PUKE

ERGEBNISBERICHT

Projekttitel: Projekt zur Unterstützung kritischer Einrichtungen (PUKE)
FFG-Projektnummer: FO999914212

Dieses Projekt wird finanziert im Sicherheitsforschungsförderprogramm KIRAS des Bundesministeriums für Finanzen (BMF) und durch die Österreichische Forschungsförderungsgesellschaft (FFG) abgewickelt.

Inhaltsverzeichnis

1. Einleitung

Nationale kritische Einrichtungen stellen einen besonders schutzbedürftigen Bereich der staatlichen Daseinsvorsorge dar. Aus diesem Grund wurde, aufbauend auf dem European Programme for Critical Infrastructure Protection (EPCIP), im Jahr 2008 das Austrian Programme for Critical Infrastructure Protection (APCIP) etabliert und 2014 weiterentwickelt (Bundeskanzleramt, 2015). Im Dezember 2022 wurde die Richtlinie über die Resilienz kritischer Einrichtungen (RKE-RL[1]) durch das europäische Parlament und den europäischen Rat beschlossen, welche einer nationalen Umsetzung in allen Mitgliedstaaten bedurfte. In Österreich erfolgte diese durch das Resilienz-kritischer-Einrichtungen-Gesetz (RKEG[2]), das am 16. Oktober 2025 verabschiedet wurde und seit 1. März 2026 in Kraft ist. Die RKE-RL stellt nicht mehr nur den Schutz einzelner Infrastrukturobjekte in den Mittelpunkt, sondern fordert einen umfassenden Resilienzansatz, der alle Gefährdungen umfasst und die Fähigkeit der Einrichtungen zur Aufrechterhaltung ihrer wesentlichen Dienste stärkt. Das vorliegende KIRAS-Projekt „Projekt zur Unterstützung kritischer Einrichtungen (PUKE)“, welches von November 2024 bis Ende Juni 2026 durchgeführt wurde, diente dazu das Bundesministerium für Inneres (BMI) bzw. die Direktion für Staatsschutz und Nachrichtendienst (DSN) bei der Umsetzung der RKE-RL und des RKEG wissenschaftlich zu begleiten und dabei die unterschiedlichen Perspektiven von Behörde, Wirtschaft und Wissenschaft bestmöglich zu integrieren, um die künftige Zusammenarbeit im Sinne der staatlichen Resilienz zu stärken.

Resilienz wird in der RKE-RL als „die Fähigkeit einer kritischen Einrichtung, einen Sicherheitsvorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Sicherheitsvorfall aufzufangen, zu bewältigen und sich von einem Vorfall zu erholen“ definiert (Art. 2 Nr. 2 Richtlinie (EU) 2022/2557). Auch Talbot und Jakeman (2009) definieren den Begriff Resilienz auf eine ähnliche Weise bzw. erweitern diesen: “A resilient organization is one that can achieve its core objectives, even in the face of adversity. It enables organizations to adapt and grow regardless of the exigencies, events, and risks within their operating environment” (S. 30). Als Sicherheitsvorfall wird in der RKE-RL ein Ereignis definiert, „das die Erbringung eines wesentlichen Dienstes erheblich stört oder stören könnte, einschließlich einer Beeinträchtigung der nationalen Systeme zur Wahrung der Rechtsstaatlichkeit“ (Art. 2 Nr. 3 Richtlinie (EU) 2022/2557). Da in der Richtlinie vor allem der Terminus kritische Einrichtungen zur Anwendung kommt, wird auch im vorliegenden Bericht dieser Begriff anstelle von kritischer Infrastruktur (KRITIS) verwendet.

[1] Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates. Amtsblatt der Europäischen Union, L 333/164. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2557.

[2] Bundesgesetz zur Sicherstellung eines hohen Resilienzniveaus von kritischen Einrichtungen (Resilienz kritischer Einrichtungen-Gesetz – RKEG), BGBl. I Nr. 60/2025

Das „Projekt zur Unterstützung kritischer Einrichtungen (PUKE)“, ist in vier Arbeitspakete (AP) gegliedert: AP01 – Projektmanagement, diente vor allem zur Organisation und Durchführung von Partner*innenmeetings, Work Group Meetings, einer Zwischenkonferenz, der Erstellung des Projektzwischen- und Endberichts sowie der Kommunikation mit der FFG. Im Arbeitspaket 02 (AP02) - Theoretische und empirische Grundlagen wurde, nach der Ausarbeitung des Standes der Wissenschaft und der Technik, der Status Quo in der Praxis erhoben. Zur Erfüllung des Art. 4 und Art. 10 der RKE-RL wurde im Stand der Wissenschaft ein systemisches Resilienz-Framework (SRF) als Grundlage für eine Operationalisierung organisationaler Resilienz konzeptualisiert, das gemeinsam mit den validierten Leitfäden (AP03) zur Umsetzung der Anforderungen Verhinderung von Sicherheitsvorfällen, physische Sicherheit, Abwehr und Bewältigung von Sicherheitsvorfällen, Fortsetzung und rasche Wiederaufnahme nach Sicherheitsvorfällen, Personelle Sicherheitsvorkehrungen sowie Sensibilisierung und Schulung des Personals gemäß Art. 13 Abs. 1 lit. a-f Richtlinie (EU) 2022/2557 sowie § 15 Abs. 2 RKEG als Input für eine nationale Resilienzstrategie und als Basis für organisationale Resilienzpläne dient. Das AP03 - Konzeption und Validierung fokussierte auf die Konzeption und Validierung dieser Leitfäden sowie validierten Empfehlungen für mögliche Vernetzungsformate. Im AP04 - Publikation und Dissemination wurden die Leitfäden als Handbuch publikationstauglich aufbereitet und bei einer abschließenden Fachkonferenz vorgestellt und diskutiert. Darüber hinaus wurde ein Policy Paper mit Empfehlungen zur Umsetzung von Vernetzungs- und Austauschformaten erstellt. Im vorliegenden Bericht werden die zentralen Projektergebnisse im Überblick beschrieben.

2. Stand der Wissenschaft

2.1. Aufgabenstellung und Kontext

Im Arbeitspaket zwei (AP02) wurde zu Beginn der Stand der relevanten theoretischen Konzepte (Stand der Wissenschaft), der jeweilige Ist-Stand der für dieses Thema relevanten Normen (Stand der Technik) sowie die gelebte Praxis in ausgewählten kritischen Einrichtungen (Stand der Praxis) erhoben, um die Ausgangslage für die Umsetzung der RKE-Richtlinie umfassend zu beschreiben. Die Auswahl und Reichweite der maßgeblichen Normen und weiterer Maßnahmen in der Praxis erfolgte über explorative, leitfadengestützte Expert*innen-Interviews, die Beschreibung der theoretischen Grundlagen der Resilienzkonzepte sowie dem Stand der Forschung basiert auf einer umfassenden Recherche in einschlägigen Publikationsdatenbanken. Hinsichtlich des Zeitraumes konzentrierte sich diese auf Studien, die die Großereignisse der jüngsten (europäischen) Geschichte – Flüchtlingskrise, Covid-Pandemie, Ukrainekrieg, Klimakrise bzw. Wetteranomalien - in ihren Ansätzen bereits berücksichtigen.

Dieser Bericht stellt – nach einer Beschreibung der spezifischen Aufgabenstellung – die Genese des Systemischen Resilienz-Frameworks (SRF) dar, das auf Basis des oben genannten Forschungsstandes für die Umsetzung der RKE-Richtlinie entwickelt wurde. Da dieses Framework einen intersektionalen und multitheoretischen Ansatz verfolgt, werden die einzelnen Elemente des SRF zunächst in ihrer Herleitung aus unterschiedlichen Kontexten beschrieben, im Zusammenhang mit der konkreten Aufgabestellung dieses Forschungsprojekt plausibilisiert und erst abschließend das vollständige Modell inklusive möglicher weiterer Operationalisierungen dargestellt.

2.1.1. Fokus RKE-Kompatibilität

Der Begriff Resilienz ist im Text der RKE-Richtlinie zentral und im Unterschied zu anderen wichtigen Begriffen wie Risiko, Risikobewertung, Sicherheitsvorfall, kritische Einrichtung etc. weniger prägnant definiert bzw. in ein semantisches Spektrum eingebettet, das einer Präzisierung bedarf. Daher fokussierte die Analyse der theoretischen Grundlagen auf den Begriff Resilienz. Die vorzunehmende Risikobewertung, die nach Art. 12 der Richtlinie ein wesentliches Element der Resilienzstrategie ist (Art. 12 Richtlinie (EU) 2022/2557), hängt inhaltlich sehr stark von dieser Resilienzdefinition ab.

Im gegenständlichen Forschungsprojekt wurden für den Stand der Wissenschaft drei zentrale Aufgabenstellungen formuliert:

1. Einen Beitrag zur Präzisierung, Differenzierung und Operationalisierung des Resilienzbegriffs, wie er in der RKE-Richtlinie verwendet wird (Art. 2. Nr. 2 Definition, Art. 4. Abs. 2 Resilienz-

Strategie, Art. 7. Abs. 1 Definition erhebliche Störung, Art. 10. Abs. 1 Unterstützung der Unternehmen, Art. 13. Abs. 1, Abs. 2 Maßnahmen und Resilienzplan) (Richtlinie (EU) 2022/2557) zu leisten, da der Begriff der Resilienz ursprünglich innerhalb der Psychologie und der Ökologie (Ökosoziologie) entwickelt wurde und sich seit etwa 30 Jahren in zahlreichen Wissenschaftsfeldern entfaltet: den Sozialwissenschaften, der Medizin, der Ökonomie, der Politikwissenschaft, der Management-Theorie, der Organisationsentwicklung, der Technik (Ingenieurwissenschaft) und der zivilen Sicherheitsforschung.

2. Eine Komplexitätsreduktion innerhalb dieser Theorielandschaft, um die Anwendbarkeit durch einen genuin für kritische Einrichtungen entwickelten Resilienzbegriff zu gewährleisten, ist daher eine darauf aufbauende weitere Aufgabenstellung.
3. Zudem wird ein Fokus auf die Unterstützungsmöglichkeiten der Einrichtungen gelegt, indem folgende Forschungsfragen beantwortet werden sollen: a) Wie können Leitfäden und Methoden zur Unterstützung der kritischen Einrichtungen gestaltet werden? b) Welche Formate eignen sich zur Überprüfung der Resilienz der kritischen Einrichtungen? c) Wie sollen geeignete Plattformen, die einen freiwilligen und rechtlich konformen Austausch von Informationen fördern, konzipiert und betrieben werden?

2.1.2. Paradigmatische Verschiebung als Ausgangslage

Nach Ansicht einiger Autoren (Scharte, 2021; Haas et al., 2022; Reckwitz, 2024) hat sich das Paradigma, innerhalb dessen die Untersuchungen zu Sicherheit und Resilienz angesiedelt sind, in den letzten Jahren von einem mechanistischen Ansatz (= stabil, robust, inflexibel), der noch vom „Kontroll- und Steuerungsoptimismus“ (Scharte, 2021) der 70-er und 80-er Jahre geprägt war, in Richtung eines systemischen Ansatzes (= anpassungsfähig, flexibel, lernend) verschoben. Vor allem jüngere Studien, welche die Erfahrungen der Covid-Pandemie und die aktuellen weltpolitischen Verwerfungen stärker berücksichtigen, betonen eine Akzentverschiebung von einer Welt, die durch das Akronym VUCA (Unkrig, 2021) gekennzeichnet wurde und durch die Faktoren volatility, uncertainty, complexity und ambiguity bestimmt war, in Richtung einer nochmaligen Verschärfung, in der aus Flüchtigkeit (volatility) Brüchigkeit wird, aus Unsicherheit Angst, aus Komplexität reihenweise unvorhergesehene „nicht-lineare“ Ereignisse resultieren und aus Ambiguität eine Art von Unerkennbarkeit oder Unlesbarkeit der Verhältnisse wird (siehe Abb. 1).

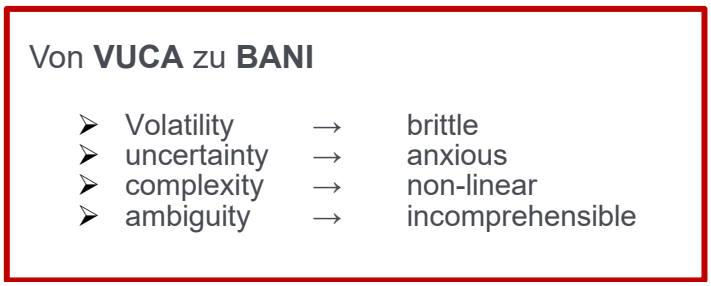


Abbildung 1: Akzentverschiebung VUCA zu BANI

Quelle: eigene Darstellung, in Anlehnung an Haas et al. (2022)

Zum immer weniger vorhandenen Steuerungs-Optimismus formuliert Reckwitz (2024) in seiner letzten großen Studie über das weitverbreitete Gefühl des Verlusts an Lebenssicherheit, Berechenbarkeit und Zukunftsoptimismus aus soziologischer Sicht; „Trotz aller Bemühungen in Sachen Risikokalkulation und Präventionsmaßnahmen wird früher oder später etwas Entscheidendes verloren gehen – und dies wird immer wieder passieren. Zugleich geht Resilienz davon aus, dass man auf das Unvermeidliche in einer Weise vorbereitet sein sollte, dass trotzdem ein gedeihliches individuelles und kollektives Leben möglich ist“ (Reckwitz, 2024). Diese Einschätzungen sind, vor allem auf Grund des All-Gefahren-Ansatzes, der hier zum Tragen kommt und des breiten Spektrums von Gefährdungen, die von intentionalen Anlässen wie Terrorismus und Kriegen, über Weltgesundheitslagen bis zu Blackouts, katastrophalen Klimaereignissen oder Erdbeben reicht, auch im Kontext der RKE-Richtlinie maßgeblich.

Die überwiegende Mehrzahl der Forscher*innen (Holling & Gunderson, 2002; Lovins & Lovins, 2001; Edwards, 2009; Walker & Cooper, 2011; Flüter-Hoffmann et al., 2016; Wink, 2016; Hoffmann, 2017; Baumann, 2020; Duchek, 2020; Max & Schulze, 2021; Scharte, 2021; Schrems, 2021; Unkrig, 2021; Meyer, 2022; Fekete, 2022; Fathi, 2019; Pechlaner & Zacher, 2022; Schellinger et al., 2022; Haas et al., 2022; Röhe, 2022; Staab, 2022; Reckwitz, 2024) vertritt die Ansicht, dass aktuell, auf Grund der skizzierten Ausgangslage, nur mehr ganzheitliche Ansätze – multitheoretisch, interdisziplinär, multiskalierbar – geeignet sind. Multitheoretisch bedeutet in diesem Fall, dass auf Grund der Unterschiedlichkeit der Handlungsfelder von Einzelpersonen bis zu institutionellen Akteur*innen, die Thematik nur durch eine Kombination mehrerer Theorien und Modelle ausreichend erfasst werden kann. Intersektional meint hier, dass insbesondere für das breite Feld der kritischen Einrichtungen, die von der Lebensmittel- und Trinkwasserversorgung bis zur medizinischen Versorgung und dem Energiesektor reicht, nur ein Ansatz sinnvoll ist, der die systemische Vernetzung dieser Stakeholderlandschaft miteinbezieht. Multiskalierbar bedeutet, dass die aus einem systemischen Resilienzmodell resultierenden Maßnahmen, nur als ein abgestimmtes Maßnahmen-Bündel vorzustellen sind, das für einzelne Bereiche die jeweils spezifischen

Möglichkeiten der Skalierung und Messbarkeit berücksichtigt. Konkret bedeutet das, dass aus der Vielzahl an Theorien und Modellen für die Entwicklung eines Resilienzmodells, das genuin auf die Aufgabenstellung der RKE-Richtlinie und des gegenständlichen Forschungsprojekts zugeschnitten ist, vor allem drei Forschungsfelder berücksichtigt wurden:

- Psychologische Resilienzforschung (individuell, interpersonal, intrapersonal)
- Organisationale Resilienz (kollektiv, strukturell, intraorganisational)
- Systemische, regionale bzw. gesellschaftliche Resilienz (Wirtschaftsgeografie, Vernetzung, regionale bzw. nationale Dimension)

Die psychologische Resilienzforschung ist deshalb von Belang, weil hier die elaboriertesten Ergebnisse vorliegen und diese Forschungen bereits seit längerem unternommen werden. Alle Szenarien, die in Bezug auf Resilienz vorstellbar sind, haben es mit konkreten einzelnen Personen (als Angehörige, Kolleg*innen, Funktionäre, Führungskräfte) zu tun, deren personale Resilienzfähigkeit eine unabdingbare Voraussetzung für die Resilienz größerer Systeme darstellt.
Das Zentrum der Recherche und Modellentwicklung liegt im konkreten Vorhaben allerdings im Bereich der organisationalen Resilienz, weil sich der Fokus auf kritische Einrichtungen richtet und die Ansätze daher auf dieser Ebene operationalisiert und die Maßnahmen hier organisiert werden müssen. Die Forschungen zur organisationalen Resilienz sind weniger weit gediehen als jene zur personalen Resilienz. Es liegen aber, vor allem auch angetrieben durch die krisenhaften Ereignisse der vergangen fünf Jahre, ausreichend Ergebnisse vor, um diese im Rahmen des vorliegenden Forschungsprojekts zu nutzen.
Aus der Intention, die die RKE-RL bzw. das RKEG verfolgt, fehlt den meisten Analysen zur organisationalen Resilienz eine systemische Perspektive, welche die größere Stakeholderlandschaft – also nicht nur andere Unternehmen und Marktteilnehmer*innen – sondern auch die gemeinsame Zugehörigkeit zur Gruppe kritischer Einrichtungen, aber auch den Kontakt zur Verwaltung, zu regionalen und überregionalen Behörden und der jeweiligen Wohnbevölkerung bzw. Kund*innengruppe ins Auge fasst. Wobei die Vernetzung mit Kund*innen hier eine Beziehung über die Marktinteressen hinaus, im Sinne einer gemeinsamen Arbeit an resilienten Verhältnissen, meint. Als drittes Feld theoretischer Ansätze wurden daher auch Theorien und Modelle regionaler oder gesellschaftlicher Resilienz berücksichtigt.

2.2. Personale Resilienz

Ein wesentlicher und zugleich basaler Baustein jeder Art von Resilienz ist die personale Resilienz (Berndt, 2013; Heller, 2019; Kalisch, 2020; Schrems, 2021; Gruhl, 2014; Fröhlich-Gildhoff & Rönnau Böse, 2023). Darunter versteht man zunächst die Resilienz von Individuen in jeglicher Hinsicht, also eine bestimmte Art von Widerstandsfähigkeit gegenüber allen möglichen

Stressfaktoren oder Ereignissen, ob sich diese auf den Bereich persönlicher Beziehungen, die Gesundheit, das berufliche Umfeld oder das Mitbetroffen-sein von größeren gesellschaftlichen Krisen bezieht. Es wurde schon darauf hingewiesen, dass in diesem Bereich der Psychologie besonders reichhaltige Forschungsergebnisse vorliegen, die von da aus erst nach und nach in andere Forschungsfelder wie Sozialpsychologie, Arbeitsplatzforschung, Organisationsentwicklung, Ökologie, Sicherheitsforschung und Politikwissenschaft eingeflossen sind. Wesentlich ist für den Zusammenhang mit einem Resilienztyp, der die besonderen Verhältnisse der kritischen Einrichtungen einbezieht, dass die Wurzeln der Konzepte personaler Resilienz in der Gesundheitsforschung, konkret dem Konzept der Salutogenese (Antonovsky, 1997) liegen. Im Zentrum stehen hier kognitive und psychologische Elemente. Nach Antonovsky spielen für das individuelle Kohärenzgefühl, dem von ihm beschriebenen Begriff psychologisch-gesundheitlicher Resilienz, drei Komponenten eine wesentliche Rolle: Die Sinnhaftigkeit (meaningfulness) der Lebensumstände oder beruflichen Verhältnisse, deren Verstehbarkeit (comprehensibility) und deren Bewältigbarkeit (manageability). Der Fokus lag anfänglich sehr stark auf rationalen Motiven, da etwa die Sinnhaftigkeit in den dazu durchgeführten empirischen Studien auch über Berechenbarkeit oder der kategorialen Einordnung von Ereignissen bestimmt wurde (siehe Abb. 2).

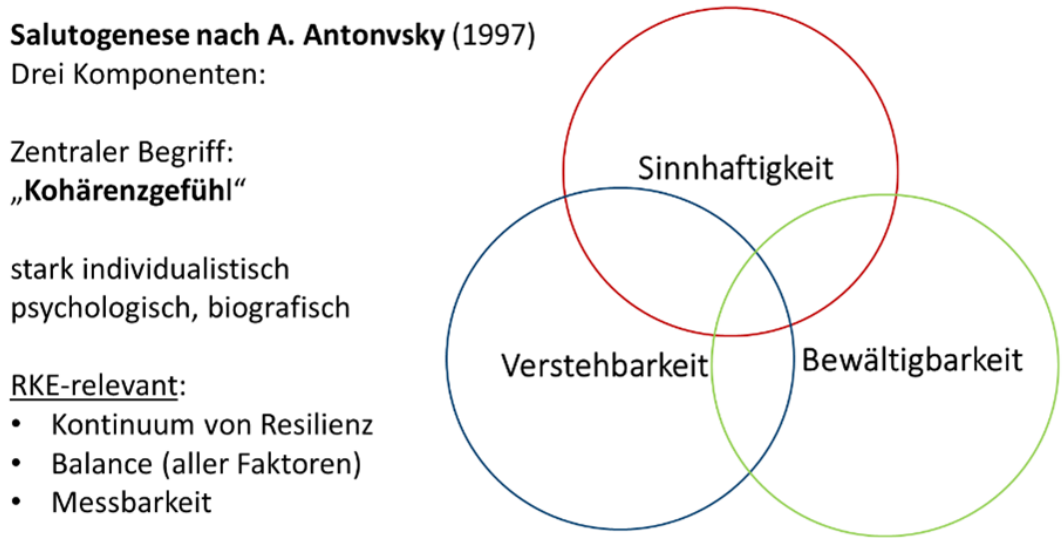


Abbildung 2: Grundlagen personale Resilienz
Quelle: Eigene Darstellung

Unter dem Kohärenzgefühl (sense of coherence) versteht die Salutogenese ein subjektives Gefühl dafür, wo man sich selbst in dem Kontinuum von Wohlsein und Kranksein (between ease and disease) befindet. Interessant ist dabei, dass dieses Kohärenzgefühl auf ein andauernd labiles Gleichgewicht bezogen ist, zu dem der Einzelne selbst etwas beitragen oder beizutragen lernen

kann. Gleichwohl wurde dieser Ansatz von Anfang an durch quantitative Ergebnisse, die aus einem ausführlichen Frageprogramm abgeleitet wurden, gestützt. Resilienz wird hier als ein Kontinuum verstanden, als eine Balance, die auf Grund dauernder Gefährdungen laufend gefunden werden muss. Die Messbarkeit der Resilienzfaktoren wurde in den weiteren Forschungen zur personalen Resilienz aufgegriffen.

Unter den zahlreichen Modellen personaler Resilienz fasst das 7+3-Modell (Schrems, 2021) jene Faktoren zusammen, auf welche sich die meisten Forscher*innen einigen können (siehe Abb. 3):

- Dieses Modell nennt als erste Qualität Akzeptanz. Gemeint ist damit eine situative Akzeptanz, also das Wahrnehmen und Realisieren des Geschehens, was die Herausforderung ist bzw. auch, dass eine Herausforderung (Gefährdung, Krise, Katastrophe) vorliegt.
- Die nächste Qualität wird als Zuversicht beschrieben und meint eine persönliche, auch in entmutigenden Situationen vorhandene, Haltung des Optimismus im Gegensatz zu resignativen Haltungen.
- Selbstwirksamkeit zielt auf die individuelle Handlungsfähigkeit aus eigenen Motiven und Einschätzungen und das Vertrauen auf die eigene Kompetenz, die gerade auch in herausfordernden Situationen zum Tragen kommt. Das Konzept ist seit den 70er Jahren Gegenstand intensiver Diskussionen und Forschungen zur Persönlichkeits- und Sozialpsychologie (Bandura, 1977).
- Mit dem Terminus Eigenverantwortung wird nicht nur auf die Fähigkeit hingewiesen, die Verantwortung für persönliche Belange zu übernehmen, sondern diese auch auf die Bewältigung umfassender Herausforderungen auszuweiten.

Die drei weiteren Faktoren sind stärker auf soziale Systeme bezogen, obwohl das hier noch nicht in demselben Ausmaß der Fall ist, wie in den Modellen organisationaler Resilienz.

- Netzwerkorientierung meint die Fähigkeit, andere Akteur*innen wahrzunehmen, Kontakte aufzubauen, zu pflegen und sich in den eigenen Handlungen in einer kooperativen Abstimmung mit anderen (Einzelnen, Gruppen, Einheiten, Hierarchien) zu bewegen.

- Die Lösungsorientierung bezeichnet auf dem Feld kollektiven oder institutionellen Handelns dasselbe wie Zuversicht und Selbstwirksamkeit auf individueller Ebene. Sie zielt daher im Sinne der Resilienz-Phasenmodelle, aber auch des salutogenetischen Ansatzes, grundsätzlich auf Bewältigung, Erholung und Lernen. Letztere Aspekte werden noch einmal durch das Stichwort Zukunftsorientierung akzentuiert.

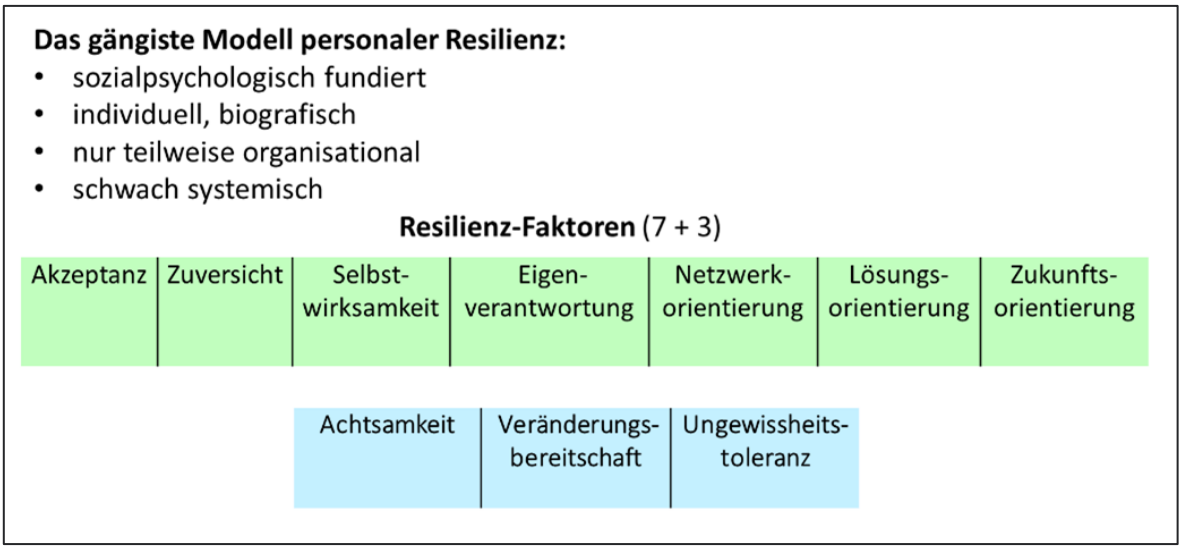


Abbildung 3: Modell Personale Resilienz
Quelle: Darstellung nach Schrems (2021)

Die drei zusätzlichen Faktoren, die in einer Reihe von Modellen auch unberücksichtigt bleiben, bringen in den Begriffen Achtsamkeit, Veränderungsbereitschaft und Ungewissheitstoleranz zusätzliche Qualitäten zum Ausdruck, die den Fokus auf das soziale Miteinander (Kommunikation, Anerkennung, Respekt) legen und berücksichtigen die in der RKE-Richtlinie skizzierte Situation, wonach die ständigen und vielfältigen Bedrohungslagen keinen Anlass für ein falsches Sicherheitsgefühl und das Verharren in erstarrten Reaktionsmustern geben.

Für den Zusammenhang zur gegenständlichen Forschung ist daher festzuhalten:

- Personale Resilienz ist eine unabdingbare Voraussetzung für alle weiteren und umfassenderen Formen von kollektiven oder organisationalen Formen von Resilienz. Insbesondere die Erfahrungen der Covid-Pandemie haben gezeigt, dass Ausfälle auf personaler Ebene durch strukturelle oder organisatorische Maßnahmen nur schwer wettzumachen sind.
- Die Modelle personaler Resilienz sind überwiegend auf subjektive und biografische Herausforderungen fokussiert. Die hier genannten individuellen Qualitäten sind unverzichtbar, aber im organisationalen Kontext nur adaptiert anwendbar.
- Der Beitrag der einzelnen Mitarbeiter*innen zur Resilienz von Teams und der Gesamtresilienz des Unternehmens muss daher systemisch an den richtigen Stellen berücksichtigt und organisatorisch eingebunden werden.

- In den Modellen personaler Resilienz fehlen zudem weitgehend die größeren systemischen Perspektiven (Stakeholder, Kommunen, Regionen, Gesellschaft), die für kritische Einrichtungen zusätzlich berücksichtigt werden müssen.

Dieses Ergebnis motiviert eine weitere Recherche im Bereich der Modelle, die für kollektive Systeme und die organisationale Resilienz entwickelt wurden.

2.3. Organisationale Resilienz: Phasenmodelle und zeitliche Dimension

Der folgende Ansatz führt auf der Suche nach einem RKE-kompatiblen Modell von Resilienz zu einem ersten heuristischen Modell (siehe Abb. 4), das versucht, das Zusammenspiel aller wesentlichen Elemente zu beschreiben. Das Modell hält folgende maßgebliche Faktoren fest: eine dreifache zeitliche Differenzierung, die die Phasen der Antizipation, der Bewältigung oder Beantwortung und der Anpassung bzw. des Lernens umfasst und die zugleich mit konkreten Fähigkeiten korreliert, die in allen Phasen notwendig sind. Es liefert zudem eine systemische Perspektive, die personale Resilienz, die Resilienz von Teams, die Resilienz der Gesamtorganisation und die systemische Vernetzung in das ökonomische, administrative und gesellschaftliche Umfeld der Organisation (Einrichtung) zeigt. Die Dimension der Maßnahmen ist in diesem Modell noch nicht inhaltlich festgelegt und lediglich durch die Begriffe Technik, Sicherheit und Organisation benannt, die auch in Art. 13 der RKE-RL angeführt werden.

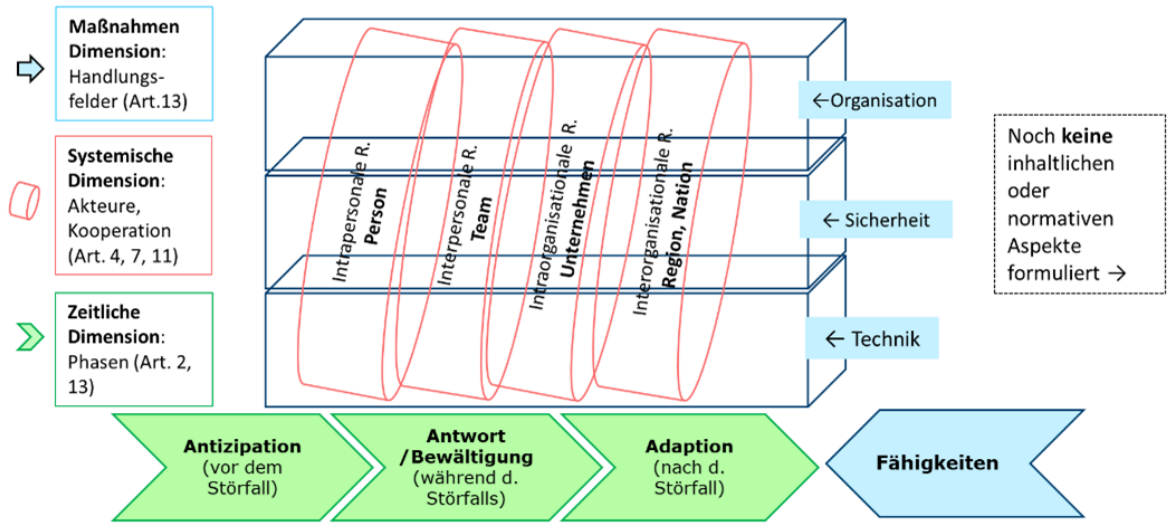


Abbildung 4: Heuristisches Resilienzmodell - RKE-kompatibel

Quelle: eigene Darstellung (Januar 2025)

Hinsichtlich der Zweckmäßigkeit einer zeitlichen Skalierung von Resilienzmodellen herrscht, trotz zum Teil unterschiedlicher Terminologie, weitgehend Konsens (Flüter-Hoffmann et al., 2018; Unkrig, 2021; Meyer, 2022; Haas et al., 2022). Das Drei-Phasenmodell – fallweise auch als Fünf-Phasen-Konzept entfaltet – ist am häufigsten zu finden und liegt sehr wahrscheinlich auch den Definitionen der RKE-Richtlinie zu Grunde (siehe Abb. 5). Es bietet den Vorteil, in jeder Phase auf spezifische Aspekte und Aufgabenstellungen fokussieren zu können. Im Sinne der Richtlinie liegt der Fokus der letzten Phase stärker auf Anpassung bzw. Erholung als auf Transformation. Ein Blick auf eines der gängigen mehrdimensionalen Modelle (Duchek, 2020) veranschaulicht auf einen Blick die Komplexität der Faktoren, die hier integriert sind.

Drei Phasen nach Duchek (2020)
Capability-Ansatz:

Kombination von zeitlicher Dimension mit **Handlungsweisen** und unterschiedlichen Formen von **Ressourcen**.

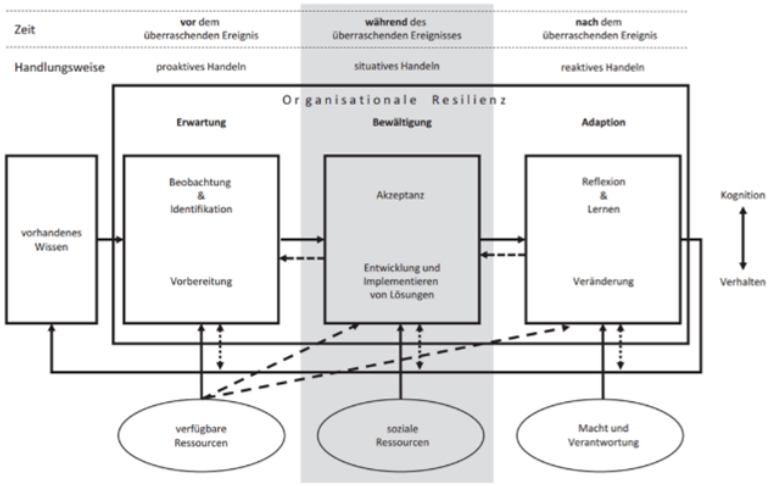


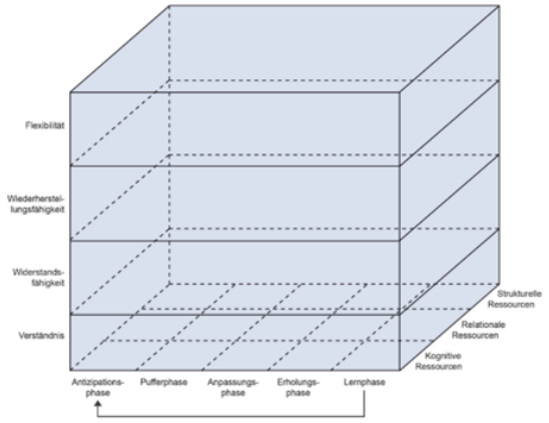
Abbildung 5: Drei-Phasen-Modell
Quelle: Darstellung nach Duchek (2020)

Die zeitliche Dimension gliedert sich in eine Phase vor dem Eintritt eines Ereignisses, eine Phase während des Ereignisses und eine Phase danach. Diese Phasen sind im Modell zudem mit Handlungsweisen korreliert, die als proaktiv, situativ und reaktiv beschrieben werden. Innerhalb des Handlungsfeldes der organisationalen Resilienz im engeren Sinn, werden die Aktionsweisen mit Erwartung, Bewältigung und Adaption markiert. Für die Operationalisierung des Modells ist dabei entscheidend, dass die Beschreibung der Handlungsfelder mit dem sogenannten Capability-Ansatz (Höfler, 2016; Nussbaum, 2015; Duchek, 2020) verknüpft wird, der konkrete Fähigkeiten benennt, die in den einzelnen Phasen relevant sind bzw. ausgebildet werden sollten. Für die Phase der Vorbereitung werden dabei Beobachtung und Identifikation (von Gefahrenquellen) genannt, für die Bewältigungsphase Akzeptanz bzw. das Entwickeln und Implementieren von Lösungen, für

die Phase der Veränderung Reflexion und Lernen. Das Modell veranschaulicht zudem eine Bewegung von kognitiven Aspekten zu Verhaltensweisen, die ihrerseits mit der Verfügbarkeit von Ressourcen korreliert sind.

Zum Teil finden sich auch komplexere Zeitmodelle, die insbesondere in sehr weitläufigen Handlungsfeldern, wie sie für kritische Einrichtungen, Verwaltungen oder ganze Regionen typisch sind, zusätzliche analytische Anhaltspunkte liefern. Innerhalb der zeitlichen Dimension wird in manchen Mehrebenenmodellen noch einmal zwischen Antizipation, Pufferphase, die sich auf die Widerstandsfähigkeit eines Systems bezieht, Anpassungsphase, Erholungsphase und Lernphase differenziert. Auch in diesem Modell ist ein enger Zusammenhang zwischen der Abfolge dieser Phasen und bestimmten Fähigkeiten vorausgesetzt, die diesen schrittweisen Durchgang auch tatsächlich ermöglichen (siehe Abb. 10). In jeder dieser Phasen ist auch ein Scheitern möglich: Man kann unvorbereitet von Ergeinissen getroffen werden, die Widerstandsfähigkeit kann sich als zu gering erweisen, die Anpassung nicht gelingen, die Erholung und der Lerneffekt ausbleiben.

Im Kontext der Resilienz von KRITIS, Verwaltungen, Kommunen und Regionen werden auch **komplexere Zeitmodelle** vorgeschlagen. Hier verknüpft mit dem **Ressourcen**-Aspekt.



Antizipation
↓
Pufferphase
↓
Anpassungsphase
↓
Erholungsphase
↓
Lernphase

Abbildung 6: Zeitliche Dimension: Fünf-Phasen-Modell
Quelle: Eigene Darstellung, in Anlehnung an Flüter-Hoffman et al. (2018)

In den Konzepten der organisationalen Resilienz, die sehr häufig Unternehmen im Kontext von Marktrisiken im Auge haben, werden Krisen immer wieder mit der Gelegenheit zu einer Transformation bestehender Strukturen und Prozesse in Verbindung gebracht (siehe Abb. 2). Im Sinne der Antifragilität trachtet man danach, Krisen nicht nur zu überleben, sondern gestärkt daraus hervorzugehen. Diese Einschätzung teilt die RKE-Richtlinie nicht, oder nicht in demselben Ausmaß. Der Fokus liegt dort eindeutig auf einer Wiederaufnahme der wesentlichen Dienste und nicht auf einer großen Transformation der bestehenden Einrichtungen. Aufrecht bleibt allerdings

das Ziel, aus Vorfällen zu lernen und in diesem Sinn die Möglichkeit, eine ständige Optimierung zu intendieren.

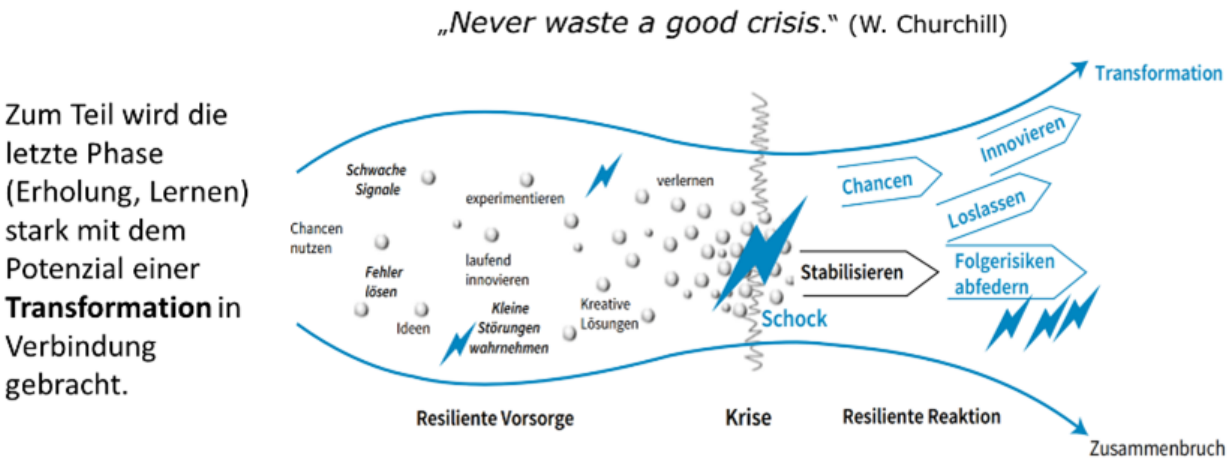


Abbildung 7: Zeitliche Dimension: Transformation durch Krise
Quelle: Eigene Darstellung in Anlehnung an Haas et al. (2022)

2.3.1. Phasenmodel und Capability-Ansatz: Fähigkeiten, Kompetenzen, Potenziale

Im Zusammenhang mit der gegenständlichen Analyse ist maßgeblich, dass eine Reihe von Autor*innen (Hollnagel et al., 2006; Lorenz, 2013; Hoffmann, 2017; Folkers, 2018; Röhe, 2022) das Phasenmodell auch mit dem Capability-Ansatz verknüpfen und für die einzelnen Phasen bestimmte Fähigkeiten oder Potenziale beschreiben, die vorhanden sein oder ausgebildet werden müssten, um im Sinne einer Gesamtresilienz über die Gesamtdauer eines Sicherheitsvorfalls samt Folgen aktiv gestaltend zu bleiben. Die häufig synonym verwendeten Begriffe wie Fähigkeit, Kompetenz, Potenzial sind in allen Definitionen von Resilienz zentral und beziehen sich auf personale bis zu umfassenden systemischen Ebenen. In diesem Sinne wird unter dem Begriff Resilienz Folgendes verstanden:

> "Resilience is the capacity of a social-ecological system to absorb or withstand perturbations and other stressors such that the system remains within the same regime, essentially maintaining its structure and functions. It describes the degree to which the system is capable of self-organization, learning and adaptation." (Resilience Alliance, 2016 zit. nach Hoffmann, 2017, S. 65)

Im Kontext von Resilienzansätzen, die über engere interpersonale Beziehungen hinausgehen und größere Einheiten wie jene der kritischen Einrichtungen betreffen (obwohl auch hier die Anzahl der Mitarbeiter*innen stark schwankt) kommen Capability-Konzepte in Betracht, die für organisationale und soziale Kontexte entwickelt wurden. Eine wesentliche Perspektive hält Lorenz (2013) fest, in dem er Anpassungs-Potenzial (adaptive capacity), Bewältigungs-Potenzial (coping capacity) und Partizipations-Potenzial (participative capacity) unterscheidet, die für die systemische Vernetzung

von Unternehmen bzw. Einrichtungen mit ihrem jeweiligen regionalen und gesellschaftlichen Umfeld eine Rolle spielen.

