, dass die Kostenträger selbst unter Geldmangel leiden und daher keine Mittel für IT-Sicherheit bei den Trägern finanzieren können. **Ankerbeispiel:** „Bei der aktuellen Entwicklung und der zukünftigen Wirtschaftslage wird die Bereitschaft der öffentlichen Hand, auch noch IT-Infrastruktur bei den Trägern örtlich oder landes- und bundesweit zu finanzieren, eher gering sein." **Art:** Induktiv
7.3 Awareness Kostenträger ja	**Erklärung:** Kostenträger haben eine Awareness für IT(-Sicherheit) **Ankerbeispiel:** „Es gelingt von Zeit zu Zeit schon, das Thema IT ins Bewusstsein zu rufen. Das heißt aber nicht, dass man das dann hinterher auskömmlich finanziert bekommt. Das auf gar keinen Fall."
7.4 Refinanzierungsverhandlungen	**Erklärung:** Textstellen, in denen beschrieben wird, wie Entgeltverhandlungen ablaufen, welche Rolle IT und IT-Sicherheit dort spielen und welche Argumente dort ausgetauscht werden. **Ankerbeispiel:** „Also für uns war …also da muss man ein bisschen die Genese auch … und es ist in Verhandlungen immer schwierig, weil Verhandlungen sind immer auch ein Kuhhandel. Das eine kriegst du, das andere kriegst du nicht." **Art:** Induktiv
7.5 Alternativen zu Refinanzierung	
7.5.1 Projektmittel/Förderprogramme	**Erklärung:** Textstellen, in denen es um die Finanzierung von IT-Sicherheitsmaßnahmen durch Projektmittel geht. **Ankerbeispiel:** „Mir fällt noch ein, wir hatten hier ein Projekt, mit dem die DiCV zusammen, das Tandem 4.0. Kennen Sie das? Das waren auch Bundesmittel, glaube ich. Die haben ja auch nur wir im Osten bekommen, um die Digitalisierung voranzutreiben. Und mit der Kollegin, da haben wir schon ein paar Veranstaltungen hier auch gemacht, um die Mitarbeiter zu schulen und zu sensibilisieren." **Art:** Induktiv
7.5.2 Rücklagen	**Erklärung:** Textstellen, in denen es um die Finanzierung von IT-Sicherheitsmaßnahmen durch Rücklagen geht. **Ankerbeispiel:** „Da hast du Glück, wenn du ein großer Verband bist, der möglicherweise irgendwo noch Rücklagen hat oder sowas auf drei vier Jahre auch noch mal strecken kann, wenn es da externe Finanzierung braucht, der entsprechend möglicherweise auch versichert ist." **Art:** Induktiv
7.6 Refinanzierung Sonstiges	
8. Datenschutz	
8.1 Datenschutz = IT-Sicherheit	**Erklärung:** Textstellen, in denen beschrieben wird, dass IT-Sicherheit und Datenschutz eng miteinander verbunden sind. **Ankerbeispiel:** „Ich habe ja vorhin erläutert, Cybersecurity ist nach meinem

	Verständnis einmal Schutz der Infrastruktur und der physische Schutz der Daten, aber es ist zum anderen natürlich auch der Schutz schützenswerter Daten vor dem Zugriff Dritter, und da ist Cybersecurity ein Aspekt und Datenschutz also im Sinne der Datenschutzgrundverordnung bzw. des KDG ein zweiter." **Art:** Induktiv
8.2 Datenschutz als Hindernis	**Erklärung:** Datenschutz wird als hinderlich für das Um-/Durchsetzen von IT-Sicherheitsmaßnahmen beschrieben. **Ankerbeispiel:** „Also wenn der Datenschutz immer negativ konnotiert ist, dann dringst du auch mit dem Thema Cybersecurity schlecht durch, weil – ich habe ja vorhin erläutert – Cybersecurity ist nach meinem Verständnis einmal Schutz der Infrastruktur und der physische Schutz der Daten, aber es ist zum anderen natürlich auch der Schutz schützenswerter Daten vor dem Zugriff Dritter, und da ist Cybersecurity ein Aspekt und Datenschutz also im Sinne der Datenschutzgrundverordnung bzw. des KDG ein zweiter. So, und wenn natürlich von diesen beiden Teilen der eine von echt schlechtem Ansehen ist, dann hat es auch der andere schwer." **Art:** Induktiv
8.0 Datenschutz Sonstiges	**Erklärung:** Textstellen, zu Datenschutz, die (noch) keinem Untercode zugeordnet werden können.
SONSTIGES	**Erklärung:** Themen, die keinen Kategorien zuordenbar sind.
S1 Sonstiges zu IT-Sicherheit	
S1.1 NIS-2	
S1.1.1 Kenntnis von NIS-2	
S1.1.2 Keine Kenntnis von NIS-2	
S1.2 Arbeitsfähigkeit	**Erklärung:** Textstellen, in denen es darum geht, dass IT-Sicherheit technisch, prozessual oder regulatorisch Arbeitsabläufe verändert oder einschränkt. **Ankerbeispiel:** „Das ist auch der Punkt zu den Mitarbeitern: wir müssen uns schon im Klaren sein, das Gleiche, was den Datenschutz betrifft, betrifft auch die IT-Sicherheit, dass manche Bestimmungen, die wir aus Sicherheitsgründen erlassen müssen, den normalen Betrieb stören." **Art:** Induktiv
S1.3 IT-Sicherheit braucht Zeit	**Erklärung:** Textstellen, die betonen, dass das Herstellen von IT-Sicherheit ein langer Prozess ist. **Ankerbeispiel:** „Also aus meiner Sicht fehlt nach wie vor – ich denke, das habe ich ja schon gesagt – das Verständnis und Verständigungskräfte, welcher lange, weiter Weg das ist und dass ich den anfangen muss. Jetzt. Weil ich Zeit brauche, um den umzusetzen. Ja und dass auch eine externe Firma, egal wie die heißt und wer das ist, nicht meinen Laden von heute auf morgen cybersicher macht. Also das beschäftigt mich immer mal." **Art:** Induktiv
S1.4 Cyberversicherung	**Erklärung:** Textstellen, die Cyberversicherungen erwähnen. **Ankerbeispiel:** „Und an der Stelle wägen die ab, auch welches Maß an IT-Security ist notwendig oder reicht es uns, wir schließen eine Versicherung ab und machen genau das, was die Versicherung braucht, damit sie greift, wenn es zu einem Angriff kommt. Ob das dann ausreicht oder nicht, steht auf einem anderen Blatt, aber dann hast du wenigstens jemanden, der den Scherbenhaufen bezahlt, dessen Beseitigung dann ansteht." **Art:** Induktiv