Aus der Vielzahl an Entwürfen zu einem Resilience Engineering kommt der Ansatz Hollnagels den Bedürfnissen eines RKE-kompatiblen Modells für kritische Einrichtungen am ehesten entgegen. Hier werden – stärker an Performanz als an Prozessen orientiert – vier Fähigkeits-Ebenen unterschieden:

1. Antwortpotenzial: „Unter Antwortpotenzial (potential to respond) ist die Aktivierung von vorbereiteten Handlungen zu verstehen. Vorbereitung ermöglicht es demnach, auf mehr oder weniger erwartbare Veränderungen im Umfeld zu reagieren, und mehr noch: Gelegenheiten zu erkennen und nützen zu können."
2. Beobachtungspotenzial: „Das Beobachtungspotenzial (potential to monitor) beschreibt das Wissen darüber, was unmittelbar und kurzfristig Auswirkungen auf die Performance des Unternehmens haben könnte und wie dies zu beobachten ist. Das System der Beobachtung muss sowohl die eigene Leistung als auch Entwicklungen im Umfeld effektiv beobachten können, um verlässliche Aussagen über mögliche positive oder negative Auswirkungen zu erhalten."
3. Lernpotenzial: „Mit Lernpotenzial (potential to learn) ist die Fähigkeit gemeint, aus gemachten Erfahrungen die richtigen Lehren zu ziehen. Es geht um die Erfassung der Entstehungsbedingungen und um die kritische Analyse der getroffenen Maßnahmen einer spezifischen Situation, um Verbesserungspotenziale heben zu können."
4. Antizipationspotenzial: „Wie schon beim Antwortpotenzial deutlich wurde, braucht es relativ konkrete und präzise Vorstellungen von der Zukunft und den damit einhergehenden Herausforderungen. Das Antizipationspotenzial (potential to anticipate) meint also die Fähigkeit, zukünftige Entwicklungen gut einzuschätzen. Das reicht von möglichen Erschütterungen über eine sich verändernde Nachfrage bis hin zu möglichen Gelegenheiten" (Hollnagel et al., 2006 zit. nach Hoffmann, 2017, S. 77f.).

Dieser Ansatz wird in etwas anderer Reihenfolge und angelehnt an zeitliche Perspektiven ein integraler Bestandteil des im Vorhaben entwickelten Systemischen Resilienz-Framework (SRF) sein.

2.3.2. Die zeitliche Dimension in der RKE-Richline

Eine Analyse der Kurzdefinition von Resilienz wie sie in Art. 2. der Richtlinie vorliegt – „Resilienz ist die Fähigkeit einer kritischen Einrichtung, einen Sicherheitsvorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalles zu

begrenzen, einen Sicherheitsvorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen“ (Art. 2 Nr. 2 Richtlinie (EU) 2022/2557) – zeigt, dass auch hier ein zeitliches Modell zu Grunde liegt, das am ehesten mit den Begriffen protect, respond, recover (Walker, 2004; Röhe, 2022) beschrieben werden kann. Zentral ist auch in dieser Definition, dass Resilienz hier als Fähigkeit aufgefasst wird. In dem für die gegenständliche Forschung maßgeblichen Abschnitt aus Art. 13. Abs. 1 Richtlinie (EU) 2022/2557 erfolgt die Darstellung der notwendigen Maßnahmen ebenfalls in einer akzentuiert zeitlichen Perspektive. Man kann die Maßnahmen nach lit. a und b Verhinderung von Sicherheitsvorfällen und angemessener physischer Schutz zur Phase der Vorbereitung zählen, die Maßnahmen nach lit. c Reaktion auf Sicherheitsvorfälle zur Phase der Bewältigung und die Maßnahmen aus lit. d Wiederherstellung nach Sicherheitsvorfällen (Art. 13. Abs. 1 Richtlinie (EU) 2022/2557) zur Phase des Lernens. Die in lit. e und lit. f genannten Maßnahmen, die sich auf Sicherheitsmanagement und Schulungen beziehen, gehen – weil stark personalbezogen – über alle Phasen. In Art. 7 und 12 der Richtlinie wird ausdrücklich darauf hingewiesen, dass bereits erarbeitete Elemente der innerbetrieblichen Sicherheitsarchitektur, also Zertifizierungen, Risikobewertungen, Risikomanagement, Krisenpläne, Krisenmanagement, Business-Continuity-Management, integraler Bestandteil der geforderten Resilienzstrategie sein sollten (Art. 7, Art. 12 Richtlinie (EU) 2022/2557). Die zeitliche Perspektive der gängigen Modelle bietet die Möglichkeit, diese bereits vorbereiteten Elemente in einer Gesamtstrategie (Stichwort: Resilienzplan) zu verorten.

Eine zeitliche Strukturierung des Phänomens wird nach dem derzeitigen Stand der Forschung allerdings kritisch gesehen, weil das Phasenmodell, das deskriptiv plausibel erscheint, für eine wirkliche Operationalisierung auch Kriterien benennen müsste, die die unterschiedlichen Phasen beschreiben. Weiters müsste ersichtlich sein, wie lange sie dauern könnten, oder welche bestimmten Bedingungen vorherrschen werden. Es wird darauf hingewiesen, dass sich Phasen im Katastrophenfall stark beschleunigen können und jede Katastrophe ihre eigene Zeitcharakteristik hat (Duchek, 2022; Meyer, 2022). Auch ist es sinnvoll zu berücksichtigen, dass unterschiedliche Phasen ineinander spielen können.

2.4. Modelle zu organisationalen Resilienzfaktoren

Die Modelle organisationaler Resilienz (McManus et al., 2007; Lengnick-Hall, 2011; Weick & Sutcliffe, 2016; Hoffmann, 2017; Gulas & Katzmair, 2018; Draht, 2018; Brunnermeier, 2021; Kleemann & Frühbeis, 2021; Unkrig, 2021; Meyer, 2022; Röhe, 2022) fußen sehr häufig auf den Konzepten und empirischen Ergebnissen personaler Resilienz, sie unterscheiden sich aber stark hinsichtlich ihres Differenzierungsgrades. Nachstehend sind die wichtigsten Ansätze dargestellt, die für die Konzeption eines Systemischen Resilienz-Frameworks (SRF) hilfreich sein können. Die Ansätze zur organisationalen Resilienz liefern nicht nur Beschreibungen von Strukturmerkmalen

und Aufgabenfeldern, sondern entwickeln auch normative Vorschläge, welche Prozesse einzuhalten und welche Ziele zu erreichen sind. Diese Vorschläge sind für eine Operationalisierung in unserem Kontext unterschiedlich gut geeignet, die Frage der Messbarkeit von Resilienzkriterien stellt eine besondere Problematik dar, sie sind aber geeignet, das vorgeschlagene RKE-kompatible Modell durch inhaltliche Aspekte zu konkretisieren.

Nach einer vergleichsweise einfachen Beschreibung der Dimensionen organisationaler Resilienz nach McManus (2007) werden folgende Faktoren festgehalten.

- Situationsbewusstsein (z.B. Fähigkeit, Krisen auch positiv wahrzunehmen)
- Umgang mit organisationalen Schlüsselstellen (z.B. Infrastruktur, aber auch Beziehungen zwischen Funktions- und Organisationseinheiten)
- Anpassungsfähigkeit (z.B. Führung und Entscheidungsstrukturen, Kreativität und Flexibilität)

Diese Auflistung weist bereits darauf hin, dass in diesen Ansätzen Faktoren personaler Resilienz in Qualitäten und Kompetenzen transformiert werden, die nicht nur im Kontext von Organisationen Sinn machen, sondern die auch organisiert, d.h. gesichtet, sinnvoll gebündelt und zugeordnet werden müssen. Weick und Sutcliffe (2016) sprechen in diesem Zusammenhang vom „achtsamen Organisieren“ und nennen dabei fünf Prinzipien:

- Konzentration auf Fehler
- Abneigung gegen Vereinfachungen
- Sensibilität für betriebliche Abläufe
- Streben nach Resilienz
- Respekt vor Expertise

Der Schwerpunkt dieses und ähnlicher Ansätze liegt stärker im Bereich der Prävention bzw. Antizipation. „Eine Form des Organisierens, die Prozesse zu fünf Schwerpunkten / Prinzipien integriert, lässt Ausfälle erkennbarer werden. Diese Prozesse stellen zwar einen aufwändigen Weg dar, um zuverlässige Leistung aufrechtzuerhalten, doch Arbeiten zu High Reliability Organizations (HROs) zeigen, dass genau diese aufwändigeren Prozesse Ausfälle schon in früheren Entwicklungsstadien offensichtlicher machen“ (Weick & Sutcliffe, 2016, S.3).

Lengnick-Hall (2011) unterscheiden hinsichtlich der organisationalen Resilienz zusätzlich kognitive, verhaltensmäßige und kontextuale Elemente. Die kognitiven Elemente beziehen sich auf gefestigte Werte, Visionen und einen Meinungsaustausch mit flachen Hierarchien, während das Verhalten sich zwischen Polen von Kreativität und routinemäßigem Handeln bewegt. In unserem Kontext ist hervorzuheben, dass in diesem Ansatz auch Bedingungen von Resilienz genannt werden,

in welchen die stärker konstruktiven Schritte deutlicher im Vordergrund stehen. Genannt werden ein geteiltes Sicherheitsgefühl, das innerhalb von Teams und Organisationen erst geschaffen werden muss, weiters ein respektvoller Umgang mit subjektivem Sicherheitsgefühl, eine diesbezügliche Vernetzung innerhalb und außerhalb der Organisation und eine strategische Personalentwicklung, um derartige Prozesse systematisch zu entwickeln. Diese Bedingungen weisen auf die Entwicklung einer Art von Sicherheitskultur in Unternehmen und Einrichtungen, die in der Breite, d.h. auf allen Mitarbeiter*innenebenen wirksam wird (Körmer et al., 2024). Dieser kulturelle Ansatz findet sich auch in anderen Modellen organisationaler Resilienz.

In einigen Ansätzen (Gulas & Katzmair, 2018; Meyer, 2022) wird darauf Bezug genommen, dass Resilienz immer schon auf Bedingungen aufsetzt – also etwa eine bestimmte Unternehmenskultur, vielleicht sogar einer Sicherheitskultur oder spezifischen Ressourcen. In diesem Sinn wird zwischen aktiven und passiven Resilienzfaktoren unterschieden, die auf unterschiedlichen Ebenen angesiedelt sind, die mehr oder weniger leicht zu verändern sind. Dieser Aspekt scheint deshalb als besonders praxistauglich, weil er den zeitlichen Aspekt einer Transformation von Unternehmen in Richtung Resilienz berücksichtigt (siehe Abb. 8).

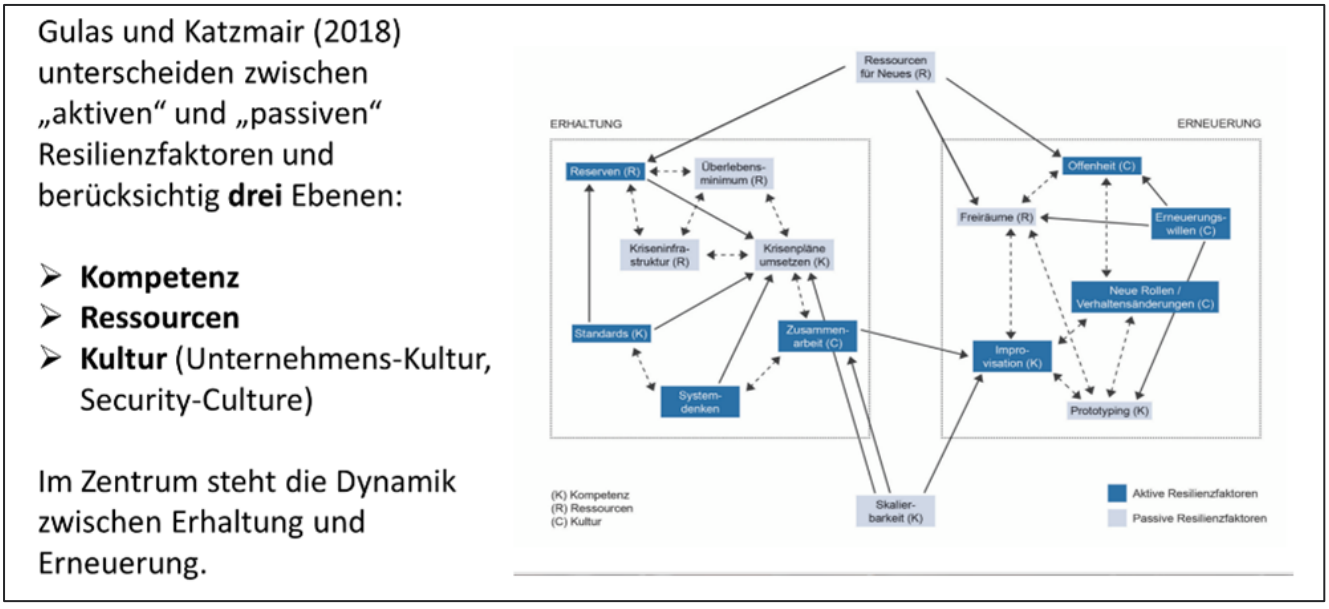


Abbildung 8: Resilienzfaktoren
Quelle: Darstellung nach Mayer, 2022

Im Kontext der gegenständlichen Recherche ist entscheidend, dass Resilienz als etwas verstanden wird, das durch das Zusammenspiel oder besser eine Kooperation unterschiedlicher Fähigkeiten, Bedingungen und Akteur*innen entsteht. Hoffmann (2017) schreibt dazu „Resilienz ist nicht einfach vorhanden, sondern entwickelt sich über die Zeit als Emergenzprodukt aus

Potenzialen, Kompetenzen und Performanzen von Individuen, Gruppen, Abteilungen und der Gesamtorganisation. Das Resilienzpotenzial einer Organisation ist als ein kollektives zu verstehen, das in Wechselwirkung zwischen der Ebene der Individuen, intersubjektiven Milieus, der Ebene der Organisation als soziales System und quer über die Ebenen generiert wird“ (Hoffmann, 2017, S. 86).

Neben der Unterscheidung von Potenzialen, Kompetenzen und Performanzen halten wir auf der Suche nach einem Modell, das für die spezifische Situation von kritischen Einrichtungen geeignet ist, fest, dass auf organisationaler Ebene Individuen, Gruppen, Abteilungen und Gesamtorganisation unterschieden werden. Damit ist auf Teams und kleine Einheiten, als einem wichtigen Zwischenglied zwischen der personalen Resilienz von Individuen bzw. einzelnen Mitarbeiter*innen und der Gesamtorganisation hingewiesen. Nach den Erkenntnissen der Arbeitsplatzforschung (Giesert et al., 2012; Treier, 2016; Giesert & Reuter, 2017) repräsentieren (Arbeits-)Teams die maßgeblichen sozialen Einheiten, in welchen die oben genannten Faktoren wie psychologische oder geteilte Sicherheit, Verlässlichkeit, offene Kommunikation und respektvoller Umgang zunächst spürbar werden. Das Modell systemischer Resilienz hält daher daran fest, dass – ganz besonders im Fall großer Unternehmen mit einer großen Anzahl von Mitarbeiter*innen – unbedingt zwischen der Ebene der personalen und jener der gesamtorganisationalen Resilienz auch die Ebene der Teams und kleinen Einheiten zu berücksichtigen ist. Plausibel ist, dass es für jede Form organisationaler Resilienz, neben den bereits erwähnten Aspekten, auch eine Art von kollektiver Zielsetzung und einer Identifikation mit diesen Zielen, eine Art von kollektivem sensemaking (Hoffmann, 2017) geben muss, wenn sich Resilienz über den personalen Bereich hinaus auf Teams und Unternehmen erstrecken soll. Stellvertretend für eine Reihe ähnlicher Versuche sei hier auf das Modell verwiesen, das Unkrig (2021) zur interpersonalen Resilienz vorgestellt hat (siehe Abb. 9).

Abbildung 9: Interpersonale Resilienz
Quelle: Darstellung nach Unkrig (2021)

Demnach ist der innere Kreis durch drei Arten von Faktoren bestimmt, die sich auf Individuen, Teams und das System insgesamt beziehen. In einem weiteren Kreis sind sieben Zielvorstellungen genannt, die allesamt darauf zielen, Qualitäten, die Resilienz fundieren, zu vergemeinschaften bzw. als kollektive Faktoren zu etablieren. Unkrig nennt in diesem Entwurf gemeinsame Ziele, gemeinsame Zecke, starke und positive Beziehungen, kollektive Achtsamkeit, starke kollektive Identität, transaktive Gedächtnissysteme im Team, kollektive mentale Modelle und die Gabe zur kollektiven Improvisation.

Hier wird deutlich, was unter dem Generieren von Resilienz auf Team- und Organisationsebene gemeint ist, da die genannten Ziele so ambitioniert sind, dass man nicht davon ausgehen kann, dass sie in Unternehmen ohne weiteres schon erreicht sind. Kollektive Ziele und Zwecke müssen erarbeitet, kommuniziert und abgestimmt werden, starke positive Beziehungen müssen wachsen, kollektive Identitäten gebildet werden. Gemeinsame mentale Modelle und Gedächtnissysteme beruhen auf gemeinsamen Erfahrungen und Analysen und brauchen Zeit. Es liegt auf der Hand, dass einige dieser Bedingungen in den Unternehmen nur im Rahmen einer echten Sicherheitskultur schrittweise etabliert werden können. Nichtsdestotrotz ist die Berücksichtigung der kollektiven Dimension, die als konkrete Bedingungen, welche zu erfüllen oder zu deren Erfüllung innerbetrieblich Anstrengungen zu unternehmen sind, plausibel und in einer verdichteten Form auch operationalisierbar sind.

Das ist bei noch differenzierten Modellen wie dem ICOR-Modell weniger leicht vorstellbar, obwohl eine derartige Konzeption ebenfalls zu einer Konkretisierung der für die kritischen Einrichtungen notwendigen Resilienzbedingungen beiträgt. Dieses Modell stellt drei Dimensionen, neun Strategien und 16 Verhaltensweisen vor, in dem Elemente der personalen und kollektiven Resilienz kombiniert werden (siehe Abb. 10). Im Zentrum stehen individuelle Qualitäten und Verhaltensweisen – wie achtsam, respektvoll, ansprechbar oder kreativ – in einem zweiten Kreis, werden kollektive Qualitäten als Ziele angeführt. Beide Sphären sind eingebettet in organisationale Aufgabenfelder, die mit Führung & Strategie, Prävention & Risikomanagement und Kultur & Verhalten gekennzeichnet werden.

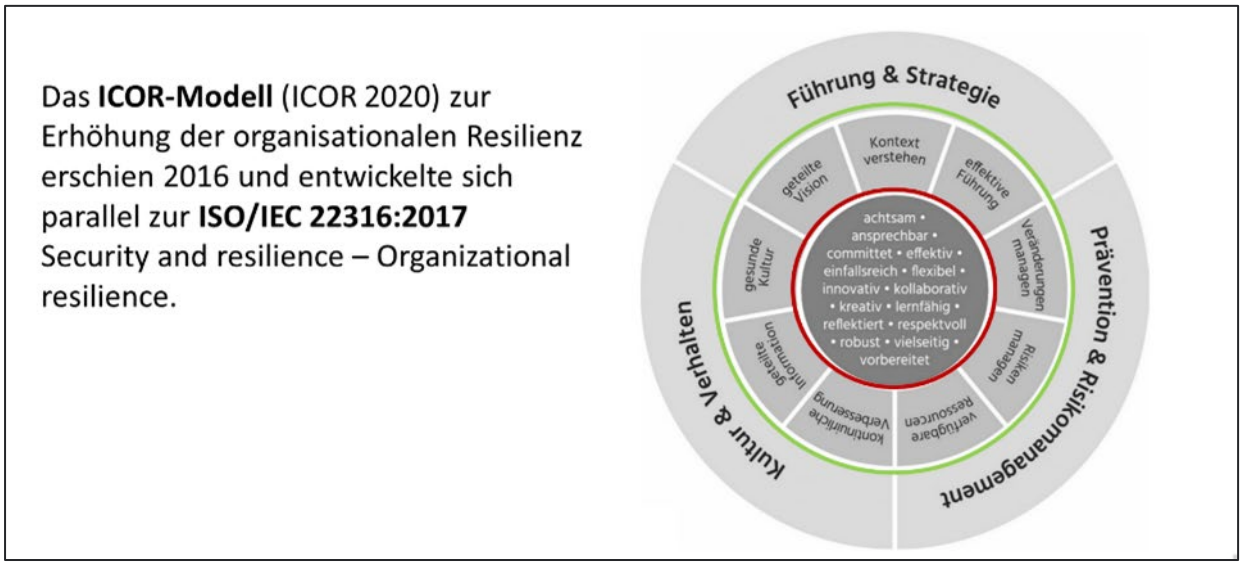


Abbildung 10: ICOR-Modell
Darstellung nach Unkrig (2021)

Operationalisierbarkeit der Kriterien organisationaler Resilienz

Wenn aus dem Blickwinkel der Aufgabenstellung des Projektes die Konzepte zur organisationalen Resilienz kritisch gesichtet werden, fällt auf, dass die meisten Modelle im Vergleich zu denen der personalen Resilienz zwar zusätzliche Differenzierungen einbringen, die Operationalisierbarkeit der Modelle jedoch abnimmt. Ihr Wert liegt stärker in einer deskriptiven Annäherung an das Phänomen Resilienz und zum Teil auch darin, ein probates Analyse-Tool zu liefern, das mithelfen kann, die Ausgangslage präziser zu bewerten.

Was die Messbarkeit und Operationalisierbarkeit der Faktoren organisationaler Resilienz anlangt, bestehen in der Forschung derzeit noch erhebliche Zweifel. Die entwickelten Kriterien werden eher als prinzipielle Haltungen oder als Beschreibung von wünschenswerten Attributen und Aktionen

gesehen. Die Vielfalt der Managementebenen, der Akteur*innen-Gruppen, der Sektionen erschwert eine einheitliche und präzise Skalierung.

Unkrig (2021) fasst seine Einschätzung zur Brauchbarkeit der ISO und ICOR-Modelle folgendermaßen zusammen:

> „Organisationen können nur mehr oder weniger belastbar sein. Der Standard nennt **kein absolutes Maß** und kein endgültiges Ziel in Bezug auf eine organisationale Resilienz. Ein erhöhtes Maß an Resilienz trägt dazu bei, dass Risiken und Schwachstellen besser antizipiert und angegangen werden können. Es geht um eine ganzheitlich verstandene organisationale Resilienz. Der Standard beschränkt sich nicht auf spezifische Betriebsmittel oder Aktivitäten wie IT oder Ausfallsicherheit der Lieferkette. Empfohlen wird eine Erweiterung im Denken, um den Einfluss der **(Unternehmens-)Kultur** auf die Resilienz zu berücksichtigen. Auch wird empfohlen, nicht nur ein Verständnis für den externen Kontext zu entwickeln, sondern auch für die **relevanten Fähigkeiten**, diesen zu beeinflussen.
>
> Resilienz ist **multidisziplinär**. Insofern spricht der Standard eine Vielzahl von Managementdisziplinen an, beispielsweise Business Continuity Management, Information Security Management, Finanzmanagement, Strategische Planung und Personalmanagement.
>
> Eine verbesserte organisationale Resilienz ist vor allem das Ergebnis eines effektiven Risikomanagements. Wenn es eine Strategie gibt, die Resilienz des Unternehmens zu erhöhen, muss dies durch die Implementierung eines wirksamen Risikomanagement-Rahmens und entsprechender Prozesse unterstützt werden. Hier bietet der Standard die Grundlage für ein robustes System organisationaler Resilienz.
>
> Der Standard ist **kein Zertifizierungsstandard**. Statt der üblicherweise mit ISO-Normen einhergehenden Zertifizierung liegt derzeit der Schwerpunkt (noch) auf **Prinzipien, Attributen** und **Aktivitäten**, die ein Unternehmen dabei unterstützen, seine Widerstandsfähigkeit zu verbessern.“ (Unkrig, 2021, S. 44, Hervorhebungen PUKE-Team)

In einer weicheren Form existieren Vorschläge (Röhe, 2022; Hunziker & Steiner, 2022; Perucca & Schellinger, 2022) zur Operationalisierung, die sich auf die bewährte Struktur des Policy-Cycle stützen und darstellen, wie sich Maßnahmen der organisationalen Resilienz in das Gesamtmanagement einer Einrichtung oder eines Unternehmens einfügen und, wo die Fragen nach Kosten, Aufwand und Verhältnismäßigkeit bzw. die Aufgaben einer kontinuierlichen Qualitätssicherung zu verorten sind.

2.5. Systemische Dimension – Resilienzsphären

Die Analyse der zu Grunde liegenden Konzepte zeigt, dass die RKE-Richtlinie auf Grund der strukturellen Besonderheit von Einrichtungen der kritischen Infrastruktur von an Anfang an einen systemischen Ansatz verfolgt. In Art 7 Abs. 1 der Richtlinie und § 11 Abs. 2 des RKEG wird dies in der Bestimmung des Ausmaßes einer Störung deutlich, wo folgendes berücksichtigt werden sollte:

a. „die Zahl der Nutzer, die den von der betreffenden Einrichtung erbrachten wesentlichen Dienst in Anspruch nehmen;

b. das Ausmaß der Abhängigkeit anderer im Anhang festgelegten Sektoren und Teilsektoren von dem betreffenden wesentlichen Dienst;
c. mögliche Auswirkungen von Sicherheitsvorfällen — hinsichtlich Ausmaß und Dauer — auf wirtschaftliche und gesellschaftliche Tätigkeiten, die Umwelt, die öffentliche Ordnung und Sicherheit oder die Gesundheit der Bevölkerung;
d. den Marktanteil der Einrichtung auf dem Markt für wesentliche Dienste oder für die betreffenden wesentlichen Dienste;
e. das geografische Gebiet, das von einem Sicherheitsvorfall betroffen sein könnte, einschließlich etwaiger grenzüberschreitender Auswirkungen
f. die Bedeutung der Einrichtung für die Aufrechterhaltung des wesentlichen Dienstes in ausreichendem Umfang, unter Berücksichtigung der Verfügbarkeit von alternativen Mitteln für die Erbringung des betreffenden wesentlichen Dienstes“. (Art. 7. Abs. 1 Richtlinie (EU) 2022/2557).

In diesen Formulierungen wird eine fundamentale Abhängigkeit von Einrichtungen und Sektoren von der Resilienzfähigkeit anderer Einrichtungen und Sektoren anerkannt und zugleich die Relevanz von Marktanteilen und geografischer Situierung hervorgehoben. Gesellschaftliche und organisationale Resilienz kann unter diesen Voraussetzungen nur systemisch gedacht werden. Resilienz ist in diesem Sinne eine Gemeinschaftsleistung, ein Zusammenwirken unterschiedlichster Akteur*innen auf mehreren Ebenen. Sie ist „…das komplexe Ergebnis aus dem Zusammenwirken von Ressourcen, Kompetenzen und Performanzen individueller, inter-subjektiver und organisationaler Art zu verstehen, in dessen Folge in Interaktion mit der Umwelt fortlaufend differenzielle Resilienzen gegenüber spezifischen, die organisationale Identität gefährdenden Ereignissen oder dauerhaft bestehenden ungünstigen Umweltbedingungen ausgebildet werden.“ (Hoffmann, 2017, S. 97f.)

An dieser Zusammenfassung ist neben dem Hinweis auf das Zusammenwirken von Ressourcen, Fähigkeiten und Performanzen wichtig, dass die Akteur*innen auf dreierlei Ebenen angesiedelt werden (individuell, intersubjektiv und organisatorisch) und das Ergebnis dynamisch beschrieben wird, das fortlaufend hervorgebracht wird, um auf die ebenfalls fortwährend gefährdenden Umweltbedingungen zu reagieren. Was in den meisten Konzepten zur organisationalen Resilienz fehlt, ist die notwendige systemische Vernetzung über die Unternehmen hinaus in Sektoren und über diese hinaus in eine sektorübergreifende Stakeholderlandschaft, die ihrerseits noch einmal in kommunale, nationale und supra-nationale Strukturen eingebettet ist. In einem Beitrag zum „Atlas: Verwundbarkeit und Resilienz“ formulieren Fekete und Hufschmidt (2016) bereits 2016 „… (es) fehlt vielerorts noch an räumlichen Analysen und es kann erwartet werden, dass regionale Verwundbarkeits- und Resilienz-Analysen von KRITIS bald nicht mehr nur im derzeitigen populären

Forschungsschwerpunkt „Resiliente Stadt“, sondern zunehmend auch in städtisch-ländlichen Wechselbeziehungen betrachtet werden.“ Mittlerweile sind auch für diesen Aspekt in den letzten Jahren brauchbare Grundlagen erarbeitet worden (Müller, 2011; Lukesch, 2016; Patel et al., 2017; Strambach & Klement, 2016; Kegler, 2022; Max & Schulze, 2022; Röhe, 2022; Pechlaner, 2022), die im Kontext der RKE-Umsetzung nutzbar sind.

Um die Ebenen, innerhalb welcher das Zusammenwirken stattfinden kann, vollständig zu beschreiben, muss man demnach zumindest folgende vier Ebenen benennen (siehe Abb. 10):

- Die Ebene personaler oder auch intrapersonaler Resilienz, zu der bereits sehr viele Forschungsergebnisse von Seiten der psychologischen Resilienzforschung vorliegen,
- die Ebene der interpersonalen Resilienz, die in unserem Kontext die Ebene der Teams und kleineren Abteilungen darstellt, darauf aufbauend
- die Ebene der intraorganisationalen Resilienz bzw. die Gesamtresilienz der Organisation
- und schließlich die interorganisationale Ebene, auf der Organisationen und Einrichtungen, wie in Art 7 der Richtlinie gefordert, ihre wechselweise Abhängigkeit von anderen Organisationen im selben Sektor und in anderen Sektoren, aber auch administrativen und gesellschaftlichen Strukturen berücksichtigen.

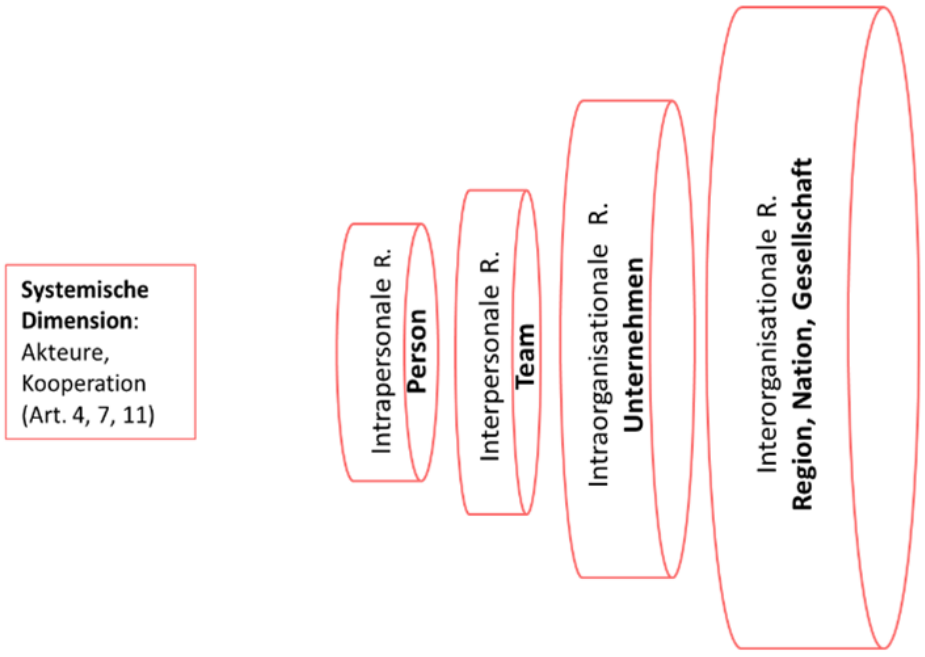


Abbildung 11: Sphären Systemischer Resilienz
Quelle: Eigene Darstellung

2.5.1. Resilienzmodelle der Makroebene

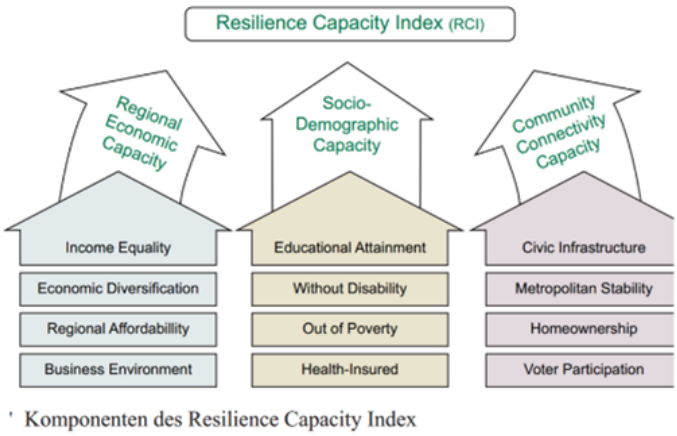
Die bisherigen Analysen haben ergeben, dass die Konzeptionen zur personalen, zur interpersonalen und organisationalen Resilienz unverzichtbare Bausteine für ein Resilienz-Framework liefern, das die spezifischen Aufgaben von kritischen Einrichtungen berücksichtigt, dass in diesen Modellen aber in der Regel eine noch weitere Perspektive fehlt, die die Einbettung und Interdependenz mit anderen Stakeholdern, Regionen und übergeordneten nationalen und internationalen Verwaltungen miteinbezieht.

Rezent werden auch für diese Resilienzsphäre verstärkt Modelle (Max & Schulze, 2021; Fekete et al., 2016; Strambach & Klement, 2016; Lukesch, 2022; Fathi, 2022; Störmann & Pechlaner, 2022) entwickelt. Auch hier kommen aber, im Sinne der vorliegenden Aufgabestellung, zu weitläufige und abstrakte Konzepte weniger in Betracht, weil hier die konkrete Anbindung an die Aufgabenstellung von kritischen Einrichtungen zwar mitberücksichtigt ist, eine konkrete Operationalisierung aber im Sinne der RKE-Richtlinie oder des RKE-G nur schwer umsetzbar ist. Der Resilience Capacity Index von 2016 ist ein Beispiel dafür. Dieser beinhaltet eine Methode, um Resilienz zu quantifizieren und stützt sich auf einen Capability-Ansatz, d.h. im Prinzip auf Fähigkeiten, die entwickelt oder vorhanden sein müssen. Jedoch ist er in einer Breite konzipiert, die eher auf nationaler Ebene sinnvoll ist.

Die Grundstruktur basiert auf drei Säulen – regional-ökologischen, sozio-ökonomischen und kommunal-vernetzten (community-connectivity) Kapazitäten, die ihrerseits durch Faktoren wie Einkommensgleichheit, Diversifizierung, Bildungsvoraussetzungen, Armutsbekämpfung, Gesundheitsversorgung, Funktionalität der zivilen Verwaltungen oder politischer Partizipation – also umfassenden politischen Programmen bestimmt sind. Obwohl diese Faktoren weit außerhalb des Rahmens liegen, der im RKE-G intendiert wird, gibt der Index doch einen Rahmen vor, der in einer nationalen Resilienzstrategie nach Art. 4 der Richtlinie mitberücksichtigt werden könnte.

Für die Aufgabenstellung der gegenständlichen Forschung, die an der Schnittstelle von Behörden und Unternehmen ansetzt und einen Beitrag zur Konkretisierung der Resilienzpläne (nach Art. 13 Abs. 2 Richtlinie (EU) 2022/2557) von Seiten der kritischen Einrichtungen liefern will, bleibt festzuhalten, dass die vertikale Logik der Säulen, die ökonomische, gesellschaftliche und vernetzungsstrategische Aspekte festhält, Sinn macht und weitere Bausteine zu einem KRITIS-kompatiblen Resilienz-Framework beisteuert (siehe Abb. 12).

In zu umfassenden, oder zu abstrakten Modellen, wie dem *Resilience Capacity Index,* ist die Problematik der KRITIS zwar miterfasst, aber eine **Operationalisierung** im Sinne der RKE-Richtlinie schwierig.



' Komponenten des Resilience Capacity Index

Abbildung 12: Resilience Capacity Index
Quelle: Darstellung nach Wink (2016)

Das gilt auch für andere Entwürfe Nationaler Resilienz (Edwards, 2009; Scharte, 2021) wie ihn Edwards (2009), der mit vier Grundbegriffen Engagement, Empowerment, Education und Encouragement operiert und die Scharte (2021) folgendermaßen interpretiert:

> „Unter **Engagement** versteht Edwards eine Weiterentwicklung der Kommunikation zwischen Regierung, lokalen Autoritäten, Katastrophenschützern, Rettungskräften, etc. auf der einen und Bürgern auf der anderen Seite. Es geht nicht um einseitige Informationsweitergabe, sondern um ein wirkungsvolles Einbeziehen der von Katastrophen potentiell direkt Betroffenen vor Ort. Die Anliegen und Kompetenzen von Bürgern sollen durch einen Dialog auf Augenhöhe ernst genommen werden.
>
> Im nächsten Schritt ist Bildung (**Education**) essentieller Bestandteil der Schaffung einer resilienten Gesellschaft. Ein grundlegendes – und je nach persönlicher (z.B. geographischer) Betroffenheit auch spezielleres – Wissen über Bedrohungen und Risiken einerseits sowie das richtige Verhalten im Katastrophenfall andererseits muss möglichst jedem Menschen vermittelt werden. Um nicht Gefahr zu laufen, durch übertriebene Warnungen Panik in der Gesellschaft zu verursachen, müssen die entsprechenden Informationen als Teil des Lehrplans in die alltäglichen Lernaktivitäten von Schülern integriert werden.
>
> Durch Bildung und Engagement wird **Empowerment** möglich. Damit meint Edwards Maßnahmen, die es Betroffenen während einer Katastrophe ermöglichen, selbst tätig zu werden und die negativen Konsequenzen des Ereignisses zu begrenzen.
>
> **Encouragement** entspricht dann einem eher psychologischen Teil von Empowerment. Die Bürger sollen dazu ermutigt werden, selbst aktiv zu werden und so zur Resilienz der Gesellschaft beizutragen“ (Scharte, 2021, S.81ff. Hervorhebungen PUKE-Team).

Dieses Konzept liefert wertvolle Ergänzungen zu den Entwürfen organisationaler Resilienz, obwohl eine Reihe von Qualitäten – Scharte sieht das Verhältnis von Resilienz und Vertrauen im Zentrum des Entwurfes – auch auf der Ebene von Einrichtungen und Unternehmen relevant sind.

Wichtig ist, dass hier unter dem Stichwort Engagement, das vielleicht auch Involvement meint, eine „Weiterentwicklung der Kommunikation zwischen Regierung, lokalen Autoritäten,

Katastrophenschützern, Rettungskräften, etc. auf der einen und Bürgern auf der anderen Seite“ (Scharte, 2021, S.81) intendiert wird, also eine gezielte Ausweitung der Vernetzung, in welcher im Rahmen unserer Fragestellung eine aktive Rolle der kritischen Einrichtungen beschrieben werden müsste. Neben diesem Aspekt und der Frage der Bildung sieht man das Modell der Selbstwirksamkeit und situativen Handlungsfähigkeit, das oben als basale Fähigkeit personaler Resilienz beschrieben wurde, hier unter den Stichworten Empowerment und Encouragement auf die Bürger*innen einer betroffenen Region bzw. im Sinne einer Resilient Nation auf Staatsbürger*innen insgesamt ausgeweitet.

2.5.2. Anpassung als Schlüsselkonzept

Auf einer noch einmal etwas grundsätzlicheren Ebene steht bei diesen Konzepten eine Auffassung von Resilienz im Hintergrund, wofür der Begriff der Anpassung zentral ist: „The capacity of an individual, community or system to adapt in order to sustain an acceptable level of function, structure and identity.” (Edwards, 2009, S. 10)

Der Begriff der Identität verweist auf die Dimension kollektiver Ziele und Selbstbilder, die in den oben beschriebenen Modellen organisationaler Resilienz hervorgehoben wurde. Der Begriff der Adaption oder Anpassung (Holling & Gunderson, 2012; Flüter-Hoffmann et al., 2018; Duchek, 2020; Bendell & Read, 2021; Staab, 2022) spielt in allen Resilienz-Modellen eine zentrale Rolle und erhält aber im Rahmen der Überlegungen zu einer gesamtgesellschaftlichen Resilienz eine ganz spezifische Bedeutung. Zum einen hat man hier den Anpassungsdruck von großen, beharrlichen Strukturen im Auge, die die Subsysteme mitbeeinflussen und nach Störungen mithelfen, dass sich Strukturen und Prozesse wieder re-etablieren. In dieser Hinsicht können übergeordnete Systeme als „memory functions“ wirken und wenn sie kulturell verankert sind, weit über das hinausgreifen, was von einem einzelnen Unternehmen oder auch einer Behörde intendiert werden kann. Kulturelle Eigenarten – wie etwa der tägliche Wasserverbrauch, das Reiseverhalten, die Kommunikationsgewohnheiten – würden im Falle einer Störung der Wasserversorgung, eines Flughafens oder der Telekommunikation quasi wie ein Erinnerungssystem fungieren, das mithilft, vor der Störung bestehende Strukturen und Prozesse wieder aufzubauen. Umgekehrt können auch Impulse aus Subsystemen auf übergeordnete Systeme überspringen – man denke an die Angewohnheit, mittels Smartphones zu kommunizieren – und diese prägen.

In der einschlägigen Literatur hat sich auf Grund der Vielfalt der möglichen Impulse der Begriff Panarchie herausgebildet (siehe Abb. 13). Arché bedeutet Ursprung, Herrschaft. Panarchie daher die gleichzeitige Herrschaft multipler Impulse und Systeme, die ineinandergreifen und deren Adaptionszyklen ineinander spielen. Wo das Hauptaugenmerk der Situation von Unternehmen gilt, wurden die Phasen dieser Zyklen auch mit dem Wachstum oder Schrumpfen von Märkten und

Einflussfeldern in Verbindung gebracht und mit unterschiedlichen Graden von Interdependenz (Connectedness) verknüpft.

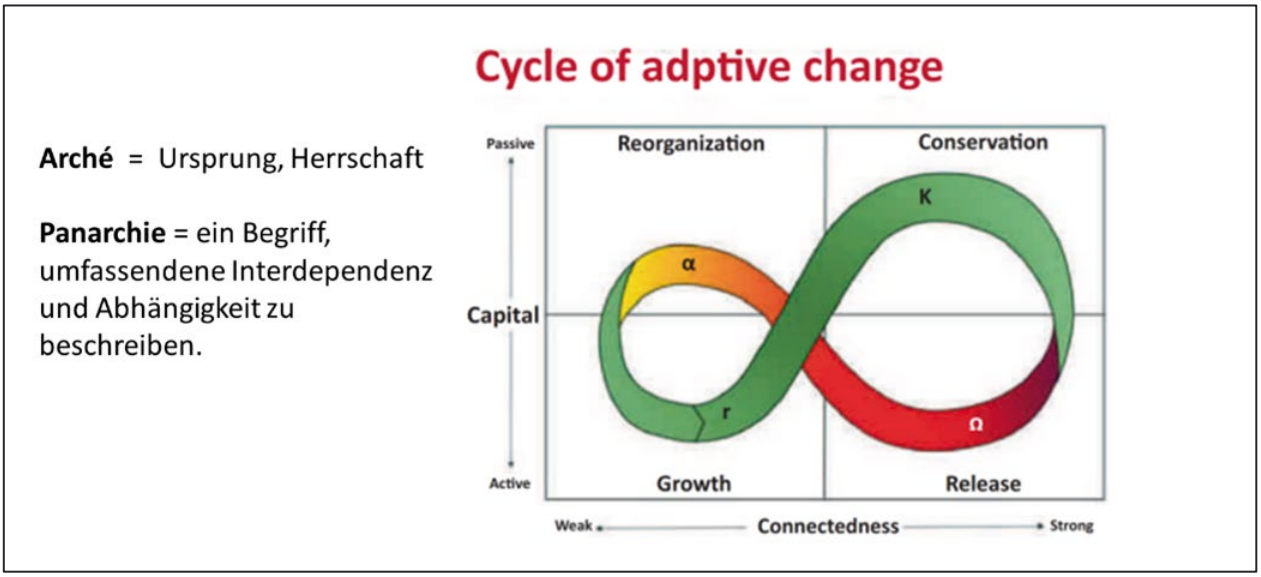


Abbildung 13: Panarchie und Adaptionszyklen
Quelle: Darstellung von Carpenter et. al. (2001)

Lukesch (2022) fasst dieses mehrdimensionale Geschehen so zusammen:

> „In Wirklichkeit greifen die Systeme auf vielen territorialen, zeitlichen und sozialen Ebenen und Größenstufen ineinander, sind einander übergeordnet oder eingebettet, so wie sie selbst wiederum aus vielfach ineinander geschachtelten und verschränkten Subsystemen bestehen. C. S. Holling nennt dieses multiskalare Ineinandergreifen Panarchie. Übergreifende, großskalierte Wandlungszyklen liefern das Gedächtnis (memory function) für die Wiederherstellung geschädigter oder zerstörter eingebetteter Systeme, während Erneuerungsimpulse (revolt function) von niedrigskalierten auf die ihnen übergeordneten Systeme überspringen können“ (Lukesch, 2022, S. 301).