S1.5 Schlussfolgerungen aus Cyberangriffen	**Erklärung:** Nicht-technische Schlüsse, die aus einer Cyberattacke gezogen werden. **Ankerbeispiel:** „Ich glaube, es geht auch nicht um den Datenabfluss damals bei uns, sondern es geht letztlich darum, Infrastruktur zu zerstören und so zu gucken, dass man Geld erpressen kann." **Art:** Induktiv
S2 Organisationsentwicklung und -kultur	**Erklärung:** Textstellen, die auf Organisationsentwicklung und Organisationskultur im Kontext von IT-Sicherheit und IT eingehen. **Ankerbeispiel:** „Und das Thema der Organisationsentwicklung, der Prozessmitnahme, der Kommunikation ist übrigens auch unser größtes Learning. In den ganzen IT-Change-Fragen ist das hochrelevant, mindestens genauso wie der Prozess selber oder die Umsetzung selber." **Art:** Induktiv
S3 Technische Veränderungen	
S3.1 Digitalisierung	**Erklärung:** Kennzeichnung von Textstellen, in denen es mehr um Digitalisierung als um IT oder IT-Sicherheit geht. **Ankerbeispiel:** „Also es gibt schon auch Bereiche, gerade da, wo die Digitalisierung vorangetrieben werden soll, wo man also da sich auch schon bemüht, auch noch mal Sonderfinanzierung... Wir hatten jetzt auch vor zwei Jahren so ein ganz kleines Ding in der Schwangerenberatung, da gab es auf einmal so ein ganz kleines Sonderprogramm des Landes, dass wir da auch die Kollegen besser mit Laptops, Handys, Beamer, was weiß ich … also, dass man im Beratungssetting eben mehr auch digital arbeiten kann." **Art:** Induktiv
S3.2 KI	**Erklärung:** Kennzeichnung von Textstellen, die sich spezifisch auf KI beziehen. **Art:** Induktiv
S3.3 TI	**Erklärung:** Kennzeichnung von Textstellen, die sich spezifisch auf Telematikinfrastruktur (TI) beziehen. **Art:** Induktiv.
S4 Systemische Veränderungen	
S4.1 Wertewandel	**Erklärung:** Textstellen, die Dysfunktionalitäten in der Sozialwirtschaft auf einen Wertewandel in Gesellschaft und Politik zurückführen. **Ankerbeispiel:** „Also wir haben schon Schieflagen, auch im solidarischen Miteinander und im Verstehen, was ist denn Solidarität oder wie funktioniert das. Und ich glaube schon, dass da auch eine Ursache für Nichtwissen ist. Stichwort ‚Was gibt es für ein Gesellschaftsbild, das committed ist?' ‚Wie ist unser Gesellschaftervertrag?' Und ich glaube, der funktioniert gerade nicht mehr gut, oder den kennen die Leute nicht mehr." **Art:** Induktiv
S4.2 Grundlegende Veränderungen im Sozialsystem	**Erklärung:** Textstellen, die das Ende der Sozialwirtschaft in der jetzigen Form thematisieren. **Ankerbeispiel:** „Von daher glaube ich tatsächlich, dass es zu einem tiefergehenden grundlegenden Wandel der Daseinsfürsorge in der Bundesrepublik kommen wird: Dass nämlich die freigemeinnützigen Träger sich in der Perspektive aus den Angeboten zurückziehen oder zurückziehen müssen oder auch in die Insolvenz getrieben werden; und dass die Angebote der Daseinsfürsorge dann durch kommunale Anbieter, wo ja auch die Verpflichtung dazu besteht, wahrgenommen werden. Und natürlich von Marktbegleitern, die aber nicht gemeinnützig sind, sondern tatsächlich profitorientiert und das dann

	definitiv zulasten der Anspruchsgruppen kommt." **Art:** Induktiv
Art der Aussage	**Erklärung:** Diese Codes sind nicht inhaltlicher Natur, sondern geben an, ob eine Aussage ein Problem, eine Maßnahme oder einen Vorschlag zur Verbesserung beschreiben. Sie werden zusätzlich zu inhaltlichen Codes vergeben. **Art:** Deduktiv (aus der Fragestellung)
A. Problem	**Erklärung:** Der/die Expert:in beschreibt eine aktuelle Problemlage.
B. Maßnahme	**Erklärung:** Der/die Expert:in beschreibt, welche Maßnahmen aktuell ergriffen werden, um Herausforderungen in Bezug auf IT-Sicherheit zu bewältigen.
C. Wunsch	**Erklärung:** Der/die Expert:in formuliert Wünsche/Ideen/Forderungen, wie Rahmenbedingungen für IT-Sicherheit / IT / die Sozia verbessert werden können / sollen.
D. Sonstiges	**Erklärung:** Textstellen, die weder ein Problem, eine Maßnahme oder einen Wunsch beschreiben.
Besondere Interview-Teile	**Erklärung:** Diese Codes markieren Antworten auf bestimmte Themenblöcke im Interview. So lassen sich die Antworten der Expert:innen zu diesen Themen besser gegenüberstellen. **Art:** Induktiv
I Cyberangriff	**Erklärung:** Beschreibung eines Cyberangriffs / IT-Vorfalls in der Organisation des Experten / der Expertin.
II Definition IT-Sicherheit	**Dazugehörige Frage im Interviewleitfaden:** „Der Einfachheit und Einheitlichkeit halber spreche ich meistens von IT-Sicherheit. Ich differenziere dabei allerdings nicht zwischen IT-Sicherheit und Cybersicherheit bzw. Cybersecurity. Bitte beschreiben Sie kurz, was Sie unter IT-Sicherheit verstehen. Ich möchte sicherstellen, dass wir nicht aneinander vorbeireden."
III Größte Herausforderung	**Dazugehörige Frage im Interviewleitfaden:** „IT-Sicherheit ist ein komplexes Thema, gerade für Organisationen der freien Wohlfahrt. Was sind Ihrer Meinung nach die größten Herausforderungen für eine Caritas-Organisation, um IT-Sicherheit in einer Caritas-Organisation herzustellen?"
IV Sonst noch wichtig	**Dazugehörige Frage im Interviewleitfaden:** „Wir sind mit unserer Zeit fast am Ende und auch ich habe mir keine weiteren Fragen mehr aufgeschrieben. Gibt es etwas, das Ihnen zu diesem Thema noch wichtig ist?"

Anhang 10: Interviewausschnitte zur kirchlichen Datenschutzaufsicht

Die katholische Kirche in Deutschland unterhält fünf Datenschutzaufsichtsbehörden, in denen jeweils mehrere Bistümer zusammengefasst sind. Die folgenden Beispiele beziehen sich auf drei verschiedene Aufsichtsbehörden.

Auszug 1: Meldung eines Cybervorfalls an eine kirchliche Datenschutzbehörde

„Da habe wir auch Einiges über den kirchlichen Datenschutz gelernt, wie sie damit umgehen oder mit uns umgegangen sind. Ich weiß nicht, wie es dem DiCV München damit ergangen ist, aber ich dachte mir ‚Okay, die waren jetzt auch nicht wirklich hilfreich in der Situation, sondern die waren auch eher ein Problem als eine Lösung'. Da musste man dann diskutieren, dass man eben Leuten, die bei uns in Schutzwohnungen leben, nicht an die Privatadresse einen Hinweis schickt, dass eventuell ihre Daten abgegriffen wurden. Wobei wir auch bis heute gar nicht wissen, was an Daten überhaupt betroffen ist. Es ist nichts im Darknet aufgetaucht, gar nichts ist. Wir wissen auch noch nicht mal, ob überhaupt Daten abgegriffen worden sind. Wir haben hier Leute, die wir schützen müssen oder psychisch Erkrankte, die im ambulant betreuten Wohnen sind. Wenn Sie jemandem mit Verfolgungswahn mal eben Brief schreiben, ‚Es könnte sein, dass…', ja, dann brechen alle Verschwörungstheorien auf, also solche Sachen. Und das fand ich irgendwie mühsam. Also die haben uns echt nicht geholfen, sondern das ist ein reiner Formalismus, der die Welt auch nicht rettet."

Auszug 2: Meldung eines Cybervorfalls an eine kirchliche Datenschutzbehörde

„So, dann habe ich unseren nächsten Schritt unseren Datenschutzbeauftragten informiert. Darüber sind wir das Ganze noch mal durchgegangen. Dann hat er gesagt ‚Naja, okay, das muss man jetzt der kirchlichen Datenschutzbehörde melden'. Das habe ich dann gemacht und dann kam eine dermaßen unverschämte Mail zurück, also da war ich richtig sauer. Wir hätten das ja auch sein lassen können mit dem Melden[50]. Da dachte ich mir: ‚Sag mal, geht's noch?' Wir haben das dann alles schön beantwortet und dann habe ich aber drunter geschrieben, dass ich mir doch einen anderen Stil wünschen würde, ich wäre hier nicht der Angeklagte wäre, sondern ich hätte das freiwillig gemeldet und mir wäre meine Verantwortung bewusst, da müssten sie jetzt nicht so einen Ton

[50] Beim vorliegenden Fall lagen keine Hinweise auf Datenabfluss vor.

anschlagen. Naja gut, danach haben wir nie wieder was von denen gehört. Das fand ich also völlig daneben."

Auszug 3: Erfahrungen mit einer kirchlichen Datenschutzaufsichtsbehörde im Allgemeinen

„Der kirchliche Datenschutz, das KDG, ist noch restriktiver als die Datenschutzgrundverordnung an manchen Stellen und das wird von den Kolleginnen und Kollegen zum Teil als massiver Hemmschuh empfunden. Dazu kommt, dass die Akteure, die für den kirchlichen Datenschutz zuständig sind, wenig – also das ist jetzt eine gefühlte anekdotische Wahrheit, das kann ich tatsächlich so anders nicht belegen – dass sie zumindest von ihrem Ansehen her als massive Bremser und wenig unterstützend wahrgenommen werden. Wie kann man in einem modernen Verband, wie kann man in einer modernen Organisation mit den anfallenden Daten so arbeiten, dass es nutzbringend ist, vor allem auch für die Klienten und auch für die Organisation, ohne ständig mit dem Datenschutz in Konflikt zu kommen? Da heißt es in der Regel von den Datenschutzbehörden nur ‚Ja, so könnt ihr es nicht machen'. Und wenn du danach fragst ‚Ja, wie sollen wir es denn machen? Wir würden gerne das und das', dann heißt es ‚Ja keine Ahnung. Aber so jedenfalls nicht'. Und das ist wenig hilfreich. Das treibt natürlich wieder die Kosten, wenn du immer wieder und immer wieder Vorschläge machen musst, dann ist es am Schluss sehr aufwendig, wenn das dann immer wieder vom Tisch gewischt wird, ohne zu wissen, in welche Richtung es denn tatsächlich gehen soll."

Anhang 11: Interviewausschnitte zur IT-Ausstattung

Die Interviewausschnitte stammen aus vier verschiedenen Interviews und repräsentieren alle Organisationsarten (OCV, DiCV, Spitzenverband).