2.5.3. Regionale räumliche Resilienz

Für die Verwertung dieser Theoriestränge für ein systemisches Resilienz-Framework, das genuin für kritische Einrichtungen konzipiert wird, ist ausschlaggebend, dass die groß skalierten Adaptionszyklen zwar nicht leicht zu beeinflussen sind, aber gekannt und analysiert werden können. Für die betroffenen Sektoren – Energie, Lebensmittel, Gesundheit etc. – sind die übergeordneten Systeme, also der Energieverbrauch, die Schwankungen im Tagesverlauf, Konsumgewohnheiten, Patientenströme usw. – zumindest teilweise bekannt. Sich mit diesen auch im Kontext einer strategischen Resilienzentwicklung bekannt zu machen, ist im Rahmen einer systematischen Berücksichtigung von Resilienzsphären, die sich bis in gesellschaftliche Bereiche erstrecken, unabdingbar.

Einen wichtigen Beitrag zu einer systemischen Analyse liefern die Entwürfe zur räumlichen oder regionalen Resilienz. Aufbauend auf einem Modell von Bauer-Wolf et al. (2009) und Lukesch (2016) werden vier unterschiedliche Räume beschrieben, die als Interaktionsraum, Intentionsraum, Identitätsraum und Institutioneller Raum bezeichnet werden (siehe Abb. 14).

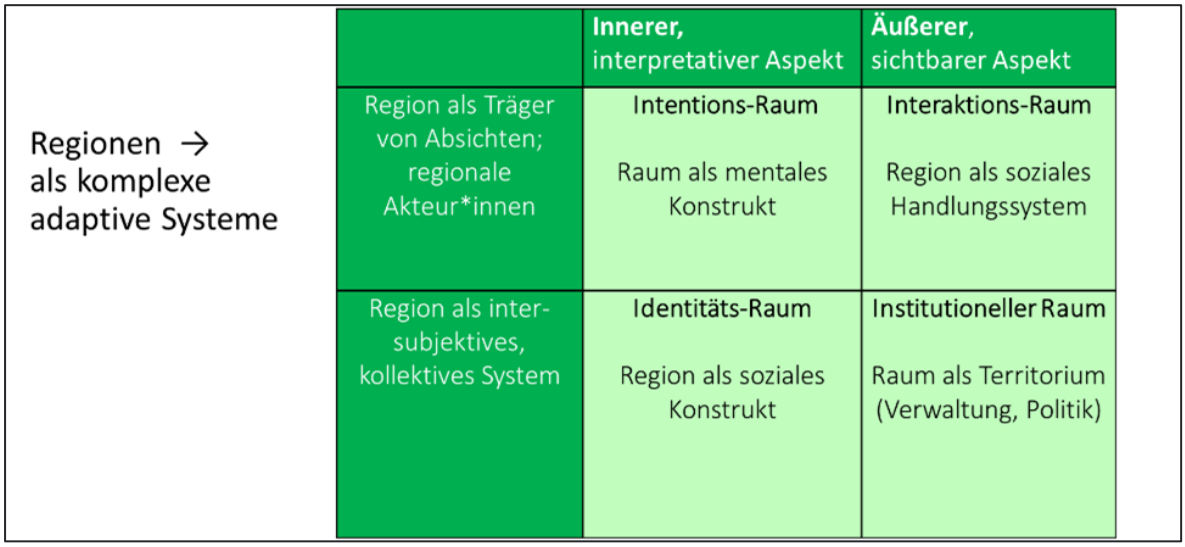


Abbildung 14: Regionale Resilienz – Räume
Quelle: Eigene Darstellung in Anlehnung an Bauer-Wolf et al. (2009)

> „Die eine Perspektive, ist die eines Wirkungsgefüges, eines sozioökonomischen **Interaktionsraums**, eines sozialen Handlungssystems. Die Region entsteht durch die Begegnung, den Austausch, die Vernetzung, die Kopplung mittels Stoffwechsel- und Kommunikationsprozessen. Eine Region ist aber auch als mentales Konstrukt (**Intentionsraum**), als Bühne für Karrierewünsche, Zukunftsträume, Vorstellungen vom guten Leben, als Ort der Selbstverwirklichung darstellbar. Gruppen von Menschen, die sich als Gemeinschaften verstehen, dient die Region als soziales Konstrukt (**Identitätsraum**). Hier bedeutet Region Zugehörigkeit und Vertrautheit, das sichere Gefühl eines Heimathafens. Schließlich ist die Region schlichtweg als Territorium (**Institutioneller Raum**) zu begreifen. Innerhalb seiner Grenzen gelten Gesetze und Regeln. Mit der Zugehörigkeit zum institutionellen Raum sind Rechte und Pflichten verbunden“ (Lukesch 2022, S. 98, Hervorhebungen PUKE-Team).

Diese Perspektive forciert die kulturellen und kommunikativen Aspekte von Resilienz unter der Voraussetzung, dass Resilienz auf dieser Ebene immer als Kooperation vieler Akteur*innen oder Akteur*innengruppen zu denken ist, die neben dem institutionellen Rahmen auch regionale Identitätsbezüge und tatsächliche Begegnung braucht. Das ist ein wichtiger Hinweis auf die regionale Situierung von kritischen Einrichtungen und formuliert zugleich eine kommunikative Aufgabe, mit dem gesellschaftlichen Umfeld, der Wohnbevölkerung, aber auch den Kund*innen, den Nutzer*innen Kontakt aufzunehmen und adäquate Informationswege aufzubauen. Man könnte sagen, dass

hinter den Entwürfen zur regionalen Resilienz implizit oder explizit das Anliegen steckt, den Zusammenhang von Vertrauen und Resilienz gründlicher zu fassen.

Exemplarisch und etwas näher an einer möglichen Operationalisierung der genannten Kriterien steht das „4-R“-Modell nach Kegler (2022), auf das sich Konzepte räumlicher Resilienz häufig beziehen. Die vier „R“ stehen für Reliability, Resistance, Redundancy und Response.

> „Widerstandsfähigkeit (Resistance): Der Fokus liegt hier auf dem unmittelbaren Schutz von Anlagen; das Ziel ist die Vermeidung von Schäden und negativen Folgen der Unterbrechung der Infrastrukturversorgung. Die Wirkung eines solchen Ansatzes kann eingeschränkt sein, wenn Schutzmaßnahmen sich nur auf Ereignisse oder Störungen beziehen, mit denen bereits in der Vergangenheit Erfahrungen gemacht wurden. Die potenziellen Gefahren sind dann hoch, wenn Resistenz die einzige Komponente einer resilienten Strategie ist.
>
> Vertrauenswürdigkeit (Reliability): Diese Komponente befasst sich mit der Frage, wie Infrastrukturen oder Organisationen verlässlich gestaltet werden können, sodass sie unter ganz unterschiedlichen Umweltbedingungen funktionieren und somit Schäden durch etwaige Störungen vermieden werden können. Treten Störungen auf, die außerhalb dieses Korridors liegen, sind Infrastruktursysteme oft nur unzureichend auf mögliche Schadensereignisse vorbereitet. Stabilität geht vor Risiko, kann die Regel lauten, was aber nicht Innovation ausschließt, wenn sie denn verantwortungsvoll angelegt wird.
>
> Redundanz (Redundancy): Diese bezieht sich auf die Kapazitäten eines Netzwerks oder eines Systems. Die Verfügbarkeit von Backup-Einrichtungen und Reservekapazitäten erlaubt im Fall von Störungen die Verlagerung des Betriebs auf andere Systemkomponenten und damit die Weiterführung der Anlagen. […]
>
> Reaktionsschnelligkeit (Response and Recovery) verfolgt das Ziel einer schnellen und effektiven Reaktion auf Störungen, um eine schnelle Erholung von den Schäden zu erreichen. Die Effektivität dieser Strategie hängt von der Kultur und den verfügbaren Kapazitäten der Organisationen ab, um reaktionsfähig zu sein. Zugleich spiegelt sie die Lernfähigkeit wider, mit der schon im Vorfeld von Schadensereignissen vorbeugende Schritte geplant und erprobt werden.“ (Kegler, 2022, S. 143ff.)

Die Konzeptionen zur räumlichen oder regionalen Resilienz verweisen auf die umfassendste Sphäre, in welcher Resilienz zu berücksichtigen wäre, wenn die Analyse systematisch durchgeführt wird. Es ist offenkundig, dass die Handlungsspielräume von Unternehmen oder kritischen Einrichtungen hier eingeschränkt sind. Um Resilienz hier umzusetzen, sind Voraussetzungen nötig, die politisch geschaffen werden müssen.
In diesem Sinn bezeichnet etwa Scharte (2021) das Projekt als „starkdemokratisch“ (S. 180) und weist darauf hin, dass Resilienz auf gesellschaftlicher Ebene mit einer Reihe anderer Werte, Grundrechte und Prozesse korreliert werden muss, um tatsächlich zu einem handlungsleitenden Paradigma zu werden.

2.6. Systemisches Resilienz-Framework (SRF)

Die Recherche zum Forschungsstand der unterschiedlichen Resilienz-Modelle wurde unternommen, um Bausteine für ein Modell zu entwickeln, das einen Resilienzbegriff formuliert, der im Kontext von kritischen Einrichtungen angewendet werden kann. Das Framework setzt sich aus Prämissen und einem Resilienzsystem zusammen (siehe Abb. 15). Es ist, wie oben im heuristischen Modell bereits festgehalten,

- multitheoretisch
- multiskalierbar
- und intersektional bzw. sektionsübergreifend anwendbar.

Die nach den Anforderungen von Art. 12 der RKE-RL zu entwickelnde Risikobewertung ist darin nicht berücksichtigt und wird separat dargestellt.

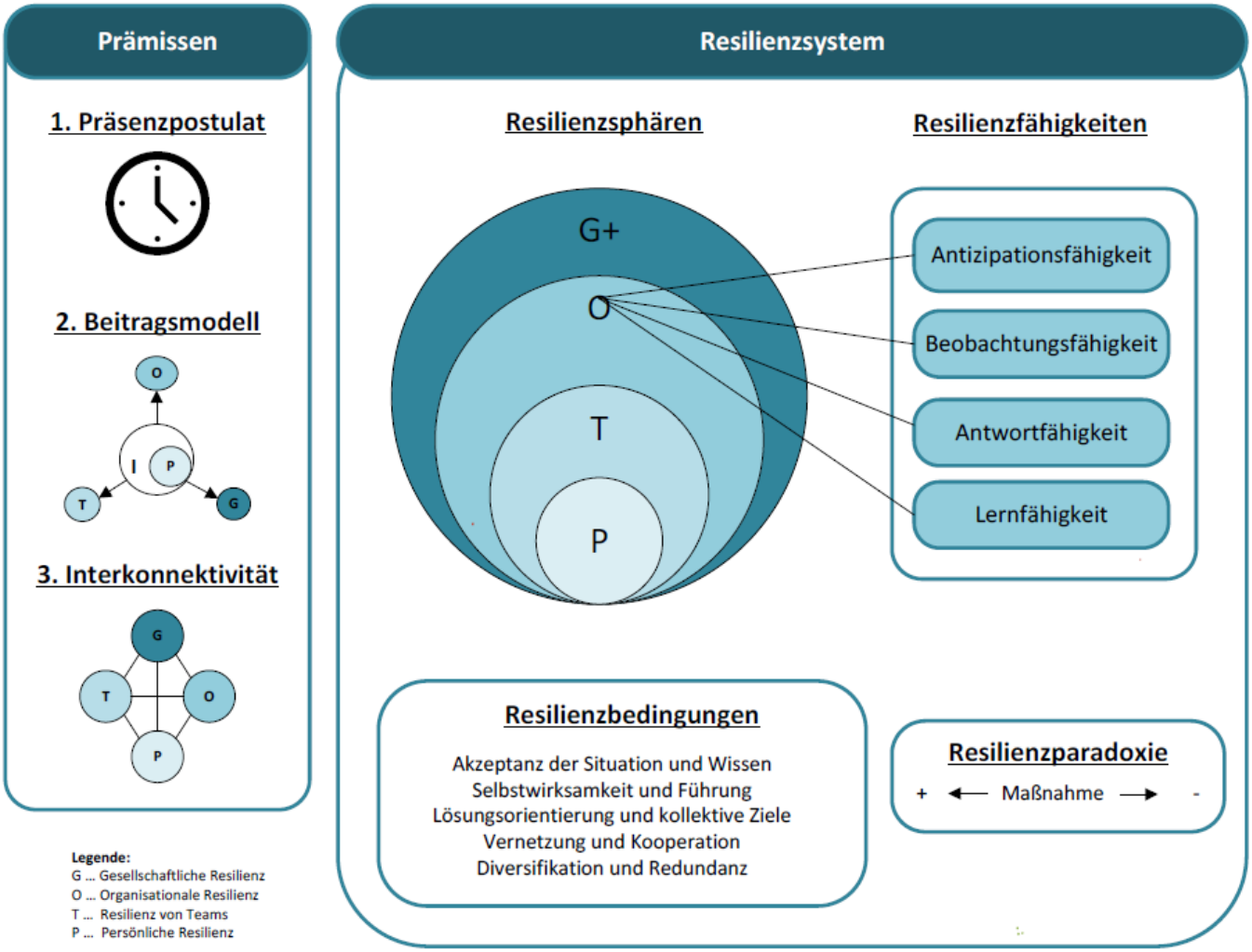


Abbildung 15: Systemisches Resilienz-Framework (SRF)
Quelle: Langer et al. (2025)

2.6.1. Grundlegende Prämissen als Ausgangsüberlegungen

Für die Entwicklung des vorliegenden Modells wurden grundlegende Prämissen formuliert, um das Phänomen Resilienz, das sich als äußerst vielschichtig und komplex darstellt, konzeptionell einzugrenzen und einer systematischen Analyse zugänglich zu machen. Diese Prämissen dienen als theoretisches Fundament und strukturgebende Leitplanken, die es ermöglichen, die Multidimensionalität des Resilienzbegriffs in einem kohärenten Framework zu erfassen. Durch diese axiomatischen Bedingungen wird eine wissenschaftlich fundierte Herangehensweise gewährleistet, die sowohl der Komplexität des Untersuchungsgegenstandes gerecht wird als auch eine methodisch stringente Modellentwicklung ermöglicht. Als wesentliche Prämissen werden 1. das Präsenzpostulat, 2. ein Beitragsmodell und 3. die Interkonnektivität als grundlegendes Strukturmerkmal benannt, die systemische Beiträge entsprechend berücksichtigen (Langer et al., 2025).

Prämisse 1: Präsenzpostulat

Im Gegensatz zu den etablierten zeitlich-sequenziellen Modellen wird im vorliegenden Ansatz eine fundamentale Neukonzeption vorgeschlagen. Die traditionelle Phaseneinteilung – mit ihrer impliziten Annahme distinkter, aufeinanderfolgender Zeitabschnitte – eignet sich aufgrund kategorialer Unschärfen nicht zu einer tauglichen theoretischen Beschreibung der operativen Praxis. Diese Problematik lässt sich am Beispiel des Krisenmanagements verdeutlichen. Traditionelle Modelle sehen das Krisenmanagement in der Phase Bewältigung, wiewohl die Tätigkeiten wie das Erstellen von Krisenplänen etc. der Phase Vorbereitung zugeordnet werden müssten. Ebenso kann die Frage gestellt werden, ob es sich bei Krisenübungen um antizipative Vorbereitung oder bereits um eine Form der Bewältigung handelt. Das hier entwickelte Präsenzpostulat basiert auf der erkenntnistheoretischen Prämisse, dass ausschließlich der gegenwärtige Moment existiert und somit alle organisationalen Handlungen im Jetzt verortet sind. Daher löst sich aus Sicht des Präsenzpostulats dieses Dilemma auf: Sämtliche Maßnahmen mit Ausnahme der realen Krise sind per Definition Vorbereitung. Diese Sichtweise lässt sich zuspitzen. Eine valide Evaluation der Krisenbewältigungskompetenz einer kritischen Einrichtung wäre streng genommen nur durch die Herbeiführung realer Krisen möglich. Alle fiktiven Szenarien – seien es Simulationen, Übungen oder theoretische Planspiele – können lediglich die Qualität der Vorbereitung, nicht jedoch die tatsächliche Bewältigungsperformanz erfassen. Dieser konzeptionelle Zugang reduziert die Komplexität und fokussiert auf das Wesentliche. Die funktionale Zuordnung einer Maßnahme – ob Vorbereitung oder Bewältigung – wird nicht durch abstrakte Modellphasen, sondern durch den aktuellen situativen Kontext determiniert (Langer et al., 2025).

Prämisse 2: Das Beitragsmodell

Das Beitragsmodell geht davon aus, dass im Zentrum der Interaktionen das Individuum steht und zwar nicht nur kommunikativ, sondern im Sinne eines aktiven Beitrages zur Resilienz, den der/die Einzelne auf allen Ebenen leistet. Diese Art von Resilienz ist individuell und rollen-spezifisch zu verstehen. Individuelle Beteiligte tragen je nach hierarchischer Stellung und Tätigkeitsbereich ihren persönlichen Beitrag zur organisationalen Resilienz bei. Ein Chief Financial Officer eines Unternehmens kann im Rahmen seiner Rolle einen Beitrag zur organisationalen Resilienz leisten, indem er bestimmte Ressourcen frei gibt, obwohl er persönlich vielleicht nicht über die Fähigkeit verfügt, einer Gruppe von Mitarbeitenden Zuversicht oder Orientierung bei Störfällen zu vermitteln. Der Beitrag Einzelner kann daher sehr unterschiedlich ausfallen. Die Annahme, dass die personale Resilienz einzelner Mitarbeiter*innen einen Beitrag zur organisationalen Resilienz leistet, wird durch den derzeitigen Forschungsstand und Erkenntnissen aus der Covid-19-Pandemie unterstützt (Bentner, & Jung, 2022; Haas et al., 2022; Kuhlmann et al., 2024; Meyer, 2022; Schellinger et al., 2022; Unkrig, 2021). Die möglichen individuellen Beiträge wirken in der Organisation zusammen und können in eine Gesamtstrategie integriert werden.

Resilienz als Beitrag für die Organisation zu verstehen, erfordert von Anfang an etwaige Sensibilisierungs- und Schulungsmaßnahmen, in denen Kooperation und die Identifikation mit Unternehmenszielen eine wesentliche Rolle spielen. Der Fokus auf aktive oder auch passive Beiträge resultiert zudem aus den übereinstimmenden Befunden (Hollnagel et al., 2006; Lukesch, 2016; Scharte, 2021; Unkrig, 2021; Haas et al., 2022), dass Resilienz ein labiler Gleichgewichtszustand ist, der immer aus dem Zusammenspiel unterschiedlicher, aber gut beschreibbarer Faktoren und der Kooperation aller involvierten Akteur*innen entsteht. Gregor Paul Hoffmann bringt es auf den Punkt, wenn er schreibt, dass das „Zusammenwirken von Ressourcen, Kompetenzen und Performanzen“ (Hoffmann, 2017, S. 97) die wesentliche Aufgabe organisationaler Resilienz ist (Langer et al., 2025).

Prämisse 3: Interkonnektivität als Antwort auf Interdependenz

Interkonnektivität ist eine wichtige Voraussetzung für die Resilienz von Einrichtungen der kritischen Infrastruktur, da sie den positiven Umgang mit Abhängigkeiten der Bevölkerung von wesentlichen Diensten (gemäß RKE-Richtlinie) sowie der Einrichtungen untereinander betont. Interkonnektivität meint einen konstruktiven und kommunikativen Umgang mit Interdependenz, also möglichen Kaskadeneffekten, die im Krisenfall drohen und aus Sicht der EU mitbedacht und gestaltet werden müssen. Diese wechselseitigen Abhängigkeiten werden somit in den aktiven Handlungsbereich der Verantwortlichen der organisationalen Resilienz integriert. Interkonnektivität muss dabei in allen vier Resilienzausprägungen bedacht werden, da Interaktionen und strukturelle Abhängigkeiten

zwischen Personen, Teams, Organisationen und der Gesellschaft in der Analyse berücksichtigt werden müssen (Langer et al., 2025).

2.6.2. Das Resilienzsystem

Das hier vorgestellte Framework operationalisiert die genannten Prämissen in einem Resilienzsystem und besteht aus den vier Elementen: Resilienzsphären, Resilienzbedingungen, Resilienzfähigkeiten und der sogenannten Resilienzparadoxie.

Eine Grundannahme des hier vorgestellten Modells ist das systemische Verständnis von Resilienz, die auf der bereits vorher erwähnten wechselseitigen Abhängigkeit von Einrichtungen der kritischen Infrastruktur und möglicher Kaskadeneffekte großräumig angebotener Dienste beruht. In den vier Resilienzsphären ist daher der systemische Charakter des Modells festgehalten, um entsprechende Interdependenzen zu verdeutlichen. Diese Sphären umfassen

- die personale Resilienz,
- die Resilienz von Teams,
- die Resilienz von Organisationen
- und die Ebene der gesellschaftlichen Resilienz.

Das Modell der Resilienzsphären verdeutlicht, dass die Resilienz von Einrichtungen der kritischen Infrastruktur systemisch gedacht werden muss, und weist zugleich über den Anwendungsbereich der kritischen Einrichtungen hinaus. Es ergänzt daher die Ansätze der organisationalen Resilienz, die zumeist den Schwerpunkt auf das einzelne Unternehmen legen, um die weiteren Stakeholder und die gesamte Bevölkerung. Diese weitere Resilienzsphäre erfordert zunächst die Identifikation relevanter Gruppen und Strukturen, um in einem nächsten Schritt, im Sinne der Interkonnektivität, diese Beziehungen gestalten zu können.

Die grundlegenden Annahmen, auf die sich das hier vorgestellte Modell stützt, sind unterschiedlich gut beforscht. Vor allem Forschungen zur personalen Resilienz zeigen, dass diese von individuellen Qualitäten geprägt und in größere Systeme eingebettet sind, wobei Wechselwirkungen zur organisationalen und regionalen oder gesellschaftlichen Resilienz bestehen. Personale oder auch interpersonale Resilienz sind von Seiten der psychologischen Resilienzforschung (Heller, 2019; Fröhlich-Glidhoff & Rönnau-Böse, 2023; Schrems, 2021) oder der Gesundheitsforschung am längsten erforscht. Die Modelle personaler Resilienz sind stark von einer Weiterentwicklung salutogenetischer Ansätze geprägt. Bewältigbarkeit und Verstehbarkeit der Verhältnisse – ob im privaten oder beruflichen Kontext – sind hier maßgeblich. Zugleich ist die personale Resilienz in einer Sinnebene fundiert, für die persönliche oder auch gemeinsame Ziele von Gruppen oder Organisationen wesentlich sind. Diese Faktoren bilden die Basis für höherstufige Formen von Resilienz, wie sie für Teams oder ganze Unternehmen in Frage kommt (Langer et al., 2025).

Die organisationale Resilienz ist ein jüngerer Forschungszweig, zu dem allerdings auch schon eine Reihe von Ergebnissen vorliegt. Dagegen ist die Analyse der gesellschaftlichen Resilienz als umfassendste Sphäre noch in den Anfängen, obwohl Ansätze zur Urbanen Resilienz (Kegler, 2014; Mueller, 2011) zur Resilienz von Regionen oder auch Nationen bereits in der einschlägigen Literatur beschrieben wurden. Der hier vorgestellte Ansatz weist der Resilienz von Teams, als einem vermittelnden Medium zwischen einzelnen Mitarbeitenden und der Gesamtorganisation, eine wichtige Rolle zu. Das erfolgt aufgrund von Forschungen zur organisationalen Resilienz, die Qualitäten wie Vertrauen, tragfähige Beziehungen und gemeinsame Ziele als besonders wichtig erachtet und somit die meso-soziale Ebene der kleinen Einheiten in den Vordergrund rückt. Ein Befund, der ebenfalls von der Arbeitsforschung (Giesert et al., 2017; Treier, 2016) gestützt wird (Langer et al., 2025).

Der Fokus des beschriebenen Frameworks liegt aufgrund der besonderen Bedeutung kritischer Einrichtungen für die gesamtgesellschaftliche Sicherheit vor allem auf der organisationalen Resilienz.

> „Unter organisationaler Resilienz ist das komplexe Ergebnis aus dem Zusammenwirken von Ressourcen, Kompetenzen und Performanzen individueller, intersubjektiver und organisationaler Art zu verstehen, in dessen Folge in Interaktion mit der Umwelt fortlaufend differenzielle Resilienzen gegenüber spezifischen, die organisationale Identität gefährdenden Ereignissen oder dauerhaft bestehenden ungünstigen Umweltbedingungen ausgebildet werden“ (Hoffmann, 2017, S. 98).

Zur Operationalisierung der personalen, teambezogenen und organisationalen Ausprägungen wird im Zuge der Beschreibung der Resilienzbedingungen und der Resilienzfähigkeiten Näheres ausgeführt. Die Sphäre der gesellschaftlichen Resilienz wird hier noch ausführlicher beschrieben.
Auf gesellschaftlicher Ebene wurden von Fekete und Hufschmidt (2016) bereits 2016 „regionale Verwundbarkeits- und Resilienz-Analysen von KRITIS“ gefordert. Für eine weitere Operationalisierung würde sich eine Reihe bereits entwickelter Ansätze (Fekete & Hufschmidt, 2016; Max & Schulze, 2021; Lukesch, 2022; Strambach & Klement, 2016) wie etwa der Resilience Capacity Index (Resilience Alliance, 2016), dessen Grundstruktur auf drei Säulen – regional-ökologischen, sozio-ökonomischen und kommunal-vernetzten Kapazitäten – beruht, hinsichtlich der analytischen Aspekte als interessant erweisen. Als Instrument, das Unternehmen eine Bewertung und Steuerung der eigenen Resilienz ermöglichen soll, ist dieser Ansatz allerdings aufgrund seiner Komplexität wenig geeignet. Ähnliches gilt für andere Entwürfe wie die 4-R-Kriterien Resistance, Reliability, Redundancy, Response, mit denen Kegler (2014) operiert (Langer et al., 2025).
Für diesen Kontext eignet sich die Sichtweise von Scharte (2021), die besagt, dass Resilienz auf gesellschaftlicher Ebene als die „Weiterentwicklung der Kommunikation zwischen Regierung, lokalen Autoritäten, Katastrophenschützern, Rettungskräften etc. auf der einen und Bürgern auf der

anderen Seite“ verstanden wird (Scharte, 2021, S. 82). Diese weist auf die notwendige Betrachtung des Ausmaßes der Vernetzung hin, innerhalb der im Rahmen unserer Fragestellung auf die aktive Rolle der kritischen Infrastruktur eingegangen werden muss. Für eine weitere Operationalisierung scheinen uns daher Ansätze zielführend, die regionale Kriterien als Ausgangspunkt wählen, wie etwa das Modell, das Lukesch (2022) aufbauend auf ein Konzept von Bauer-Wolf vorgestellt hat. Hier werden vier unterschiedliche Räume beschrieben, die als Interaktionsraum, Intentionsraum, Identitätsraum und Institutioneller Raum bezeichnet werden. Diese machen plausibel, inwiefern große übergeordnete Strukturen, in die Einrichtungen der kritischen Infrastruktur eingebettet sind, mithelfen, Störungen verdauen, Prozesse wieder etablieren und Anpassungszyklen – ein Schlüsselkonzept der Resilienzforschung – fundieren.

Diese Perspektive forciert die kulturellen und kommunikativen Aspekte von Resilienz unter der Voraussetzung, dass Resilienz auf dieser Ebene immer als Kooperation vieler Akteur*innen oder Akteursgruppen gedacht wird, die neben dem institutionellen Rahmen auch regionale Identitätsbezüge und tatsächliche Begegnung braucht. Dieser wichtige Hinweis auf die regionale Situierung von Einrichtungen der kritischen Infrastruktur formuliert die kommunikative Aufgabe, mit dem gesellschaftlichen Umfeld, der Wohnbevölkerung, aber auch den Kund*innen bzw. den Nutzer*innen Kontakt aufzunehmen und adäquate Informationswege zu etablieren (Langer et al., 2025).

2.6.3. Resilienzbedingungen

Wie bereits erläutert, wird hier davon ausgegangen, dass Resilienz durch das Zusammenspiel bzw. die Kooperation unterschiedlicher Bedingungen, Fähigkeiten sowie Akteur*innen entsteht. Daher wird als nächster Schritt im SRF zwischen Resilienzbedingungen und -fähigkeiten unterschieden. Resilienzbedingungen umfassen weitgehend alle Mitarbeiter*innen und müssen in Unternehmen so entwickelt werden, dass sie in der Breite verankert werden können, während Resilienzfähigkeiten vor allem Personen oder Abteilungen, die im Speziellen mit Sicherheitsaufgaben befasst sind, betreffen. Dabei wird vor allem berücksichtigt, dass der Schritt von personaler Resilienz zu einer Resilienz, die für Teams oder ganze Unternehmen relevant ist, nur durch ein kollektives sensmaking (Hoffmann, 2017, S. 72), d.h. das Artikulieren kollektiver Ziele, das Schaffen von Zugehörigkeit sowie den Aufbau belastbarer Beziehungen und eingeübter Kooperationen zu etablieren ist.

Die folgenden Bedingungen greifen Ansätze auf, die sowohl in den Forschungen zur personalen als auch zur organisationalen und regionalen Resilienz (Brunnermeier, 2021; Draht, 2018; Hoffmann, 2017; Kleemann & Frühbeis, 2021; Lengnick-Hall et al., 2011; McManus et al., 2007; Meyer, 2022; Röhe, 2022; Weick & Sutcliffe, 2016; Unkrig, 2022; Unkrig, 2021) genannt werden, und beziehen sich auf die notwendigen psychosozialen, organisatorischen und technischen Maßnahmen.

- Akzeptanz der Situation und Wissen: Bedingungen, die es Mitarbeitenden auf allen Ebenen ermöglichen, eine Situation als bedrohlich einzustufen, realisieren, dies als Herausforderung zu akzeptieren und die nötigen Informationen dafür zur Verfügung zu haben.
- Selbstwirksamkeit und Führung: Diese Bedingungen sind wesentliche Elemente gelungener sozialer Interaktion. Selbstwirksamkeit meint hier selbstständiges Handeln, Urteilsvermögen und Verantwortungsgefühl, das durch eine geeignete Führung in Handlungsabläufe integriert wird, um die Resilienz einer Abteilung bzw. der gesamten Organisation zu erhöhen.
- Lösungsorientierung und kollektive Ziele: In fast allen Modellen der personalen und organisationalen Resilienz erscheinen diese beiden Eigenschaften unverzichtbar. Lösungsorientierung wird hier als persönliche Ausrichtung auf Basis gemeinsamer Ziele verstanden.
- Vernetzung und Kooperation: Diese Bedingungen beziehen sich auf belastbare Strukturen und Prozesse, die etabliert werden müssen, um Information, Abstimmung und Zusammenarbeit zu ermöglichen.
- Diversifikation und Redundanz: Dies bezieht sich auf organisatorische bzw. technische Bedingungen, die im Vorfeld von Störfällen etabliert werden müssen und – nach Maßgabe aller Studien – entscheidend dazu beitragen können, dass wesentliche Dienste im Störfall (zumindest teilweise) aufrechterhalten werden können. Diversität innerhalb einer Organisation meint hier eine möglichst hohe Vielfalt an Sichtweisen, die eine breite Analyse und achtsame Lösungsansätze ermöglicht (Langer et al., 2025).

Für die Entwicklung von Resilienz auf Team- und Organisationsebene müssen kollektive Ziele und Zwecke erarbeitet, abgestimmt und kommuniziert werden. Diese dienen als Grundlage für belastbare Beziehungen sowie kollektive Identitäten. Gemeinsame mentale Modelle und Gedächtnissysteme, die auf gemeinsamen Erfahrungen und Analysen beruhen, brauchen Zeit. Hier wird deutlich, dass die genannten Ziele sehr ambitioniert sind und man nicht davon ausgehen kann, dass sie in Unternehmen bereits vollständig etabliert wurden. Das hier vorgestellte Modell unterliegt der Annahme, dass die genannten Resilienzbedingungen alle vier Resilienzsphären, wenn auch nicht gleichermaßen, betreffen. Aus der Perspektive kritischer Einrichtungen liegt die Steuerung der Resilienzstrategie trotz allem auf organisationaler Ebene, obwohl die Wichtigkeit der personalen Ebene und die Einbettung in regionale und gesellschaftliche Dimensionen aus systemischer Sicht betont werden muss (Langer et al., 2025).

2.6.4. Resilienzfähigkeiten

Die Resilienzfähigkeiten müssen in allen Resilienzsphären ausgebildet werden und manifestieren sich vor allem bei Schlüsselpersonen, die mit Sicherheitsaufgaben oder spezifischen Managementaufgaben in Organisationen der kritischen Einrichtungen betraut sind und dafür relevante Qualifikationen erworben haben. Diese Fähigkeiten müssen in strategischer Weise in der Organisation implementiert werden. Am ehesten kommen hierfür Capability-Konzepte (Duchek, 2020; Hollnagel et al. 2006; Nussbaum, 2015; Pariès et al., 2013) die für organisationale und soziale Kontexte entwickelt wurden, in Betracht. Eine wesentliche Perspektive dazu formuliert Daniel Lorenz (2013) bereits, in dem er Anpassungs-Potenzial (adaptive capacity), Bewältigungs-Potenzial (coping capacity) und Partizipations-Potenzial (participative capacity) unterscheidet, die für die systemische Vernetzung von Unternehmen bzw. Einrichtungen mit ihrem jeweiligen regionalen und gesellschaftlichen Umfeld eine Rolle spielt. Besonders anschlussfähig zeigt sich der Ansatz dadurch, dass auch in der RKE-Richtlinie explizit auf die Stärkung von Fähigkeiten (capabilities) im Kontext von Resilienz Bezug genommen wird. Dies ermöglicht eine konsistente konzeptionelle Verknüpfung mit dem hier vorgestellten systemischen Ansatz. Im Rahmen des Resilience Engineering adaptiert Hoffmann (2017) den Ansatz Hollnagels, der sich besonders als RKE-kompatibles Resilienzmodells für kritische Einrichtungen eignet. Es werden dabei vier Resilienzfähigkeiten unterschieden:

- Antizipationsfähigkeit: Diese Fähigkeit ermöglicht es künftige Entwicklungen und Risiken im Sinne des All-Gefahren-Ansatzes, der nicht nur für die RKE-Richtlinie maßgeblich ist, zu beurteilen und alle notwendigen präventiven Maßnahmen auf technischer, ökonomischer und organisatorischer Ebene abzuleiten.
- Beobachtungsfähigkeit: Hiermit ist, im Sinne eines systemischen Ansatzes, die Wahrnehmung und Beobachtung von internen und externen Ereignissen und Tendenzen gemeint, die Auswirkungen auf das Unternehmen bzw. die Einrichtung haben.
- Antwortfähigkeit: Diese Fähigkeit ermöglicht die Aktivierung von einerseits geplanten und geübten Handlungsabläufen, die sich auf erwartbare Gefahren beziehen, aber andererseits auch von kollektiv improvisierendem Handeln, das durch das geeignete Ausmaß an Flexibilität in die Lage versetzt, unvorhergesehene Situationen und Herausforderungen zu bewältigen.
- Lernfähigkeit: Hier ist die Fähigkeit gemeint, aus gemachten Erfahrungen durch eine systematische Fallanalyse und Manöverkritik, die richtigen Lehren zu ziehen und Veränderungen durchzuführen bzw. diese in künftige Vorbereitungs- und Schulungsmaßnahmen einzubeziehen.

Die hier genannten Fähigkeiten eigenen sich zur Normierung von konkreten Schulungsmaßnahmen und indirekt auch der Personalentwicklung in kritischen Einrichtungen. Sie machen prinzipiell für die gesamte Belegschaft Sinn, sind aber aus Ressourcengründen für Einzelne oder Teams mit besonderen Sicherheitsaufgaben gedacht, da für Präventionsarbeit, Monitoring und Manöverkritik nur bestimmte Personen zuständig sind (Langer et al., 2025).

2.6.5. Resilienzparadoxie

Die Resilienzparadoxie stellt eine konzeptionelle Besonderheit des SRF dar, mit der das Modell selbstreferenziell auf seine eigenen Begrenzungen hinweist. Sie greift das Prinzip der Verhältnismäßigkeit auf, indem sie mögliche Zielkonflikte zwischen Aufwand und Wirkung von Resilienzmaßnahmen sichtbar macht. Ein Aspekt, auf den ebenfalls in Art. 13 der Richtlinie Bezug genommen wird. Insbesondere bei größeren Investitionen, wie sie etwa im Bereich der physischen Sicherheit vorkommen können, ist zu berücksichtigen, dass durch den erhöhten Einsatz von Ressourcen die Resilienz geschwächt werden kann. Es ist daher erforderlich, dass alle Maßnahmen im Hinblick auf die Anzahl der Personen, einbezogenen Standorte, das Ausmaß der Technik sowie des Umfangs und der Häufigkeit von spezifischen Schulungsmaßnahmen modellierbar sein müssen. Einige der genannten Resilienzbedingungen können in den Unternehmen nur mit Hilfe einer positiven Sicherheitskultur etabliert werden und erfordern Zeit. Da die Maßnahmen insgesamt verhältnismäßig sein müssen, ist eine kontinuierliche Beurteilung der Maßnahmenumsetzung erforderlich. Aus diesem Grund wird das Kriterium der Verhältnismäßigkeit als wesentliches Steuerungselement der Unternehmensführung verstanden. Die Verhältnismäßigkeit der getroffenen Maßnahmen sollte daher für die Selbsteinschätzung im Rahmen des erforderlichen Resilienzplanes und die Einstufung durch die Behörde im Sinne des RKE-Gesetzes berücksichtigt werden (Langer et al., 2025).

2.7. Fazit und Ausblick

Mit dem SRF wird kritischen Einrichtungen ein wissenschaftlich fundiertes, praxistaugliches Instrument zur Operationalisierung der Anforderungen bezüglich strukturierter Risikobewertung sowie maßnahmenorientierter Planung und Umsetzung zur Verfügung gestellt. Dies unterstützt sowohl die betroffenen Einrichtungen bei der Erstellung wirksamer Resilienzpläne als auch Behörden bei deren systematischer Bewertung. Das SRF berücksichtigt sowohl funktionale Anforderungen als auch organisationale Fähigkeitsdimensionen. Es ermöglicht eine kontextadaptive Resilienzsteuerung auf der Grundlage anerkannter Standards (u.a. ISO 31000, ISO 22301, ISO 22361 etc.) und ergibt in Verbindung mit den zugeordneten Normelementen ein hybrides Modell, das Elemente regel- und prinzipienbasierter Steuerung miteinander kombiniert. Der zugrundeliegende Ansatz

sieht demgemäß vor, dass zunächst eine organisationsspezifische Risikoanalyse (gemäß Art. 12 Richtlinie (EU) 2022/2557) durchgeführt wird. Deren Ergebnisse werden in einem Resilienzplan (gemäß Art. 13 Abs. 2 Richtlinie (EU) 2022/2557) konsolidiert und mit geeigneten Normen und technischen Richtlinien hinterlegt. Im Zuge dessen wird zwischen Managementnormen – mit hoher systemischer Adaptionseignung – und technischen Normen – mit unmittelbarer Anwendungsorientierung – differenziert (Langer et al., 2025).

3. Stand der Technik

Aufgabe von Sicherheitskonzepten ist der Schutz von Assets oder Personen gegenüber Bedrohungen. Bei diesen spielen Barrieren und Sicherheitserrichtungen eine zentrale Rolle, wobei davon ausgegangen wird, dass Systeme, die sich durch einen hohen Technologieeinsatz kennzeichnen lassen, viele Abwehrschichten aufweisen (z.B. physische Barrieren, Alarmmeldeanlagen etc.). Im folgenden Kapitel wird nach der Beschreibung wissenschaftlich fundierter Sicherheitskonzeptmodelle, wie dem Schweizer-Käse-Modell oder Security-in-Depth zunächst ein genereller Überblick über Zwecke und Arten von Normen gegeben, um deren Ausgestaltung und Zusammenspiel auf nationaler und internationaler Ebene zu verstehen. Die RKE-RL verweist darauf, dass die Mitgliedstaaten „die Verwendung von europäischen und internationalen Normen und technischen Spezifikationen fördern, die für die Maßnahmen zur Sicherheit und Resilienz kritischer Einrichtungen relevant sind“ (ErwGr 34 Richtlinie (EU) 2022/2557). In weiterer Folge werden daher die Schwerpunkte des Art. 13 Abs. 1 lit. a-f (Richtlinie (EU) 2022/2557) sowie des § 15 Abs. 2 Z 1 bis Z 6 RKEG Verhinderung von Sicherheitsvorfällen, physischer Schutz, Abwehr und Reaktion bei Sicherheitsvorfällen, Wiederherstellung nach Sicherheitsvorfällen und Sicherheitsmanagement von Mitarbeitenden erläutert und die jeweils relevanten Normen beschrieben. Die Erläuterungen stützen sich zudem auf leitfadengestützte Interviews mit Expert*innen aus den jeweiligen Themenfeldern (siehe Kennzeichnung der Quelle mit INT_XX).

3.1. Relevante wissenschaftliche Sicherheitskonzepte

Reason (2000) differenziert zwischen zwei Zugängen zum Umgang mit menschlichen Fehlern, nämlich einem personenzentrierten und einem systemischen Zugang. Der systemische Zugang geht von der Annahme aus, dass menschliche Fehler erwartbar sind und das Individuum nicht veränderbar ist, sondern lediglich dessen Arbeitsbedingungen. Zentrale Überlegungen dabei sind, wie und warum Abwehrmechanismen bei Eintritt eines sicherheitsbedrohlichen Ereignisses versagt haben. Das Schweizer-Käse-Modell von Reason versucht zu veranschaulichen, wie eine Vielzahl an Fehlern bzw. Schwachstellen das Eintreten von Vorfällen ermöglicht. Im Schweizer-Käse-Modell steht dabei jede einzelne Scheibe für eine Schutzbarriere, die sich auf unterschiedliche Arten von Bedrohungen bezieht (Talbot & Jakeman, 2009). Im bestmöglichen Fall würde eine

Käsescheibe keine Löcher aufweisen und somit sicherheitsrelevante Bedrohungen problemlos abwehren (Reason, 2000). Analog zu Schweizer Käse weisen die einzelnen Scheiben jedoch Löcher auf, aber erst, wenn sich die Löcher mehrere Scheiben überlappen, ergibt sich daraus eine Möglichkeit für das Eintreten eines Sicherheitsvorfalles (Reason, 2000; Talbot & Jakeman, 2009). Löcher können einerseits durch Menschen entstehen, die aktiv Fehler begehen sowie andererseits durch latente Bedingungen (Reason, 2000).

Als weiteres wichtiges Konzept zum Schutz von Assets gilt Security-in-Depth (Talbot & Jakeman, 2009), bei dem ebenfalls verschiedene Schichten (vergleichbar mit den Schichten des Schweizer-Käse-Modells) zusammenwirken. Das Modell suggeriert, dass es nur einen einzigen bestmöglichen Ansatz für Sicherheitsmaßnahmen gibt, jedoch werden Sicherheitsbarrieren durch das Umfeld einer Organisation bestimmt. So befinden sich beispielsweise Sicherheitspersonen in einer militärischen Einrichtung vor dem Tor, während sich sicherheitsverantwortliche Personen zum Schutz der diversen Assets in einem Museum im Gebäude befinden. Abbildung 16 zeigt ein Beispiel des Security-in-Depth Konzeptes.

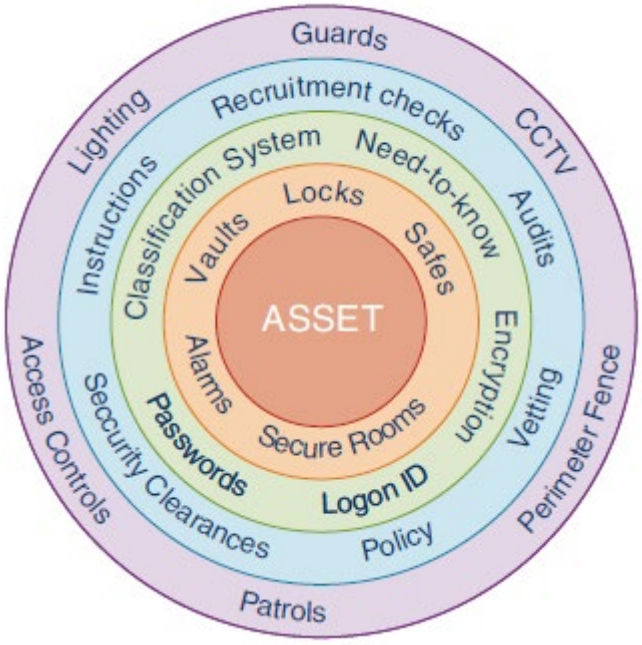


Abbildung 16: Security-in-Depth-Konzept
Quelle: Talbot & Jakeman, 2009, S. 169

In einem Expert*inneninterview zur physischen Sicherheit in Organisationen wurde darauf hingewiesen, dass unterschiedliche Schutzzonen ineinandergreifen sollten (INT_08). In der wissenschaftlichen Literatur werden vier Schutzzonen zwecks Sicherheit unterschieden, wobei jede Zone als Kreis dargestellt werden kann und auf physische Inhalte darin verweist. „A zone forms a line of protection; it is used to identify the security level required for a particular area“. Zone 1 bezieht sich

dabei auf das Grundstück, auf dem sich das schützenswerte Gebäude befindet, während Zone 2 auf „building perimeter and its facade“ (Kingsley-Hefty, 2013, S.14) verweist. Bei dieser Zone sind auch alle Zugänge zum Gebäude, wie z.B. Türen, berücksichtigt. Die dritte Schutzzone umfasst öffentliche Flächen bzw. Gemeinschaftsflächen des jeweiligen Gebäudes, wie etwa Lobbies, Gänge etc.. Die höchste Schutzzone ist Zone 4. Diese bezieht sich auf Flächen, die besonders stark geschützt werden müssen und bei denen der Zugang nur restriktiv erfolgt. Diese Flächen befinden sich zumeist im Inneren eines Gebäudes (z. B. Labore), können sich aber ebenfalls im Außenbereich befinden (z. B. Geräte zwecks Stromerzeugung) (Kingsley-Hefty, 2013).