Auszug 1:

„Und ich habe von der Finanzierung und von der Manpower im Verband nicht die Möglichkeiten mir eine große IT-Abteilung aufzubauen. Ja, das ist ja ein Grundsatz, glaube ich, insgesamt im sozialen Bereich. Wir müssen ja mit den Sätzen, die wir haben, auskommen. Wir können ja nicht frei verhandeln. Wir haben natürlich Berechnungen, wie wir unser Entgelt … und können ja da ein schon auch ein bisschen einpreisen. Aber in der Jugendhilfe, sind die Sachkostenpauschalen begrenzt. Ja, das heißt, Sie können nicht wie ein freies Unternehmen sagen, wir satteln da jetzt auch noch mal richtig auf und hauen da wirklich Ressourcen rein, weil wir als kleiner Verband natürlich auch gar nicht die internen IT-ler bekommen."

Auszug 2:

„Die sind aber noch dabei – zum Teil in unterschiedlicher Geschwindigkeit – ihre IT Systeme auf das Jahr 2015 zu modernisieren."

Auszug 3:

„Zunächst mal stellt sich ja bei kleinen Trägern die Frage, haben sie denn überhaupt eine eigene IT-Abteilung oder haben sie einen externen Anbieter? Und wenn sie eine eigene IT-Abteilung haben, dann ist das häufig eine IT-Abteilung, die aus einem, maximal anderthalb Personen besteht, wo unterstellt werden darf, dass sie gar nicht das Know-how vorhalten, sowohl Infrastruktur als auch Software-Administration etc. vorzuhalten. Dann kommt noch IT-Sicherheit on top und das heißt, dort ist davon auszugehen, dass das nur nebenher irgendwie mitgemacht wird, dass man natürlich weiß, was eine Firewall ist etc., aber damit endet es ja nicht. Über Notfallkonzepte, über die wir hier sprechen, brauchen wir schon gar nicht weiter diskutieren oder weiter überlegen, weil das ist dann bestimmt nicht vorhanden."

Auszug 4:

„Was – glaube ich – schon immer ein Thema ist in der Wohlfahrt, ist die Frage, Dienstgerät oder nicht. Also ich vermute mal, oder weiß, dass es da irgendwie so unausgesprochene Agreements oder Erwartungen gibt, dass übers private Handy irgendwelche Sachen laufen. Bei uns selber

wurden halt Kolleginnen und Kollegen mit Zoom-Lizenzen nach Hause geschickt auf ihr Privatgerät, um zu Hause coronakonform arbeiten zu können. Also Nutzung von Privatgeräten, das ist schon noch mal so eine besondere Lücke, die vermutlich auch in der Konstellation mit den fehlenden Mitteln und der fehlenden Refinanzierung ein Treiber sein kann, ein Risikotreiber. Also bei uns war es tatsächlich so – und das war an anderen Standorten meines beruflichen Arbeitens auch so –, dass man das private Handy nutzt, um eine Multi-Faktor-Authentifizierung zu machen. Beispielsweise dein Privathandy oder was auch immer, Nutzung von irgendwelchen Messengerdiensten oder sowas und das als offene Flanke für Klientenkommunikation. Solche Themen sind schon mal spezifisch, diese Risiken und damit auch die Angriffsflächen."

Anhang 12: Interviewausschnitte zur Sensibilisierung für IT-Sicherheit durch Cyberattacken auf die Sozialwirtschaft

Um aufzuzeigen, wie wichtig das Teilen von Erfahrungen mit Cyberattacken auf soziale Organisationen ist, um andere Organisationen der Sozialwirtschaft für das Thema zu sensibilisieren, sind hier einige Interviewausschnitte dazu zusammengestellt. Bis auf eine Dopplung stammen die Zitate von verschiedenen Expert:innen.

Auszug 1:

„Unsere Ortsvereine haben natürlich den Angriff auf uns mitbekommen, was natürlich auch noch mal verbandlich sensibilisiert."

Auszug 2:

„Also ich glaube, dass sich durch den Angriff auf uns die Mitglieder überhaupt erst die Frage nach deren Cybersicherheit gestellt haben."

Auszug 3:

„Gleichzeitig merken wir schon, dass IT-Security insbesondere durch den Cyberangriff in München und Freising und auf die KJF in Augsburg erhöhte Aufmerksamkeit bekommt."

Auszug 4:

„Und dabei hat uns die Konstellation, dass München so lahmgelegt war, schon geholfen, dass es eine hohe Anerkennung und Anerkenntnis und eine Sensibilität für die Themen gab und wir die auch organisational signifikant einfacher durchsetzen konnten als vorher. Das ist bitterbös, wenn man das ehrlich anguckt."

Auszug 5:

„Und sicherlich sind solche Treffen auch hochrelevant. Oder Veranstaltungen zu irgendwelchen Cyberangriffsthemen oder was auch immer. In *[Name der Stadt]* war letzthin auch was, wo der Thomas Schwarz *[Der für IT zuständige Vorstand des DiCV München/Freising]* da war. Also das ist schon, glaube ich, der richtige Weg, so für das Wachsen des Verständnisses. Und da braucht man, glaube ich, einen Invest an der Stelle."

Auszug 6:

„Ich glaube, das ist tatsächlich durch diese prominenten Angriffe auch in der Caritasfamilie in den letzten zwei, drei Jahren weiter nach vorne gerückt. Also wir waren schon nachher auch gefragte Gesprächspartner. Sowohl jetzt hier im Bistum, aber auch darüber hinaus, also auch auf Bundesland-Ebene bin ich immer mal wieder auch von Kollegen angesprochen worden, die davon gehört haben. Sie haben dann auch gefragt: ‚Wie stellt ihr euch auf, was habt ihr gemacht?' Ich habe das damals auf einer Seite kurz zusammengeschrieben; so ein paar Regeln, was muss man tun, wenn es passiert, also so die Erfahrungswerte, die wir hatten. Das ist nichts Großes, das sind so zehn Sätze, so Spiegelpunkte auf einer Seite. Das ist immer unheimlich nachgefragt, viele haben mich gefragt ‚Können wir das haben?' Also da merkte man eine große Unsicherheit und ich glaube, dann haben viele noch mal nachgedacht, weil ich auch immer gesagt habe, dieser Experte sagte uns ‚Also, man muss sich nicht einbilden, man sei sicher, es wird jeder gehackt, es ist immer nur eine Frage wann'. Mit diesem Spruch bin ich viel rumgegangen und da hat man schon gemerkt, dass viele sich dann auch mit diesem Thema noch mal ganz anders beschäftigt haben und so ein bisschen durch uns alarmiert, dann auch erst mal gefragt haben ‚Wo stehen wir denn, was haben wir, wo müssen wir noch mal gucken?' Also ich glaube, wenn es in der Nähe einschlägt, dann wird man dann auch noch mal vorsichtiger."