> „The application of multiple zones, in a series of concentric circles, provides for increasing security as you move toward the center. Each subsequent zone adds another level of protection to your operation’s overall security system“ (Kingsley-Hefty, 2013, S.14).

Werden zum Beispiel Büros in verschiedene Schutzzonen unterteilt, so fallen Gänge in Zone 2, während das Büro oder die Arbeitsnische jeder Person Zone 3 und der persönliche Schreibtisch Zone 4 zugeordnet werden kann. „As with all forms of security, it is the responsibility of all personnel (employees, supervisors, managers) to follow the security procedures appropriate to each zone of protection” (Kingsley-Hefty, 2013, S.14).

3.2. Allgemeiner Überblick über Normen und normative Dokumente

Normen sind standardisierte Regeln und Anforderungen, die in unterschiedlichen Bereichen und für verschiedene Zwecke entwickelt werden und beziehen sich mittlerweile nicht mehr ausschließlich auf den technischen Sektor (GS1 Austria, 2024). „Sie dienen dem Wohl und der Sicherheit aller und machen das Leben einfacher“ (ÖNORM EN 1627:2021). Durch Normen werden u.a. Qualitätsanforderungen an Produkte gewährleistet, Abläufe und Methoden sowie Begriffe geregelt, durch die ein einheitliches Verständnis gefördert wird (Bundeskanzleramt, 2024a). Es gibt daher unterschiedliche Arten von Normen, wie Planungs- oder Produktnormen, die sich auf technische Aspekte beziehen, aber auch Verfahrensnormen oder Ausführungs-/Verarbeitungsnormen, wobei durch Letztere Anforderungen geregelt sind, wie die Ausführung einer Tätigkeit zu erfolgen hat und daher vor allem auf die Vereinheitlichung von Arbeitsprozessen abzielt (Ellmer, 2014; INT_09). Mit Produkt- und Prüfnormen setzen sich überwiegend fachspezifische Spezialist*innen in Unternehmen und Normungsgremien auseinander. „Als anerkannte Regeln der Technik fördern sie Innovation, erleichtern den globalen Marktzugang und steigern damit nachhaltig die Produktivität und Wettbewerbsfähigkeit“ (Austrian Standards, 2024b). Zentrale Bereiche, in denen Normen zur Anwendung kommen, sind neben Elektrotechnik (z. B. die Regelung der Zuverlässigkeit von elektrischen Einrichtungen), der Arbeitsplatz (z. B. Vorgaben bei etwaigen Schutzausrüstungen), Umwelt (z. B. Regelung des Strahlenschutzes oder der Abfallentsorgung), Gesundheit (z. B.

Regelung des Qualitätsmanagements bei Pflegeprozessen) sowie Managementprozesse, zu denen Normen des Sicherheits- als auch des Risikomanagements zählen (Bundeskanzleramt, 2024b).

Die Anwendung von Normen ist keine Verpflichtung, sondern basiert auf Freiwilligkeit, somit können Normen als qualifizierte Empfehlungen bezeichnet werden (Bundeskanzleramt, 2024a). Jedoch besteht die Möglichkeit für den Gesetzgeber, die Verbindlichkeit von Normen zu deklarieren (Brühwiler & Glaser, 2021; Wirtschaftskammer Österreich, 2024). Normen können ebenfalls zwischen Geschäftspartner*innen in einem Vertrag beschlossen werden. Wird diesen Normen nicht Folge geleistet, handelt es sich somit um eine Vertragsverletzung. Brühwiler & Glaser (2021) unterscheiden demnach zwei Typen von Normen:

1. Empfehlende Standards (Typus B), welche einen viel größeren Spielraum für Erklärungen und Beschreibungen bieten und
2. Standards, die Anforderungen festschreiben (Typus A) und damit zertifiziert werden können. Diese Normen müssen präzise formuliert sein, um eine klare und überprüfbare Umsetzung zu ermöglichen (Brühwiler & Glaser, 2021).

Relevant ist die weitere Einteilung von Normen in Grund-/Basisnormen sowie spezifischen Unternormen, wobei als Grundnorm eine Norm gilt, „die ein weit reichendes Anwendungsgebiet hat oder allgemeine Festlegungen für ein bestimmtes Gebiet enthält“ (Ellmer, 2014, S.5). Grundlage für die Erstellung von Normen bilden verifizierte Ergebnisse aus Wissenschaft, Technik sowie Erfahrungswerte. Sie werden in Normungsgremien unter Einigkeit der jeweils involvierten Fachpersonen entwickelt. Austrian Standards International forciert die Teilnahme relevanter Stakeholder aus unterschiedlichen Branchen wie Wirtschaft, Forschung, Behörden an Normungsgremien (Austrian Standards International, 2024b).

Terminologisch kann eine Abgrenzung des Normenbegriffs zum Begriff Standard vorgenommen werden. Standards werden nicht von einem offiziellen Normengremium bzw. in keinem öffentlichen Einspruchsverfahren beschlossen, sondern durch Unternehmen bestimmter Wirtschaftsbereiche auf Basis gewisser Erfordernisse definiert. Sie beziehen sich auf eine einheitliche Weise der Herstellung von Produkten, welche sich gegenüber anderen Verfahren behauptet hat. Standards fokussieren darauf die Wirtschaftlichkeit von geschäftlichen Abläufen zu maximieren, sowohl unternehmensintern als auch zwischen einzelnen Unternehmen, während Normen darauf abzielen, den Status Quo der Technik darzustellen (GS1 Austria, 2024). Im Englischen wird zwischen diesen beiden Begriffen nicht differenziert. Da auch im alltäglichen deutschen Sprachgebrauch sowie im Unternehmenskontext zwischen diese beiden Begriffe selten unterschieden wird, erfolgt im weiteren Verlauf des vorliegenden Textes eine synonyme Verwendung dieser beiden Begrifflichkeiten.

Eine grundsätzliche Unterscheidung gibt es zwischen internationalen, europäischen sowie nationalen Normen, worauf im Folgenden näher eingegangen wird.

3.2.1. Internationale Normen (ISO)

ISO-Normen, die von der Internationalen Organisation für Normung (International Standards Organization - ISO) in einem internationalen Prozess ausgearbeitet und veröffentlicht werden sind von erheblicher Bedeutung. ISO-Normen können in nationale Normen übertragen werden, dafür besteht aber keine Verpflichtung. Die Gültigkeit von ISO-Normen ist global und sie zielen darauf ab, internationale Handelsprozesse zu fördern sowie Sicherheit zu gewährleisten. Als internationale Normungsorganisation ist neben der International Standards Organization auch die International Electrotechnical Commission (IEC) zu nennen (Bundeskanzleramt, 2024d; DOCUmedia, 2024).

High Level Structure / Harmonized Structure

Die High-Level Structure (HLS) wurde von der International Standards Organization im Jahr 2012 als Leitfaden eingeführt, mit dem Ziel, einen einheitlichen Aufbau bzw. eine einheitliche Struktur sowie gemeinsame Begriffe für ISO-Normen zu etablieren. Hintergrund dafür ist, dass eine Vielzahl an Managementsystemnormen besteht (z.B. ISO 9001, ISO 14001) und z. B. darin beschriebene Definitionen zu gleichen Begrifflichkeiten Unterschiede aufweisen. Durch die Einführung der HLS wurde intendiert, die verschiedenen ISO-Normen untereinander besser abzustimmen und in weiterer Folge zu harmonisieren. Seit Frühjahr 2021 wird die HLS Harmonized Structure (HS) bzw. Harmonized Approach (HA)[3] genannt, wobei die HLS „einer Revision mit diversen Klarstellungen, Ergänzungen, aber auch Streichungen“ unterzogen wurde (Dröge, 2024). Grundsätzlich kam es aber zu einer Aufrechterhaltung der grundlegenden Kernanforderungen der HLS, auch inhaltlich kam es zu keinen wesentlichen Adaptierungen. Zu betonen ist, dass „die gemeinsamen Grundanforderungen die Integration verschiedener Systeme in ein Unternehmen“ begünstigen (Dröge, 2024).

Die HS, welche mit der nächsten Überarbeitung der entsprechenden Norm wirksam wird, weist eine Grundstruktur von zehn Kapiteln auf, wobei zu Beginn immer auf den Anwendungsbereich, normative Verweise und Definition von Begriffen eingegangen wird. Gewichtung liegt vor allem auf dem vierten Kapitel, bei dem es um die Führungsebene geht sowie auf dem fünften Kapitel, welches das Umfeld der Organisation thematisiert. Des Weiteren sind die einzelnen Kapitel mit dem Plan-Do-Check-Act-Zyklus (PDCA) vereinbar, der einen Regelkreis für die Lösung von Problemen und Förderung von Arbeitsprozessen in Organisationen bezeichnet (Dröge, 2024; Durst et al.,

[3] In weiterer Folge wird im Bericht statt High-Level-Structure somit der Begriff Harmonized Structure bzw. Harmonized Approach verwendet.

2021). Vor allem bei den ersten drei Kapiteln zeigen sich starke Parallelen zum Aufbau der OVE-RL oder Europäischen Normen. Die ISO 27001:2022 zur Informationssicherheit folgt bereits einer HS. Darüber hinaus wird „die Einführung mehrerer Managementsysteme, zum Beispiel Qualität, Umwelt, Informationssicherheit, wesentlich vereinfacht und effizienter“ (Dröge, 2024).

3.2.2. Europäische Normen (EN)

Europäische Normen (EN) werden in einem europäischen Prozess erarbeitet und von einer der drei europäischen Normungsorganisationen Comité Européen de Normalisation – Europäisches Komitee für Normung (CEN), Comité Européen de Normalisation Electrotechnique – Europäisches Komitee für elektrotechnische Normung (CENELEC) bzw. European Telecommunications Standards Institute – Europäisches Normungsinstitut für Telekommunikation (ETSI) herausgegeben. Normen von CEN und CENELEC haben zentrale Bedeutung für den Arbeitsschutz und zielen darauf ab, die Konkurrenzfähigkeit von Unternehmen zu fördern (Bundeskanzleramt, 2024d; DOCUmedia, 2024; IAS Gruppe, 2024). Im Gegensatz zu den internationalen ISO-Normen ist es bei Europäischen Normen verpflichtend, diese direkt und ohne Adaptierung in nationale Normen zu übernehmen (Bundeskanzleramt, 2024d).

3.2.3. Deutsche Normen (DIN)

In Deutschland sind die sogenannten DIN-Normen des Deutschen Instituts für Normung (DIN) von zentraler Bedeutung, wobei die DIN-Formate zu den Normen mit der größten Bekanntheit zählen. Ein klassisches Beispiel ist das Format DIN A4. Durch diese Norm ist gewährleistet, dass jedes Papier, das diesem Format entspricht, mit einem Drucker etc. kompatibel ist. DIN-Formate wurden im Jahr 1922 erstmals veröffentlicht und sind heutzutage durch die Bezeichnung DIN EN ISO 216 abgedeckt. Das deutsche Normenwerk umfasst derzeit mehr als 30 000 Normen. Eine große Bandbreite an Alltagsgegenständen wird durch DIN-Normen geregelt, von Anforderungen an Schrauben bis hin zu Zahnbürsten etc. (Deutsches Institut für Normung, 2024).

3.2.4. Österreichische Normen und normative Dokumente

In Österreich sind unterschiedliche Arten von Standards, wie Normen, Richtlinien oder Regeln vorhanden, welche den Stand der Technik abbilden. Überblicksmäßig kann dabei zwischen ÖNORMEN, OVE-Richtlinien sowie ON-Regeln differenziert werden.

ÖNORM

Österreichische Normen werden ÖNORMEN genannt und von Austrian Standards International (ASI) entwickelt bzw. herausgegeben. Des Weiteren ermöglicht ASI die Mitarbeit an der europäischen sowie internationalen Normung. Laut aktuellem Stand gibt es zirka 24 000 ÖNORMEN.

Durch diese werden Anforderungen, Spezifikationen etc. für Dienstleistungen, Prozesse sowie Produkte definiert und wie auch bei internationalen und europäischen Normen sollen dadurch die Qualität und Sicherheit gestärkt werden. Wie bereits in den oben genannten Erläuterungen ersichtlich, kann zwischen tatsächlichen österreichischen Normen sowie von ASI übernommenen Normen differenziert werden (Bundeskanzleramt, 2024d; DOCUmedia, 2024). Den Großteil der Normen bilden europäische Normen, die in das österreichische Normensystem übernommen wurden. Sind ÖNORMEN vorhanden, die in einem Konflikt zu europäischen Normen stehen, werden die entsprechenden ÖNORMEN entweder adaptiert oder zurückgezogen (DOCUmedia, 2024). Handelt es sich lediglich um ÖNORMEN und keine übernommenen Normen, so werden sie gegliedert und mit verschiedenen Buchstaben versehen, die für unterschiedliche Bereiche stehen, z.B. A für allgemeine Norm, B für Bauwesen etc. Nach der Nennung des entsprechenden Buchstabens ist die Normennummer, welche aus vier Ziffern besteht, angegeben bzw. wenn es sich um ÖNORMEN handelt, die aus mehreren Teilen bestehen, so wird die Norm mit einer angehängten Nummer angegeben (z.B. ÖNORM B 1300 oder ÖNORM B 3800-1). Die ÖNORM B 1600 stellt beispielsweise Planungsgrundlagen für barrierefreies Bauen dar. Auf die Normennummer folgend, erfolgt die Angabe des Erscheinungsjahres der jeweiligen Norm (Bundeskanzleramt, 2024d; DOCUmedia, 2024).

OVE-RL

Für den Bereich der Elektrotechnik in Österreich gibt es sogenannte OVE-Richtlinien (OVE-RL), welche in Zusammenarbeit mit dem Österreichischen Verband für Elektrotechnik (OVE) ausgearbeitet werden (Bundeskanzleramt, 2024b). Bei diesen Richtlinien handelt es sich um „normative Dokumente mit technischen Anforderungen oder Anleitungen, die von einer Interessensgruppe ausgearbeitet wurden“. Sie bieten die Möglichkeit, „neue normative Anforderungen in einer kurzen Zeitspanne zu veröffentlichen“ (Österreichischer Verband für Elektrotechnik, 2024).

ONR

Des Weiteren ist in Österreich die sogenannte ONR (ON-Regel) etabliert. Dabei handelt es sich um eine technische Spezifikation, die ebenfalls von ASI herausgegeben wird. Diese Norm „dokumentiert den Stand einer neuen oder sich schnell verändernden Entwicklung und muss nicht alle Anforderungen einer ‚klassischen‘ Norm erfüllen“. Durch eine ONR soll eine Art Grundlage für die etwaige Entwicklung einer späteren Norm geboten werden (Austrian Standards International, 2024b).

3.3. Entstehung von Normen am Beispiel von ÖNORMEN

Normen werden aus der Praxis generiert und zielen auch auf diese ab. Bei Bedarf an anerkannten Regelungen sind an der Entstehung von Normen Unternehmen, Organisationen, Branchen etc. beteiligt (Bundeskanzleramt 2024c). Ausgangspunkt bildet somit eine Neuschöpfung, etwa ein Produkt oder Technologie, die Standardisierung sowie einheitliche Regelungen erfordert (Austrian Standards International, 2024b). Zu Beginn ist ein Projektantrag einzureichen (über ein Online-Formular bei ASI). Falls schon ein Komitee zu diesem Themenfeld vorhanden ist, kommt es zur Prüfung des Antrages durch das Komitee in Kooperation mit den antragstellenden Einheiten. Ziel dabei ist, die ÖNORM erstmals zu entwickeln bzw. zu modifizieren. Ab diesem Zeitpunkt kann die Öffentlichkeit innerhalb von 28 Tagen Stellungnahmen abgeben, ehe im Anschluss an die erste Prüfung und die Berücksichtigung der Stellungnahmen über die Aufnahme des Antrages in das Arbeitsprogramm entschieden wird. Nach einer positiven Beurteilung des Vorschlags, kommt es zur Bekanntgabe an die Öffentlichkeit, bei dem sich in weiterer Folge unterschiedliche Interessent*innen am Normungsprozess beteiligen können. Nach der Ausarbeitung eines Vorschlags, geleitet durch einen Komitee-Manager von ASI anhand eines vorgegebenen Zeitplans, wird der Entwurf veröffentlicht. Innerhalb von sechs Wochen können, über das Normen-Entwurf-Portal, Stellungnahmen dazu abgegeben werden, die in einem nächsten Schritt geprüft werden. Daraus folgend wird entschieden, ob der Entwurf als ÖNORM herausgegeben, überarbeitet, oder keine weitere Berücksichtigung des Entwurfs erfolgt. Bei einer Herausgabe von ÖNORMEN werden folgende drei Prinzipien beachtet: Konsens, Publizität und Widerspruchsfreiheit. Beim Prinzip Konsens ist gemeint, dass ÖNORMEN vom jeweiligen Komitee einstimmig, unter Beseitigung aller möglichen Einwände, beschlossen werden. Das zweite Prinzip Publizität bedeutet, dass vor dem Publizieren einer Norm, die Öffentlichkeit die Möglichkeit hat Stellungnahmen abzugeben. Das letzte Prinzip Widerspruchsfreiheit meint, dass stichhaltige Gegenargumente vom Komitee zu beachten sind und vor Veröffentlichung die Unität der Norm vorliegen muss. Nach der Herausgabe einer Norm, ist deren Gültigkeit in einem Abstand von mindestens drei Jahren einer Prüfung zu unterziehen (DOCUmedia, 2024). Normen unterliegen somit einer laufenden Anpassung und es ist daher wichtig, bei der Anwendung einer Norm auf deren Gültigkeit zu achten (Austrian Standards, 2024b).

3.4. Kombination ÖNORM, EN, ISO

Die Bezeichnung von Europäische Normen (EN), welche verpflichtend ins österreichische Normensystem zu übernehmen sind, lautet ÖNORM EN. Wird eine internationale Norm (ISO) in das österreichische Normensystem übernommen, so wird es als ÖNORM ISO angegeben. Wenn eine Norm international, europäisch sowie national anerkannt ist, wird sie ÖNORM EN ISO genannt. Diese Kombination von Normen bedeutet somit, dass eine ISO-Norm von europäischen Ländern

akzeptiert und parallel dazu in das österreichische Normensystem einbezogen wird bzw. die internationalen Normen in Zusammenarbeit mit dem CEN entstehen und in weiterer Folge somit europäische sowie nationale Normen sind. Als Basis dafür fungiert das sogenannte Vienna Agreement, welches 1991 den Ausgangspunkt für die Kooperation zwischen ISO und CEN bildet. Auf diese Weise können gegensätzliche Festsetzungen sowohl international als auch auf europäischer Ebene ausgeschlossen werden, getreu dem Motto „One standard, one test – accepted everywhere“ (Austrian Standards, 2024a; Bundeskanzleramt, 2024d; DOCUmedia, 2024).

Abbildung 17 zeigt die Bezeichnung der Kombination von ISO, EN und ÖNORMEN sowie weitere relevante Informationen, die in der Bezeichnung einer Norm angegeben sind.

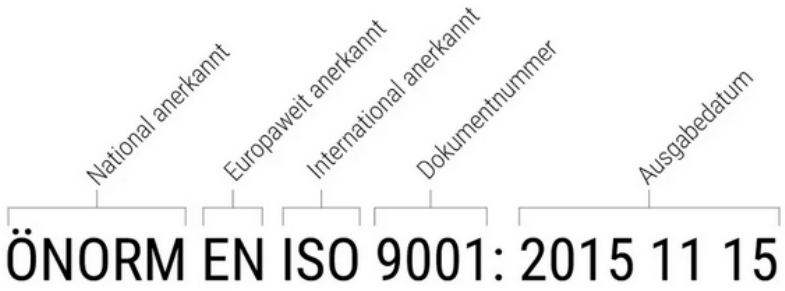


Abbildung 17: Kombination von ÖNORMEN, EN, ISO-Normen
Quelle: Austrian Standards, 2024a

Eine weitere Kombination von Normen in Österreich bilden die sogenannten ÖVE/ÖNORMEN, welche durch die Zusammenarbeit von CEN und CENELEC entwickelt wurden und in Österreich in Kombination von ASI und OVE veröffentlicht werden. Diese Normen „legen im elektronischen Bereich Anforderungen an Produkte, Dienstleistungen, Systeme und Qualifikationen fest und definieren, wie die Einhaltung dieser Anforderungen überprüft wird (Austrian Standards International, 2024b).

3.5. Normen nach spezifischen Themenfeldern gemäß RKE-RL Artikel 13

Im nächsten Abschnitt werden in einem ersten Schritt allgemeine Normen zu Resilienz beschrieben und anschließend relevante Normen und Richtlinien nach Themenfeldern des Artikels 13 der RKE-RL identifiziert und deren praktische Anwendbarkeit im Kontext der RKE-RL diskutiert.

3.5.1. Normen mit Relevanz für organisationale und gesellschaftliche Resilienz

Normen, die einen Handlungsrahmen anbieten, sind generisch gestaltet, da nicht jeder Teilbereich eines Unternehmens oder Asset denselben Schutz erfordert (Garcia, 2008). Allgemeine Normen müssen daher an jede Einrichtung angepasst werden. Voraussetzung für eine sinnvolle und anwendungsorientierte Implementierung normgeleiteter Prozesse ist das Definieren von Schutzgütern in jeder Organisation. Expert*innen aus der Praxis bestätigen, dass erst wenn Schlüsselstellen identifiziert wurden, zielgerichtete Resilienzpläne entwickelt werden können (INT_05).

Im Kontext der Umsetzung der RKE-Richtlinie 2022/2557 sind gemäß ASI mehrere internationale Normen von Bedeutung, die sich mit organisationaler und gesellschaftlicher Resilienz befassen.

Die ISO 22316 bietet grundlegende Leitlinien zur Organisationsresilienz und kann dabei unterstützen, strukturelle und kulturelle Voraussetzungen für widerstandsfähige Organisationen zu schaffen. Ergänzend dazu vertieft die ISO/CD 22316 diese Ansätze in einer überarbeiteten Fassung. Die Normen ISO/DIS 22354, ISO/DIS 22372 und ISO 22396 erweitern den Fokus auf gesellschaftliche und gemeinschaftsbasierte Resilienz, etwa durch den Aufbau lokaler Resilienzkapazitäten, den Schutz kritischer Infrastrukturen sowie durch die Förderung strukturierter Informationsflüsse zwischen Organisationen. Darüber hinaus liefert die IEC 62351 konkrete Sicherheitsanforderungen für Kommunikationsprotokolle in Energieversorgungsnetzen – ein zentraler Aspekt für Betreiber kritischer Einrichtungen im Energiesektor im Sinne der RKE-RL. Die ISO/TS 22375 unterstützt Organisationen bei der systematischen Bewertung von Komplexität, ein essenzieller Bestandteil in der Vorbereitung auf schwer vorhersehbare Störungen in hochvernetzten Systemen. Ergänzend bietet die ISO 22392 praxisnahe Hinweise zur Durchführung von Peer Reviews, die den Austausch zwischen Organisationen fördern und als Instrument zur kontinuierlichen Verbesserung der Resilienz dienen können.

Diese Normen bieten damit nicht nur methodische und strategische Grundlagen für sektorübergreifende und systemische Resilienzplanung, sondern unterstützen auch die konkrete Umsetzung zentraler Vorgaben der RKE-Richtlinie – insbesondere im Hinblick auf Kooperation, Kommunikation, Informationssicherheit und die Fähigkeit zur adaptiven Selbstbewertung. Sie ermöglichen es kritischen Einrichtungen, sowohl ihre internen Strukturen zu stärken als auch ihre Einbettung in resiliente Gesamtsysteme aktiv zu gestalten.

3.5.2. Verhinderung von Sicherheitsvorfällen

Die RKE-Richtlinie verpflichtet kritische Einrichtungen unter anderem regelmäßig umfassende Risikobewertungen durchzuführen, um Risiken zu identifizieren und zu bewerten, die ihre wesentlichen Dienste beeinträchtigen könnten. Diese Risikobewertungen müssen mindestens alle vier

Jahre erfolgen oder bei besonderen Entwicklungen und Umständen angepasst werden (RKE-Richtlinie 2022/2557).

Dabei verfolgt die RKE-Richtlinie einen breiten Risikobegriff im Sinne eines All-Gefahren-Ansatzes. Als Risiken gelten alle Ereignisse und Entwicklungen, die die Erbringung wesentlicher Dienste einschränken können. Dazu zählen unter anderem Wetterextreme, Klimawandel und Naturkatastrophen ebenso wie systemische Risiken, etwa durch sektorübergreifende Abhängigkeiten oder Störungen in Lieferketten. Darüber hinaus werden auch vorsätzliche und unbeabsichtigte Bedrohungen berücksichtigt, beispielsweise durch Terrorismus, Sabotage, Fehlverhalten oder Unfälle, das heißt es werden sowohl Security- als auch Safety-Aspekte[4] berücksichtigt.

Risikobewertungen sind ein wesentlicher Bestandteil eines übergeordneten Risikomanagements (Romeike & Hager, 2020). Risikomanagement wird als systematischer Umgang mit Unsicherheiten beschrieben, der darauf abzielt, Prozesse und Ziele in Organisationen zu steuern, mit dem übergeordneten Ziel Sicherheitsvorfälle zu verhindern (ÖNORM ISO 31000; Romeike & Hager, 2020). Dabei werden Risiken nicht nur als negative Szenarien betrachtet, sondern auch als potenzielle Chancen – ein Aspekt, der in der Praxis häufig seltener beachtet wird und für die RKE-RL derzeit keine Relevanz hat (ÖNORM D 4900; Romeike & Hager, 2020). Zentrale Bestandteile des Risikomanagement-Prozesses sind die Risikobeurteilung, welche Risikoidentifikation, -analyse und -bewertung subsumiert, sowie die Risikobewältigung. Zudem beinhaltet dieser Prozess die systematische Überwachung und Überprüfung von Risiken sowie die fortlaufende Kommunikation über sich möglicherweise ändernde Risiken (ISO 31000:2009). Es gibt eine Vielzahl an Normen im Bereich des Risikomanagements, die von generischen Normen wie der ISO 31000 bis zu branchenspezifischen Regelungen, wie im Banken- oder Arzneimittelbereich, reichen. Andere relevante Standards im Kontext des Risikomanagements sind die Basel-Regelungen für den Finanzsektor und der COSO ERM – Enterprise Risk Management Framework, welcher ein prozessorientierter internationaler Standard ist, der auf strategischer Ebene operiert (INT_01; INT_06). Ob Organisationen ihr Risikomanagement auf ISO-Normen stützen oder Rahmenwerke wie COSO heranziehen ist unter anderem abhängig von den Branchen sowie vom Produkt beziehungsweise der Dienstleistung. Ein wichtiges Kriterium ist zudem, ob Standards zertifizierbar sind – wobei weder COSO, noch ISO 31000 zertifiziert werden können (INT_06).

Der COSO-Würfel adressiert das Zusammenspiel zwischen Zielsetzungen und den Komponenten des Risikomanagements, wobei das gesamte Unternehmen und alle Ebenen betrachtet werden. Jedes System wird dabei in Komponenten, Einheiten (Entitäten), Zielsetzungen und Prinzipien unterteilt. Zielsetzungen werden dabei formuliert und bilden den Rahmen für die Analyse (INT_06.). Im Gegensatz zum Rahmenwerk der COSO ERM ist die ISO 31000 generisch

[4] Siehe Unterscheidung „Safety“ und „Security“ in Endbericht SIKU-KRITIS

ausgestaltet und differenziert nicht explizit zwischen unterschiedlichen Einheiten innerhalb einer Organisation (ÖNORM D 4900:2021-01; INT_01, INT_06). Sie verfolgt einen Top-down Ansatz und nimmt ihren Ausgangpunkt in der strategischen Ausrichtung einer Organisation (Brühwiler, 2026). „Die ISO 31000 enthält Empfehlungen wie eine Organisation Risikomanagement planen und umsetzen soll“ (Brühwiler & Glaser, 2021, S. 28). Konkrete Handlungsanleitungen gibt die Norm nicht. Sie beschreibt Grundsätze, Systemelemente und Prozesse, die in einem weiteren Schritt jedoch an die jeweilige Organisation angepasst und damit lebbar gemacht werden müssen (Brühwiler, 2016; INT_01; INT_03; INT_05). „Die ÖNORM-Reihe D 490x Risikomanagement für Organisationen und Systeme zeigt auf, wie die ÖNORM ISO 31000 konkret in der Praxis umgesetzt werden kann. Die Anforderungen der ÖNORM D 4901 werden als überprüfbare Anforderungen dargestellt und können auditiert und extern zertifiziert werden“ (ÖNORM D 4900:2021-01, S. 4). Die ÖNORM-Reihe D 490x beinhaltet aktuell sechs weitere ÖNORMEN, welche die ISO 31000 spezifizieren (siehe Abb. 18).

Abbildung 18: Risikomanagement für Organisationen und Systeme
Quelle: ÖNORM D 4900:2021-01, S. 4

Relevante Begriffe im Risikomanagement

In den unterschiedlichen Normen werden für den jeweiligen Schwerpunkt einleitend einige relevante Begriffe angeführt. Die Anzahl der Begriffsdefinitionen variiert dabei stark. Die unterschiedlichen Normen verweisen teilweise auch hinsichtlich Begriffsbestimmung aufeinander.

In der RKE-RL findet sich folgende Definition von Risiko und Risikobewertung:

> „6. Risiko das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird;
>
> 7. Risikobewertung den gesamten Prozess zur Bestimmung der Art und des Ausmaßes eines Risikos, bei dem potenzielle entsprechende Bedrohungen, Schwachstellen und Gefahren, die zu einem Sicherheitsvorfall führen könnten, ermittelt und analysiert und die durch den Sicherheitsvorfall verursachten potenziellen Verluste oder Störungen bei der Erbringung eines wesentlichen Dienstes bewertet werden.“ (Art. 2 Nr. 6, Nr. 7 Richtlinie (EU) 2022/2557)

Die Definition von Risiko in der ÖNORM ISO 31000, welche in der ÖNORM D 4900 aufgegriffen wird, lautet:

> „Risiko: Auswirkung von Unsicherheit auf Ziele
>
> Anmerkung 1 zum Begriff: Eine Auswirkung stellt eine Abweichung vom Erwarteten dar. Diese Abweichung kann positiv, negativ oder beides sein und kann auf Möglichkeiten und Bedrohungen eingehen, diese verursachen oder durch diese verursacht werden.
>
> Anmerkung 2 zum Begriff: Ziele können verschiedene Aspekte und Kategorien umfassen und auf allen Ebenen angewendet werden.
>
> Anmerkung 3 zum Begriff: Das Risiko wird üblicherweise anhand der Risikoursachen (3.4), der potenziellen Ereignisse (3.5), ihrer Auswirkungen (3.6) und ihrer Wahrscheinlichkeit (3.7) dargestellt“ (ÖNORM ISO 31000).

Es zeigen sich auch Unterschiede zwischen den Normen. Beispielsweise finden sich in der ISO 31000 aus dem Jahr 2009 28 Begriffsdefinitionen und 11 Prinzipien. Dahingegen werden in der ÖNORM ISO 31000 von 2018 jeweils acht Begriffsbestimmungen und Prinzipien angeführt (ISO 31000-2009; ÖNORM ISO 31000-2018).

Darüber hinaus sind im Risikomanagementprozess Begriffe zentral, die nicht explizit in der Norm genannt werden. Dazu gehören zum Beispiel Assets, Vulnerabilitäten und mögliche Bedrohungen. Diese Begriffe helfen dabei, das Risikomanagement in einer Organisation zu definieren und Risiken abzuleiten. Indem man die Kombination dieser drei Faktoren betrachtet, analysiert man, welchen Einfluss Unsicherheiten auf die Assets haben können (INT_05). Zu Beginn muss definiert werden, was Schutzgüter sind bzw. worauf das Risikomanagement abzielen soll (INT_01; INT_05). Darauf folgt die Identifikation davon, was die bekannten Risiken (Vulnerabilitäten) sind.

Risiken sollen zudem bewertet und beschrieben werden (Risikoanalyse). Anschließend erfolgt die Risikobehandlung, die festlegt, wie mit den identifizierten Risiken umgegangen werden soll. Die ISO 31000 unterscheidet dabei nicht explizit zwischen bestimmten Arten der Risikominderung, verweist jedoch auf die Möglichkeit, sowohl die Eintrittswahrscheinlichkeit eines Risikos als auch dessen potenzielle Auswirkungen zu verändern. In der Praxis lassen sich diese Strategien oft in zwei grundlegende Ansätze unterteilen:

1. Probability Mitigation, also die Reduktion der Eintrittswahrscheinlichkeit eines Risikos, und
2. Impact Mitigation, die Minimierung der negativen Folgen im Fall eines Risikoeintritts. Die Begrenzung der Auswirkungen erfolgt stufenweise. Diese lassen sich wiederum in zwei Arten unterscheiden:
    a. Aktive Risikosteuerung, also direkte Maßnahmen zur Einflussnahme auf den Risikoverlauf, etwa durch Vermeidung (z. B. durch die Unterlassung riskanter Aktivitäten), Verminderung oder Begrenzung der Auswirkungen (z. B. durch Notfallpläne, bauliche Schutzmaßnahmen oder Redundanzsysteme).
    b. Passive Risikosteuerung, also der Umgang mit verbleibenden Risiken, u. a. durch Risikotransfer bzw. Überwälzung (z. B. durch Versicherungen oder vertragliche Regelungen), oder Risikoübernahme (bewusste Inkaufnahme des Risikos, z. B. wenn es als akzeptabel oder unausweichlich bewertet wird).

Unter dem Label der Risikobehandlung fällt allerdings nicht nur die Minderung, sondern auch das bewusste Eingehen eines Risikos, z. B. wenn der erwartete Nutzen die potenziellen Nachteile überwiegt, wenn keine realistischen Alternativen bestehen oder wenn das Risiko mit den vorhandenen Ressourcen akzeptabel erscheint. Auch dieser Umgang wird im Sinne eines verantwortungsvollen und dokumentierten Risikomanagements als legitime Form der Risikobehandlung betrachtet.

Ein Restrisiko bleibt jedoch bestehen, selbst nach der Umsetzung von Maßnahmen. Am Ende des Prozesses stehen die erwarteten Verluste (expected losses), die durch Modelle quantifiziert werden können sowie die unerwarteten Verluste (unexpected losses), die darüber hinausgehen. Diese Begriffe kommen häufig aus dem Finanzbereich, lassen sich jedoch in vielen Fällen anwenden, wo Risiken berechnet werden können. Auf Grundlage dieser Analysen können dann beispielsweise finanzielle Rücklagen geplant oder gezielte Maßnahmen zur Bewältigung erwarteter Verluste sowie für unvorhersehbare Schäden gesetzt werden (INT_05).

Trotz aller Analysen und Planung bleiben unbekannte sowie unerwartete und unwahrscheinliche Risiken, die jedoch erhebliche Auswirkungen haben können, sogenannte Schwarze Schwäne (Taleb, 2018). Deren Natur liegt gerade darin, dass sie sich kaum vorhersagen oder einplanen lassen und der Aufwand einer konkreten Planung oft unverhältnismäßig hoch wäre. Für deren

Bewältigung ist vor allem das Krisenmanagement als integraler Bestandteil des Business Continuity Management (BCM) entscheidend, welches darauf abzielt, Strukturen und Abläufe zu schaffen, um bei ihrem Eintritt angemessen reagieren zu können (siehe Kapitel 3.6.2). Notfallpläne und konkrete Planungen sind im Ernstfall möglicherweise nicht ausreichend. Zudem erfordern diese Risiken eine gewisse organisatorische Resilienz, um die Organisation auch in unvorhergesehenen Szenarien handlungsfähig zu halten (INT_05).

Risiko- und Sicherheitskultur

Ein weiterer wichtiger Aspekt, auf den in den Normen explizit eingegangen wird, ist die Unternehmenskultur (IEC 31010:2019; ISO 31000-2009; ÖNORM D 4900:2021-01). Speziell bei der Implementierung und Umsetzung von Normen spielt die Sicherheitskultur eine wichtige Rolle unter anderem dabei, wie und welche Richtlinien, Vorgaben und Empfehlungen Organisationen von oben (Tone from the top) zur Erreichung der Unternehmensziele vorgeben. Zudem prägt diese Kultur auch, wie diese Vorgaben sowohl von der Managementebene sowie den Mitarbeitenden, sozusagen von unten, gelebt wird (Körmer et al., 2024; Nicolai, 2020; Pfeiffer, o.D.).

Den Normen folgend betrachtet ein integrierter Ansatz des Risikomanagements die Unternehmenskultur als wesentlichen Bestandteil von Entscheidungen, Prozessen und Organisationsstrukturen. Die Integration einer positiven Risikokultur in die Organisationskultur fördert deren Entwicklung und zielt darauf ab, unsichere Handlungen zu minimieren und eine proaktive Auseinandersetzung mit Risiken zu gewährleisten. Sie trägt dazu bei, Werte zu schützen und die Organisation langfristig resilienter zu machen. Ein zentrales Ziel des Risikomanagements besteht laut Norm auch darin, eine solche Kultur aufzubauen und zu erhalten (ÖNORM D 4900:2021-01, S. 15).

In den Normen werden die Begriffe Risikokultur und Sicherheitskultur unterschieden:

> „Risikokultur
>
> Art des Denkens, Handelns und Verhaltens einer Organisation und ihrer Führungskräfte und Mitarbeiter im Umgang mit Risiken
>
> Anmerkung 1 zum Begriff: Die Risikokultur beinhaltet die Fehler-, Sicherheits- und Innovationskultur.
>
> Sicherheitskultur
>
> Denken, Entscheiden, Handeln und Verhalten einer Organisation und ihrer Führungskräfte und Mitarbeiter im Umgang mit Sicherheit“ (ÖNORM D 4900:2021-01, S. 8).

Des Weiteren betont die ÖNORM D 4900 folgendes:

> „Die konkrete Ausgestaltung des Risikomanagements ist auch wesentlich von der Sicherheitskultur einer Organisation geprägt. Diese umfasst als Teil der Organisationskultur Einstellungen, Überzeugungen, Wahrnehmungen, Werte und Verhaltensweisen von Führungskräften und Mitarbeitenden in

> Bezug auf Sicherheit von Menschen, Objekten, Prozessen und der Organisation“ (ÖNORM D 4900:2021-01, S. 10).

Während Normen somit zwar die Bedeutung kultureller und sozialer Aspekte wie sozioökonomischer Status, ethnische Herkunft, Geschlecht und soziale Beziehungen betonen, bleiben die Begriffe insgesamt vage (IEC 31010:2019, S. 14; INT_01; INT_06). Diese unpräzise Definition der „Kultur-Begriffe“ verhindert, dass Kultur in Organisationen an spezifischen Kriterien messbar ist (INT_01; INT_06). Es wird Organisationen somit bewusst gemacht, dass soziale und kulturelle Aspekte von zentraler Bedeutung sind. Allerdings wird nicht näher darauf eingegangen, wie diese Aspekte konkret in die Praxis umgesetzt werden können.

Problemfelder bei Normen im Bereich Risikomanagement

Aufgrund ihres prozessualen Charakters fehlt es Normen im Risikomanagement mitunter an konkreten Anleitungen, wie diese Prozesse umgesetzt werden sollen. Werden Normen unreflektiert angewendet, kann dies möglicherweise zu einer Scheinsicherheit führen, da Risiken zwar formal erfasst werden, die tatsächlichen Herausforderungen jedoch nicht immer ausreichend hinterfragt oder adressiert werden (INT_05).

> „Also mir sind sie als Norm für jemanden, der nicht Experte ist, viel zu lose formuliert. Für einen Experten ist es klar, wenn man 20 Jahre in dem Bereich arbeitet. Man liest sich die Norm durch, ist eigentlich völlig klar, wie man die Sachen umsetzen muss. (…) Also ich habe das Gefühl, dass nicht viele wirklich verstehen, was Risikomanagement ist. Wenn sie sich die ISO 31000 durchlesen, geschweige denn das dann auch umsetzen können“ (INT_04).

Zwischen den Anforderungen der Norm und der Umsetzung kann zudem eine Diskrepanz bezogen auf die Definition von Zielen beziehungsweise Schutzgütern entstehen. Die Normen setzen oft voraus, dass die Ziele einer Organisation bereits klar definiert sind, bieten hierfür jedoch selbst wenig Orientierung. Vor allem mit Blick auf das vorliegende Projekt ist es von Seiten der Behörden wichtig zunächst zu definieren: Was ist die Mindestleistung, die erbracht werden muss? Was wird von der Organisation erwartet, und auf welche Szenarien soll sie sich vorbereiten? Ohne eine klare Zielsetzung bleibt das Risikomanagement in vielen Fällen unvollständig (INT_05).

Ein weiteres Problem ist die fehlende Bewertung und Anleitung zu den in Normen enthaltenen Werkzeugen und Konzepten. Ein Beispiel hierfür ist die Risikomatrix, die dann beispielsweise in Normen als Konzept angeführt wird, jedoch ohne Hinweise auf ihre Anwendbarkeit und Grenzen. Organisationen können dann mitunter zu wenig einschätzen, wann und wie solche Tools sinnvoll eingesetzt werden können oder wo sie möglicherweise unzureichend sind. Eine kritische Auseinandersetzung und klare Handlungsanweisungen zur Bewertung der Tools wären hier hilfreich (INT_05). Zudem werden Personen oft ausschließlich auf Risikomanagementprozesse geschult, denen ein umfassenderes Verständnis für wirtschaftliche Zusammenhänge fehlt. Dies kann dazu führen, dass Risiken isoliert betrachtet werden, ohne die Auswirkungen auf das Gesamtsystem zu

berücksichtigen. Gerade in komplexen Situationen, in denen unterschiedliche Ereignisse verschiedene Auswirkungen auf ein System haben, reichen die Normen oft nicht aus, um praktikable Lösungen zu bieten (INT_05).

Fazit

Während Normen wie die ISO 31000 einen allgemeinen Rahmen für die Implementierung eines Risikomanagements in kritischen Einrichtungen bieten, bleiben prozessorientierte Normen in ihren Handlungsanweisungen vage. Die ÖNORM D 4900 hingegen konkretisiert die ISO 31000 und macht sie durch überprüfbare Anforderungen anwendbar.

Hinsichtlich Begriffsdefinitionen fassen die Normen den Risikobegriff sehr breit. Konkretisierungen erfolgen in den Anmerkungen. Dahingegen bietet die RKE-Richtlinie eine präzisere Erläuterung. Besonders der Begriff der Schutzgüter erfährt in den Normen nicht diese Wichtigkeit und wird nicht als solcher hervorgehoben. Viel mehr wird in den Normen von Zielen gesprochen, welche unkonkret und damit unklar bleiben. Eine klare Definition von Zielen im Hinblick auf die Schutzgüter, damit deren Vulnerabilität und mögliche Bedrohungen auf diese identifiziert werden können, ist dabei essenziell. Ohne eine präzise Zielsetzung bleibt das Risikomanagement unvollständig. Im Zusammenhang mit der RKE-Richtlinie wären die Schutzgüter demnach jene, die für die Aufrechterhaltung der wesentlichen Dienste relevant sind.

Darüber hinaus sollten Risiken nicht isoliert betrachtet werden. Ein entscheidender Aspekt ist der Umgang mit Restrisiken, da trotz aller Maßnahmen immer ein gewisses Risiko bleibt. Ein weiteres Defizit vieler Normen ist das Fehlen konkreter Anleitungen zur Anwendung der in den Normen thematisierten Instrumenten wie der Risikomatrix. Ohne eine kritische Auseinandersetzung besteht die Gefahr, dass diese Werkzeuge unzureichend oder falsch eingesetzt werden. Schließlich spielt die Risiko- und Sicherheitskultur eine entscheidende Rolle bei der Entwicklung und Implementierung von Maßnahmen zur Verhinderung von Sicherheitsvorfällen. Obwohl Normen diese Aspekte thematisieren, bleiben auch hier ihre Definitionen unscharf [5].

3.5.3. Physischer Schutz

Gemäß RKE-RL sind die Mitgliedstaaten verpflichtet, sicherzustellen, dass die kritischen Einrichtungen Maßnahmen zur Sicherstellung der Resilienz ergreifen, um „einen angemessenen physischen Schutz ihrer Räumlichkeiten und kritischen Infrastrukturen zu gewährleisten, unter gebührender Berücksichtigung zum Beispiel von dem Aufstellen von Zäunen und Sperren, Instrumenten und Verfahren für die Überwachung der Umgebung, Detektionsgeräten und Zugangskontrollen“ (Art. 13 Abs. 1 lit. b Richtlinie (EU) 2022/2557).

[5] Zur Entwicklung der Sicherheitskultur finden sich Empfehlungen in Körmer et al. 2025.

Physische Sicherheit kann in diesem Zusammenhang folgendermaßen definiert werden:

> „Erhaltung von Verfügbarkeit, Vertraulichkeit und Integrität von Assets durch die Nutzung von ganzheitlichen Maßnahmen (STOP-Prinzip-Maßnahmen). Anmerkung 1 zum Begriff: STOP-Prinzip-Maßnahmen beschreiben die Substitution oder technische, organisatorische und personelle Maßnahmen“ (ÖNORM S 2412:2017, S.7).

Es geht somit vor allem um den Schutz von Objekten und Freigeländen sowie Assets und Personen, die sich auf diesen Flächen befinden (INT_02). Gemäß ÖNORM S 2412 wird unter dem Begriff Asset eine „materielle und/oder immaterielle Ressource, welche einen Wert für eine Organisation hat“ verstanden. Als Beispiele sind „Standorte, Information, Reputation, Mitarbeitende“ zu nennen (ÖNORM S 2412:2017, S.4). Neben dem klassischen Objektschutz sowie dem Schutz von Personen zählt auch Travel Risk Management (Reisesicherheit) zur physischen Sicherheit (INT_08). Außerdem ist bei physischer Sicherheit ebenfalls wichtig, stets die Raumordnung zu beachten (INT_09).

Die Bereiche Physische Sicherheit und Informationssicherheit sollten in einer Organisation nicht gänzlich voneinander entkoppelt betrachtet werden. So ist Informationssicherheit, welche Schutzgüter wie Daten etc. vorgibt, auch stets abhängig von physischer Sicherheit, da sich z.B. Serveranlagen immer an schützenswerten Orten in einer Organisation befinden. Hier lässt sich somit die Schnittstelle dieser beiden Bereiche festmachen. Einer Expert*innenmeinung folgend sollte man die physische Sicherheit einer Organisation als übergeordnete Säule im Zusammenspiel mit Informationssicherheit betrachten (INT_08). Jedoch sind unter dem Begriff Informationssicherheit nicht nur digital vorhandene Informationen zu verstehen, Informationen können auch physisch vorliegen (z.B. Dokumente) sowie in Form von Wissen der Mitarbeiter*innen (OVE ÖNORM EN ISO IEC 27000:2020)

Wichtig bei der physischen Sicherheit ist der Schutz aller als schützenswert für die Organisation definierten Assets gegenüber intentionalen Bedrohungen, Gefahren und Ereignissen wie Diebstahl, Vandalismus und Terrorismus. Als zentrale sichtbare Form des physischen Schutzes sind physische Hindernisse wie Sicherheitstüren oder Zäune zu nennen, welche darauf abzielen, unbefugten Zugang zu verhindern bzw. diesen zeitlich hinauszuzögern. Dabei ist zwischen natürlichen und strukturellen Barrieren zu differenzieren (Talbot & Jakeman, 2009). Der Errichter einer physischen Schutzanlage sollte abwiegen, welche Ziele bzw. Funktionen die jeweilige Anlage bieten soll sowie, welche Ressourcen oder Voraussetzungen gegeben sind, ehe bewertet wird, inwiefern die Ausgestaltung des physischen Schutzsystems den Zielen entspricht. Ein derartiges System zeigt bessere Leistungen, wenn die Detektion sich weitestmöglich entfernt vom Ziel befindet. Die grundlegendsten Aufgaben von physischen Schutzsystemen sind die Identifikation sowie die zeitliche Hintanhaltung von Angreifer*innen sowie das Eingreifen von geeigneten sicherheitsverantwortlichen Personen bzw. Institutionen (Garcia, 2008). Damit ein physisches Schutzsystem als

nutzbringend gilt, ist es erforderlich, dass sowohl interne als auch externe Angreifer*innen schnellstmöglich bemerkt oder identifiziert werden, um zu gewährleisten, dass eine Reaktionskette bei Sicherheitsverantwortlichen (z.B. Polizei) initiiert wird, bevor die unerwünschte Tat durch die Angreifer*innen vollendet ist (Garcia, 2008; INT_02). Garcia (2008) betont die Wichtigkeit des zeitlichen Hinauszögerns: „After an adversary has been detected, delay elements will prevent completion of the malevolent act, provide delay until an adequate response force can arrive" (Garcia, 2008, S.219). "A few minutes of delay may have a significant effect on the outcome of an adversary intrusion" (Garcia, 2008, S. 221).

Normen- „Fleckerlteppich" im Bereich physischer Schutz als Problemfeld

Generell ist festzuhalten, dass die Normenlandschaft im Bereich physischer Schutz als „skurril bis divers" zu beschreiben ist (INT_02). Im Bereich der physischen Sicherheit werden 74 Normen als relevant für die Umsetzung der RKE-RL und des RKEG eingestuft (Protectum, 2024b). Darunter finden sich Leitnormen sowie spezifische Unternormen. Als eine zentrale Leitnorm in diesem Bereich ist z. B. die ÖNORM EN 1627:2021 zu nennen, weiters sind die OVE-Richtlinien R 2 (+AC):2017, R9:2012 und R10:2016 von hoher Relevanz (INT_02; Protectum, 2024b).

OVE-Richtlinien R2+AC, R9 und R10

Die OVE-Richtlinie R2+AC regelt Planung, Einbau, Betrieb sowie Instandhaltung von Einbruch- und Überfallmeldeanlagen. Sie ist die Berichtigung der OVE-Richtlinie R2:2017-04-01, bei der eine bestimmte Tabelle ersetzt wurde. Daraus resultiert, dass die Richtlinie den Zusatz AC in der Kennzeichnung aufweist (Austrian Standards, 2024c).

Die OVE-Richtlinie R9 regelt das Auswählen, Planen und Errichten von CCTV-Überwachungsanlagen für Sicherungsanwendungen, die aus Kamera(s), Monitor(en), Bildaufzeichnungsgerät(en), Übertragungs-, Schalt-, Steuer- und Hilfseinrichtungen bestehen (Austrian Standards, 2024d). Ziel dieser Richtlinie ist es, u. a. ein Rahmenwerk bereitzustellen, um Errichter*innen und Kund*innen (Betreiber*innen) derartiger Anlagen bei den Anforderungen zu unterstützen (OVE-Richtlinie R9:2012).

Bei der OVE-Richtlinie R10 handelt es sich um Erfordernisse bei Alarmanlagen - Zutrittskontrollanlagen und sie enthält Mindestanforderungen an Planung, Einbau, Betrieb und Instandhaltung von Zutrittskontrollanlagen der Klassen: Privat/Standard, Gewerbestandard-Nieder oder Gewerbestandard-Hoch, Werteschutz und Hochsicherheit (Austrian Standards, 2024e).

Die OVE-Richtlinien R2+AC:2017, R9:2012, R10:2016 weisen eine ähnliche Struktur hinsichtlich des Aufbaus auf. Zuerst wird der Anwendungsbereich angegeben, ehe Verweise auf andere Normen angeführt sind, die für die Anwendung der jeweiligen Richtlinie unerlässlich sind (OVE-

Richtlinie R2+AC:2017). Als ein weiterer wesentlicher Bestandteil sind eine Vielzahl an Begriffsdefinitionen und Abkürzungen zu nennen. Die Begriffe werden hauptsächlich mittels eines kurzen Satz(-teil)es definiert. Auch die Themen Wartung und Instandhaltung sind in allen drei Richtlinien berücksichtigt. Generell variiert die Gesamtlänge der drei Richtlinien sehr stark, diese reicht von zirka 70 Seiten (OVE-Richtlinie R9) bis etwa 130 Seiten (OVE-Richtlinie R2+AC). Außerdem ist die Anzahl der jeweils in den drei Richtlinien definierten Begriffen unterschiedlich, die Spannweite reicht von zirka 70 Begriffen bis hin zu etwa 160 definierten Termini. Dazu zählen u.a. Begriffsklärungen wie Alarm, Einbruchmeldesystem, Gefahrenmeldeanlage, Objektschutz, Überfallmeldung, Unscharf (Zustand) etc. (OVE-Richtlinie R2+AC:2017).

Wichtig ist die in der OVE-RL R2+AC:2017 sowie in der OVE-RL R10:2016 vorgenommene Differenzierung der Risikoklassen von Einbruchmeldeanlagen bzw. Sicherungsbereichen von Zutrittskontrollanlagen. Die Klassifizierung spiegelt das zunehmende Niveau an Sicherheitsgraden wider. Unterschieden werden dabei die Risikoklassen Privatstandard (PS), Gewerbestandard-Nieder (GS-N), Gewerbestandard-Hoch (GS-H), Werteschutz (WS) sowie Hochsicherheit (HS). Bei Einbruchmeldeanlagen sind die einzelnen Klassen durch das erwartete Ausmaß an Kenntnissen der Einbrecher*innen über Einbruchmeldeanlagen, den Schutz hinsichtlich Überwindung und darüber hinaus durch die erwartete Verwendung bestimmter Werkzeuge von Täter*innen gekennzeichnet.

Der Einsatz der Einbruchmeldeanlagen reicht dabei von Gebäuden wie einfachen Einfamilienhäusern über Infrastrukturen des Handelsgewerbes bis zu Gebäuden, die besonders von Terror bedroht sind. Weiters sind auch Einbruchmeldeanlagen mit gemischten Risikoklassen möglich (OVE-Richtlinie R2+AC:2017). Ein zentrales Element in den OVE-RL bildet die Interventionszeit, welche die Zeit ab der Meldung eines Angriffs bei entsprechenden Sicherheitsstellen bis zum Eintreffen von geeigneten Hilfsorgangen am Ort des Geschehens bezeichnet. Hier müssen aber auch zeitliche Behinderungen wie etwa die Verkehrsdichte einkalkuliert werden (OVE-Richtlinie R2+AC:2017). Mechanische Sicherungseinrichtungen und die Überwachung mittels Einbruchmeldeanlage unter Berücksichtigung der Interventionszeit müssen zusammenwirken, um zu gewährleisten, dass geeignete Einsatzkräfte bestmöglich vor Abschluss der Tat am Ort des Geschehens ankommen (siehe Abb. 19).

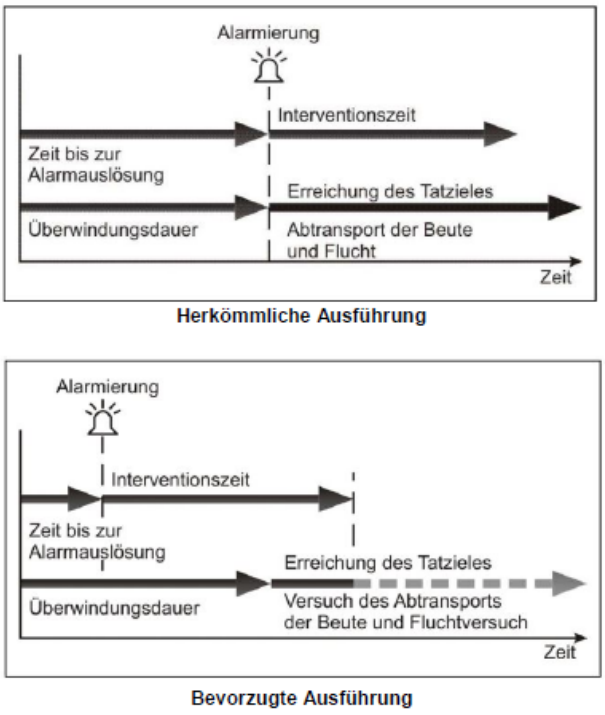


Abbildung 19: Interventionszeiten

Quelle: OVE-Richtlinie R2+AC:2017, S. 31

ÖNORM EN 1627:2021

Als eine weitere, wesentliche Norm im Bereich physischer Schutz ist die ÖNORM EN 1627:2021, welche das Dokument EN1627:2011 ersetzt, und „die Anforderungen und die Klassifizierung der einbruchhemmenden Eigenschaften von Türelementen, Fenstern, Vorhangfassaden, Gitterelementen und Abschlüssen“ festlegt, zu nennen (ÖNORM EN 1627:2021, S.4). Diese Norm bildet die Basis für eine einheitliche Bewertung der Einbruchhemmung von Bauelementen, ermöglicht die Einteilung in Widerstandsklassen und findet vor allem bei Bau- und Sicherheitskonzepten Berücksichtigung (ChatGPT, persönliche Kommunikation, 08. Januar 2025). Sie richtet sich somit an Hersteller*innen von Sicherheitsfenstern und -türen, sowie an Unternehmen, welche sich um den Verkauf und Einbau dieser Bauprodukte kümmern (INT_02). Hinsichtlich der Struktur bzw. des Aufbaus der Norm zeigen sich Ähnlichkeiten zu den OVE-RL, so sind auch bei dieser ÖNORM zu Beginn der Anwendungsbereich sowie normative Verweise angegeben, ehe auf Begriffe und in weiterer Folge normspezifisch auf Baubeschläge, mechanische Festigkeit, und manuelle Einbruchsversuche etc. eingegangen wird.

In dieser Norm sind deutlich weniger Begriffe als in den OVE-RL R2+AC, R9, R10, nämlich genau 14 Begriffe definiert, jedoch gelten für die Anwendung des Dokuments ÖNORM EN 1627:2021 die

Begriffe, welche in drei weiteren Normen thematisiert werden (z.B. EN 12519:2018, EN ISO 80000-1:2013. Als relevant können in der ÖNORM EN 1627:2021 Begriffe wie Widerstandsklasse, Einbruchhemmung sowie Widerstandszeit gewertet werden. Einen zentralen Inhalt bildet die Einteilung von Bauteilen etc. in Widerstandsklassen (RC=resistance class). Dabei wird zwischen sechs Widerstandsklassen differenziert, wobei eine große Bandbreite, von Gelegenheitstäter*innen bis hin zu professionellen Täter*innen, abgedeckt wird. Den einzelnen Widerstandsklassen sind somit stereotypische Arten von Einbrecher*innen zugeordnet. Gemäß der Norm gibt es „kein linear ansteigendes Sicherheitsniveau“, wobei ein starker Unterschied zwischen RC3 und RC4 liegt (ÖNORM EN 1627:2021, S.27). Bei den ersten drei Widerstandsklassen (RC1 bis RC3) wird davon ausgegangen, dass der*die Täter*in keine besonderen Kenntnisse weder über die Widerstandsklasse der jeweiligen Angriffsfläche noch über das potenzielle Diebesgut hat. Diese Widerstandsklassen beziehen sich somit auf Gelegenheitstäter*innen, welche versuchen, kein Risiko beim Einbruchsversuch einzugehen sowie möglichst wenig Lärm zu verursachen. Zur Anwendung kommen simple Werkzeuge wie Schraubenzieher etc., wobei auch mittels Tretens versucht wird, Zugang zum Gebäude zu erlangen. Die Widerstandsklassen RC4, RC5 und RC6 sind auf Eindringlinge ausgerichtet, die erprobt sind sowie professionell agieren. Es wird davon ausgegangen, dass diese Informationen über das potenzielle Diebesgut und die Widerstandsfähigkeit der Angriffsfläche haben sowie weder Risiko noch Lärm bei der Einbruchstätigkeit scheuen. Es wird erwartet, dass sich die Einbrecher*innen spezielleren Werkzeugen, z.B. Axt, Winkelschleifer, bedienen, um beim Einbruchsversuch erfolgreich zu sein (ÖNORM EN 1627:2021).

Laut Expert*innen und Praktiker*innen im Bereich physischer Schutz braucht es für das Funktionieren von physischer Sicherheit stets ein Mischsystem aus mechanischer Sicherheit sowie Detektion (=elektronische Sicherheit) bzw. auch Dokumentation beispielsweise in Form von Videokameras, wie bereits bei den OVE-RL betont wurde (OVE-RL2+AC:2017; INT_02; INT_08). Als Schwachstelle der Leitnorm ÖNORM EN 1627:2021 ist zu nennen, dass die mechanischen Aspekte laut eines*einer Expert*in oft nicht gut geregelt sind. In der anglikanischen Literatur im Bereich physische Sicherheit, bei der die Begriffe Safety und Security voneinander abgegrenzt werden (z.B. Garcia, 2008), wird, wie beim Risikomanagement, der Ausgangspunkt dadurch gebildet, dass es ein definiertes Asset gibt. Weiters wird davon ausgegangen, dass idealtypisch ein Zusammenwirken zwischen mechanischen Barrieren, Detektion sowie Interventionskräften vorhanden ist. Als Schlüsselprinzip fungieren entsprechend gut gestaltete mechanische Barrieren sowie der erwünschte Zustand, dass die Detektion eines*einer Angreifer*in möglichst weit entfernt bzw. frühestmöglich erfolgt, was wiederum eine Interventionskette initiiert und der Situation entsprechende Interventionskräfte alarmiert. Als bedeutender Faktor in diesem Zusammenhang ist die bereits oben erwähnte Interventionszeit zu nennen (INT_02). Die ÖNORM EN 1627:2021 beschreibt all dies nicht in Anlehnung an die wissenschaftliche Literatur. Ein starkes Defizit der ÖNORM EN

1627:2021 besteht somit darin, dass keine Angabe über die Interventionszeit vorhanden ist und folglich auch nicht nach der Interventionszeit geplant wird, sondern nach der Typisierung von Täter*innen, von denen erwartet wird, dass sie ein bestimmtes Objekt angreifen. Auch habe man es in der Praxis mittlerweile überwiegend mit professionell vorgehenden Täter*innen zu tun, nicht nur bei besonders vulnerablen Einrichtungen wie Juwelieren etc. sondern auch bei einfachen Einfamilienhäusern. All diese Ausführungen unterstreichen die zentrale Bedeutung des Zusammenspiels von mechanischen Barrieren und Detektionselementen.

OVE ÖNORM EN 50131-1:2010

Eine weitere Norm, mit der man sich im Rahmen der RKE-RL auseinandersetzen sollte, ist die Grundnorm OVE ÖNORM EN 50131-1, welche Anforderungen für Einbruch- sowie Überfallmeldeanlagen festlegt, aber keine Erfordernisse beispielsweise w. hinsichtlich Planung, Installation und Instandhaltung beinhaltet. Insgesamt finden sich darin 84 mit wenigen Worten definierte Begriffe, wobei vor allem Begrifflichkeiten wie Alarmzustand, Einbruchsignal sowie Meldebereich von Bedeutung sind. Des Weiteren erfolgt eine Angabe darüber, was überhaupt unter einer Einbruch- sowie Überfallmeldeanlage in diesem Dokument zu verstehen ist. Ein zentrales Element in dieser Norm bilden die Sicherheitsgrade, welche in mehreren Europäischen Normen vorkommen. Dabei wird unterschieden zwischen vier Sicherheitsgraden, die die Leistung von Einbruch- und Überfallmeldeanlagen festlegen. Die einzelnen Grade beziehen sich auf unterschiedliche Risikoausmaße und gehen mit unterschiedlichen Erwartungen gegenüber Einbrecher*innen (z. B. welche Werkzeuge beim Angriffsversuch verwendet werden) einher. An dieser Stelle zeigen sich Ähnlichkeiten zu den Widerstandsklassen - RC - in der ÖNORM EN 1627:2021. Ein geringes Risiko zeichnet den Grad 1 und ein geringes bis mittleres Risiko Grad 2 aus. Hier wird davon ausgegangen, dass die Täter*innen wenig Wissen über Einbruch- und Überfallmeldeanlagen haben und sich Werkzeugen, die unkompliziert verfügbar bzw. zu erwerben sind, bedienen. Grad 3 bezieht sich auf ein mittleres bis hohes Risiko, Grad 4 (hohes Risiko) als höchster Grad kommt zum Einsatz „wenn Sicherheit Vorrang vor allen anderen Faktoren hat“ (OVE ÖNORM EN 50131-1, S. 16). Hier wird Angreifer*innen zugetraut, dass sie über einen genauen Plan sowie über spezielles Werkzeug für den Einbruchversuch verfügen (OVE ÖNORM EN 50131-1). Die weiteren spezifischen Unternormen dieser Normenreihe (z. B. OVE ÖNORM EN 50131-2-3, OVE ÖNORM EN 50131-2-4) beinhalten deutlich weniger Begriffsdefinitionen (z. B. neun), weisen aber daraufhin, dass alle Begriffe der Grundnorm 50131-1 auch für diese Dokumente gelten. Im Gegensatz zu den oben beschriebenen OVE-RL wird in der OVE ÖNORM EN 50131-1 die Interventionszeit nicht thematisiert. Es ist lediglich angegeben, dass beispielsweise w. Einbruchssignale binnen 10 Sekunden ausgegeben werden müssen (OVE ÖNORM EN 50131-1). Generell ist bei den verschiedenen Normen bzw. Richtlinien auf die unterschiedlichen Begrifflichkeiten Risikoklasse (in OVE-RL) und Risiko-

bzw. Sicherheitsgrad (in EN) hinzuweisen. Dennoch ist es möglich, „Übersetzungen“ (INT_08) zwischen diesen vorzunehmen, so sei es zulässig, den Sicherheitsgrad 3 einer Einbruch- und Überfallmeldeanlage in Europäischen Normen mit der Risikoklasse Gewerbestandard-hoch in den OVE-RL gleichzusetzen.

ÖNORM S 2420 – 2013

Eine weitere Norm, die in Österreich in der Praxis Anwendung findet, aber nicht europäischen Ursprungs ist, ist die ÖNORM S 2420. Mithilfe dieser Norm wird das Verfahren zwecks Erstellung von Schutzkonzepten diverser Objekte vereinheitlicht. Die Norm ist auf den Schutz von Objekten und deren Inhalt ausgerichtet (z.B. Maschinen, aber auch auf Personen). Durch die Norm wird eine große Bandbreite an Objekten abgedeckt, etwa Objekte kritischer Einrichtungen oder für Großveranstaltungen. Zentrale Begriffe dieser Norm lauten Schutzkonzept, womit das „Konzept zum Schutz von Objekten vor intentionalen Gefahren“ gemeint ist sowie Schutzziel, welches die „Festlegung, welche Objekte oder Objektteile vor welchen intentionalen Gefahren zu schützen sind“, bezeichnet (ÖNORM S 2420:2013-06-01, S.5). Der Ist-Zustand beschreibt die „aktuelle Beschaffenheit des Objektes oder der Objektteile, die aktuelle Nutzung und die bestehenden Sicherheitsmaßnahmen“, während der Soll-Zustand als die „angestrebte Beschaffenheit des Objektes oder von Objektteilen, die angestrebte Nutzung und die erforderlichen Sicherheitsmaßnahmen“ definiert wird (ÖNORM S 2420:2013-06-01, S.4, 5).

Das Verfahren zwecks Erstellung von Schutzkonzepten kann in sechs Phasen gegliedert werden. In einem ersten Schritt wird das Schutzziel von der obersten Leitung bestimmt, ehe der Ist-Zustand beschrieben wird. Bei letzterem wird der Aufbau des Objektes, die Maschinen etc. dokumentiert. Weiters werden die intentionalen Gefahren beurteilt (hier sind etwa Personen- und Sachschaden zu berücksichtigen) und die Maßnahmensetzung priorisiert. Darauffolgend kommt es zur Bestimmung des akzeptierten Restrisikos und der notwendigen Maßnahmen, die ergriffen werden sollten, ehe in einem letzten Schritt das Schutzkonzept erfolgt (ÖNORM S 2420:2013-06-01). Hier wird somit ebenfalls auf das Restrisiko eingegangen, welches laut dieser Norm das „Risiko, das nach Behandlung von Risiken“ bleibt, bezeichnet (ÖNORM S 2420:2013-06-01, S.4). Es ist essenziell, dass die verschiedenen Arten von Maßnahmen (mechanisch, elektronisch und organisatorisch) zusammenwirken, um einen möglichst umfassend wirksamen Schutz des Objektes bzw. der Objektteile zu erzielen (ÖNORM S 2420:2013-06-01). „Die oberste Leitung muss den Vorschlag für das Schutzkonzept dahingehend prüfen, ob das verbleibende Restrisiko im gewünschten Verhältnis zu den Kosten der Umsetzung des Schutzkonzeptes steht oder ob Hindernisse für die Umsetzung des Vorschlags bestehen“ (ÖNORM S 2420:2013-06-01, S.13). Bestehen das gewünschte Verhältnis zwischen Restrisiko und Kosten der Umsetzung des Schutzkonzeptes und keine

weiteren Barrieren für die Umsetzung, ist das Schutzkonzept anzunehmen (ÖNORM S 2420:2013-06-01).

Vergleich Europäische Normen und OVE-Richtlinien

Im Zuge der Normenanalyse wird eine Kluft zwischen den OVE-RL und europäischen Normen deutlich, da die OVE-RL R2, R9, R10 stets vorgeben, dass ein umfassendes Schutzkonzept beim z. B. Einbau von Alarmanlagen bestehen muss, das aus einer Kombination von Mechanik und Elektronik besteht. Diese Richtlinien lehnen sich somit an theoretischen Schutzkonzepten aus der anglikanischen Literatur an, während bei einer europäischen Norm ausschließlich beispielsweise w. die Alarmanlage an sich von Interesse ist – diese „steht singulär da“ (INT_02). Auch ein*e weiter*e Expert*in betont, dass europäische Normen stark auf bestimmte Themen fokussieren. Es wird nicht das gesamte System berücksichtigt, was „als Schwachstelle zu werten“ sei (INT_02). Wie oben bereits erwähnt, bildet die Wartung und Instandhaltung von Alarmanlagen etc. einen weiteren wesentlichen Bestandteil der OVE-RL, in denen genau geregelt ist, welche Personen oder Einrichtungen befugt sind, in Österreich eine Wartung durchzuführen. (siehe OVE-RL R2+AC:2017, R9:2012, R10:2016).

Im militärischen Bereich etwa findet sich keine Anwendung von europäischen Normen, sondern nur der OVE-RL R2+AC:2017, R9:2012 und R10:2016. Jedoch bilden europäische Normen die Grundlage für die Ausformulierung der OVE-RL, wobei die OVE-RL 2+AC:2017, R9:2012 und R10:2016 zusammenhängen, also „aufeinander abstellen“ (INT_02).

Als Zwischenfazit lässt sich feststellen, dass Europäische Normen die Grundvoraussetzungen beschreiben, um beurteilen zu können, ob die technischen Voraussetzungen eines Systems vorhanden sind und in weiterer Folge, ob ein System funktional ist oder nicht. Wie bereits oben angedeutet, sind Europäische Normen sehr auf bestimmte Themenfelder spezifiziert, so handelt die OVE ÖNORM EN 50131-1 vor allem von Einbruch- und Überfallmeldeanlagen, das Thema Zutrittskontrollanlagen findet hingegen keine Berücksichtigung (INT_08). Mit diesem Thema beschäftigt sich z. B. die OVE ÖNORM EN 60839, wobei auch in dieser Norm wieder auf die unterschiedlichen Sicherheitsgrade eingegangen wird. Bei der europäischen Norm bezüglich Einbruch- und Überfallmeldeanlagen ist beispielsweise ebenfalls nicht festgelegt, wie eine Meldeanlage verbaut bzw. der entsprechende Raum gemäß dem Risiko geschützt sein muss. Die Norm bezieht sich somit nur auf technische Aspekte bzw. Funktionen des Systems. Hingegen wird bei der OVE-RL thematisiert, welche Melder eingebaut werden müssen, des Weiteren verfolgen die OVE-RL, die Vernetzung des gesamten Konzepts über die verschiedenen Themenfelder hinweg. Diese konzeptionellen Anforderungen, kommen so in den Europäischen Normen nicht vor (INT_08). Darüber hinaus lassen sich die OVE-RL im Gegensatz zu den Europäischen Normen dadurch charakterisieren, dass diese eher Verbindlichkeiten determinieren durch Formulierungen wie „Sind die

Bedrohungsarten nicht bekannt, müssen diese im Rahmen einer angemessenen Risikoanalyse festgestellt werden“ (OVE-RL R2+AC:2017, S. 100). Bei Europäischen Normen sind demgegenüber Formulierungen wie „kann“ oder „soll“ vorzufinden, dies stellt aber einen problematischen Aspekt für die Auditierung der jeweiligen Norm dar (INT_08), da derartige Formulierungen großen Interpretationsspielraum bieten. Den Dreh- und Angelpunkt in den OVE-RL bildet, wie bereits erwähnt, das Zusammenwirken von mechanischen und elektronischen Elementen sowie die Interventionszeit, welche bei den Europäischen Normen keine Berücksichtigung findet (INT_08). Weiters könne argumentiert werden, die Europäischen Normen seien etwas „zu grob“ (INT_08) und die OVE-RL eher „zu detailliert“ (INT_08) formuliert.

In den Europäischen Normen sind zudem minimale Widersprüche zu finden, welche aber durch die vorhandenen OVE-RL geklärt werden können (INT_08). Dennoch sind auch in den OVE-RL teilweise Widersprüchlichkeiten festzumachen. Es ist wichtig zu betonen, dass die RKE-RL auf die Erfüllung von europäischen Normen und nicht auf die Erfüllung von Richtlinien abzielt, auch bei einem Audit ließe sich daher schneller mit europäischen Normen als mit normativen Richtlinien verfahren (INT_02).

Vereinbarkeit Theorie und Normen

Generell ist ein szenariobasierter Ansatz im Bereich der physischen Sicherheit von großer Bedeutung. Dabei geht es darum, dass es für den Schutz eines Objektes ein Szenario benötigt, wobei dafür Kenntnis über die Bedrohung sowie das Asset notwendig ist. Es ist somit wichtig, das gesamte System zu betrachten (INT_08).

Das zuvor beschriebene Schutzzonenkonzept ist für den physischen Schutz relevant. Erfolgt eine Auseinandersetzung mit Normen in dieser Hinsicht wird deutlich, dass in den Normen im Bereich physische Sicherheit das Konzept Schutzzone lediglich vereinzelt angesprochen wird, beispielsweise wird in der OVE-RL R9:2012 das „Zuordnen zu Schutzzonen“ (OVE-RL R9:2012, S. 43) angesprochen. In der OVE ÖNORM EN 50131-1:2010 sowie in den spezifischen Unternormen oder in der ÖNORM EN 1627:2021 wird der Begriff hingegen nicht thematisiert. Somit lässt sich auch hier ein Defizit in den Europäischen Normen erkennen. Laut einem*einer Expert*in ergibt sich aber auch aus der Theorie zur physischen Sicherheit, dass es „ohne Zonierung eigentlich nicht wirklich geht“ (INT_08). Eine der (möglichen) Grundlagen für die Planung eines Sicherheitskonzepts ist, dass Objekte zu zonieren sind, wobei diese Zonierung wiederum stark mit der Zutrittskontrolle zusammenhängt (z. B. welche Zugangsmaßnahmen werden in welcher Schutzzone benötigt?) (INT_08). Des Weiteren sind keine Normen im Bereich physischer Schutz vorhanden, die explizit auf Gefährdungen wie Terrorismus eingehen. Dennoch sind Erfordernisse wie Perimeterschutz, die Verwendung von nicht brennbaren Materialien für Gebäude oder der Bau von massiven Dächern etc. auch für die Abwehr von Terrorgefährdungen essenziell (INT_09).

Umsetzung von Normen in die Praxis

Bei kritischen Einrichtungen erfolgt der Aufbau der physischen Sicherheit in der Praxis oftmals durch die Betreiber selbst und es werden zur Umsetzung der Normen keine Fachfirmen herangezogen. Dadurch besteht die Gefahr, dass Organisationen, nicht ausreichend für etwaige Bedrohungen gerüstet sind. Vor allem beim Einbau diverser Anlagen durch externe Fachfirmen können Auditor*innen davon ausgehen, dass die jeweiligen Erfordernisse normkonform ausgeführt werden, so ein*e Expert*in (INT_08). Da Schutzzonen errichtet werden sollten, die ineinandergreifen, wird ein Anknüpfungspunkt zum Risikomanagement deutlich. Für ein kohärentes Gesamtkonzept werden Personen benötigt, die im Risikomanagement versiert sind. Dieser Gesamtüberblick fehlt den Errichter*innen einzelner Anlagen wiederum und kann daher von diesen nicht gewährleisten werden (INT_08). Zusammenfassend lässt sich somit festhalten, dass im Bereich physischer Sicherheit ein ausgereiftes Gesamtkonzept innerhalb einer Organisation erstellt werden sollte, das allen Anforderungen entspricht, wobei dies herausfordernd ist. Das Konzept sollte für Außenstehende transparent, nachvollziehbar sowie auditierbar sein (INT_08).

Fazit

Neben der Verhinderung von Sicherheitsvorfällen bezieht sich eine weitere zentrale Forderung der RKE-RL auf den physischen Schutz von Infrastrukturen. So ist durch die kritischen Einrichtungen ein adäquates Niveau an physischer Sicherheit, etwa durch die Errichtung von Zäunen, Zugangskontrollmaßnahmen oder die Verwendung von Überwachungsgeräten zu etablieren. Als grundlegend erweist sich dabei die Definition von Assets bzw. die Auseinandersetzung mit Schutzzielen einer Organisation gegenüber intentionalen Bedrohungen, welche in manchen Normen bzw. normativen Richtlinien berücksichtigt wird. Im Bereich physischer Schutz besteht eine Vielzahl an Normen, die sich für die RKE-RL als relevant erweisen, wobei festzuhalten ist, dass die Normenlandschaft als undurchsichtig charakterisiert werden kann. Es existieren u.a. europäische Normen (ÖNORM EN) sowie österreichische Normen (ÖNORM) und normative Richtlinien (OVE-RL). Keine Berücksichtigung in den Normen und normativen Richtlinien findet derzeit etwa das Konzept der Schutzzonen, welches aber gemäß der wissenschaftlichen Literatur im Bereich physischer Schutz eine hohe Bedeutung hat.

Defizite weisen hier insbesondere Europäische Normen auf. Während diese stark technisch ausgerichtet sind und Sicherheitsaspekte meist isoliert betrachten, verfolgen OVE-Richtlinien einen ganzheitlicheren Ansatz, der mechanische, elektronische Elemente sowie Interventionszeiten miteinander kombiniert. Sicherheitselemente sollten dabei nicht nach den zu erwartenden Handlungen von Täter*innen bei einem Angriffsversuch ausgerichtet sein, sondern eine Kombination aus Mechanik, Elektronik und Interventionszeit sein. Dies kann zwar einen höheren Aufwand verursachen, führt aber zu differenzierteren und praxistauglicheren Umsetzungsmaßnahmen. Weiters

legen OVE-RL Verbindlichkeiten fest, während europäische Normen unverbindlicher formuliert sind. Drüber hinaus werden von Europäischen Normen und OVE-RL unterschiedliche Begrifflichkeiten (z.B. Sicherheitsgrade) verwendet, welches die Vergleichbarkeit der einzelnen Dokumente erschwert.

Für resiliente Organisationen ist es wichtig, in der Praxis vor allem von professionell agierenden Täter*innen auszugehen, die einen Angriffsversuch auf eine kritische Einrichtung ausüben könnten. Dennoch werden viele Gefährdungen, die für kritische Einrichtungen relevant sein könnten (z.B. Terrorismus), in den vorhandenen Normen nicht thematisiert. Die RKE-RL verweist darauf, dass ebenfalls gegenüber Angriffen wie Terror, Maßnahmen ergriffen werden sollten, da auch solche Sicherheitsvorfälle neben Unfällen oder Naturkatastrophen eine Bedrohung für die Aufrechterhaltung des wesentlichen Dienstes darstellt. Eine enge Verzahnung von physischer Sicherheit auch mit Risikomanagement-Prozessen sowie eine fortlaufende Evaluierung und Anpassung an neue Bedrohungsszenarien sind essenziell, um die Sicherheit und Resilienz kritischer Einrichtungen nachhaltig zu gewährleisten. Bei physischer Sicherheit wird deutlich, dass Normen immer nur Anhaltspunkte sind, die an die jeweilige Organisation angepasst werden müssen.

Ein vorhandener angemessener physischer Schutz dient zudem als wichtige Basis für ein in weiterer Folge entsprechend ausgearbeitetes Notfall- und Krisenmanagement sowie Business Continuity Management.

3.5.4. Abwehr und Bewältigung von Sicherheitsvorfällen

Zentrale Bestandteile eines ganzheitlichen Sicherheits- und Risikomanagements gemäß RKE-RL sind das Notfall- und Krisenmanagement, das der Abwehr und Bewältigung von Sicherheitsvorfällen dient (Richtlinie (EU) 2022/2557; Romeike & Hager, 2020; ÖNORM S 2415-1:2020-07). Im vorliegenden Kapitel wurden diesbezüglich vorrangig Normen zum Aufbau und zur Weiterentwicklung von Krisenmanagementfähigkeiten (DIN EN ISO 22361:2023-02) sowie die ÖNORM-Reihe „Security Management System“ (ÖNORM S 241x), ein Regelwerk zur Unterstützung einer ganzheitlichen Betrachtung von Security Management, herangezogen.

> „Das Ziel eines Krisenmanagement-Rahmens ist es, die Organisation dabei zu unterstützen, das Krisenmanagement in ihre Tätigkeiten und Funktionen zu integrieren. Der Krisenmanagement-Rahmen dient dazu, die Beziehung zwischen den Krisenmanagement-Grundsätzen, den Kernmerkmalen des Krisenmanagements und den Schlüsselelementen des Managementprozesses, die sich aus den Krisenmanagement-Grundsätzen ergeben, zu verdeutlichen. Die Akzeptanz des Rahmens sollte das Verständnis für die Beziehung zwischen dem Krisenmanagement-Prozess und anderen Management-Prozessen erleichtern“ (DIN EN ISO 22361:2023-02, S.17).

Da die unterschiedlichen Konzepte ineinandergreifen, wird die Abgrenzung zwischen Risikomanagement, Notfall- und Krisenmanagement sowie BCM nicht explizit formuliert. Der physische Schutz stellt ebenfalls einen Teil des übergeordneten Sicherheits- und Risikomanagements dar.

Für eine theoretische Analyse und zur Umsetzung in die Praxis ist eine die Trennung in einzelne Konzepte jedoch erforderlich.

> „Die Fähigkeit einer Organisation zum Krisenmanagement wird durch ihre Beziehung zu anderen, sich gegenseitig beeinflussenden Bereichen wie Risikomanagement, Aufrechterhaltung der Betriebsfähigkeit, Informationssicherheit, (physische) Sicherheit, Bevölkerungsschutz, Reaktion auf einen Notfall und Notfallmanagement beeinflusst (DIN EN ISO 22361:2023-02)."

In diesem Sinne verweisen Normen teilweise aufeinander und überschneiden sich in ihrer Anwendung. Ein Beispiel ist die ÖNORM D 4902-3, die als „Leitfaden zur Umsetzung der ISO 31000" dient und spezifisch auf das Notfall-, Krisen- und Kontinuitätsmanagement eingeht. Ebenso verweist die DIN EN ISO 22361:2023-02 auf andere Normen wie die DIN EN ISO 22300 (Begriffe für Sicherheit und Resilienz) und die DIN EN ISO 22313 (Anleitung zur Anwendung von Business Continuity Management nach ISO 22301). Auch zentrale Aspekte, wie die Wiederherstellung nach einem Vorfall, werden in der Norm behandelt (DIN EN ISO 22361:2023-02). Die Normen verdeutlichen zudem, dass das Krisenmanagement dynamisch ist und auf einem soliden Risikomanagement aufbaut. Die enge Verzahnung zwischen den verschiedenen Standards unterstreicht folgende Aussage eines Experten:

> „Es ist fast ein bisschen Henne und Ei. Was war zuerst? Oder die Frage ist die, ich sage immer, die BCM-Manager sehen natürlich BCM als das Hauptthema und das Risikomanagement untergeordnet als Werkzeug das BCM. Ja, der Risikomanager sieht es aber genau andersrum. Der sieht Risikomanagement als Überbau und das BCM als Werkzeug vom Risikomanagement. Ja, ich sehe es im Übrigen auch mittlerweile so, Überbegriff Resilienz. Und darunter sind dann angesiedelt eben die Werkzeuge, um Resilienz zu erreichen. (…) Und ich denke mir oft, ich hätte es auch gerne natürlich, wenn wir alles super sauber abgetrennt hätten und immer alles den Normbegriffen folgend. Für mich umgekehrt aber viel wichtiger, dass Unternehmen diese Dinge haben und letztlich hinten auch das Richtige dabei herauskommt" (INT_04).

Aus der dargestellten Schwierigkeit der Abgrenzung ist ebenso eine Quantifizierung der Normen zu Notfall- und Krisenmanagement schwierig[6]. Viele Normen thematisieren Notfallreaktion und Notfallbewältigung, obwohl dies nicht ihr primärer Fokus ist (ebd.). Ein Beispiel hierfür ist die Norm zu Travel Risk Management (Reisesicherheit), die einen anderen Schwerpunkt setzt, aber dennoch Risiko- und Notfallaspekte enthält, ohne primär für dieses Thema relevant zu sein (ISO 31030:2021). Diese Verlinkung und Verzahnung verschiedener Normen erschwert eine klare Zuordnung und macht die Übersicht über das Themenfeld komplex (INT_04).

Zurückkommend zu den spezifischen Aspekten Notfall- und Krisenmanagement unterscheiden sie sich unter anderem in deren Bewältigungsansätzen. Während das Notfallmanagement eher kurzfristig auf akute Bedrohungen reagiert, bietet das Krisenmanagement eine strategische Antwort auf tiefergreifendere Herausforderungen. Notfällen kann man gezielter präventiv begegnen. Außerdem lassen sich Notfallszenarien konkret vorbereiten und üben, beispielsweise mittels Erste-

[6] Dasselbe trifft auf Normen im Bereich des Risikomanagement und des BCM zu.

Hilfe-Kurse (ebd.). Die Krise ist demgegenüber komplexer, wobei sie oftmals durch einen Notfall ausgelöst wird. „Es bestehen [insgesamt] einige gemeinsame Merkmale, die sowohl bei einem Notfall als auch bei einer Krise vorhanden sind“ (DIN EN ISO 22361:2023-02). Die Norm diskutiert daher die Beziehung zwischen Problemen, Notfällen und Krisen sowie deren Merkmale, aber auch Unterschiede (ebd.).

Ergänzend dazu ist ein Security Management System nach den ÖNORMEN ein wesentlicher Bestandteil des umfassenden Schutzes einer Organisation. Es schafft die Voraussetzungen, um Bedrohungen proaktiv zu begegnen und die Auswirkungen von Sicherheitsvorfällen durch ein strukturiertes Notfall- und Krisenmanagement zu minimieren. Beide Systeme arbeiten Hand in Hand, um die Resilienz und Handlungsfähigkeit einer Organisation in unsicheren oder kritischen Situationen sicherzustellen.

Relevante Begriffe im Notfall- und Krisenmanagement

Relevante Begriffe in den analysierten Normen zu Notfall- und Krisenmanagement sind eng mit anderen Normen verknüpft, da diese auf Begriffsdefinitionen aus verwandten Standards verweisen.

Die ÖNORM D 4902-3:2021-01 etwa greift auf die Begriffe der ÖNORM D 4900 zurück, die stark auf Risikomanagement fokussiert und detailliert auf Risikobegriffe ausdifferenziert ist. Im Gegensatz dazu verweist die ISO 22320:2019-07 auf die ISO 22300, welche insgesamt 77 allgemeine Begriffe zu den Themen:

- Societal security,
- Management of societal security,
- Operational – Risk reduction,
- Operational – Exercise sowie
- Operational – Recovery, Technology definiert.