Anhang 13: Interviewausschnitte zum fehlenden Verständnis für die freie Wohlfahrts seitens politischer Akteur:innen

Die zitierten Ausschnitte stammen von verschiedenen Expert:innen und decken alle befragten Verbandsarten ab.

Auszug 1:

„Da würde ich mir wünschen, dass wir da eben nicht nur als Unternehmen wahrgenommen werden, sondern auch als eine der … also als Verband tragen wir auch ein Stück Gesellschaft, Zivilgesellschaft und Staat mit. Und da auch in unserer Rolle noch mal wahrgenommen zu werden."

Auszug 2:

Interviewerin: „Warum wird denn die Sozialwirtschaft Ihrer Meinung nach weder als systemrelevant noch als wirtschaftlicher Akteur wahrgenommen?"

Expert:in: „Weil wir für den Staat in seinen Haushalten in der Regel einfach ein Kostenfaktor sind. Der Staat schaut sich nicht die Leistungen an, die dafür kommen, sondern zunächst mal den Kostenfaktor. Dass – und da gibt es gute Untersuchungen zum Social Return on Investment – jeder Euro, den du in die Sozialwirtschaft investierst, 1,20 € oder 1,30 €, je nachdem wie man rechnet, wieder volkswirtschaftlich zurückbringt, nutzt halt in der Haushaltslogik, die immer von einem Jahr zum nächsten geht, nichts. Aber es ist immer das Gedankenspiel, was würde passieren, wenn wir von jetzt auf gleich alle unsere Kitas und alle unsere Pflegeheime und alle unsere Behindertenheime zumachen würden und sagen ‚Hier, kümmert euch selber!' Dann gehen auf einmal die Hälfte der Leute nicht mehr arbeiten, weil sie sich um ihre Angehörigen, also Kinder, Alte, Behinderte, kümmern müssen. Und das hat einen massiven volkswirtschaftlichen Impact. Mal davon abgesehen, dass wir im Jahr ungefähr – also nicht nur die Caritas, sondern die ganze freie Wohlfahrtspflege – ungefähr 8 Milliarden Euro umsetzen allein in Bayern. Das ist natürlich im Vergleich zu Unternehmen wie BMW oder so jetzt nicht so viel, aber ich habe letztens gelesen, in Deutschland arbeiten 770.000 Leute in der Automobilbranche. Ja, Freunde, so viele – also ein paar weniger – aber so viele arbeiten bei der Caritas alleine, ohne die anderen Wohlfahrtsverbände! Natürlich, die Wertschöpfung ist eine andere. Ich sage ganz bewusst eine andere, natürlich zum einen größenordnungsmäßig. Dass das Geld irgendwo herkommen muss, ist völlig klar und natürlich. Wir sind nicht gewinnorientiert, das Geld, was wir haben, fließt ungefähr zu 85 bis 90 %, je nachdem welchen Dienst und welche Einrichtungen man betrachtet, ans Personal. Aber die geben das wieder

aus. Die mieten sich Wohnungen, die kaufen Autos, die gehen einkaufen, die schicken ihre Kinder irgendwohin. Das Geld bleibt volkswirtschaftlich wirksam. Und es hat eben auch Sekundäreffekte, die der Wirtschaft enorm nutzen."

Auszug 3:

„Weder das Finanzministerium noch das Wirtschaftsministerium eine haben Vorstellung davon, wie groß die Sozialwirtschaft ist und wie wichtig es ist, hier in eine Förderung mitzugehen. Ich bin ja auf der Bundesebene etwas aktiv und da war ein Vertreter des Wirtschaftsministeriums, der dann total überrascht war, dass wir bei der der Förderung der Nachhaltigkeit als Sozialwirtschaft exklusiv ausgeschlossen worden sind, weil man sie nicht auf dem Schirm hatte. Das heißt, bei der Förderung von Industrie – auch also auch was Digitalisierung angeht – da gibt es entsprechende Förderprogramme, von denen die Sozialwirtschaft exklusiv ausgeschlossen wird. Sie können gar keinen Antrag dort stellen. Sei das jetzt eine KfW-Thematik oder eine direkte Förderung durch das Ministerium. Von daher kommt natürlich den Parlamentariern eine entsprechend hohe Bedeutung zu, aber natürlich auch eine Akzentuierung bei den Ministerien, weil die ja dann in die Umsetzung auch der Förderprogramme gehen. Ich sage mal, Förderung ist eine kurzfristige Möglichkeit, auch hohen Impact zu erzeugen in sehr kurzer Zeit. Der Weg über die Gesetzgebung ist ein deutlich längerer und beide Wege sind momentan nach meinem Kenntnisstand der Sozialwirtschaft eher verschlossen."

Auszug 4:

„Ja, wobei es etwas schwierig ist, weil einfach die Wohlfahrtspflege, so wie wir sie in Deutschland haben, eigentlich EU-weit gar nicht so vorkommt. Wir sind ja wirklich eine Ausnahme mit dem Konstrukt, das wir haben. Darum ist das manchmal so schwierig auch die Wohlfahrtspflege, glaube ich, da aus den Gesetzen wieder rauszunehmen, weil wir aus EU-Sicht mehr als Gesundheits- oder Sozialunternehmen gelten und nicht den Sonderstatus haben, den eigentlich Wohlfahrtspflege in Deutschland zu Recht genießt. Das macht es an manchen Stellen schwieriger […]."

Auszug 5:

Expert:in: „Da die Europäische Union jetzt den Wohlfahrtsstaat, wie wir ihn in Deutschland haben, so nicht kennt, ist es sicherlich etwas, was nicht im Blick ist und wo auch Bundespolitik dann in Übersetzungsleistungen gehen muss, solange sie noch weiß, was freie Wohlfahrtspflege ist. Kann man darauf hoffen."

Interviewerin: „Weiß sie das?“

Expert:in: „Nein, das weiß sie nicht mehr überall und durchgehend. Also manchmal weiß sie es noch, aber es ist schon spürbar, je nach politischer Farbenlehre, die gerade in Verantwortung ist, dass da auch ordentlich Missverständnisse und oder Fehlverständnisse da sind. Das wird sicherlich eine große Aufgabe in den nächsten zehn Jahren. […]

Ich glaube, das ist nicht so ganz weit hergeholt, dass da immer mehr Politiker wenig Kernwissen haben, wie die Mechanismen sind und was Gemeinnützigkeitsrecht ist. “

Anhang 14: Interviewausschnitte zu Refinanzierungsverhandlungen

Die Literaturrecherche zu Refinanzierungsverhandlungen hatte sich insofern als schwierig gestaltet, da die Zuständigkeit je nach Hilfefeld und Bundesland stark variieren. Folglich kann man kaum allgemeingültige Beschreibungen abliefern, außer der Aussage: Es ist kompliziert. Entsprechend spannend sind die Einblicke, die die Expert:innen in ihre Verhandlungserfahrungen geben. Aus diesem Grund ist die Zitatsammlung zu Refinanzierungsverhandlungen besonders ausführlich.

Beispiel 1: OCV

Interviewerin: „Inwieweit sind Sie denn da in die Verhandlungen eingebunden mit der Kommune?"

Expert:in: „Genau. Also, die Verhandlungen führe ich mit, ja. Und wenn Sie da jetzt darauf hinauswollen, welchen Kostenanteil dort für Digitalisierung vorhanden ist, dann kann ich Ihnen sagen, es gibt Sachkosten und prozentuale Anteile zu den Personalkosten und daraus ist das zu finanzieren. Deshalb sagte ich ja am Anfang, das ist ein langer Weg und ich kann nicht hundert Rechner auf einmal kaufen, ich kann immer nur peu à peu kaufen."

[…]

*Interviewerin: „*Das heißt also, dass Sie die Entgeltvereinbarungen selber machen. Aber machen Sie auch die Leistungsvereinbarungen komplett selbst?"

Expert:in „Also für das, was wir hier anbieten, ja, weil wir hier ja direkt mit den Jugendämtern verhandeln und mit den Sozialämtern auch. Das passiert ja alles auch auf kommunaler Ebene. Deshalb reichen wir immer die Kosten mit einer Leistungsbeschreibung ein. Und nur für die ambulante Pflege, in der wir mit tätig sind, das wird auf Bistumsebene verhandelt mit den Kranken- und Pflegekassen. Dort gibt es ja wiederum einen Rahmenvertrag für die Pflege, aber da ist ja Digitalisierung nicht enthalten."

Interviewerin: „Und können Sie da auf das Bistum mit einwirken? Haben Sie da eine Stimme oder macht das dann komplett der DiCV oder irgendeine Liga? Wer ist dafür zuständig?"

Expert:in: „Der DiCV verhandelt für uns die ambulante Pflege und hier arbeiten wir alle unsere Zahlen zu. Mittlerweile wird ja der Ist-Lohn der beschäftigten Mitarbeiter in den Verhandlungen gefordert und fließt dort ein und das arbeiten wir alles dem DiCV zu. Der bündelt das von allen. Also wir haben hier Sozialstationen im Bistum in Caritas-Trägerschaft, in pfarrgemeindlicher

Trägerschaft, von den Maltesern und haben wir da noch andere? Ich glaube, das ist jetzt die größte Gruppe und für die Gruppe wird dann in der Verhandlung zusammengeführt."

Interviewerin: „Und spielt da IT-Sicherheit oder grob IT-Kosten eine Rolle?"

Expert:in: „Nein. Nein."

Beispiel 2: OCV

Interviewerin: „Welche Rolle spielen denn IT-Kosten und vor allem IT Sicherheitskosten in den Verhandlungen mit den Kostenträgern, um das überhaupt refinanziert zu bekommen? Ist das ein Thema?"

Expert:in: „Unterschiedlich. Also es ist zum Beispiel beim Kreis [*Name des Kreises*], mit dem wir die Entgelte verhandeln müssen für den Bereich Jugendhilfe SGB VIII, da können wir nicht viel tun. Da gibt es im Grunde genommen feste Pauschalen für alles Mögliche und die werden auch nicht von uns festgesetzt, die werden ich glaube sogar auf LVR[51]-Ebene festgesetzt. Ich kann es Ihnen aber jetzt nicht … oder auf Landesebene … ich kann es Ihnen nicht ganz genau sagen, aber da können die Jugendämter auch nicht weit drüber weg. Das heißt also, da sind wir gedeckelt."

[…]

Interviewerin: Ist das dann ein Argument, also, dass Sie sagen, ‚Na ja, wir müssen Mitarbeitende schulen, wir brauchen neue Server, um die sicher zu machen, das kostet halt'?"

Expert:in: „Ja, das kann man in den Verhandlungen und bei den Diskussionen auch mit vorbringen. Aber meistens ist das ja pauschaliert. Dann heißt es ‚Okay, dann müsst ihr sehen, dass ihr das mit den Pauschalen auch abdeckt'. Also das wird dann schon ein Stück weit mit eingepreist, das ist ja meistens dann eher so der Bereich Overhead. Du kriegst einen Zuschuss, um Tablets anzuschaffen, dann gibt es immer noch ein bisschen was obendrauf für das ganze Drumherum."

[…]

Interviewerin: „Wer verhandelt denn bei Ihnen die Pauschalen? Macht es dann der DiCV? Wie funktioniert das in NRW?"