Die ÖNORM S 2415-1:2020-07 bezieht sich auf die ÖNORM S 2412, die spezifisch Terminologien für Security Management Systeme festlegt.

Dadurch setzen die Normen unterschiedliche Schwerpunkte, was ihre Anwendung und den Kontext der Begriffe betrifft. Zusätzlich bieten die ISO und IEC über Online-Plattformen wie die ISO Online Browsing Platform (http://www.iso.org/obp) und die IEC Electropedia (http://www.electropedia.org/) zentrale Ressourcen für normbezogene Terminologien.

Fazit

Ein umfassendes Sicherheits- und Risikomanagement, das den Anforderungen der RKE-RL gerecht wird, erfordert entsprechendes Notfall- und Krisenmanagement. Im Rahmen des

vorliegenden Projekts wurde der Fokus vorrangig auf Normen zur Entwicklung und Stärkung von Krisenmanagementfähigkeiten (DIN EN ISO 22361:2023-02) sowie die ÖNORM-Reihe Security Management System (ÖNORM S 241x) als Regelwerk gelegt, um eine umfassende Betrachtung des Security Managements zu unterstützen. Im Vordergrund steht die Beziehung zwischen den verschiedenen Bereichen Risikomanagement, Notfall- und Krisenmanagement und BCM, welche auch die Normen thematisiert. Dies zeigt sich besonders – wie dargestellt – in den Normen ÖNORM D 4902-3 oder DIN EN ISO 22361:2023-02.

Notfall- und Krisenmanagement unterscheiden sich insbesondere in der Art ihrer Bewältigung. Während das Notfallmanagement darauf ausgerichtet ist, akute Bedrohungen kurzfristig zu bewältigen und durch präventive Maßnahmen sowie Übungen gezielt vorbereitet werden kann, zielt das Krisenmanagement auf eine langfristige und strategische Bewältigung tiefgreifender Herausforderungen ab. Krisen entstehen häufig aus einem Notfall und sind in der Regel komplexer. Trotz dieser Unterschiede weisen beide Konzepte Überschneidungen auf, weshalb Normen wie die DIN EN ISO 22361:2023-02 ihre Zusammenhänge und Abgrenzungen systematisch erfassen.

Wie sich zeigt, ist aufgrund dieser engen Vernetzungen besonders wichtig, dass die unterschiedlichen Bereiche sorgfältig entwickelt und durchdacht sind. Zudem bauen die Teilbereiche aufeinander auf. Das heißt, nicht-identifizierte Risiken sowie unzureichende physische Schutzbarrieren können in Notfällen und Krisen wirksam werden.

3.5.5. Fortsetzung und rasche Wiederaufnahme nach Sicherheitsvorfällen

Zur Gewährleistung von Resilienz in kritischen Einrichtungen fordert die RKE-Richtlinie von betroffenen Unternehmen „nach Sicherheitsvorfällen die Wiederherstellung zu gewährleisten, unter gebührender Berücksichtigung von Maßnahmen zur Aufrechterhaltung des Betriebs und der Ermittlung alternativer Lieferketten, um die Erbringung des wesentlichen Dienstes wiederaufzunehmen“ (RK-RL 2022/2557). Das BCM befasst sich dabei mit der Sicherstellung der Betriebskontinuität und ist somit ein zentraler Bestandteil der Resilienzstrategie eines Unternehmens. BCM hat das Ziel, Organisationen vor Betriebsunterbrechungen zu schützen, die Wahrscheinlichkeit solcher Zwischenfälle zu verringern und eine gezielte Vorbereitung sicherzustellen. Im Falle einer Störung ermöglicht es eine systematische Reaktion und eine rasche Wiederherstellung des Betriebs, unabhängig vom Zeitpunkt des Eintretens (EN ISO 22301:2019).

Die im Sinne der RKE-RL relevanten Störungen beziehen sich auf einen Vorfall, welcher „ein Ereignis oder eine Verkettung von Ereignissen [ist], wobei mit hoher Wahrscheinlichkeit unerwartete, ungeplante oder unerwünschte Auswirkungen auftreten können“ (Kersten & Klett, 2017, S. 15; Richtlinie (EU) 2022/2557). Wie bereits beschrieben ist die Abgrenzung von BCM zum Risikomanagement, Incident Management und Krisenmanagement in der Praxis unscharf. Einerseits wird BCM teilweise als übergeordnetes Konzept betrachtet, welches Incident Management und Krisenmanagement integriert. Andererseits greift laut Aussage eines*einer Expert*in das BCM dort, wo das Risikomanagement aufhört. Nachdem Risiken identifiziert und Maßnahmen zur Risikominderung sowie Restrisiken definiert wurden, übernimmt BCM die Planung und Umsetzung von Maßnahmen, um die Auswirkungen von Restrisiken zu steuern (INT_03).

Allerdings ist diese Abgrenzung nicht deckungsgleich mit jener von internationalen Normen. Nach der ISO 22313 setzt BCM anschließend an das Notfall- und Krisenmanagement und nach dem Eintreten eines Ereignisses (Incident), Zwischenfalls oder einer Betriebsstörung an, als Absicherung zeitkritischer Geschäftsprozesse (EN ISO 22313:2014). Die ISO 22301 konkretisiert den Anwendungsbereich von BCM noch weiter und sieht ihn im Kontext einer Organisation, die

- eine Übereinstimmung mit der erklärten Politik zur Aufrechterhaltung der Betriebsfähigkeit sicherstellen will,
- die Fähigkeit benötigt, die Belieferung mit Produkten und Dienstleistungen mit einer akzeptablen, zuvor festgelegten Kapazität während einer Störung fortzusetzen,
- anstrebt, ihre Resilienz durch die effektive Anwendung des BCMS zu verbessern.

Damit wird deutlich, dass BCM nicht einfach dort ansetzt, wo das Risikomanagement endet, sondern vielmehr als Teil bzw. Werkzeug der Risikosteuerung zu verstehen ist – insbesondere im Hinblick auf die Aufrechterhaltung der Betriebsfähigkeit angesichts definierter Risiken. Damit definieren die Normen BCM enger (EN ISO 22313:2014; INT_03).

Im Zuge des BCM müssen Pläne entwickelt werden, die auch auf Restrisiken anwendbar sind. Das bedeutet, diese Pläne müssen generisch und auf eine Vielzahl potenzieller, unvorhergesehener Szenarien anwendbar sein, da eine ausschließliche Fokussierung auf spezifische Risiken und Zwischenfälle zu unflexibel wäre (INT_03).

> „Also generell sollten eigentlich in der Organisation die Themen so konzipiert sein, dass sie generisch mal formuliert sind. Ich kann nicht jede Krise extra ausformulieren, ich brauche quasi ein generisches Krisenmanagement. Genauso bräuchte es in Unternehmen ein generisches Business Continuity Management“ (ebd.).

Diese Pläne können auf einzelne Bereiche, Geschäftsprozesse oder Standorte einer Organisation ausgearbeitet werden. Der Anwendungsbereich muss sich nicht notwendigerweise auf die gesamte Einrichtung, sondern auf die kritischen Geschäftsprozesse beziehen (Kersten & Klett, 2017). Hierbei berücksichtigt das BCM auch wirtschaftliche Abwägungen, um angemessene Ressourcen zu planen (ebd.; INT_03).

Mit Blick auf die Anforderungen der RKE-Richtlinie sind folgende Normen für den Bereich BCM relevant:

- EN ISO 22301:2019 ist eine zertifizierbare Norm, welche „die Struktur und Anforderungen für die Implementierung und Aufrechterhaltung“ eines BCMs festlegt (EN ISO 22301:2019).
- Die EN ISO 22313:2020 bietet Leitlinien zur Anwendung der in ISO 22301 festgelegten Anforderungen. Sie ist somit auf die Planung und langfristige Absicherung der Betriebskontinuität ausgerichtet.
- ISO 22320:2011 ist darauf ausgerichtet, Leitlinien für die organisatorische und operative Zusammenarbeit sowie die Kommunikation in Notfallsituationen bereitzustellen, um effektive Notfallmaßnahmen zu ermöglichen.
- ISO/TS 22317 ist eine Technische Spezifikation zur ISO 22301. Sie enthält Vorgaben zur Implementierung einer Business Impact Analyse.

Des Weiteren sind im D-A-CH-Raum die Standards BSI 200/4 und Good Practice Guide (GPG) zur Implementierung eines BCM von Bedeutung, wobei beide einen anderen Schwerpunkt setzen. Der BSI 200/4 ist ein Standard, der BCM je nach Reifegrad in drei Stufen unterscheidet: Reaktives BCM, Aufbau-BCM und Standard-BCM. Der GPG des Business Continuity Instituts bietet eine breiter gefasste Anleitung für ein BCM. Beide Standards berücksichtigen dabei die ISO 22301 und übernehmen Begriffe aus dieser Norm (INT_03). Normen und Standards bieten damit einen Rahmen, um ein BCM systematisch aufzubauen und erlauben gleichzeitig individuellen Freiraum bei der Umsetzung. Dieser Freiraum kann für Organisationen, die weniger Erfahrung mit BCM haben jedoch auch Herausforderungen darstellen, da es stark auf die Kompetenz der ausführenden Mitarbeitenden ankommt. Zu strikte Vorgaben hingegen schränken die Flexibilität ein (INT_03;

INT_05). Zudem erfordert ein effektives BCM Übungen, um Pläne zu überprüfen und Schwachstellen zu identifizieren (EN ISO 22301:2019). Dies entspricht auch den Vorgaben der RKE-Richtlinie regelmäßige Trainings durchzuführen (RK-RL 2022/2557). Darüber hinaus adressieren Normen wie die ISO 22301 Themen wie Führung, Rollen und Verantwortlichkeiten, doch bleiben Details wie die Anzahl benötigter Sicherheitsvertrauenspersonen oft vage (INT_03).

Fazit

Um der RKE-RL Rechnung zu tragen, müssen Unternehmen die Wiederherstellung nach Sicherheitsvorfällen gewährleisten, die der Aufrechterhaltung des Betriebs, der Erbringung des wesentlichen Dienstes sowie der Ermittlung alternativer Lieferketten dienen.

BCM ist dabei ein systematischer Ansatz zur Wiederaufnahme der Betriebsfähigkeit einer Organisation nach dem Krisenfall, indem gezielte Maßnahmen gesetzt werden, um Ausfallzeiten zu minimieren und den Betrieb aufrechtzuerhalten. Während die Abgrenzung zu Risikomanagement und Krisenmanagement in der Praxis oft unscharf ist, konzentriert sich BCM normativ auf die Absicherung zeitkritischer Geschäftsprozesse nach einem Störfall. Ein effektives BCM erfordert generische, flexibel anwendbare Pläne sowie regelmäßige Übungen zur Überprüfung und Optimierung. Wichtige Normen in diesem Bereich sind unter anderem die EN ISO 22301, die Anforderungen an ein BCM definiert, die EN ISO 22313 sowie die ISO 22320, welche Leitlinien zur Umsetzung bietet und die ISO/TS 22370 zur Implementierung einer Business Impact Analyse. Ergänzende Standards wie der BSI 200/4 oder der GPG liefern weitere praxisorientierte Ansätze. Auch hier ist festzuhalten, dass Normen Handlungsanleitungen bieten, aber keine detaillierten Vorgaben bereitstellen. Daher erfordert die Umsetzung eines wirksamen BCM auch qualifiziertes Personal, um individuelle Anpassungen und effektive Maßnahmen zu gewährleisten.

3.5.6. Personelle Sicherheitsvorkehrungen

Die RKE-RL fordert von den betroffenen Organisationen/Unternehmen „ein angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeiter zu gewährleisten, unter gebührender Berücksichtigung von Maßnahmen wie der Festlegung von Kategorien von Personal, das kritische Funktionen wahrnimmt, der Festlegung von Zugangsrechten zu Räumlichkeiten, kritischen Infrastrukturen und zu sensiblen Informationen und der Einführung von Verfahren für Zuverlässigkeitsprüfungen […]“ (Art. 13 Abs. 1 lit. e Richtlinie (EU) 2022/2557).

Talbot und Jakeman (2009) definieren in ihrem Buch die Begriffe people security sowie personnel security. People security wird dabei auf zwei Arten verstanden, einerseits bezieht sie sich darauf, dass Personen, wie beispielsweise Mitarbeiter*innen oder die gesamte Gesellschaft, gegenüber Schäden geschützt werden. Andererseits bezieht es sich auf Folgendes: „the protection of an organization or other people from threats to security that are most appropriately controlled by the

interaction of people, i.e., vetting and personal protective practices“ (Talbot & Jakeman, 2009, S.63). Somit wird ebenfalls berücksichtigt, „that these groups can also pose a threat to security“ (Talbot & Jakeman, 2009, S.63). Personnel Security kann dadurch beschrieben werden, dass es sich um einen Prozess handelt, „whereby only suitable people obtain and retain access to sensitive or security classified resources“ (Talbot & Jakeman, 2009, S.65). Für ein*e Expert*in in diesem Bereich ist nicht eindeutig definiert, welche Aspekte genau unter personeller Sicherheit zu verstehen sind. Demnach sind darunter erstens Risiken sowie Gefahren zu verstehen, welche von Mitarbeiter*innen einer Organisation ausgehen, wobei in weiterer Folge Maßnahmen etabliert werden müssen, um diesen Bedrohungen entgegenzuwirken. Zweitens sind aber auch Maßnahmen darunter zu verstehen, die von Mitarbeiter*innen einer Organisation gesetzt werden und das Ziel verfolgen, das Ausmaß von Risiken und Bedrohungen zu verkleinern. Hier geht es also darum, welche Handlungen das Personal beim Eintritt einer Krise setzt (INT_07).

Als zentrale Norm im Bereich personelle Sicherheit, die für die RKE-RL relevant ist, ist die ÖNORM S 2450:2014 zu nennen, welche den Umgang mit klassifizierten Informationen regelt. Somit zielen die in dieser Norm genannten Maßnahmen auf den „Schutz klassifizierter Informationen vor unbefugtem Zugriff oder unberechtigter Weitergabe“ ab (ÖNORM S 2450:2014, S.3). In dieser Norm werden insgesamt 21 relevante Begriffe definiert, darunter fallen beispielsweise w. klassifizierte Information und Sicherheitsüberprüfung. Weiters werden Begriffe wie Sicherheitsbeauftragter thematisiert.

> „Klassifizierte Informationen sind materielle und immaterielle Informationen, unabhängig von Darstellungsform und Datenträger, die aufgrund ihres Inhalts eines besonderen Schutzes bedürfen und die daher nur einem begrenzten Personenkreis zugänglich gemacht werden sollen“ (Parlament Österreich, o.D.)

In der ÖNORM S 2450:2014 wird der Begriff klassifizierte Information folgendermaßen verwendet: „im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, unabhängig von deren Darstellungsform, welchen entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung eine Klassifizierungsstufe zugeordnet wurde, um den Schutz vor Missbrauch, Zerstörung, Entfernung, Bekanntgabe, Verlust oder Zugriff durch Unbefugte oder jede andere Art der Preisgabe an Unbefugte sicherzustellen“ (ÖNORM S 2450:2014, S. 4). Laut ÖNORM S 2450:2014 sind klassifizierte Informationen in vier Stufen zu unterteilen: eingeschränkt, vertraulich, geheim sowie streng geheim, wobei bei Informationen, die dieser Kategorie zuzuordnen sind, keine Übermittlung an die Wirtschaft erfolgen darf (ÖNORM S 2450:2014).

Sobald eine Organisation Zugang zu klassifizierten Informationen, welche der Kategorie „vertraulich“ zugeordnet werden können, hat, ist es unabdingbar, eine*n Sicherheitsbeauftragte*n in der Organisation zu etablieren, welche*r neben zahlreichen weiteren Aufgaben vor allem zu gewährleisten hat, dass die Sicherheit klassifizierter Informationen vorhanden ist, sei es durch technische

oder auch organisatorische Mittel. Des Weiteren dürfen Mitarbeiter*innen einer Organisation, welche tätigkeitsbezogen mit klassifizierten Informationen zu tun haben, nur nach einer Unterweisung sowie einer im Vorfeld abgeschlossenen Sicherheitsprüfung in Berührung mit dieser Art von Informationen kommen (ÖNORM S 2450:2014). Talbot und Jakeman (2009) argumentieren in diesem Zusammenhang folgendermaßen: „When a person is appointed to a position of trust, an organization should determine whether the initial appointment checks provide enough assurance that the employee can be entrusted with sensitive information" (S. 65). Die Sicherheitsüberprüfung von Mitarbeiter*innen ist als eine von mehreren Maßnahmen der personellen Sicherheit zu werten, welche dazu beitragen, dass nur vertrauenswürdige Personen Umgang mit klassifizierten Informationen haben" (ÖNORM S 2450:2014, S.8). Weiters sind in dieser Norm Anforderungen an das Sicherheitspersonal festgelegt, wobei unternehmensinterne Personen sowie Personen von externen Dienstleistern als Sicherheitspersonal fungieren können. Hier ist vor allem der Sicherheitsbeauftragte verantwortlich, der die Tätigkeiten des Sicherheitspersonals bestimmt. Dieses hat über passende Medien zur Kommunikation zu verfügen und erhält genaue niedergeschriebene Anweisungen vom Sicherheitsbeauftragten zur Erfüllung der zugeteilten Aufgaben (ÖNORM S 2450:2014).

Als problematisch stellt sich dar, dass in dieser Norm lediglich eine zu erfolgende Sicherheitsüberprüfung thematisiert wird, wenn ein*e Mitarbeiter*in neu im Unternehmen aufgenommen wird. Jedoch handelt es sich beim Pre-Employment Screening nur um eine Momentaufnahme. Laut Norm gibt es keine Festlegungen, dass derartige Überprüfungen auch erfolgen sollten, wenn eine Person bereits seit Längerem in der Organisation tätig ist. Folglich kann dies als Schwachstelle in der ÖNORM S 2450:2014 gewertet werden. Im Gegensatz dazu ist in der ISO 27002:2022 geregelt, dass auch Personen, die bereits im Unternehmen etabliert sind, einem Screening unterzogen werden sollten (INT_07). Auch Talbot und Jakeman (2009) weisen darauf hin, dass ein regelmäßiges Überprüfen des Personals notwendig ist:

> „Screening does not, on its own, provide a guarantee of integrity and trustworthiness. Because individuals and their circumstances change, screening is only as good as the investigations done at the time, and an ongoing review or aftercare program should also be undertaken to ensure the screening process remains valid. Any new information or concerns that may affect an employee's reliability must be advised promptly to the appropriate authority" (S. 65).

Diese Norm ist in einer high-level-structure aufgebaut und bietet sozusagen einen Leitfaden mit unterschiedlichen Bereichen, wie Sicherheit aufgebaut sein soll, nämlich organisatorisch, personell, physisch sowie technisch (INT_07).

In der ÖNORM S 2450:2014 sind neben Maßnahmen der personellen Sicherheit auch Maßnahmen der materiellen Sicherheit angeführt. Hierbei ist angegeben, dass der/die im Unternehmen etablierte Sicherheitsbeauftragte Maßnahmen des materiellen Geheimschutzes je nach Einstufung der Bedrohungslage festlegt. Im Rahmen dessen ist „ein Risikomanagementprozess anzuwenden,

um sicherzustellen, dass der Umfang des materiellen Schutzes dem festgelegten Risiko entspricht“ (ÖNORM S 2450:2014, S. 9). An dieser Stelle zeigt sich erneut die Verknüpfung der Themenbereiche physische Sicherheit, Risikomanagement (und personelle Sicherheit). Unter anderem ist die Örtlichkeit, an dem die klassifizierten Informationen aufbewahrt werden, sowie das geschätzte Ausmaß der Bedrohung durch Wirtschafts- und Industriespionage etc. zu beachten (ÖNORM S 2450:2014). Außerdem ist in dieser Norm angegeben, dass Verwaltungsbereiche oder sehr geschützte Bereiche mit Abhörschutz eingerichtet werden müssen, damit der materielle Schutz von klassifizierten Informationen gewährleistet werden kann. Organisatorische Maßnahmen beziehen sich beispielsweise auf die Vernichtung von klassifizierten Informationen, dabei geht es vor allem darum, dass möglichst wenig klassifizierte Informationen in einer Organisation etc. vorhanden sein sollten (ÖNORM S 2450:2014).

Fazit

Aufgrund der RKE-RL sind die kritischen Organisationen eines Mitgliedsstaates dazu verpflichtet, Mitarbeiter*innen entsprechend zu schulen, zu überprüfen, deren Zutritt zu physischen Objekten zu regeln etc.. Zentral in der ÖNORM S 2450 ist das Schutzziel der klassifizierten Informationen, welche in die Kategorien, eingeschränkt, vertraulich, geheim und streng geheim unterteilt werden können. In der genannten Norm werden die Begriffe Risikomanagement und physischer Schutz in Beziehung gesetzt. Somit wird auch in dieser Norm die Bedeutung des Risikomanagements für eine Organisation untermauert. Als Mangel dieser Norm ist die Tatsache zu werten, dass eine Sicherheitsüberprüfung des Personals lediglich zu Beginn des Arbeitsverhältnisses zu erfolgen hat und im weiteren Verlauf der Anstellung dies nicht mehr thematisiert wird. Laut dieser Norm soll Sicherheit organisatorisch, technisch, personell sowie technisch aufgebaut sein.

Ist ein adäquates Sicherheitsmanagement der Mitarbeiter*innen einer Organisation etabliert, so ist dies eine gute Voraussetzung für die Funktionsfähigkeit und Anpassungsfähigkeit im Krisenfall. Es ist somit in diesem Zusammenhang davon auszugehen, dass das Security-Bewusstsein der einzelnen Individuen bzw. in weiterer Folge die gesamte Sicherheitskultur einer Organisation eine zentrale Rolle spielt, auch wenn dies in der Norm nicht explizit angeführt wird.

3.6. Resümee und Ausblick

Insgesamt bieten Normen klare Kriterien, die Organisationen helfen, Managementsysteme wie Risikomanagement, Notfall- und Krisenmanagement, BCM sowie physischen Schutz und den Umgang mit Informationen und Mitarbeiter*innen systematisch zu implementieren. Sie fördern eine gemeinsame Sprache und definieren Mindeststandards, die erfüllt sein sollen (Bundeskanzleramt 2004a). Normen spielen somit eine entscheidende Rolle bei der Sicherstellung von Sicherheit und

Resilienz kritischer Einrichtungen. Sie bieten eine Anleitung für die Etablierung von Prozessen und Standards, die Organisationen als Rahmen für ihre Sicherheitsstrategien nützt.

Dabei kann zwischen internationalen (ISO), europäischen (EN) und nationalen (ÖNORM, DIN) Normen sowie zwischen allgemeineren Grund- beziehungsweise Basisnormen und spezifischen Unternormen unterschieden werden. Hervorgehoben wird die Bedeutung der HS, die eine einheitliche Struktur sowie die gemeinsame Definition von Begriffen fördert und so Vergleichbarkeit sowie eine vereinfachte Integration in Unternehmensprozesse ermöglicht (Dröge, 2024). Nicht zuletzt aufgrund dessen, dass diese Vereinheitlichung nur für ISO-Normen gilt, bleibt ein gewisser Interpretationsspielraum bei der Anwendung einzelner Normen bestehen, welcher gleichzeitig Handlungsspielraum für die spezifische Implementierung von Normen zulässt (INT_05). Eine gut strukturierte Norm sollte nach Ansicht von Expert*innen einen klaren Prozess abbilden und die zentrale Frage aufgreifen: Wie wird eine Bestandsaufnahme des aktuellen Zustands systematisch durchgeführt? Erst darauf aufbauend kann analysiert werden, welche Maßnahmen erforderlich sind (INT_02). Darüber hinaus sollten einheitliche Begriffsbestimmungen in den Normen geregelt sein sowie Bezug auf weitere (verwandte) Normen genommen werden (INT_09). Hinsichtlich dieser beiden Anforderungen leistet die Etablierung der HS bereits einen wesentlichen Beitrag.

Ein effektiver normativer Ansatz sollte risikobasiert sein, indem er klärt: Welche Risiken bestehen? Welche Bedarfe gibt es? Und wie sollten diese Risiken gezielt adressiert werden? Zudem sollte eine Norm auch die Anforderungen relevanter Stakeholder berücksichtigen und prüfen, ob diese in den risikobasierten Ansatz integriert sind. Immer wieder werden solche Aspekte vernachlässigt, vor allem wenn es sich bei Stakeholdern z. B. um Versicherungen handelt, obwohl sie maßgeblichen Einfluss auf die Sicherheitsstrategie haben können (INT_02). Letztlich spielt auch die wirtschaftliche Perspektive eine entscheidende Rolle: Unternehmen müssen abwägen, inwieweit die Erfüllung bestimmter Anforderungen wirtschaftlich sinnvoll ist oder, ob sie für die eigentliche Geschäftstätigkeit eine untergeordnete Relevanz haben (INT_02). Darüber hinaus müssen Unternehmen angesichts der Vielzahl an Normen mit starken Überschneidungen und zunehmender Komplexität sorgfältig prüfen, welche Standards für ihre spezifischen Ziele tatsächlich relevant und hilfreich sind (INT_04; INT_09).

Zusammenfassend zeigt sich, dass Normen zwar eine Struktur bieten, jedoch in ihrer Prozessualität und Praktikabilität zu wenig handlungsleitend sind. Die konkrete Umsetzung in die Praxis bleibt zumeist unklar und ist stark vom individuellen Verständnis abhängig. Eine stärkere Fokussierung auf Zieldefinition, konkrete Anleitungen und die Bewertung von Tools könnte die Lücke zwischen Vorgaben der Norm und der Praxis schließen und die Wirksamkeit des gesamten Sicherheits- und Risikomanagements verbessern. Dabei besteht ein schmaler Grat in der Ausgestaltung von Normen zwischen nicht zu einengend, da Anwender*innen die Vorgaben dann nicht mehr flexibel auf

die jeweilige Organisation anpassen können, und nicht zu grob, weil eine Norm in diesem Fall keine ausreichende Orientierung bietet. Die erfolgreiche Implementierung von Normen hängt somit maßgeblich von der geeigneten Anpassung an die Einrichtung, regelmäßigen Übungen von Notfällen, Krisen, der Wiederherstellung nach Sicherheitsvorfällen, der Sensibilisierung von Mitarbeitenden sowie der Unterstützung durch die Unternehmensführung ab. Ein generischer Ansatz für den Umgang mit Restrisiken und wirtschaftlich durchdachte Maßnahmen sind dabei entscheidend, um die Resilienz in kritischen Einrichtungen sicherzustellen.

4. Stand der Praxis

Im vorliegenden Kapitel wird das Forschungsziel, die Methode sowie die Ergebnisse der durchgeführten leitfadengestützten Expert*innen-Interviews zum Stand der Praxis in Bezug auf das Verständnis von Resilienz, Umgang mit relevanten Normen und weiterer umgesetzter Sicherheitsmaßnahmen sowie Erwartungen an die nationale Umsetzung der RKE-RL in der jeweiligen Organisation beschrieben.

4.1. Forschungsziel und Methode

Anschließend an die Recherche zum Stand der Wissenschaft bezüglich Resilienzforschung und Risikoanalysen sowie die Erhebung der relevanten Normen und einer Reihe von leitfadengestützter Expert*innen-Interviews zu dieser Thematik, wurden im Februar und März 2025 in einer Reihe von Unternehmen sieben leitfadengestützte Interviews mit jeweils ein bis zwei Sicherheitsexpert*innen aus kritischen Einrichtungen der Bereiche Verkehr und Transport, Energie, (Ab-)Wasser, Kommunikation, Gesundheit und Lebensmittel geführt, um den Stand der Praxis wissenschaftlich zu erheben. Als theoretische Stichprobe dieser explorativen Interviews wurden seitens des Bedarfsträgers BMI/DSN Organisationen unterschiedlicher Größe und Beschäftigtenanzahl ausgewählt. Dementsprechend erwiesen sich die für Resilienz zuständigen Abteilungen unterschiedlich stark strukturiert und ausgebaut.

Die Leitfäden wurden im Vorfeld übermittelt, die Gespräche wurden vom Forschungsteam der Hochschule Campus Wien (HCW) direkt vor Ort in den Unternehmen geführt. Die Gespräche wurden aufgezeichnet und im Anschluss transkribiert. Die wichtigsten Ergebnisse wurden anonymisiert und in einem Work-Group-Meeting am 31. März 2025 präsentiert. Ziel der Gespräche war es, eine realistische Einschätzung zur derzeitigen Praxis in Sicherheitsfragen zu erhalten und zu erheben, welche Vorarbeiten (Gap-Analysen, Status Quo Resilienzplan, strukturelle Maßnahmen) in den Unternehmen bisher bezüglich der bevorstehenden Verlautbarung des RKEG unternommen wurden. Zudem sollte erhoben werden, welche Form der Umsetzung der RKE-RL aus Sicht der Unternehmen praxistauglich wäre und welche bestehenden Normen und Maßnahmen (Risikobewertungen, Krisenpläne, Handbücher, Teams) derzeit schon im Sinne einer Stärkung der Resilienz wirksam sind.

4.2. Ergebnisse der Expert*inneninterviews

Allen Sicherheitsexpert*innen wurde zu Beginn die Frage gestellt, was sie unter dem Begriff Resilienz verstehen. Sehr häufig und mit großer Übereinstimmung lautete die Antwort – fast wortident – dass mit Resilienz eine Art von Widerstandsfähigkeit gemeint sei. Diese beziehe sich sowohl auf außerordentliche Belastungen oder Störfälle größeren Ausmaßes, ohne dass zwischen diesen

Anlässen weiter differenziert wurde. Zum Teil wurde dieser Definition noch hinzugefügt, dass Resilienz auch die Fähigkeit meine, sich von Störfällen rasch zu erholen.
Aus der Sicht der HCW war zunächst auffällig, dass die ad hoc formulierten Definitionen - obwohl im Kern passend - insgesamt den Begriff Resilienz nicht mit einer der RKE-Richtlinie angemessen Differenziertheit erklärten. Das in den Gesprächen kommunizierte Vorverständnis von Resilienz muss daher aus wissenschaftlicher Sicht als unterkomplex eingestuft werden. Das gilt insbesondere für einen Begriff von Resilienz, der im Zuge der Recherchen zum Stand der Wissenschaft, aus unterschiedlichen Forschungsfeldern hergeleitet werden konnte.
Eine Reihe von Aspekten, die aus der Sicht einer systemischen Herangehensweise als unverzichtbar erscheint, wurde in den ersten spontanen Definitionsversuchen von Seiten der Befragten gar nicht angesprochen. Dazu zählt insbesondere das Augenmerk auf einzelne Beschäftigte und die Wichtigkeit ganz kleiner Einheiten und Teams für Gesamtresilienz des Unternehmens. Einzelne Mitarbeitende sind zwar überall in Sicherheitsmaßnahmen einbezogen (Schulungen, Zugangskontrollen, Krisenpläne), es besteht im Rahmen dieser Bemühungen allerdings kein erkennbarer Fokus auf die personale Resilienz einzelner Mitarbeiter*innen. Die Notwendigkeit einer systemischen Vernetzung der personalen, interpersonalen, organisationalen bis zur gesellschaftlichen Ebene von Resilienz, ist als solche fast gar nicht im Bewusstsein der Verantwortlichen und das, obwohl auf allen diesen Ebenen Maßnahmen zum Teil schon gesetzt werden und Vernetzungen bereits etabliert sind.
In den spontanen Definitionen von Resilienz wurde eine Ausweitung der Resilienz über die Grenzen des Unternehmens hinaus allenfalls über das Eingebunden-sein in größere Konzernstrukturen reflektiert, aber nicht im eigentlichen Sinn als ein Aufgabenfeld im Sinne einer verstärkten Resilienz betrachtet. Sehr wohl bewusst ist die Tatsache, dass das jeweils eigene Unternehmen in übergeordnete Krisenpläne einbezogen ist. Dementsprechend fehlen – in dem, was selbst formuliert wurde - derzeit bei den Befragten auch noch weitgehend konkrete Vorstellungen hinsichtlich der Ausbildung von Resilienz-Fähigkeiten, die über Risikomanagement und Krisenpläne hinausgehen.

Verantwortliche für Resilienz im Unternehmen

In Unkenntnis der konkreten Anforderungen, die durch das RKEG auf sie zukommen werden, vermuten die meisten Gesprächspartner, dass sie selbst in Zukunft für Themen der Resilienz zuständig sein werden. Die zuständigen Teams sind üblicherweise Teil der Sicherheitsabteilungen oder Teil der Technik-Abteilung. Die Personen dieser Teams sind üblicherweise eng mit den Krisenstäben ihrer Unternehmen assoziiert bzw. mit Krisenplänen vertraut und sie sind in der Regel in präventive Maßnahmen wie Schulungen, bauliche Maßnahmen und das hierzu nötige Monitoring involviert. Das gilt ebenfalls für die Aufgaben der Risikobewertung, die allerdings häufig in Kooperation mit externen Unternehmen durchgeführt werden.

Die Größe der einsatzfähigen und ausgebildeten Teams schwankt stark und hat sehr unterschiedliche operative Schwerpunkte: In einem befragten Krankenhaus sind operativ die Betriebsfeuerwehr und der Sicherheitsdienst eine Art Exekutive vor Ort, durch die auch eine dauernde Einsatzbereitschaft gewährleistet wird. Der Schwerpunkt der Aufgaben liegt hier bei der Verhinderung von Sicherheitsvorfällen, dem Einsatz bei Unfällen und dem Konfliktmanagement bei Besucher*innen und Patient*innen. In einem anderen Unternehmen sind demgegenüber 300 Mitarbeiter*innen für Risiko und Resilienz zuständig, von welchen 100 noch einmal eigens für Einsätze im Katastrophenfall oder erhebliche Störungen (Blackout, Unwetter) vorbereitet wurden. Diese Vorbereitung erstreckt sich auch auf die Fähigkeit zu eigenverantwortlichem Handeln im Sinne des Unternehmens, selbst wenn Informationswege, Verkehrswege etc. ausfallen. Diese Abteilung ist daher vergleichsweise breit aufgestellt und besteht aus fünf Bereichen (Operatives Risikomanagement, Third Party Security, Krisenmanagement, Business Continuity Management und physische Sicherheit). Ein ganz anderes Beispiel stellt eine weitere Organisation dar: Störfälle, mit welchen man hier rechnet, sind technische Störfälle, oder technisch zu behebende Störfälle.

Relevante Normen und Resilienzplan

Für die befragten Sicherheitsverantwortlichen stellte die Anknüpfung an bekannte Normen einen wichtigen Bezugspunkt dar. In allen Interviews wurde daher gefragt, welche Normen derzeit bereits im Kontext von Resilienz berücksichtigt werden, bzw. bei welchen Normen die Ansicht vorherrscht, dass sie im Zusammenhang mit dem RKEG relevant sein könnten. Aus der Vielzahl von Normen werden einige als besonders relevant bzw. beispielhaft praktisch in der Anwendung genannt:

- Dazu zählte vor allem ISO 31000, welche im Zusammenhang mit dem IT-Risikomanagement genannt wurde (INT04; INT07). Weiters wurde von einer Organisation die ÖNORM D 4900 Reihe hinsichtlich der Risikodefinitionen und Bewertungsmethoden als vorbildlich und „extrem praktisch“ (INT04) hervorgehoben.
- Die ÖNORM S 2420 Norm wird hinsichtlich des physischen Schutzes und der Bewertung der Kritikalität von Objekten von den Verantwortlichen aus Organisationen der Bereiche Energie sowie Verkehr und Transport als „nützlich“ (INT04; INT05) eingestuft.
- Die Organisationen im Lebensmittelbereich sowie Kommunikation hoben die Relevanz von ISO 27001 bezüglich der Datensicherheit hervor und ISO 22301 hinsichtlich des BCM.
- Nach Einschätzung der Technik- und Sicherheitsverantwortlichen der Organisation im Bereich Wasser sind Fragen der Informationssicherheit nach NIS und ISO 27003 zu behandeln.
- Im selben Unternehmen wurde darauf hingewiesen, dass das ÖVGW Regelwerk W 103 maßgeblich für die Planung, den Bau von Trinkwasserbehältern und die Versorgung sei

und dass in ihrem Bereich zudem die EU Trinkwasser Richtlinie maßgebliche Standards vorgebe.

- In der Organisation im Bereich Lebensmittel, in der nach Auskunft der Gesprächspartner nur Lager, Logistik und Rechenzentren zur Kritischen Infrastruktur zählen, seien letztere nach EN 5060 zertifiziert.

Was den Vorbereitungsstand eines Resilienzplanes betrifft, wurde in den Unternehmen generell die Ansicht vertreten, dass man die meisten Bausteine dafür bereits vorbereitet habe. „Vieles haben wir schon."(INT02) „Wesentliche Elemente der Sicherheitsarchitektur existieren."(INT04) Nach Einschätzung der meisten Sicherheitsverantwortlichen werde der Resilienzplan so etwas wie eine systematische Vereinheitlichung und Synchronisierung der bestehenden Maßnahmen notwendig machen. „Es gibt eine Toolbox, um Resilienz von Teams und Mitarbeitenden zu stärken, aber noch keine Gesamtorganisation aller Maßnahmen." (INT03) „Es gibt noch keine zentrale Anlaufstelle für Resilienz." (INT04) Mit der konkreten Ausarbeitung des Resilienzplanes will man in den meisten Fällen bis zum Vorliegen des Gesetzes bzw. der Verordnung warten.

Wichtige Lernerfahrungen

Dem Lernen aus Erfahrungen, der Bewältigung von Krisen oder auch simulierten Gefahren in Übungssituationen kommt in allen Modellen organisationaler und regionaler Resilienz ein hoher Stellenwert zu. Die Modelle gehen davon aus, dass Fallstudien und Manöverkritik ein unverzichtbarer Bestandteil organisationalen Lernens sind. In diesem Sinn wurden die Unternehmen auch nach wichtigen Lernerfahrungen aus vergangenen Krisen gefragt.

Erwartungsgemäß stellte die Covid-19 Pandemie in dieser Hinsicht einen wichtigen Referenzpunkt dar. Am häufigsten geschildert wurden Herausforderungen im Zusammenhang mit dem Personalmanagement, d.h. der Vollständigkeit der personellen Besetzung, der Resilienz und Gesundheit der einzelnen Teammitglieder, aber auch der Aufrechterhaltung der Kommunikation. Die Belastung der Teams im Falle einer besonders lang andauernden Krisensituation wurde vor allem im Gesundheitsbereich betont. Ebenfalls im Kontext der Covid-19 Pandemie wurde von einer Optimierung der Informationssicherheit und der Lieferketten berichtet. Als eine besonders wichtige Erfahrung wurde von mehreren Befragten die Mitarbeit in Krisenstäben, ob auf Unternehmensebene oder in regional übergeordneten Einheiten hervorgehoben (INT04; INT03, INT06).

Ein anderer wichtiger Bezugspunkt waren die Erfahrungen mit dem Hochwasser im Sommer 2024. Dieses hatte nach Einschätzungen einiger Organisationen (INT03; INT02, INT07; INT06; INT04; INT01; INT05) überraschend viele Schwachstellen und die wechselseitige systemische Abhängigkeit der Einrichtungen voneinander sichtbar gemacht. Als vulnerable Punkte wurden vor allem Informationsausfälle oder -verzögerungen, unterbrochene Energieversorgung, die Kapazitäten der

Einsatzkräfte, die Sicherheit von Lagern und Lieferwegen und die herausfordernde Arbeit in Krisenstäben angeführt. „Wir waren auf der letzten Sicherheitsstufe“ (INT03).
Eine nicht unwesentliche Rolle für das hier angesprochene organisationale Lernen stellt – wie sich im Zuge der Interviews herausstellte – die Bewältigung täglicher kleiner Störfälle dar. Ob es sich um intentionale Vorfälle (Gewalt, Kriminalität, Vandalismus), um Schäden durch Unfälle, Wetterextreme oder auch technische Gebrechen handelt, sehr häufig führen gründliche Fall-Analysen im Rahmen einer Manöverkritik zu Einsichten und Optimierungsmaßnahmen, die mithelfen, künftigen Ereignissen besser vorbereitet zu begegnen. Diese Art von Fall-Analysen zählen in fast allen Betrieben zu den obligatorischen Maßnahmen nach Sicherheitsvorfällen (INT04; INT03; INT01; INT07; INT02; INT05; INT06). Hinsichtlich der Frage der Trainings und der Übungen, die Störfälle großen Ausmaßes mit einer Reihe von Kaskadeneffekten in Betracht ziehen, stellte sich heraus, dass Blackouts in allen Betrieben am häufigsten simuliert und in Übungen durchgespielt wurden.

Verhinderung von Sicherheitsvorfällen: Physischer Schutz

Die Fragen zu diesem Themenbereich orientierten sich an den in Art. 13 der RKE-RL aufgezählten Maßnahmenbereichen a bis f. Nach den konkreten Maßnahmen zur Verhinderung von Sicherheitsvorfällen befragt, zeigte sich einerseits ein durchaus hoher Standard, der durch eine Reihe von bereits umgesetzten Maßnahmen illustriert werden konnte, zum anderen wurde deutlich, dass für die Betriebe noch nicht abschätzbar ist, welche zusätzlichen Maßnahmen im Zuge der Umsetzung der RKE-RL noch ergriffen werden müssen. Grundsätzlich stellte sich heraus, dass Risikobewertungen und Risikomanagement überall üblich und selbstverständlich sind. „Eine störfallrobuste Anlagenkonzeption ist normal“ (INT03) und die umgesetzten Maßnahmen reichen von baulichen, wirtschaftlichen, technischen und organisatorischen Maßnahmen bis zu Cyber-Defense-Centern, Prävention und Mitarbeiter*innen-Schulungen. Ein weiterer Befund, der übereinstimmend fast gleichlautend zu hören war, lautet: „Sehr viel wird schon gelebt“ (INT03). Hingewiesen wurde in diesem Zusammenhang auf Zutrittskontrollen, Zutrittssteuerungen, Schließsysteme, Alarmsicherungen, Zäune, Zonenkonzepte und Handbücher (INT05; INT06; INT01; INT03).
Ein anderer Befund zum Thema physische Sicherheit lautete allerdings auch, dass hier noch mehr getan werden könnte, dass das aber Zeit und eine ausreichende Budgetierung brauche. Hingewiesen wurde auf sehr unterschiedliche Strukturen der einzelnen Unternehmen und Einrichtungen, insbesondere deren regionale Erstreckung sowie Umfang und Vielfalt der einzubeziehenden Maßnahmen und Objekte: Zäune, Tore, Schranken, Sensoren, Kameras, Luftüberwachung, Leitungen, Schienen, Gebäude, Stationen, Bahnhöfe. In diesem Kontext wurde auf die hohen Kosten hingewiesenen, die mit Investitionen in diesen Bereichen verbunden wären. „Bei baulichen Maßnahmen reden wir von Millionen. Dazu brauchen wir ein Sonderbudget“ (INT04). „Aus der Luft, durch Drohnen, sind wir wahnsinnig verwundbar“ (INT05). Zwei Einschätzungen fanden sich in diesem

Zusammenhang besonders häufig: 1) Kleinere Sicherheitsvorfälle seien aus der Sicht der Sicherheitsverantwortlichen unvermeidlich. 2) Hinsichtlich der „Flughöhe der RKE“ (INT02) – also hinsichtlich großflächiger, langandauernder Ausfälle und Kaskadeneffekte – ist man der Ansicht, dass diese nur sehr selten eintreffen werden.

Abwehr von und Reaktion auf Sicherheitsvorfälle und Wiederherstellung

Nach den präventiven Maßnahmen wurde im Zuge der leitfadengestützten Interviews auch nach Maßnahmen zur Abwehr und Reaktion auf Sicherheitsvorfälle gefragt sowie nach Maßnahmen, die geeignet sind, nach Störfällen zur Erholung und Wiederherstellung des regulären Betriebes, im konkreten Fall der wesentlichen Dienste beizutragen. Was die Frage der Abwehr von möglichen gravierenden Vorfällen anlangt, zeigte sich generell, dass sich die Unternehmen im Wesentlichen gerüstet fühlen. Man verwies auf Krisen- und Notfallversorgungskonzepte, Krisenhandbücher, Hotlines, Pläne, Stäbe, Schulungen zur Steigerung der Awareness und die Sicherung der Informationswege.