[51] Landschaftsverband Rheinland

Expert:in: „Also die Rahmenverträge werden bei uns von der LAG verhandelt, von der Landesarbeitsgemeinschaft der der freien Wohlfahrt. Und da sitzt dann auch der DiCV mit in den verschiedenen Gremien. Also wir haben ja keine übergeordnete Ebene nochmal über den Diözesen, sondern wir haben ja sechs Diözesen in NRW und die vertreten sich jeweils auch selber."

Beispiel 3: DiCV

Expert:in: „Also es gibt in unserem Bundesland nach meinem Kenntnisstand keine Refinanzierung für Digitalisierung im laufenden Geschäft. Wenn, dann für einzelne Digitalprojekte und die über die Kanäle von Bund und Land und in Einzelfällen. Die regelmäßige Refinanzierung von Aufgaben läuft entweder über Pflegesätze oder Zuschüsse und in Pflegesätzen werden Digitalkosten als Gemeinkosten, wenn ich sie ausweise, in der Regel nicht anerkannt. Wenn ich es geschickt mache, preise ich sie ein unter Sach- und Gemeinkosten, aber ich habe keine Position, unter der ich sie angeben kann. Im Kontext von Zuschüssen, da werden in jeder Kommune andere Vereinbarungen getroffen und da sind Gemeinkosten durchaus auch manchmal flexibler anerkennungsfähig, also da kann ich auch schon mal eine IT-Pauschale mit reinrechnen, aber das kann man jetzt nicht flächendeckend oder grundsätzlich sagen, sondern das hängt an den Verhandlungstraditionen, manchmal an dem Sachverstand der Verhandler vor Ort, an der Durchsetzungsfähigkeit, an der Art, wie ein Landkreis, ein Jugendamt, ein Sozialamt unbedingt will, dass ich die Leistung durchführe usw. Also das ist total individualisiert.

[…]

Ich sag mal, die Verhandlungen in so einer Pflegesatzverhandlung sind am Ende immer auch so eine Art türkischer Basar. Ich gehe mit einer Aufforderung rein, bekomme ein Gegenangebot und dann gibt es im Grunde Regelungen, die heißen ‚80 % Personalkosten, 20 % Sachkosten' oder ‚90 % Personalkosten, 10 % Sachkosten'. Und die werden jeweils nicht aufgeschlüsselt. Und das ist sozusagen Teil des Verhandlungsgeheimnisses oder Geschehens, ob da 3,1 oder 3,05 oder 4,37 rauskommt. Und da hat natürlich jede Seite sozusagen ihren Rechenmechanismus. Inzwischen gibt es zum Glück eine Anerkennung von tariflichen Steigerungen und da ist man, glaube ich, schon mal ganz froh, dass das gelungen ist. Seit ungefähr sechs oder sieben Jahren gab es ein Urteil des Bundesverwaltungsgerichts, glaube ich, dass tarifliche Steigerungen anerkennungsfähig sind, in der Pflege zu mindestens. Und das hat dann mal dazu geführt, dass zum Beispiel 80 % meiner Kostensteigerung durch die Personalkostensteigerung nicht diskutiert werden.

Jetzt sind die Mechanismen der Finanzierung natürlich komplex. Dann gibt es immer noch den sogenannten Investkostenanteil, also den Teil, wo auch Gebäude mitfinanziert werden usw. und exakte Vorgaben, was ist wo reinzurechnen, und ich sag mal der wird einmal fix verhandelt, da gibt es keinen Anteil für Digitalisierung. Bei den Gemeinkosten und Sachkosten rede ich dann im Zweifel über pauschale Kostensteigerung pro Jahr, weil ich die nicht dezidiert aufschlüssele. Und dann mache ich im Grunde einen Aufschlag von keine Ahnung, Inflation 2,5 %, dann rufe ich 2,5 % auf. Die andere Seite bietet, was auch immer, 1 % an und dann trifft man sich im Zweifel bei zwei und liegt sogar einen halben Prozent unter der Inflation. Und das meine ich mit türkischem Basar oder Verhandlungsgeheimnis. Also da gibt es auch sozusagen versteckte Kosten drin. Und es ist noch nicht gelungen, die notwendige Transparenz für alle Kosten herzustellen und auch auf einer Rahmenvertragsebene anzuerkennen, dass Kosten für Digitalprozesse eine Rolle spielen, würde ich jetzt mal sagen, sondern das sind im Grunde allgemeine Gemeinkosten, die über eine Abschreibung mitzufinanzieren sind."

Beispiel 4: Spitzenverband

Expert:in: Also an den *[Name des Kostenträgers]* bin ich herangetreten mit einer Bachelorarbeit. Dort hat eine Studentin eine Arbeit zum Thema Ressourcen oder Wirkungen und Einsparpotenziale durch digitale Tools geschrieben, den sogenannten Innovationsrechner entwickelt. Da war meine Argumentation so: Wenn ich den jetzt anwende, und sie hat das in verschiedenen Bereichen, das war, glaube ich, Küche, Verwaltung und Pflege angewendet. Wenn ich da jetzt ein Tool fix für das Haus Y nehme, was ist das für ein Vorteil für die Bewohner? Was haben die Mitarbeiter für Vorteile? Hat das Sozialamt Vorteile? Spart die Einrichtung was ein? Und da gibt es tatsächlich sogenannte Kompensationspotenziale. Und meine Argumentation war dieses Kompensationspotenzial umgerechnet in Vollzeitäquivalente. Also das möchte ich gerne nutzen, um nicht vorhandenes Personal durch Digitalität zu ersetzen, solange bis ich genug Personal habe, sprich, ich muss dann vielleicht kein Bett leer stehen haben, weil ich die und die und die Tools ansetze und damit so und so viel Personal sparen kann. Und dieses Geld, was ja für Köpfe im Pflegesatz ist, das möchten wir gerne behalten um es zweckgebunden dann zur Digitalisierung, zum Unterhalt der Digitalisierung, Schulung, Sicherheit oder auch Anschaffung Weiterentwicklung anwenden zu dürfen. Beim *[Kostenträger]* ist man der Meinung, dass man das aber alles erstmal wissenschaftlich evaluieren muss. Da habe ich denen gesagt, ‚Das können Sie alles gerne tun, aber geben Sie es trotzdem frei, weil wir haben nicht fünf vor zwölf, wir haben halb eins, also eigentlich haben wir die Zeit dafür nicht."

Beispiel 5: Spitzenverband

Expert:in: „Also, unser Verband ist mandatiert, Vereinbarungen (Leistungsvereinbarungen, Rahmenleistungsvereinbarungen, also solche Refinanzierungen) […] zu verhandeln und zu schließen. Das ist unser Brot-und-Butter-Geschäft, das ist das, was wir jeden Tag machen. […] Das ist ein unfassbarer Gremien-Hurz – also ich kann das anders echt nicht bezeichnen. Das ist eine total komplexe Gremienstruktur, auch deswegen, weil wir in der Regel im Schulterschluss mit den anderen Wohlfahrtsverbänden verhandeln, und da gilt Einstimmigkeitsprinzip. Das heißt, man muss die Caritasposition mit den anderen Verbänden der freien Wohlfahrtspflege abstimmen.

[…]

Wir verhandeln mit den Kostenträgern - so allgemein muss man es vielleicht sagen - über die Entgelte und über die Refinanzierung. In der Regel ist es so - und das kann man so allgemein tatsächlich schon sagen: Wir werden in der Regel finanziert auf Basis dessen, was wir brauchen. Also wir müssen plausibel darlegen, wie unsere Kostenstrukturen sind und diese Kostenstrukturen kriegen wir dann refinanziert. Das betrifft insbesondere natürlich das Personal. Aber es gibt eben auch eine Investitionskostenpauschale, einen Anteil an Invest, der im Kostensatz enthalten ist. Und dieser Investanteil, da fällt alles drunter, was Infrastruktur betrifft, und zwar von der Eingangstür bis zum Serverkeller, also die Häuser, die Abwasserkanalisation usw., Bürobedarf und eben IT, ist da mitabgebildet. Und es ist enorm schwierig das Thema IT da entsprechend abzubilden. Eines der Argumente ist zum Beispiel: ‚Was wollt ihr denn im Pflegeheim oder in dem Behindertenwohnheim? Die sitzen ja nicht alle am Computer. Wieso braucht ihr da drei Laptops? Es reicht doch einer im Büro der Pflegedienstleitung!'. Und dann kriegst du halt einfach die 2.500 €, die du für diese drei Laptops noch bräuchtest, nicht. Geschweige denn, dass man sagen könnte ‚Passt mal auf, wir haben echt ein Thema mit IT -Sicherheit, wir müssen unsere Systeme mal aufbohren. Wir sind eine große Einrichtung. Könnt ihr uns mal 3 Millionen Euro überweisen, weil wir brauchen neue Server und wir müssen das einrichten und wir müssen die Mitarbeiter schulen?' Dann sagen die ‚Nee, wir zahlen euch einen Beitrag und wenn ihr sowas habt und das braucht, dann seid ihr dafür verantwortlich. In der Leistungsvereinbarung steht drin, ihr bringt die Leistungen und da gehört das mit dazu. Also bitte: Macht mal!' Das sind tatsächlich so diese Argumentationsmuster, die da kommen."

Anhang 15: Zitate zur Unterrepräsentation von Frauen in den obersten Führungsebenen in Caritas-Organisationen

Auch wenn zum Entstehungszeitpunkt der Vorstand des Deutschen Caritasverbandes paritätisch besetzt ist, ist dies bei den ca. 6.200 Mitgliedsorganisationen weit weniger der Fall. Einem Gesamt-Frauenanteil unter allen Beschäftigten von 83 % stehen 23 % Frauen in den obersten Führungsebenen entgegen (Dihle 2021). In den Interviews thematisieren beide weiblichen Expert:innen ihren Sonderstatus als weibliche Vorständinnen. Diese Arbeit hat keine Genderfragen zur Grundlage, dennoch sollen die entsprechenden Auszüge aus den Interviews zumindest im Anhang einen Platz finden.

Auszug 1:

Expertin 1: „Ich habe ja vor zehn Jahren angefangen, auf der Führungsebene der Caritas zu arbeiten. Wenn ich mich da zurückerinnere, war ich da der bunte Punkt unter ganz viel grau-schwarz. Und weiß mehliert. Und männlich. […]"

Auszug 2:

Expertin 2: „Ich bin [in unserer Diözese] die erste Vorstandssprecherin. Bei Doppelspitzen ist es selbstverständlich, dass natürlich der Sprecher immer der Mann ist – obwohl die Caritas zu 80 % weiblich ist. Ich liebe meine Kollegen über alles, die sind toll, aber als ich da ankam in der Runde, war das Erste, was die mir sagten: ‚Aha. Sie sind also der Grund, warum wir nicht mehr Geschäftsführertreffen sagen dürfen'. Der Diözesan-Caritasdirektor hatte nämlich gesagt, jetzt wo eine Frau dabei sei, könne man die Runde nicht mehr Geschäftsführertreffen nennen. Das fanden die gar nicht lustig. Also, bei so etwas fängt das dann schon an und man muss schon um Akzeptanz werben. Es ist tatsächlich immer noch ein wenig schwierig. Wenn es wirklich um Macht und Entscheidungen geht, dann ist das schon sehr männlich strukturiert."

Interviewerin: „Das ist zwar ein gesamtgesellschaftliches Phänomen, aber ich denke, dass bei der Caritas noch mitreinspielt, dass sie an der katholischen Kirche dranhängt. In vielen Verbänden ist es auch noch normal, dass der Direktor ein Priester ist."

Expertin 2: „Ja, wenn der Vorstandssprecher schon kein Priester sein kann, dann muss es aber doch mindestens ein Mann sein, so ist die Hierarchie."

Ehrenwörtliche Erklärung

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbständig angefertigt habe. Die aus fremden Quellen direkt und indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde weder einer anderen Prüfungsbehörde vorgelegt noch veröffentlicht.

München, den 20. März 2025 Katharina Schlotthauer