Als eine wichtige organisatorische und technische Maßnahme, wurde überall das Achten auf Redundanzen (Brunnen, Pumpen, Leitungen, Rechenzentren, Logistikzentren, Notstromaggregate, Dienstpläne, Teams, Lieferwege, Fahrzeuge, Gebäude...) genannt. Diese Maßnahme wurde von allen befragten Organisationen ausdrücklich erwähnt. Sie kommen in ganz unterschiedlichen Formen von lokal getrennten und unabhängigen Rechenzentren (INT02) bis zu Ersatzpumpen und -brunnen (INT03) oder alternativen Energieversorgungen zum Ausdruck. Häufig erwähnt wurde in diesem Kontext die Wichtigkeit einer kontinuierlichen Energieversorgung und der Kontakt zu Exekutive und Einsatzkräften vor Ort (INT06; INT07; INT04; INT05). Wie auch bei anderen Gelegenheiten wurde betont, wie maßgeblich in dieser Frage der Scope der Störfälle sei. „Wenn der halbe 19. Bezirk unter Wasser steht, kommt das noch gar nicht ins Krisenmanagement“ (INT04).

Etwas weniger gut vorbereitet ist man nach Einschätzung der meisten Befragten hinsichtlich der Fähigkeit der Wiederherstellung des Betriebes bzw. der wesentlichen Dienste nach Sicherheitsvorfällen. Sehr häufig wurde zugestanden, dass man mit dem BCM „noch nicht sehr weit“ sei oder, dass daran gerade gearbeitet werde. Andererseits wurde auch darauf hingewiesen, dass die Aufrechterhaltung des Betriebes, oder die rasche Wiederinbetriebnahme „Teil der DNA“ der Unternehmen sei. Das sei schon durch die Natur der Dienstleistungen – Wasser, Energie, Lebensmittel, Transport, Kommunikation – vorgegeben. „Wir haben Wertkontrakte mit Bauunternehmen, um im Gebrechensfall auch die physischen Mittel zu sichern“ (INT03).

Erneut wurde in diesem Zusammenhang das „Lernen aus Krisen“ als essenzieller Aspekt der Erholung nach Störfällen von den meisten Befragten angesprochen. Das werde vor allem durch eine gründliche Manöverkritik möglich, die Reaktionen der Mitarbeiter*innen, der Funktionsträger*innen, der Prozesse, der Technik, der Geschwindigkeit, der Kommunikation analysiere und

„Ableitungen für den Vorstand“ (INT02) vornehme. „Monitoring und Analyse der Vorfälle ist eine Stärke von uns“ (INT04).

Sicherheitsmanagement Beschäftigte

Die Auskünfte auf die Frage nach Maßnahmen im Personalbereich – wie in Art. 13, f der RKE-RL festgehalten – fiel etwas unergiebig aus. Das lag vor allem daran, dass auf der Ebene der Mitarbeiter*innen in allen befragten Unternehmen schon zahlreiche Maßnahmen (Schulungen, Trainings) gesetzt werden, zum anderen aber der Zusammenhang mit der in der RKE-RL angesprochen Resilienz für die meisten Sicherheitsverantwortlichen zum Zeitpunkt der Befragung noch schwer greifbar war.

Ohne noch genaue Planungsschritte unternommen zu haben (nur in einem Fall wurde anhand der RKE-RL bereits eine konkrete Gap-Analyse durchgeführt) gehen die Sicherheitsexpert*innen der Unternehmen davon aus, dass im Zuge der RKE-Umsetzung eine Ausweitung der Sensibilisierungsmaßnahmen über das derzeitige Ausmaß hinaus auf jeden Fall notwendig sein werde. Wiederholt wurde aber darauf hingewiesen, dass die Anzahl der Mitarbeiter*innen für den Umfang der Maßnahmen maßgeblich sein werde. Die Frage, wie viele Personen wie intensiv in Übungen oder in E-Trainings einbezogen werden, hänge davon ab. In der kleinsten untersuchten Einrichtung sind 35 Personen tätig, der Beschäftigtenstand beim größten befragten Unternehmen nach Auskunft der Sicherheitsverantwortlichen 47.000 Personen. Aus den Schilderungen der befragten Unternehmen ging auch hervor, dass die Größe der wirklich gut geschulten Teams von Betrieb zu Betrieb stark differiert und auch die Schwerpunktsetzungen (Cybersicherheit, Blackout, Zutrittskontrolle) sehr unterschiedlich ausfallen. Die Aufgabenzuteilung orientiert sich derzeit stark an den gängigen Risikobewertungen. Resilienz im Sinne der RKE-RL ist dabei nur teilweise oder indirekt berücksichtigt. Ausdrücklich darauf hingewiesen wurde, dass bauliche Sicherheitsmaßnahmen häufig auch Maßnahmen im Personalbereich nach sich ziehen würden. „Die Mitarbeiter*innen müssen durch diese Awareness-Thematik, also durch Schulungen und bei aufgepeppten Standorten ergeben sich automatisch mehr Aufgaben und man muss dann nachziehen“ (INT04).

Stärken, Schwächen, Verbesserungspotenziale

Die Unternehmen wurden auch gebeten, ihren jeweiligen Vorbereitungsstand zu beurteilen und auch etwaige Schwächen oder Verbesserungspotenziale im Hinblick auf die bevorstehende Umsetzung der RKE-RL zu benennen. Hinsichtlich der Stärken, war ein Ergebnis, dass man sich in spezifischen und neuralgischen Bereichen gut vorbereitet fühlt und in allen Betrieben mögliche Szenarien durchgespielt hat (INT06: Brand, Evakuierung, Blackout; INT02: Cyberattacken, Leitungsstörungen; INT04: Unfälle, Gewalt, Hochwasser; INT01: Starkregen, Stromausfall, INT07: Unwetter, Unterbrechung Lieferketten, Blackout) und Trainings absolviert. Im Kernbereich wird das

Krisenmanagement bzw. das Notfall- und Störungsmanagement in allen befragten Unternehmen als „potent“ eingestuft. Ein enger Kontakt zu Behörden, die Einbindung in die öffentliche Verwaltung und der Kontakt zu Krisenstäben (Land, Bund) werden als Stärke genannt (INT01; INT03; INT05; INT04; INT06). Gute Ortskenntnisse (Tankstellen, Verkehrsverbindungen, Bank) und eine gute regionale Vernetzung werden ausdrücklich nur im Gesundheitsbereich erwähnt.

Unter den Schwächen wurden in mehreren Gesprächen das BCM genannt, das im Vergleich zu anderen Maßnahmen als am wenigsten weit entwickelt beurteilt wird. Als ein zweiter schwieriger Bereich wird die oft noch mangelhafte Awareness der Mitarbeiter*innen genannt. Systematische und umfangreiche Schulungen könnten aus der Sicht der Sicherheitsexpert*innen häufiger sein. „Wir testen und üben noch viel zu wenig. Und es wird zu wenig dokumentiert“ (INT07). „Also diesen Kulturgedanken, die Sicherheitskultur einzupflanzen, das kann eine Dekade dauern“ (INT04). Das betreffe auch die Führungskräfte. Weniger gut vorbereitet sieht man sich auf kriegerische Angriffe und Terrorattacken insbesondere auf hybride Attacken oder Angriffe durch Drohnen, sieht aber eine Notwendigkeit, sich auch hier vorzubereiten (INT06; INT05; INT01). Als noch mangelhaft wird eine weitgehende gesellschaftliche und institutionelle Vernetzung mit anderen Stakeholdern eingestuft, um Interdependenzen zu berücksichtigen und Kaskadeneffekte zu vermeiden. Es gebe aber – mitausgelöst durch die RKE-RL – ausreichend Bewusstsein davon, dass große Störfälle mehrere Ministerien, mehrere Bundesländer und eine Vielzahl von nachgeordneten Behörden involvieren würden und dass hinsichtlich dieser Koordination noch viel zu tun sei (INT04; INT06; INT05). Im Kontext dieser Frage wurden auch einzelne Vorhaben genannt, die zur Optimierung des Vorbereitungsstandes ergriffen wurden. Darunter sicherheitspolizeiliche Überprüfung der Mitarbeiter*innen (INT05), die verbesserte Kommunikation mit Energieversorgern im Sinne der Stakeholder Resilienz (INT02), die Verbesserung der Cyber-Sicherheit (INT06) sowie die nochmalige Überprüfung und Optimierung der Alarm- und Meldeketten (INT04).

Praxistaugliche und überschießende Vorgaben

Mit Blick auf die Normierungen durch das RKEG bzw. nachfolgende Verordnungen wurde abschließend auch danach gefragt, welche Vorgaben seitens der Behörden als „praxistauglich“ und was als „überschießend“ eingestuft werden würde. Die übereinstimmende Antwort der Unternehmen auf die Frage was hinsichtlich der Vorgaben des Gesetzgebers als praxistauglich gelten würde, lautete: „Nicht mehr Auflagen als bisher.“

Als ein möglicher positiver Effekt wurde genannt, dass das RKEG ein „Hebel“ sein könnte, um Vieles, was bereits vorbereitet sei, nun zu bündeln und tatsächlich umzusetzen und, um als Security-Abteilung noch bessere Argumente gegenüber der Unternehmensleitung zu haben im Sinne von „Wasser auf Mühlen der Sicherheits-Manager“ (INT02). Durchgehend wünscht man sich möglichst konkrete und sektorspezifische Vorgaben hinsichtlich dessen, was der Resilienzplan zu

enthalten habe. Zusätzlich wären Best Practice Beispiele und Fallbeispiele (z.B. für physischen Schutz) hilfreich (INT04; INT07). Mehrfach wurde betont, dass es entscheidend sein werde, den Scope des gesamten Projekts so anzusetzen, dass es für die Betriebe möglich werde, normale (tägliche) Störfälle von solchen im Sinne der RKE-RL abzugrenzen. Zudem wurde vorgeschlagen, technologie-offen vorzugehen. Also seitens der Behörde nur Ziele vorzugeben, ohne festzulegen, wie diese zu erreichen seien. „Wir nehmen dann aus unserer Toolbox, was wir brauchen“ (INT04). Hinsichtlich der Normen und möglicher Checklisten gab es einige ganz konkrete Vorschläge: „Die 2420er funktioniert und reicht. Es sollte nicht mehr sein“ (INT05). „Am besten wäre ein Leitfaden nach der 31000er mit kleinen Vorgaben, mit Mindestvorgaben. Leitfäden für Implementierung angelehnt an 22301, 22361 und 2420 (physische Sicherheit). Und knappe Checklisten mit Mindestanforderungen, um Sicherheit gegenüber Auditoren zu haben“ (INT07). Außerdem wurde angemerkt, dass es vor allem eine Synchronisierung der Fristen brauche, damit man nicht jedes Jahr Ressourcen durch ein anderes Audit binde (INT05).

Überschießend wären dagegen inkonsistente Vorgaben, die zu einem noch höheren bürokratischen Aufwand führen, die tatsächliche Umsetzung sehr erschweren würden und auch wirtschaftlich bedenklich wären (INT02; INT04; INT07; INT05). Auf Grund der Einschätzung, im Kerngeschäft gut vorbereitet zu sein, wäre die Vorgabe, funktionierende Praktiken und Lösungen zu überarbeiten, naturgemäß wenig willkommen. „Überschießend wäre, wenn wir bewährte Instrumente, zum Beispiel das Winterhandbuch, wegen der RKE umschreiben müssten“ (INT04). Bezüglich der Fristen (und Strafen) wurde angemerkt, dass zu hoher Zeitdruck bei baulichen und technischen Maßnahmen, schon auf Grund der hohen Kosten, ein Problem darstellen würde (INT02; INT05; INT01; INT04; INT07).

5. PUKE-Zwischenkonferenz: Input aus der Praxis

Am 12. Juni 2025 fand eine Zwischenkonferenz des Forschungsprojektes statt, um die bisherigen Erkenntnisse, vor allem das entwickelte SRF, Vertreter*innen aus unterschiedlichen Branchen der kritischen Einrichtungen vorzustellen und mit diesen zu diskutieren. Außerdem wurden Vorschläge zur Risikoanalyse und Risikobewertung+, welche auch im Rahmen des Projektes entwickelt wurden, präsentiert (siehe Abb. 20).

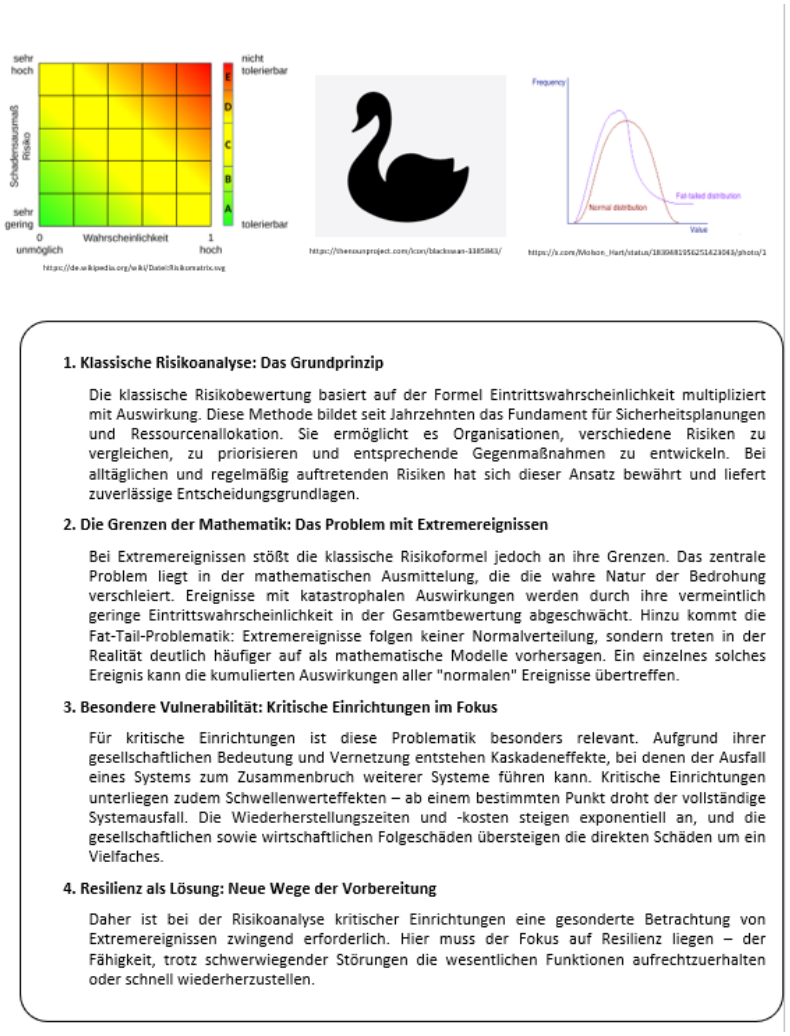


Abbildung 20: Risikobeurteilung von kritischen Einrichtungen

Quelle: eigene Darstellung

Im Rahmen der Konferenz wurden folgende drei Fragen an die Konferenzteilnehmer*innen gestellt:

1. Was ist hinsichtlich der Risikobewertung+ aus Sicht Ihrer Organisation zu beachten (Methoden, Tools etc.)?
2. Was ist in Bezug auf die geplante, ganzheitliche Steuerung (SRF) wichtig, damit dieses praxistauglich und anwendbar ist?

3. Welche Art von Factsheets und Checklisten in Bezug auf die Maßnahmenbereiche (Verhinderung von Sicherheitsvorfällen, physischer Schutz, Abwehr und Reaktion bei Sicherheitsvorfällen, Wiederherstellung nach Sicherheitsvorfällen, Sicherheitsmanagement von Mitarbeitenden) sind hilfreich?

Die wesentlichen Eindrücke bzw. Rückmeldungen aus der Praxis werden im Folgenden zusammenfassend dargestellt.

Zur ersten Frage hinsichtlich Risikobewertung nannten die Vertreter*innen aus Organisationen der kritischen Einrichtungen Folgendes:

- Ein risikobasierter, ganzheitlicher Ansatz wurde positiv bewertet.
- Je nach Branche wird der Risikobegriff unterschiedlich definiert, daher könne das Risiko nicht vereinheitlicht werden.
- Für die Umsetzung der Risikobewertung+ wird ein qualifizierter Risikomanager gefordert.
- Hilfreich wäre es, die Risiken anderer Sektoren zu kennen (dies wurde von anderen Organisationen jedoch nicht begrüßt).
- Hinsichtlich Risikoanalyse soll das BMI allgemeine Informationen zu Szenarien, Erdbeben, Wahrscheinlichkeiten etc. zentral zur Verfügung stellen.

Zur zweiten Frage hinsichtlich SRF kam es zu nachstehenden Äußerungen:

- Wichtig ist, dass die Verantwortlichkeiten klar definiert sind (Ansprechpartner, Vernetzung).
- Leitung einer Organisation müsse bewusst sein, dass nicht der*die Risikomanager*in, sondern die operative Ebene für die Umsetzung verantwortlich ist – dies müsse in der Richtlinie klar ersichtlich sein.
- Zu viele Stäbe, keine Vernetzung untereinander, fachspezifische Stäbe seien aber notwendig.
- Awareness von Mitarbeiter*innen in kritischen Einrichtungen erweist sich als bedeutend.
- Akzeptanz der Situation ist wichtig.
- Respekt für Expertise ist bedeutend.
- Lagebeurteilungen sollten erfolgen.
- Schnittstellen zwischen NIS und RKE sind einzubeziehen.
- Positive Hervorhebung, dass Theorie und Praxis kombiniert werden.

Hinsichtlich der dritten Frage zu Factsheets, Checklisten und Leitfäden wurden die folgenden Aspekte seitens der Konferenzteilnehmer*innen geäußert:

- Es besteht der Wunsch nach branchen-/sektorspezifischen Checklisten, am besten seitens BMI bestätigt.
- Der Wunsch nach Factsheets wie bei NIS wurde geäußert, die Mindestanforderungen sollten definiert werden.
- Keine „Flut“ an Normen, welche berücksichtigt werden müssen, ist gewünscht.
- Zielvorgaben sollen über Erwartungshaltungen erfolgen, z. B. wie lange der Dienst aufrechterhalten werden soll, wären sinnvoll.
- Sorge, dass durch weitere Checklisten zusätzlicher Aufwand entsteht, da bereits Checklisten existieren (z.B. Lebensmittelbranche).
- Black-Out-Vorgaben sollten bei Checklisten inkludiert sein.
- Es besteht der Wunsch nach Notfallnummern und Ansprechpartner*innen auf Behördenseite.

Abschließend wurde von den Vertreter*innen aus der Praxis Folgendes angemerkt:

- Generell sollten die Konzepte an Bisheriges in den Organisationen anknüpfen (z.B. Risikoanalyse).
- Wichtig ist, dass Auditor*innen ein gemeinsames Verständnis haben und nicht unterschiedlich agieren.
- Aus Ernstfällen/praktischen Erfahrungen sollte gelernt werden (lessons learned), daher bei der Erstellung von Erfahrungsberichten, auch die Berücksichtigung von Beinahe-Vorfällen miteinbeziehen.
- Meldeprozesse sollten möglichst einfach gestaltet sein, die Art und Weise, wie es bei NIS erfolgt, wird empfohlen.

6. Vernetzungsformate und Beratungsmöglichkeiten

Im Rahmen des Artikels 10 der RKE-RL wird gefordert, dass jeder Mitgliedsstaat gewährleistet, „dass die zuständigen Behörden mit den kritischen Einrichtungen der im Anhang festgelegten Sektoren zusammenarbeiten sowie Informationen und bewährte Verfahren austauschen“ (Art. 10 Abs. 2 Richtlinie (EU) 2022/2557). Des Weiteren ist in der Richtlinie festgelegt, dass die Mitgliedsstaaten „den freiwilligen Informationsaustausch zwischen kritischen Einrichtungen in unter diese Richtlinie fallenden Fragen im Einklang mit dem Unionsrecht und dem nationalen Recht, insbesondere in Fragen bezüglich Verschlusssachen und sensibler Informationen, des Wettbewerbs und des Schutzes personenbezogener Daten“ (Art. 10 Abs. 3 Richtlinie (EU) 2022/2557) unterstützen.

Im RKEG (BGBl. 60/2025) finden sich zu dieser Intention der Richtlinie hingegen keine näheren Bestimmungen. Im Rahmen des KIRAS-Projektes PUKE wurden zum Thema des „freiwilligen Informationsaustausches“ zwischen Unternehmen sowie Unternehmen und Behörden, dennoch einige Empfehlungen für die Konzeption eines Vernetzungsformates formuliert, da diese Thematik in naher Zukunft zu bearbeiten sein wird.

Die folgenden Ausführungen beziehen sich auf Vernetzungs- und Austauschplattformen für Organisationen zwecks des Teilens von Informationen über Sicherheitsbelange. Dazu wird zuerst das Konzept von Information Sharing Analysis Centers (ISACs) näher erläutert (z.B. deren Zwecke, Modelle, Rollen und Finanzierung). In weiterer Folge wird auf empirische Forschung in Österreich eingegangen, die aufzeigt welche Anforderungen bzw. Charakteristika eine derartige Plattform aufweisen sollte, ehe konkret das Beispiel des Austrian Trust Circle in Österreich erläutert wird.

6.1. Austauschformat Information Sharing Analysis Centers (ISACs)

Im Bereich der Cybersicherheit werden mit dem Namen ISACs Non-Profit Organisationen bezeichnet, welche der Sammlung und Verfügbarkeit von Informationen über Sicherheitsvorfälle und Bedrohungen, vor allem im Bereich der kritischen Einrichtungen sowie zur Zusammenarbeit zwischen der öffentlichen Hand und dem privaten Sektor dienen.

Im Zentrum von ISACs steht das Verbreiten und Rezipieren von negativen Informationen, wie z.B. Vorkommnisse, Bedrohungen, aber auch positiven Erfahrungen, wie Best-Practice-Beispiele unter den teilnehmenden Organisationen. „ISACs create a platform for such cooperation in term (!) of sharing information about root causes, incidents and threats, as well as sharing experience, knowledge and analysis” (ENISA, 2017, S.7). Das Konzept von ISACs hat seinen Ursprung in den Vereinigten Staaten und wurde nach den Angriffen auf das World Trade Center als Empfehlung zur Förderung des Austausches zwischen öffentlichem und privatem Sektor ausgesprochen. Auf

die Bereiche Energie und Finanzwesen konzentrierte sich die Errichtung der ersten ISACs in europäischen Ländern (ENISA, 2017).

Zu den Motiven für die Gründung von ISACs zählen u.a. soziale und wirtschaftliche Interessen sowie regulatorische Erfordernisse. Vor allem ökonomische Interessen stellen den häufigsten Beweggrund für den privaten Sektor dar, ISACs zu errichten, um auf Bedrohungen etc. besser vorbereitet zu sein, wobei meist mehrere Motive gemeinsam zur Etablierung dieses Austauschformats dienen. In den überwiegenden Fällen wird durch den privaten Sektor eines Staates veranlasst, dass ein ISAC gegründet wird, wobei die Verwaltung bzw. Regierung durch die Bereitstellung von finanziellen Mitteln eine unterstützende Rolle einnehmen kann. Am relevantesten sind regulatorische Erfordernisse als Grund in jenen Staaten, die eine starke öffentliche Verwaltung aufweisen. Weitere Gründe, warum ein ISAC etabliert wird, sind z. B. die Durchführung von Forschungsprojekten in diesem Themenfeld. Die Errichtung von ISACs durch den privaten Sektor, welche in weiterer Folge Kenntnisse, Informationen etc. mit der öffentlichen Verwaltung teilen, wird von den europäischen Regierungsinstitutionen überwiegend befürwortet, da diesen sowohl finanzielle als auch personelle Mittel dafür fehlen. Jedoch kann ein ISAC auch durch die Regierung selbst generiert oder durch europäische Institutionen wie die European Union Agency for Cybersecurity (ENISA) unterstützt werden (ENISA, 2017).

Für die Teilnahme an einem ISAC, gibt es aus Sicht der öffentlichen Hand und dem nicht-öffentlichen Sektor unterschiedliche Gründe. Generell sind das Wissen über Cybersicherheit und das Teilen von Informationen, wie bei einem Sicherheitsvorfall weiter vorgegangen werden kann, die häufigsten Beweggründe. Für Institutionen des privaten Sektors sind überwiegend folgende Gründe am relevantesten, um an einem ISAC zu partizipieren:

- Teilen und Erhalt von Informationen über Sicherheitsvorfälle,
- Zugang von Einrichtungen, welche weniger stark entwickelt sind, zu Wissensvorräten und Erkenntnissen anderer, ausgereifterer Organisationen, sowie
- die Möglichkeit der Kooperation und das Zusammengehörigkeitsgefühl.

Die Involvierung des öffentlichen Sektors an diesem Vernetzungsformat birgt die Vorteile, dass dieser besser über die Bedürfnisse des privaten Sektors Bescheid weiß, um in weiterer Folge diese Erkenntnisse z.B. in der Gesetzgebung zu berücksichtigen. Einen weiteren Nutzen, den die Beteiligung der öffentlichen Hand an ISACs aufweist, ist, dass dadurch ein „single coordination point“ etabliert werden kann. Dieser kann vor allem bei Vorfällen mit großer Reichweite hilfreich sein (ENISA, 2017). Ein wesentlicher Faktor der Funktionalität eines ISACs ist Vertrauen zwischen den einzelnen partizipierenden Einheiten. „Trust plays the key role in ISACs´ success” (ENISA, 2017, S. 34). Die beste Möglichkeit, um eine Vertrauensbasis zu generieren, sind persönliche Beziehungen bzw. eine Interaktion, die face-to-face stattfindet. Darüber hinaus erweisen sich z.B.

Zuverlässigkeit und Expertise als relevant für die Entwicklung einer vertrauensvollen Basis. Auf formeller Ebene gibt es einerseits die Option, Geheimhaltungsvereinbarungen, welche von allen Mitgliedern zu unterzeichnen sind und in denen u.a. detailliert festgehalten ist, wie mit den geteilten, sensiblen Informationen umzugehen ist, zu implementieren. „It is recommended that a mutual NDA should be signed to ensure that each side can potentially share information" (ENISA, 2017, S. 34). Andererseits kann anstelle einer Geheimhaltungsvereinbarung ein Code of Conduct implementiert werden, um vertrauensbildende Elemente innerhalb eines ISAC zu fördern. Eine Herausforderung für eine etablierte Vertrauensbasis könnte der Wechsel der Kontaktperson einer teilnehmenden Organisation sein. Außerdem sollten Mitglieder, welche nicht regelkonform agieren und wichtige Informationen nicht mit anderen teilen, von der Teilnahme exkludiert werden (ENISA, 2017).

Die Art und Weise, wie im Rahmen eines ISAC kommuniziert wird, kann differieren. Wie bereits zuvor angesprochen, ist die beste und häufigste Interaktionsweise persönliche Interaktion im Sinne von direkten Besprechungen unter den einzelnen Mitgliedern, diese finden für gewöhnlich halb- oder vierteljährlich statt. Hierbei besteht theoretisch die Möglichkeit, externe Personen, welche nicht am ISAC partizipieren, einzuladen, um etwa eine Präsentation abzuhalten, jedoch stehen die Mitglieder diesem Aspekt in der Regel eher kritisch gegenüber. Sehr häufig werden auch webbasierte Lösungen im Sinne einer Online-Plattform zur Kommunikation herangezogen. Auch innerhalb eines ISACs können wiederum „circles of trust" (ENISA, S. 31) etabliert werden, bei denen nur ausgewählte Mitglieder das Recht haben teilzunehmen. Während beispielsweise w. allgemeinere Rahmenbedingungen eines Vorfalles, der sich in einer Organisation ereignet hat, an eine größere Anzahl partizipierender Organisationen weitergegeben werden kann, könnten detailliertere Informationen lediglich bestimmten Mitgliedern kommuniziert werden. „Usually people involved in such an internal circle are the management team (or steering committee) with good knowledge of the organization and high(er) levels of trust among each other" (ENISA, 2017, S. 31).

Des Weiteren kann es neben Working Groups auch Ad hoc investigative Working Groups geben, welche für einen gewissen Zeitraum ins Leben gerufen werden, um sich mit akuten Vorfällen oder Bedrohungen intensiv zu beschäftigen, um Lösungen zu erarbeiten zu teilen. Auch jährliche Konferenzen, bei denen auf die Tätigkeiten von ISACs aufmerksam gemacht wird und potenzielle Stakeholder eruiert werden können sowie Kommunikation via E-Mail sind mögliche Kommunikationswege. Bei Letzterem findet für gewöhnlich das Traffic Light Protocol (TLP) Anwendung, um Dokumente und Informationen untereinander zu teilen, außerdem werden vor dieser Weitergabe die zu teilenden Informationen einer Validierung unterzogen. Ist letzteres in einem Information ISAC nicht etabliert, so kann die Person, welche die Information erstellt und kommuniziert hat, anhand einer Liste nachvollzogen werden (ENISA, 2017).

Werden innerhalb eines ISACs Vorfälle kommuniziert, so kann hier die Bandbreite von intendierten, aber nicht geglückten, bis hin zu schweren Vorfällen sein sowie Details über das Motiv des*der Täter*in, des Modus Operandi und des Ausmaßes des Schadens. Auch die Kommunikation über potenzielle Bedrohungen (z.B. verdächtige Dateien etc.) ist sinnvoll, da dies den Teilnehmenden ermöglicht Erfahrungen, wie Best-Practice Beispiele (z. B. wirksame Anti-Virus-Programm) sowie Analysen auszutauschen und adäquate Präventionsmaßnahmen in ihrer Organisation einleiten zu können. Durch diesen positiven unterstützenden Austausch wird die Kooperation zwischen den Organisationen gefördert (ENISA, 2017).

Die Mitglieder eines ISACs lassen sich in drei Rollen differenzieren. Zunächst ist eine Person erforderlich, die organisatorische Tätigkeiten übernimmt, indem sie die organisatorischen Rahmenbedingungen bereitstellt und Abläufe koordiniert, wie das Organisieren von Meetingräumlichkeiten und das Anfertigen von Protokollen etc.. Hierbei handelt es sich um das so genannte Sekretariat (facilitator), das gewöhnlich von der öffentlichen Verwaltung bereitgestellt wird. Neben der zur Verfügungstellung von Räumlichkeiten, leistet die öffentliche Verwaltung auch die Aufgabe, die gesetzlichen Rahmenbedingungen für die Etablierung und für den Informationsaustausch innerhalb von ISACs bereitzustellen. Eine weitere, bedeutende Rolle ist die des herkömmlichen Mitglieds (member), das eine aktive Teilnahme am Vernetzungsformat im Sinne der Verbreitung von Informationen über sicherheitsrelevante Themen der eigenen Organisation erbringt bzw. auch finanzielle Unterstützung durch die Zahlung des Mitgliederbeitrages leistet. Durch den Begriff des Partners (partner) werden Organisationen einbezogen, welche gelegentlich an ausgewählten Sitzungen des ISACs partizipieren, um beispielsweise wissenschaftliche Daten zu teilen oder über die Umsetzung einer Richtlinie in nationales Recht zu informieren. Die Organisationen, welche am ISAC teilnehmen, gehören mit mehr als der Hälfte (zirka 56%) zum privaten Sektor, die restlichen Institutionen können der öffentlichen Hand zugeordnet werden (ENISA, 2017). Zu den Hauptakteur*innen von ISACs zählen wirtschaftliche Organisationen, da diese einerseits stets ein hohes Niveau an Sicherheit ihrer Abläufe, Produkte etc. gewährleisten möchten. „Secondly, the industry is obliged by law to report incidents and to ensure continuity of critical services (e.g. critical infrastructure and crisis management regulations)" (ENISA, 2017, S. 26).

Hinsichtlich der Bedeutung des öffentlichen Sektors bei ISACs kann Folgendes festgehalten werden: Wie bereits angedeutet, werden ISACs meist durch die Wirtschaft geleitet, die öffentliche Verwaltung hat hingegen eine untergeordnete Rolle: „Even when the public administration is involved, it is the industry that determines the shape and functioning of their cooperation" (ENISA, 2017, S. 26). Das Ausmaß der geteilten Informationen innerhalb eines ISACs hängt von der Miteinbeziehung von Vertreter*innen der Industrie bzw. der Wirtschaft ab. „The industry is therefore either a facilitator or a member in the ISAC. In case a representative from another sector participates sporadically in the ISAC meetings (probably dedicated open sessions), they become partners" (ENISA,

2017, S. 26). Zu den Sektoren, welche am stärksten an diesen Austauschformaten partizipieren, zählen vor allem die Finanzbranche und der Energiebereich, gefolgt von Gesundheit und beispielsweise Luftfahrt (ENISA, 2017).

Im Allgemeinen können die folgenden drei Arten von ISACs differenziert werden: länderbasiert (country-focused model), sektorspezifisch (sector-specific model) und internationale Zusammenarbeit (international collaboration model). Das Modell, das auf ein gesamtes Land fokussiert, intendiert, alle Fachkundigen und CERTs (Computer Emergency Response Teams) eines Landes zu vereinen und den Informationsaustausch zu erleichtern, wobei sich diese Art der Zusammenarbeit als weniger formell charakterisieren lässt.

Das sektorspezifische Modell von ISACs legt das Hauptaugenmerk auf die einzelnen Sektoren der kritischen Einrichtungen. „The goal is to share information and analysis with other information and security experts that are active within the sector, so that the operator could benefit as much as possible from sectorial knowledge and experience" (ENISA, 2017, S. 20). Bei dieser Art von ISACs lässt sich hinsichtlich der Zusammenarbeitsform zwischen ISACs, die vom Sektor selbst initiiert, und ISACs, die von der Regierung initiiert werden, unterscheiden. Bei ersterem legt der jeweilige Sektor selbst aktiv fest, welche Struktur des Informationsaustausches benötigt wird. Üblicherweise erhält diese Art von ISACs keine monetäre Unterstützung durch die öffentliche Hand, sondern diese finanzieren sich selbst über verpflichtende Mitglieds- oder freiwillige Beiträge. Im Einklang damit ist auch der öffentliche Sektor meist nicht in sektorspezifische ISACs involviert, wobei in einzelnen Ausnahmefällen eine Zusammenarbeit bestehen kann, wie beispielsweise bei schwerwiegenden Vorfällen. Diese Art von ISACs ist vor allem in größeren Staaten aufzufinden, in denen der private Sektor sehr stark ist und die relevanten Akteur*innen sehr an Informationsflüssen interessiert sind.

Bei zweiterem (government facilitated ISACs) gibt es eine stärkere Bindung zwischen dem privaten Sektor und der öffentlichen Hand. Letztere bietet sowohl administrative (Sekretariat) als auch finanzielle Unterstützung. Eine besondere Eigenschaft dieses Ansatzes ist, dass der öffentliche Sektor einen „multi-sectoral approach" (ENISA, 2017, S. 21) aufweist. In diesem Fall werden ISACs in mehreren Sektoren gegründet und eine Stärkung der Cybersicherheit über verschiedene Bereiche hinweg wird intendiert, wobei dennoch zu konstatieren ist, dass jeder Sektor spezifisch ist und Eigenheiten aufweist. Im Unterschied zu den sector operators facilitated ISACs, welche in großen Ländern vorkommen, sind ISACs, die Unterstützung von der Regierung erhalten, vor allem in kleineren Staaten aufzufinden, da weniger Stakeholder vorhanden sind und leichter finanzielle Mittel lukriert werden können.

Internationale ISACs ermöglichen eine europa- bzw. weltweite Kooperation zwischen Organisationen, wobei sich vor allem der Finanz-, Energie- und Flugsektor international vernetzen. Bei

diesem Typus fungiert vor allem der private Sektor als Initiierungs- sowie Dreh- und Angelpunkt, und alle Akteur*innen nehmen aktiv an diesem Vernetzungsformat teil. Die Rolle des Sekretariats wird meist von einem aktiven Mitglied selbst und somit nicht, wie sonst meist üblich, von der öffentlichen Verwaltung übernommen. Allerdings ist an dieser Stelle zu erwähnen, dass sich die Entwicklung der bereits oben erwähnten, zentralen Ressource Vertrauen bei diesem Typus am schwierigsten etabliert (ENISA, 2017).

Wie bereits kurz erwähnt, können ISACs auf verschiedene Weisen finanziert werden. Die häufigste Form stellt dabei die Zahlung von Mitgliedsbeiträgen der am ISAC involvierten Organisationen dar, wobei sich die geleisteten Beiträge beispielsweise nach der Größe der jeweiligen Organisation richten und für gewöhnlich einmal pro Jahr zu entrichten sind. An zweiter Stelle stehen freiwillige Abgaben. Erwähnenswert ist, dass unter Expert*innen in diesem Bereich Konsens herrscht, dass durch die Zahlung eines Mitgliedsbeitrags die jeweiligen Akteur*innen stärker motiviert sind, sich aktiv am ISAC zu engagieren. Etwas mehr als ein Fünftel stellen andere Quellen dar, wobei diese Art der Finanzierung Abgaben auf freiwilliger Basis stark ähneln, am geringsten sind Subventionen durch die öffentliche Hand (ca. 17%). „It is a rather rare funding option, since governments all over Europe believe that this is the private sector's role to secure its services through information sharing" (ENISA, 2017, S. 29).

6.2. Vernetzungsplattformen in Einklang mit Art.10 der RKE-RL

Im Folgenden wird konkret auf die Ergebnisse einer empirischen Untersuchung von Enne (2025) eingegangen, die sich auf die Errichtung eines Austauschformats in Österreich konzentriert. Zudem werden Ergebnisse einer Fokusgruppe mit Experten (es nahmen nur männliche Teilnehmer teil) aus kritischen Einrichtungen und der DSN vorgestellt, die in einem Policy Paper mit konkreten Empfehlungen verschriftlicht wurden.

Ergebnisse aus der Untersuchung von Enne (2025)

Im Rahmen einer studentischen Abschlussarbeit, welche im Fachbereich Risiko- und Sicherheitsmanagement der Hochschule Campus Wien entstanden ist, richtete sich der Fokus auf die potenzielle Ausgestaltung eines Sicherheitsaustauschformates für kritische Einrichtungen in Österreich, welches den Anforderungen des Artikels 10 der RKE-RL gerecht wird. Im Zuge wissenschaftlicher Leitfadeninterviews zeigte sich, dass ein Vernetzungsformat für Organisationen als notwendig erachtet wird, um sich über Sicherheitsbelange austauschen zu können. Als Hauptgründe, an Austauschplattformen teilzunehmen, kristallisieren sich vor allem die Reduktion von Kosten sowie die Möglichkeit, hochwertige Informationen über Sicherheitsthemen anderer Organisationen (z.B. Vorfälle, Bedrohungen, aber auch Best-Practice-Beispiele) zu erhalten, heraus. Neben diesen Motiven

spielt auch der soziale Aspekt eine Rolle, da kritische Einrichtungen eine erhebliche Verantwortung für das Funktionieren der Gesellschaft tragen und sich dessen bewusst sind (Enne, 2025).

Aus Expert*innensicht wird die Organisation sektorspezifischer ISACs empfohlen, da erstens Organisationen innerhalb eines Sektors mit ähnlichen Bedrohungen etc. konfrontiert sind, wodurch wiederum die geteilten Informationen für alle Teilnehmer*innen am Austauschformat wertvoll sein können. Zweitens deckt die RKE-RL eine Bandbreite von Sektoren ab, somit wären sektorübergreifende Austauschformate schwer zu koordinieren. Dadurch, dass sich Organisationen innerhalb eines Sektors untereinander meist bereits kennen, erweist sich dies auch für die Entwicklung einer Vertrauensbasis, auf welche später näher eingegangen wird, als förderlich. Die partizipierenden Akteure sollten vor allem operative Akteur*innen aus den jeweiligen Organisationen sein. Die Gruppengröße sollte eher klein gehalten werden, weiters sollte auf kontinuierliches Wachstum und konstante Mitglieder geachtet werden. Trotz der sektoralen Organisation des Sicherheitsaustauschformates sollte auch eine sektorübergreifende Koordinationsstelle etabliert werden, „um sowohl branchenspezifische Herausforderungen als auch gesamtgesellschaftliche Bedrohungen adäquat adressieren zu können“ (Enne, 2025, S. 137). Es sollte somit ein hybrides Modell (zentral und dezentral) angestrebt werden mit einem zentralen Hub, welcher steuert, vernetzt und „sicherheitsrelevante Meldungen an alle Teilnehmer*innen streut und inhaltlich anreichert“ (Enne, 2025, S. 138). Im Rahmen der Austauschplattform sollte hinsichtlich des Governance-Modells ein neutrales Sekretariat, wie bei ISACs üblich, eingerichtet werden, welches zwischen den partizipierenden Akteur*innen vermittelt. Die Rolle des Sekretariats könnte gemäß den interviewten Expert*innen durch das österreichische Bundeskanzleramt ausgeübt werden. Darüber hinaus wäre es empfehlenswert, eine Steuerungsgruppe bzw. einen Beirat aus Expert*innen der kritischen Einrichtungen zu implementieren, zwecks strategischer Ausrichtung und Einflussnahme auf das Sekretariat. Die Finanzierung könnte durch den Staat sowie durch Mitgliedsbeiträge gewährleistet werden (Enne, 2025).

Grundlegend für den Aufbau und die Aufrechterhaltung des Austauschformates für kritische Einrichtungen ist, wie bereits bei der Studie von ENISA (2017) festgehalten, die Entwicklung von Vertrauen zwischen den partizipierenden Einheiten. Nur auf diese Weise kann ein adäquater, wertvoller Austausch stattfinden. Diese Vertrauensbasis kann vor allem durch ausgeprägte Sicherheitsstandards und formelle Regelwerke, wie z. B. einen Code of Conduct gefördert werden (Enne, 2025).

Die Einbindung von staatlichen Einrichtungen (z.B. Aufsichtsbehörden) bei Vernetzungsformaten bzw. Austauschplattformen erweist sich als etwas herausfordernd. Eine stetige, aktive Partizipation von Behörden an der Plattform wäre schwierig, da die teilnehmenden Unternehmen etc. dadurch gehemmt werden könnten, sicherheitsrelevante Informationen bzw. Vorfälle zu

kommunizieren. Staatliche Behörden wären gemäß Offizialprinzip dazu verpflichtet, vorhandenen Vorfällen einer Organisation nachzugehen. Sollten Mitarbeiter*innen der Behörde sich nicht vorschriftsgemäß verhalten riskieren auch sie, strafrechtlich belangt zu werden. Dennoch werden Informationen des BMI/der DSN als wertvoll betrachtet, daher wäre es zu empfehlen, diese Einrichtungen teilweise in die Vernetzungsplattform einzubinden. Staatliche Einrichtungen sollten einerseits eine regulatorische Funktion wahrnehmen, welche sich auf die Umsetzung der RKE-RL bezieht, anderseits eine operative Funktion wahrnehmen und Analysen und Bedrohungsbewertungen bereitstellen sowie beratend zur Verfügung stehen. „Verpflichtend abzugebende Meldungen an die Behörde – wie es die RKE-RL vorsieht – sind entsprechend an die betroffenen kritischen Einrichtungen zu spiegeln und weiterzutragen; eine einseitige Meldeschiene ist dabei jedenfalls zu verhindern“ (Enne, 2025, S. 138). Generell sollten somit für die Partizipation von Behörden am Format die Bedingungen, unter welchen staatliche Stellen teilnehmen können, vorab genau festgelegt werden (Enne, 2025).

Hinsichtlich der Kommunikation innerhalb des Austauschformates ist festzuhalten, dass diese mittels physischer Treffen sowie digital stattfinden sollten. Regelmäßige face-to-face Meetings fördern, wie bereits erwähnt, die Vertrauensbasis. Neben physischen Treffen, für die entsprechende Sicherheitsvorkehrungen zu berücksichtigen sind, erweisen sich die Kommunikationskanäle E-Mails und andere Chatplattformen als hilfreich und relevant. Eine Verschlüsselung mittels TLP ist empfehlenswert. Auch die Einrichtung eines Intranets wäre denkbar. Generell muss ein gutes Verhältnis zwischen ausgeprägter Sicherheit und Benutzerfreundlichkeit der Kommunikationstools gewählt werden. Des Weiteren sollte die Option bestehen, Meldungen anonym abzugeben (Enne, 2025).

Barrieren für die Etablierung von und Teilnahme an Austausch- und Vernetzungsformaten können rechtlicher, organisatorischer und kultureller Natur sein. Ein stabiles Gruppengefüge erweist sich als zentral. Unklarheiten hinsichtlich Haftung können beispielsweise dazu führen, dass sich Organisationen am Austauschformat nicht beteiligen. Das Risiko, dass Trittbrettfahrer sich am Format beteiligen, kann durch entsprechende Evaluierungen in gewissen zeitlichen Abständen und Transparenzmaßnahmen sowie Sanktionen minimiert werden. Bei Verstößen gegen Sicherheitsregeln sollte zunächst das Gespräch mit den betreffenden Personen gesucht und eruiert werden, warum sich diese abweichend verhielten. Bei erneuten Verstößen sollten Verwarnungen erfolgen, die Exklusion eines Mitglieds von der Plattform sollte nur in besonders begründeten Fällen vorgenommen werden. Bei der Bearbeitung dieser Angelegenheiten steht vor allem das Sekretariat im Vordergrund (Enne, 2025).

Zusammenfassend sieht Enne (2025) für die Ausgestaltung des Sicherheitsaustauschformates gemäß Artikel 10 der RKE-RL sieben Schritte vor: Identifikation relevanter Akteure und

Stakeholder (operative Sicherheitsverantwortliche aus kritischen Einrichtungen der RKE-Sektoren, Leitung der Plattform, nationale Behörden, sonstige Partner wie Forschungseinrichtungen), Definition der Zielsetzung und Mehrwerte des Formats, Entwicklung der Governance- und Organisationskultur, Bildung von Vertrauen und Teilnahme, Aufbau von formellen Regeln, Etablierung von Kommunikationsstrukturen und Schutzmaßnahmen sowie als letzten Schritt die Qualitätssicherung (Enne, 2025).

Als österreichisches Beispiel für ein Austauschformat im Bereich Informations- und Kommunikationstechnologie kann der Austrian Trust Circle (ATC) genannt werden. Mithilfe des ATC wird eine Vertrauensbasis aufgebaut, sodass bei Notfällen gemeinsam reagiert werden kann. Es geht vor allem um den sektorinternen, aber auch sektorübergreifenden Austausch zwischen Expert*innen, Teilnehmer*innen und Behörden zur Förderung der Sicherheit in Organisationen. Diese Austauschplattform wurde durch das österreichische Bundeskanzleramt und CERT.at initiiert. Es handelt sich um „einen formellen Rahmen für praxisnahen Informationsaustausch und gemeinsame Projekte im Sicherheitsbereich“ (Austrian Trust Circle, 2012).

Ergebnisse aus der Fokusgruppe im Rahmen des Projekt PUKE

Die zu der Thematik am 22. Juni 2026 abgehaltene Fokusgruppe ergab, dass bereits seit einiger Zeit sowohl informelle als auch standardisierte Austauschformate zwischen einzelnen Unternehmen bestehen. Dieser Austausch findet zum Teil innerhalb von Sektoren zum Teil aber auch sektorübergreifend statt. Die Struktur entspricht in den meisten Fällen den oben als hybrid bezeichneten Formaten.

Aus der Energiewirtschaft wird von zwei regelmäßigen Arbeitsgruppen in Bereiche Netze und im Bereich Erzeugung berichtet, in welchen man sich kontinuierlich austausche. Aus dem Lebensmittelsektor wurde berichtet, dass die Vernetzung schon 2022 begonnen habe und durch die Behörde und auch die WKO eingeleitet wurde. Hier seien zunächst die Schwellenwerte in Zentrum der Diskussion gestanden. Es befänden sich Lieferkettenunternehmen, aber auch Händler in der Gruppe, in welcher ein sehr reger Austausch in Bezug auf Krisenmanagement und Prävention stattfinde. Es wurde ausdrücklich festgehalten, dass jedes einzelne Unternehmen unterhalb des Schwellenwertes der RKE-VO liege, man aber „in Summe“ vorbereitet sein wolle.

Eine sektor-übergreifende Kommunikation gebe es bereits zu unterschiedlichen Themen, beispielsweise hinsichtlich bestimmter Szenarien wie Black Out oder Pandemie. Außerhalb des eigenen Sektors wird die Energiebranche als besonders relevant eingestuft. Mehrfach wurde betont, dass eine Vernetzung über den Sektor hinaus am leichtesten mit Hilfe der Behörden (BMI, DSN) gelinge. Im Sinne eines Austausches in größerem Rahmen wurde das Format Tag der kritischen Infrastruktur ausdrücklich gelobt und eine halbjährliche oder zumindest jährliche Frequenz

angeregt. Übergeordnete Veranstaltungen dieses Formats werden ausdrücklich dem Aufgabenbereich der Behörden zugeordnet.

In hybriden Formaten sind sektor-übergreifende Kooperationen – nach Schilderung der Anwesenden – derzeit häufig noch informell organisiert. Man „kenne sich“ eben persönlich und das bilde auch die Basis für das Vertrauen, das für einen solchen Austausch nötig sei. Dass auf persönlichen Beziehungen beruhende Netzwerke weniger stabil seien, als standardisierte Formate, wurde zugestanden. Oberste Sicherheitsverantwortliche seien zudem häufig in internationale Netzwerke und Plattformen einbezogen, die ebenfalls stark zur Orientierung hinsichtlich globaler Trends und Strategien beitragen. Die Teilnahme an diesen Netzwerken hänge aber stark von der Agilität der jeweils verantwortlichen Personen ab.
Die Frage, welche Inhalte im Rahmen des Informationsaustausches kommuniziert werden sollen, ist nach Ansicht der anwesenden Experten heikel und derzeit noch nicht klar zu beantworten. Selbst bei einem gemeinsamen Fokus auf Abhängigkeiten und Verwundbarkeiten würden – auch innerhalb der Sektoren – „schutzwürdige Interessen“ der Unternehmen bestehen bleiben. Praktikabel sei daher u.U. ein Austausch über Best-Practice bei Resilienzmaßnahmen, gemeinsame Strategien und Analysemethoden, über typische Abläufe, Szenarien und Gefährdungslagen und weniger über Ergebnisse dieser Analysen, da diese auch spezifische Schwächen einzelner Unternehmen offen legen würden. Es wurde von Seiten der Branchenvertreter mehrfach betont, dass auch angesichts gemeinsamer Gefährdungen der Konkurrenzdruck weiter bestehen bleibe. Hinsichtlich übergeordneter Themen wurden die Nationale Sicherheitsanalyse und erste Resilienz-Audits als etwas genannt, dass nur in Kooperation mit der Behörde diskutiert werden könne.
Auf die Frage, welche Personenkreise und Funktionen jeweils in die Vernetzung einzubeziehen seien, ist man sich weitgehend einig, dass weiterhin informelle (persönliche) und formelle Kontakte sinnvoll seien. Es wird darauf hingewiesen, dass innerhalb der Sektoren über die Verbände meist ein Code of Conduct bestehe, der Spielregeln für den Umgang mit vertraulichen Informationen festlege. Die Effizienz einer solchen Vernetzung hänge aber immer auch vom Engagement aller Beteiligten ab. Wobei kleine Kreise mit wirklich interessierten Teilnehmer*innen wahrscheinlich am produktivsten seien.
Alles, was über eine sektorenspezifische Vernetzung hinausreiche, sollte am zweckmäßigsten über Einladung der DSN erfolgen. Wobei die Größe und Häufigkeit der Treffen gut zu überlegen sei. Treffen mit großer Teilnehmer*innenanzahl könnten Themen „nur überblicksartig“ behandeln, und zu häufige Treffen, würden kleine Unternehmen überfordern, die personell nicht über die Ressourcen verfügen, sich sehr häufig einzubringen.

Die beschriebenen Vor- und Nachteile der verschiedenen Formen bisheriger Vernetzungsformate sowie Erkenntnisse aus dem relevanten Stand der Forschung und der Fokusgruppe mit Sicherheitsverantwortlichen kritischer Einrichtungen zu Erwartungen und Herausforderungen flossen, in ein Policy-Paper für Entscheidungsträger*innen ein, dass darauf basierende Empfehlungen zur Gestaltung einer Vernetzungsplattform gemäß RKE-RL beinhaltet.

7. Leitfäden

Die in den vorangegangenen Kapiteln dargestellten Ergebnisse – der theoretische Rahmen des SRF, die Analyse relevanter Normen sowie die Befunde aus der Praxiserhebung – bildeten die Grundlage für die Entwicklung konkreter Unterstützungsformate im Rahmen des AP03. Auf Basis der einrichtungsinternen Risikoanalyse gemäß § 14 RKEG und der Anforderungen des § 15 RKEG wurden im Projekt Leitfäden zu den sechs Maßnahmenbereichen konzipiert, die in Art. 13 Abs. 1 der RKE-Richtlinie und im RKEG (BGBl. I Nr. 60/2025) festgelegt sind. Die Leitfäden wurden in einem iterativen Prozess in sieben Fokusgruppen mit Praxispartner*innen validiert und in ihrer vorliegenden Form finalisiert.

Die sieben Teile des Leitfadens – ein allgemeiner Teil (Z 0) zu übergreifenden Grundlagen sowie sechs Einzelleitfäden (Z 1–Z 6) – bilden ein zusammenhängendes System, das eine umfassende Resilienz kritischer Einrichtungen abdeckt: von der Verhinderung von Sicherheitsvorfällen über den physischen Schutz, die Abwehr und Bewältigung von Sicherheitsvorfällen, die Fortsetzung und Wiederaufnahme nach Sicherheitsvorfällen, personelle Sicherheitsvorkehrungen bis hin zur Sensibilisierung und Schulung des Personals. Die Leitfäden orientieren sich dabei an den Prinzipien der Geeignetheit und Verhältnismäßigkeit und vereinen EU-Leitlinien, gesetzliche Anforderungen, sowie einschlägige Normen in einem anwendbaren Anforderungsrahmen für kritische Einrichtungen.

Die Leitfäden berücksichtigen, dass Österreich bereits über eine Vielzahl an Regularien für die unterschiedlichen Sektoren sowie in den verschiedenen relevanten Sicherheitsbereichen verfügt. Bestehende Maßnahmen wie zum Beispiel aus Bereichen wie Anlagensicherheit, Brandschutz oder ArbeitnehmerInnenschutz sind daher nicht zu duplizieren, sondern in den Resilienzplan gemäß RKEG einzubeziehen. Die Leitfäden setzen dort an, wo bestehende Regelungen die spezifischen Anforderungen des RKEG an kritische Einrichtungen nicht vollständig abdecken – insbesondere beim physischen Schutz gegen intentionale Bedrohungen, beim Krisenmanagement und bei der dokumentierten Gesamtbetrachtung aller Resilienzmaßnahmen, dem organisationalen Resilienzplan.

Bei Einhaltung der Leitfadenvorgaben, können Einrichtungen grundsätzlich von einer Konformität mit § 15 RKEG ausgehen. Abweichungen sind zulässig, müssen aber nachvollziehbar begründet und mit dem Nachweis dokumentiert werden, dass die gewählte Alternativlösung eine gleichwertige Resilienzwirkung erzielt. Je größer die Abweichung, desto höher die Anforderungen an die Begründungsqualität. Diese Dokumentation bildet zugleich die Grundlage für die behördliche Überprüfung.

Die sieben Teile gliedern sich demnach wie folgt:

Z 0 – Allgemeine Grundlagen und Anwendung des Leitfadens bildet das gemeinsame Fundament für alle Einzelleitfäden. Hier wird der rechtliche Rahmen des RKEG erläutert und die Anwendungslogik beschrieben – insbesondere das Verhältnis zu bestehenden Regelungen und Normen – und die übergreifenden Grundsätze wie Geeignetheit, Verhältnismäßigkeit und Konformitätsvermutung erklärt.

Z 1 – Verhinderung von Sicherheitsvorfällen behandelt Prävention als integrierten Ansatz: technische Anlagensicherheit, sichere Betriebsführung und Instandhaltung, Katastrophenvorsorge und strukturelle Härtung, Klimawandelanpassung sowie die systematische Erfassung von Ereignissen und das Lernen aus Vorfällen. Ergänzt wird dies durch Maßnahmen zur Prävention menschlicher Fehler.

Z 2 – Physischer Schutz umfasst den Schutz der physischen Infrastruktur gegen natürliche Gefahren und menschengemachte Bedrohungen. Er behandelt bauliche und mechanische Maßnahmen (Perimeter, Gebäude), elektronische Systeme (Einbruchmeldeanlagen, Videoüberwachung, Zutrittskontrolle) sowie organisatorische und personelle Maßnahmen. Besondere Berücksichtigung finden hybride Bedrohungen durch ausländische Akteure sowie Risiken durch unbemannte Systeme. Der Leitfaden schließt mit Anforderungen an ein dokumentiertes Gesamtkonzept.

Z 3 – Abwehr und Bewältigung von Sicherheitsvorfällen richtet sich auf die Phase des eingetretenen oder sich entwickelnden Vorfalls. Im Mittelpunkt stehen eine belastbare Reaktions- und Führungsorganisation mit klarer Aktivierungs- und Eskalationslogik, geregelte Kommunikations- und Meldewege zu Behörden und Einsatzorganisationen sowie technische und ressourcenbezogene Maßnahmen zur Wirkungsminimierung. Der Leitfaden betont das Prinzip des „sicheren Versagens“, um kaskadierende Auswirkungen zu begrenzen.

Z 4 – Fortführung und Wiederaufnahme nach Sicherheitsvorfällen betrifft die strukturierte Rückführung in einen belastbaren Betriebszustand nach einem Sicherheitsvorfall. Behandelt werden die Definition von Mindestleistungsniveaus und Priorisierungslogiken, Business Continuity Management sowie Not- und Ersatzverfahren, die Sicherstellung erforderlicher Ressourcen und Redundanzen sowie das Management von Lieferketten und Versorgungssicherheit.

Z 5 – Personelle Sicherheitsvorkehrungen behandelt die strukturelle personelle Absicherung: die systematische Identifikation und Dokumentation kritischer Funktionen – einschließlich externen Personals –, die Steuerung von Zugangsberechtigungen, die Durchführung von Zuverlässigkeitsüberprüfungen sowie die Festlegung von Ausbildungs- und Qualifikationsanforderungen. Ausdrücklich berücksichtigt wird dabei auch die Integration von Geschlechtergleichstellung in die Resilienzplanung.

Z 6 – Sensibilisierung und Schulung schließt den Resilienzkreislauf durch die Verankerung einer Resilienzkultur im Personal. Der Leitfaden beschreibt Schulungsmaßnahmen, Informationsmaterialien und Übungsformate und betont, dass wirksame Sensibilisierung nicht durch Einzelmaßnahmen, sondern durch ein kohärentes, dauerhaftes Programm entsteht. Bestehende Cyber-Awareness-Programme gemäß NIS-2-RL sollen dabei integriert werden.

Der vollständige Leitfaden ist als eigenständiges Dokument veröffentlicht (DOI: https://doi.org/10.34895/hcw.0033).

8. Schlussfolgerung und Forschungsbedarf

Mit dem vorliegenden wissenschaftlichen Ergebnisbericht des KIRAS-Projekts „Projekt zur Unterstützung kritischer Einrichtungen - PUKE“ erfolgt erstmals ein wissenschaftlich aufbereiteter Überblick zur organisationalen Resilienz kritischer Einrichtungen in Österreich.

Dieser Überblick umfasst relevante theoretische Konzepte inklusive der Bewertung, ob diese bei einer Anwendung in der Praxis den erforderlichen Mehrwert bieten, die fachliche Aufarbeitung der relevanten Normenlandschaft gemäß den Anforderungen von Art. 13 Abs. 1 lit. a-f Richtlinie (EU) 2022/2557und § 15 Abs. 2 Z 1 bis Z 6 RKEG sowie gelebte Praxen am Beispiel ausgewählter kritischer Einrichtungen in Österreich.

Darüber hinaus wurde im Rahmen von PUKE erstmals ein organisationales Resilienzmodell auf Basis der Anforderungen der RKE-RL, das SRF, für weitere theoretische und angewandte Forschung zur organisationalen Resilienz konzeptualisiert und publiziert. Dieses systemische Framework beschreibt das Verständnis von organisationaler Resilienz, das diesem Forschungsprojekt zugrunde liegt, einerseits durch Resilienzbedingungen und -fähigkeiten, die organisationale Resilienz gestalten, und andererseits durch das Transparentmachen der Vernetzung organisationaler Resilienz (Mesoebene) mit der Mikro- (persönliche Resilienz) und Makroebene (gesellschaftliche Resilienz).

Die in der RKE-RL geforderten Leitfäden und Checklisten wurden als Handbuch „Leitfäden kritische Einrichtungen: § 15 Abs. 2 Z 1 bis Z 6 RKEG“ ausgearbeitet, in Fokusgruppen validiert und Vertreter*innen der kritischen Einrichtungen im Rahmen einer Fachkonferenz zum Projektabschluss präsentiert sowie als Online-Publikation übermittelt. Diese Leitfäden dienen sowohl als Orientierungshilfe zur Umsetzung der gesetzlichen Anforderungen zur Entwicklung organisationaler Resilienz in kritischen Einrichtungen als auch als Checklisten zur Überprüfung der Wirksamkeit der gesetzten Maßnahmen durch innerbetriebliche, behördliche oder weitere fachliche Kontrollmechanismen.

Die Anforderung zur Etablierung eines Austauschformats zwischen verantwortlicher staatlicher Behörde und kritischen Einrichtungen zur Vernetzung und zum Informationsaustausch über sicherheitsrelevante Vorfälle zur Erhöhung der gesamtstaatlichen Resilienz wurde durch ein Policy-Paper, das die derzeitige Ausgangslage, praxisrelevante Einschätzungen und wissenschaftliche Empfehlungen zur Umsetzung eines solchen Formates enthält, umgesetzt.

Ganzheitlich betrachtet bieten die Ergebnisse des Projekts PUKE umfassende Orientierung für künftige theoretische und angewandte Forschung wie auch zur Evaluation von Umsetzungsmaßnahmen durch die Behörde und kritische Einrichtungen zur Entwicklung der organisationalen Resilienz in Österreich. Aufbauend auf diesen Ergebnissen ergibt sich weiterer Forschungsbedarf zur Konkretisierung gesellschaftlicher Resilienz, um eine gesamtstaatliche Resilienz entwickeln und weiterführend gestalten zu können.

9. Literaturverzeichnis

Antonovsky, A. (1997). Salutogenese. Zur Entmystifizierung der Gesundheit. Dgvt-Verlag.

Austrian Standards. (2024a). Standards verstehen. https://www.austrian-standards.at/de/standardisierung/standards-verstehen (Zugriff: 20.12.2024).

Austrian Standards. (2024b). Info. Erläuternde Informationen zu ÖNORMEN. https://www.austrian-standards.at/de/hilfe-support/erlaeuternde-informationen (Zugriff: 20.12.2024).

Austrian Standards. (2024c). OVE-Richtlinie R2+AC. https://www.austrian-standards.at/de/shop/ove-richtlinie-r-2-ac-2017-04-01~p2295544 (Zugriff: 20.12.2024).

Austrian Standards. (2024d). OVE-Richtlinie R9. https://www.austrian-standards.at/de/shop/ove-richtlinie-r-9-2012-04-01~p1935099 (Zugriff: 20.12.2024).

Austrian Standards. (2024e). OVE-Richtlinie R10. https://www.austrian-standards.at/de/shop/ove-richtlinie-r-10-2016-03-01~p2190891 (Zugriff: 20.12.2024).

Austrian Trust Circle (ATC). (2012). Austrian Trust Circle. https://www.austriantrustcircle.at/ (Zugriff: 22.08.2025).

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84(2), 191–215.

Baumann, D. (2020). Resilienz und Resilienzmanagement als geeignetes Instrument in unsicheren Zeiten? In EAB Publishing (Hrsg.), Essays der Wissenschaft XVIII. Akademische Essays aus dem Bereich der interdisziplinären Wissenschaft zur Anwendung in Theorie und Praxis (S. 112–121). EAB Publishing. ISBN 978-3-96163-179-7.

Bauer-Wolf, S., Baumfeld, L. & Lukesch, R. (2009). Steuerung regionaler Entwicklung?! Nachträglich erweitertes und finalisiertes Grundlagenpapier zur gleichnamigen Tagung des Österreichischen Bundeskanzleramts (IV/4) im Rahmen von Strat.at plus (2007–13) am 28.11.2008 in Wien. ÖAR Regionalberatung GmbH. [Unveröffentlichtes Manuskript].

Bendell, J. & Read, R. (Hrsg.). (2021). Deep Adaptation. Polity.

Bentner, A. & Jung, J. P. (2022). Resilient durch Krisen: Wie Führungskräfte und Teams schwierige Zeiten bewältigen. Carl-Auer Verlag.

Berndt, C. (2013). Resilienz. Das Geheimnis der psychischen Widerstandskraft. dtv.

Brunnermeier, M. K. (2021). Die resiliente Gesellschaft. Wie wir künftige Krisen besser meistern können. Aufbau Verlag.

Brühwiler, B. (2016). Risikomanagement als Führungsaufgabe. Umsetzung bei strategischen Entscheidungen und operationellen Prozessen (4. aktualisierte Auflage). Haupt Verlag.

Brühwiler, B. & Glaser, A. (2021). Risikomanagement nach ISO 31000:2018 und ÖNORM-Reihe D 490x:2021. Der zertifizierbare Standard. Mit 10 Praxisbeispielen (3. aktualisierte und erweiterte Auflage). Austrian Standards Plus GmbH.

Bundeskanzleramt Österreich (Hrsg.). (2015). Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP). Masterplan 2014. Bundeskanzleramt Österreich.

Bundeskanzleramt. (2024a). Informationen zu Normen. https://www.oesterreich.gv.at/themen/gesetze_und_recht/oenormen-und-standards/Seite.2560001.html (Zugriff: 19.12.2024).

Bundeskanzleramt. (2024b). Allgemeines zu Normen. https://www.oesterreich.gv.at/themen/gesetze_und_recht/oenormen-und-standards/Seite.2560000.html (Zugriff: 19.12.2024).

Bundeskanzleramt. (2024c). Normen-Entwicklung. https://www.oesterreich.gv.at/themen/gesetze_und_recht/oenormen-und-standards/Seite.2560005.html (Zugriff: 20.12.2024).

Bundeskanzleramt. (2024d). Nationale/Europäische/Internationale Normen. https://www.oesterreich.gv.at/themen/gesetze_und_recht/oenormen-und-standards/Seite.2560002.html (Zugriff: 20.12.2024).

Bundesnetzagentur. (2024). ETSI-Koordinierungsstelle. https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Technik/Standardisierung_alt/Koordinierungsstelle/ETSI/etsi-node.html (Zugriff: 20.12.2024).

Carpenter, S., Walker, B., Anderies, J. M. & Abel, N. (2001). From metaphor to measurement: Resilience of what to what? Ecosystems, 4(8), 765–781.

Deutsches Institut für Normung. (2024). DIN-Norm. https://www.din.de/de/ueber-normen-und-standards/din-norm (Zugriff: 20.12.2024).

Diederichs, M. (2023). Risikomanagement und Risikocontrolling. Verlag Franz Vahlen.

Diller, C., Schnorr, M. et al. (2023). Kritische Infrastruktur aus einer doppelten Schutzperspektive: Methodische Identifizierungsprobleme und planerischer Handlungsbedarf. Standort, 47(4).

DOCUmedia. (2024). Glossar: ÖNORM. https://www.documedia.at/wissenswertes/glossar/oenorm/#definition-was-ist-eine-oenorm (Zugriff: 20.12.2024).

Drath, K. (2018). Die resiliente Organisation. Haufe Gruppe.

Dröge, U. (2024). Was ist eine High Level Structure oder Harmonized Structure? https://www.dqs-global.com/de-de/wissen/dqs-wiki/was-ist-eine-high-level-structure (Zugriff: 30.01.2025).

Duchek, S. (2020). Organizational resilience: a capability-based conceptualization. Business Research, 13, 215–246. https://doi.org/10.1007/s40685-019-0085-7

Durst, M., Hertkorn, S., Eischer, C. & Schweisser, N. (2021). Was ist ein PDCA-Zyklus? Plan-Do-Check-Act einfach erklärt. https://der-prozessmanager.de/aktuell/wissensdatenbank/pdca-zyklus (Zugriff: 31.01.2025).

Edwards, C. (2009). Resilient Nation. Demos.

Ellmer, H. (2014). Normen für jeden Bedarf – die Normenarten. Austrian Standards. https://cdn.austrian-standards.at/asset/reb_dokumente/Produkte-Leistungen/Service-Extras/Download%20Library/Fachinformationen/Fachinformation%2019.pdf (Zugriff: 17.01.2025).

Enne, L. (2025). Modellierung eines Sicherheitsaustauschformats – im Hinblick auf die Belange des Artikel 10 der RKE-Richtlinie – zur Steigerung der Resilienz kritischer Einrichtungen in Österreich [Bachelorarbeit]. Hochschule Campus Wien.

ENISA (European Union Agency for Network and Information Security). (2017). Information Sharing and Analysis Centres (ISACs). Cooperative models. https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-1-3%202%20Information%20Sharing%20and%20Analysis%20Center%20%28ISACs%29%20Cooperative%20models.pdf (Zugriff: 04.08.2025).

Fathi, K. (2019). Resilienz im Spannungsfeld zwischen Entwicklung und Nachhaltigkeit: Anforderungen an gesellschaftliche Zukunftssicherung im 21. Jahrhundert. Springer.

Fekete, A. & Hufschmidt, G. (2016). Atlas: Verwundbarkeit und Resilienz. Pilotausgabe zu Deutschland, Österreich, Schweiz und Liechtenstein.

Fekete, A. (2022). Kritische Infrastruktur und Versorgung der Bevölkerung. Springer.

Flüter-Hoffmann, C., Hammermann, A. & Stettes, O. (2018). Individuelle und organisationale Resilienz: Theoretische Konzeption und empirische Analyse auf Basis eines kombinierten Beschäftigten-Betriebsdatensatzes. Institut der deutschen Wirtschaft Köln Medien GmbH (IW Medien).

Folkers, A. (2018). Das Sicherheitsdispositiv der Resilienz. Katastrophische Risiken und die Biopolitik vitaler Systeme. Campus.

Fröhlich-Gildhoff, K. & Rönnau-Böse, M. (2023). Resilienz und Resilienzförderung über die Lebensspanne. Kohlhammer.

Gander, H.-H. & Riescher, G. (2014). Sicherheit und Offene Gesellschaft: Herausforderungen, Methoden und Praxis der gesellschaftspolitischen Sicherheitsforschung. Nomos.

Garcia, M. L. (2008). The Design and Evaluation of Physical Protection Systems (2. Auflage). Butterworth-Heinemann.

Giesert, M. et al. (2012). Das Haus der Arbeitsfähigkeit im Unternehmen bauen. VSA.

Giesert, M., Reuter, T. & Liebricht, A. (Hrsg.). (2017). Arbeitsfähigkeit 4.0: eine gute Balance im Dialog gestalten. VSA.

Gruhl M. (2014). Resilienz - die Strategie der Stehauf-Menschen. Krisen meistern mit innerer Widerstandskraft. Freiburg, Herder.

GS1 Austria. (2024). Standard oder Norm – was ist der Unterschied? https://www.gs1.at/newsroom/standard-oder-norm-was-ist-der-unterschied (Zugriff: 19.12.2024).

Gulas, H. & Katzmair, C. (2018). Resilienz – Das Vermögen zur Erneuerung. Wirtschaftspolitische Blätter, 2.

Haas, O., Huemer, B. & Preisegger, I. (2022). Resilienz in Organisationen. Erfolgskriterien erkennen und Transformationsprozesse gestalten. Schäffer-Poeschel.

Heller, J. (Hrsg.). (2019). Resilienz für die VUCA-Welt. Individuelle und organisationale Resilienz entwickeln. Springer.

Heuchemer, J. (2024). Mentale Stärke und Resilienz. Remote Verlag.

Hoffmann, G. P. (2017). Organisationale Resilienz. Kernressource moderner Organisationen. Springer.

Höfler M. (2016). Bewältigungskapazität als Bildungsauftrag. In: Wink (Hrsg.): Multidisziplinäre Perspektiven der Resilienzforschung. Wiesbaden, Springer.

Holling, C. & Gunderson, L. (2002). Panarchy: Understanding transformations in human and natural systems. Island Press.

Hollnagel, E., Woods, D. D. & Leveson, N. (Hrsg.). (2006). Resilience engineering: Concepts and precepts. Ashgate.

Hollnagel, E. & Wreathall, J.-P. (2013). Resilience Engineering in Practice. A Guidebook. Ashgate Studies.

Hunziker, A. & Steiner, C. (2022). Mit agilem Mindset zur Resilienz. In: Schellinger; Tokarski; Kissling-Näf (Hrsg.): Resilienz durch Organisationsentwicklung. Wiesbaden: Springer, Gabler.

IAS-Gruppe. (2024). CEN/CENELEC. https://www.ias-gruppe.de/glossar-uebersicht/glossar/cen-cenelec (Zugriff: 20.12.2024).

Jossé, G. (2020). Krisenmanagement und Business Continuity: Umgang mit Krisen und Großstörungen. Vahlen.

Kalisch, R. (2020). Der resiliente Mensch. Piper.

Kegler, H. (2022). Resilienz – Strategien und Perspektiven für eine widerstandsfähige und lernende Stadt (2., erweiterte Auflage). Birkhäuser.

Kersten, H. & Klett, G. (2017). Business Continuity und IT-Notfallmanagement. Grundlagen, Methoden und Konzepte. Springer.

Kingsley-Hefty, J. (2013). Physical Security Strategy and Process Playbook. Elsevier.

Kleemann, C. & Frühbeis, R. (2012). Resiliente Lieferketten in der VUCA-Welt. Springer Gabler.

Körmer, C., Habisreutinger, M. & Hauer, K. (2024). Sicherheitskultur in der Kritischen Infrastruktur (SiKu-KRITIS). Forschungsprojekt – Kurzbericht. Hochschule Campus Wien. https://doi.org/10.34895/fhcw.0019

Kuhlmann, S., Franzke, J., Peters, N. & Dumas, B. P. (2024). Krisen-Governance im europäischen Vergleich: Kommunen und Staat im Pandemiemodus. Nomos.

Langer, M., Bajwa, N. H. & König, C.J. (2021). Arbeits- und Organisationspsychologie im 21. Jahrhundert. Springer.

Langer, M.; Tomaschitz, W.; Körmer, C.; Habisreutinger, M.; Hauer, K. (2025). Ein „Systemisches Resilienz-Framework“ für die kritische Infrastruktur, SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (4), 11-22, Online: https://dx.doi.org/10.7396/2025_4_B.

Lengnick-Hall, C., Beck, T. & Lengnick-Hall, M. (2011). Developing a capacity for organizational resilience through strategic human resource management. Human Resource Management Review, 21(3).

Lorenz, D. F. (2013). The diversity of resilience: contributions from a social science perspective. Natural Hazards, 67(1), 7–24.

Lovins A. & Lovins L. (2001): Brittle Power. Energy Strategy for National Security. Energy Politics for Resilience and National Security. New Edition. Andover MA, Brick House.

Lukesch, R. (2016). Resiliente Regionen. Zur Intelligenz regionaler Handlungssysteme. In R. Wink (Hrsg.), Multidisziplinäre Perspektiven der Resilienzforschung (S. 295-332). Springer Fachmedien.

Lukesch, R. (2022). Prozesse regionaler Resilienz. In H. Pechlaner et al. (Hrsg.), Resilienz als Strategie in Region, Destination und Unternehmen. Eine raumbezogene Perspektive (S. 95–131). Springer Fachmedien.

Max, M. & Schulze, M. (2021). Hilfeleistungssysteme der Zukunft: Analysen des Deutschen Roten Kreuzes zur Aufrechterhaltung von Alltagssystemen für die Krisenbewältigung. transcript.

McManus, S., Seville, E., Brunsdon, D. & Vargo, J. (2007). Resilience Management. A Framework for Assessing and Improving the Resilience of Organisations. http://ir.canterbury.ac.nz/bitstream/10092/2810/1/12606763_Resilience%20Management%20Research%20Report%20ResOrgs%2007-01.pdf (Zugegriffen: 21.04.2025).

Meyer, F. (2022). Destination Resilienz. Erfolgreiche Unternehmen in Zeiten der Unsicherheit. Nomos.

Mueller, B. (Hrsg.). (2011). Urban regional resilience: How do cities and regions deal with change? Springer.

Münch, S. (2015). Interpretative Policy-Analyse. Springer.

Nicolai, C. (2020). Informale Organisation. In C. Nicolai (Hrsg.), Betriebliche Organisation (3. Auflage). UVK Verlag. https://eli-brary.utb.de/doi/book/10.36198/9783838587578

Niehaus, U. (2019). Organisationale Resilienz in volatilen Strukturen. Ein ganzheitliches Modell. Carl-Auer Verlag.

Nikitina, T. & Renker, C. (2022). Pandemie als nichtalltägliches Event-Risk. Auf der Suche nach Resilienz für Staaten, Unternehmen, Banken und Vermögen. Springer.

Nussbaum, M. (2015). Fähigkeiten schaffen. Neue Wege zur Verbesserung der menschlichen Lebensqualität. Karl Alber Verlag.

OECD (Hrsg.). (2019). Resilience strategies and approaches to contain systematic threats. SG/NAEC(2019)5. OECD.

Österreichischer Verband für Elektrotechnik. (2024). Normen und Produkte. https://www.ove.at/ove-standardization/normen-produkte/richtlinien/ (Zugriff: 20.12.2024).

Palzkill, A. (2017). Geschäftsmodell Resilienz. Springer.

Pariès, J., Hollnagel, E., Woods, D. D. & Wreathall, J. (2013). Resilience Engineering in Practice. A Guidebook. Ashgate.

Parlament Österreich. (o. D.). Informationsordnungsgesetz. https://www.parlament.gv.at/verstehen/nationalrat/rechtsgrundlagen/InfOG/InfOG01-10/index.html (Zugriff: 09.01.2025).

Patel, S.S; Rogers, M.B.; Amlôt, R.; Rubin, G.J. (2017). What Do We Mean by 'Community Resilience'? A Systematic Literature Review of How It Is Defined in the Literature. PLoS Curr.

Pechlaner, H. & Zacher, D. (2022). Resilienz als Strategie in Region, Destination und Unternehmen. Eine raumbezogene Perspektive. Springer.

Pedell, B., Seidenschwarz, W. & Sondermann, H. (2020). Vorausschauend Resilienz aufbauen, statt das Unternehmen durch kurzsichtiges Cost Cutting in einen Organizational Burnout zu treiben. Controlling – Zeitschrift für erfolgsorientierte Unternehmenssteuerung, 32(2), 36–39.

Perucca, A. & Schellinger, J. (2022). Resilienz durch Unternehmenskultur. In: Schellinger; Tokarski; Kissling-Näf (Hrsg.): Resilienz durch Organisationsentwicklung. Wiesbaden: Springer, Gabler.

Pfeiffer, S. (o. D.). Compliance Strategien. Tone at the top. Warum ist der Tone at the top in einem Compliance Management System so wichtig? https://compliance-strategien.de/wp-content/uploads/2020/06/toneatthetop.pdf (Zugriff: 17.01.2025).

Posselt, T., Welz, J. et al. (2022). Resilienz für die Zukunft von Wertschöpfungsketten. Perspektiven, Werkzeuge und Beispiele aus angewandter Forschung. Fraunhofer Verlag.

Protectum. (o. D.). EU Richtlinien NIS2/RKE. https://www.protectum.solutions/security/eu-richtlinien-nis2/rke/ (Zugriff: 07.02.2025).

Protectum. (2024a). Physische Sicherheit. https://www.protectum.solutions/security/physische-sicherheit/ (Zugriff: 09.12.2024).

Protectum. (2024b). Normenliste RKE-RL. Stand November 2024. [Unveröffentlichtes Dokument].

Reason, J. (2000). Human error: Models and management. BMJ, 320, 768–770.

Reckwitz, A. (2024). Verlust. Ein Grundproblem der Moderne. Suhrkamp.

Resilience Alliance. (2016). Resilience. http://www.resalliance.org/resilience (Zugegriffen: 15.04.2025).

Rifkin, J. (2022). Das Zeitalter der Resilienz: Leben neu denken auf einer wilden Erde. Campus.

RKE-Richtlinie. (2022). Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates. Amtsblatt der Europäischen Union, L 333/164. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2557

Rød, B., Lange, D., Theocharidou, M. & Pursiainen, C. (2020). From risk management to resilience management in critical infrastructure. Journal of Management in Engineering, 36(4). https://ascelibrary.org/doi/10.1061/%28ASCE%29ME.1943-5479.0000795

Romeike, F. & Hager, P. (2020). Erfolgsfaktor Risiko-Management 4.0. Methoden, Beispiele, Checklisten – Praxishandbuch für Industrie und Handel (4. Auflage). Springer. https://doi.org/10.1007/978-3-658-29446-5

Röhe, A. (2022). Das resiliente Unternehmen – Die Krisen der Zukunft erfolgreich meistern. Springer.

Scharte, B. (2021). Resilience Engineering: Oder die Kunst, in der zivilen Sicherheitsforschung mit Komplexität umzugehen. Nomos.

Schellinger, J., Tokarski, K. O. & Kissling-Näf, I. (2022). Resilienz durch Organisationsentwicklung: Forschung und Praxis. Springer Fachmedien.

Schrems, A. (2021). Resilienz – Die organisationale Widerstandsfähigkeit. Resilienz in Unternehmen und Organisationen in der Praxis. TÜV Austria.

Staab, P. (2022). Anpassung. Leitmotiv der nächsten Gesellschaft. Suhrkamp.

Stobel, M. (2002). Der kokreative Dialog in Unternehmen: Was salutogene Kommunikation bewirken kann. Schäffer-Poeschel.

Störmann E. & Pechlaner, H. (2022). Einfluss von regionalen Netzwerken und Innovationssystemen auf Resilienz in Regionen. In: Pechlaner H.; Zacher D. & Störmann E. (Hrsg.). Resilienz als Strategie in Region, Destination und Unternehmen. Eine raumbezogene Perspektive. Wiesbaden, Springer

Strambach, S. & Klement, B. (2016). Resilienz aus wirtschaftsgeographischer Perspektive: Impulse eines neuen Konzepts. In R. Wink (Hrsg.), Multidisziplinäre Perspektiven der Resilienzforschung (S. 263–294). Springer Fachmedien.

Talbot, J. & Jakeman, M. (2009). Security Risk Management Body of Knowledge. John Wiley & Sons.

Taleb, N. N. (2018). Antifragilität. Anleitung für eine Welt, die wir nicht verstehen. Penguin Random House.

Treier, M. (2016). Betriebliches Arbeitsfähigkeitsmanagement. Springer.

Unkrig, E. (2021). Resilienz im Unternehmen – den Faktor Mensch fördern: Handlungsempfehlungen und praktische Umsetzung. Springer.

Unkrig, E. (2022). Mentale Stärke im Beruf. Resilienz und Leistungsfähigkeit maximieren. Springer.

Walker, J. & Cooper, M. (2011). Genealogies of Resilience. From Systems Ecology to the Political Economy of Crisis Adaptation. Security Dialogue, 42(2), 143–160.

Weick, K. E. & Sutcliffe, K. (2016). Das Unerwartete managen. Wie Unternehmen aus Extremsituationen lernen. Schäffer-Poeschel.

Wink, R. (Hrsg.). (2016). Multidisziplinäre Perspektiven der Resilienzforschung. Springer Fachmedien.

Wirtschaftskammer Österreich. (2024). Grundlagen der Normung in Österreich. https://www.wko.at/ce-kennzeichnung-normen/grundlagen-normung-oesterreich (Zugriff: 20.12.2024).

10. Normenverzeichnis

DIN EN ISO 22300:2021-06. Sicherheit und Resilienz – Begriffe für Sicherheit und Resilienz. Deutsches Institut für Normung, Berlin.

DIN ISO 22320:2019-07. Sicherheit und Resilienz – Gefahrenabwehr – Leitfaden für die Organisation der Gefahrenabwehr bei Schadensereignissen. Deutsches Institut für Normung, Berlin.

DIN EN ISO 22361:2023-02. Sicherheit und Resilienz – Krisenmanagement – Leitlinien. Deutsches Institut für Normung, Berlin.

ISO 22316:2017. Security and resilience – Organizational resilience – Principles and attributes. ISO, Genf.

ISO 22372:2025. Security and resilience – Community resilience – Guidelines for infrastructure resilience. ISO, Genf.

ISO 22392:2020. Security and resilience – Community resilience – Guidelines for conducting peer reviews. ISO, Genf.

ISO 22396:2020. Security and resilience – Community resilience – Guidelines for information exchange between organizations. ISO, Genf.

ISO/DIS 22354: Security and resilience – Community resilience – Guidelines to develop a local resilience capability to enhance societal resilience to disruption. ISO, Genf.

ISO/IEC 27002:2022-03. Information security, cybersecurity and privacy protection – Information security controls. Genf.

IEC 31010:2019-06. Risk Management – Risk Assessment Techniques. International Electrotechnical Commission, Genf.

IEC 62351:2026. SER. Power Systems Management and Associated Information Exchange – Data and Communications Security – All Parts. International Electrotechnical Commission, Genf.

ISO 31030:2021. Travel Risk Management – Guidance for Organizations. ISO, Genf.

ISO/TS 22317:2021. Security and Resilience – Business Continuity Management Systems – Guidelines for Business Impact Analysis. ISO, Genf.

ISO/TS 22375:2018. Security and resilience – Guidelines for complexity assessment process. ISO, Genf.

OVE ÖNORM EN ISO IEC 27000:2020. Informationstechnik – Sicherheitsverfahren. Informationssicherheitsmanagementsysteme – Überblick und Terminologie, Wien

OVE-Richtlinie R2+AC:2017-04-01. Einbruch- und Überfallmeldenanlagen. Planung, Einbau, Betrieb und Instandhaltung. Österreichischer Verband für Elektrotechnik, Wien.

OVE-Richtlinie R9:2012-04-01. Alarmanlagen – CCTV-Überwachungsanlagen für Sicherheitsanwendungen. Planung, Einbau, Betrieb und Instandhaltung. Österreichischer Verband für Elektrotechnik, Wien.

OVE-Richtlinie R10:2016-03-01. Alarmanlagen – Zutrittskontrollanlagen. Planung, Einbau, Betrieb und Instandhaltung. Österreichischer Verband für Elektrotechnik, Wien.

ÖNORM EN 1627:2021-11-01.Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse – Einbruchhemmung. Anforderungen und Klassifizierung. Austrian Standards International, Wien.

ÖNORM EN ISO 22313:2020-10. Sicherheit und Resilienz – Business Continuity

Management Systems. Anleitung zur Verwendung von ISO 22301. Austrian Standards International, Wien.

ÖNORM ISO 31000-2018. Risikomanagement – Leitlinien. Austrian Standards International, Wien.

ÖNORM ISO 31000:2010. Risikomanagement – Grundsätze und Richtlinien. Austrian Standards Institute, Wien.

ÖNORM D 4900:2021-01. Risikomanagement für Organisationen und

Systeme – Begriffe und Grundlagen. Anleitung zur Umsetzung der ISO 31000. Austrian Standards International, Wien.

ÖNORM D 4902-3:2021-01. Risikomanagement für Organisationen und

Systeme – Leitfaden. Teil 3: Notfall-, Krisen- und Kontinuitätsmanagement. Austrian Standards International, Wien.

ÖNORM EN ISO 22301:2019. Sicherheit und Resilienz - Business Continuity Management

System – Anforderungen. Austrian Standards International, Wien.

ÖNORM S 2412:2017-05. Security Management System. Benennungen und Definitionen. Austrian Standards Institute, Wien.

ÖNORM S 2415-1:2020-07. Security Management System – Teil 1: Anforderungen an ein Security Management System. Austrian Standards International, Wien.

ÖNORM S 2420:2013-06-01. Corporate Security Management – Anforderungen an Konzepte zum Schutz von Objekten vor internationalen Gefahren. Austrian Standards Institute, Wien.

ÖNORM S 2450:2014-05-01. Umgang mit klassifizierten Informationen – Anforderungen an den Schutz von Verschlusssachen. Austrian Standards Institute, Wien.

ÖVE ÖNORM EN 50131-1:2010-04-01. Alarmlanlagen – Einbruch- und Überfallmeldeanlagen. Teil 1: Systemanforderungen. OVE Österreichischer Verband für Elektrotechnik / Austrian Standards Institute, Wien.

ÖVE ÖNORM EN 50131-2-3:2009-07-01. Alarmanalagen – Einbruch- und Überfallmeldeanlagen. Teil 2-3: Anforderungen an Mikrowellenmelder. OVE Österreichischer Verband für Elektrotechnik / Austrian Standards Institute, Wien.

ÖVE ÖNORM EN 50131-2-4:2008-12-01. Alarmanlagen – Einbruch und Überfallmeldeanlagen. Teil 2-4: Anforderungen an Passiv-Infrarotdualmelder und Mikrowellenmelder. OVE Österreichischer Verband für Elektrotechnik / ON Österreichisches Normungsinstitut, Wien.

ÖVE ÖNORM EN 60839-11-2:2016-03-01. Alarmanlagen. Teil 11-2: Elektronische Zutrittskontrollanlagen – Anwendungsregeln. OVE Österreichischer Verband für Elektrotechnik / Austrian Standards Institute, Wien.

11. Abbildungsverzeichnis