universität wien

MASTER THESIS | MASTER'S THESIS

Titel | Title

Effizientes Krisenmanagement in kritischen Infrastrukturen
Eine Untersuchung zur Flexibilität, Digitalisierung und Effizienz unter Berücksichtigung der HRO-Ansätze

verfasst von | submitted by

Michael Meier BSc

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien | Vienna, 2024

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 992 242
Universitätslehrgang lt. Studienblatt | Postgraduate programme as it appears on the student record sheet:	Risikoprävention und Katastrophenmanagement
Betreut von | Supervisor:	Dipl.-Ing. Dr. Stefan Schauer

I. Inhaltsverzeichnis

II. Tabellenverzeichnis

III. Abbildungsverzeichnis

1 Einleitung

Die Arbeit konzentriert sich auf die Optimierung der Stabsarbeit in Krisensituationen, insbesondere in Bezug auf kritische Infrastrukturen. Ziel ist eine ganzheitliche Untersuchung durchzuführen, die Flexibilität, mögliche Digitalisierungsmöglichkeiten und Effizienz in den Mittelpunkt stellt. Dabei stehen die Verbesserung der Krisenbewältigung und die Anwendung von Hochzuverlässigen Organisationen (high reliability organization)-Ansätzen (HRO-Theorie) im Fokus.

Inhaltlich wird sich die Arbeit mit folgenden Themen befassen:

- Flexibilität und menschliche Fehler in der Stabsarbeit: Untersuchung der Organisationsstruktur von Stäben und Maßnahmen zur Minimierung menschlicher Fehler unter Stress, Zeitdruck und Ermüdung.
- Vorbereitung der Stabsmitglieder: Entwicklung von Ansätzen zur besseren Vorbereitung von Stabsmitgliedern auf komplexe Ereignisse
- Evaluierung von Stabsarbeit in kritischen Infrastrukturen: Eine Analyse zur Effektivität von Stabsstrukturen und -prozessen in kritischen Infrastrukturen, einschließlich der Anwendung der HRO-Theorie zur Verbesserung der Krisenbewältigung.
- Digitalisierung und Effizienz in Stabsarbeit: Die Integration von digitalen Werkzeugen und Organisationsstrukturen zur Steigerung der Effizienz in der Stabsarbeit.

1.1 Ausgangslage

Seit dem Frühjahr 2020 sind die Fachbegriffe Krisenmanagement, Krisenstab und Kritische Infrastruktur in den Mittelpunkt der öffentlichen Wahrnehmung gerückt. Es folgten (sicherheitspolitischen) Ereignisse, die Themen der Resilienz und der ständigen Verfügbarkeit in den Fokus der öffentlichen Wahrnehmung gebracht haben. Die Absicherung und die Aufrechterhaltung der Kernprozesse in den kritischen Infrastrukturen sind dadurch in den Fokus der Öffentlichkeit geraten. Hinsichtlich Risiko- und Sicherheitsmanagement entstand eine Vielzahl an normativen Vorgaben. Auf europäischer Ebene wurden Ende 2022 zwei wesentliche Richtlinien verabschiedet. Das Netz- und Informationssicherheitsgesetz wurde grundlegend überarbeitet (NIS2 - EU 2022/2555) und für kritische Einrichtungen wurde eine Richtlinie erarbeitet (RKE-Richtlinie - EU 2022/2557). Hierbei werden Maßnahmen hinsichtlich Risiko- und Krisenmanagements gefordert. Das Zusammenwirken der jeweiligen Organisationen ist für die Aufrechterhaltung essenziell.

Die Corona-Pandemie, die Unterbrechung von wichtigen Lieferketten sowie die sicherheitspolitische Situation haben ein Umdenken in Europa bewirkt. Die Pandemie löste in den Organisationen einen Digitalisierungsturbo aus (vgl. Christian Schuldt, o. J., S. 15). Im Auftrag von Cisco untersuchte Arthur D. Little die Auswirkungen der Covid-19-Krise in Österreich auf Wirtschaft und Digitalisierung. Ziel war es, den Digitalen Aktionsplan durch Einschätzungen von über 50 österreichischen Top-Führungskräften sowie internationale Best Practices zu präzisieren. Die Interviews

bestätigen: Die Digitalisierung ist entscheidend für die Krisenbewältigung (vgl. Little 2020).

1.2 Ziel der Arbeit

Diese Masterthesis wurde verfasst, um zu untersuchen, ob die bewusste Einbettung der High-Reliability-Organization (HRO)-Prinzipien die Arbeit von Krisenstäben verbessert und effizienter gestalten kann. Die SKKM-Richtlinie in Österreich zielt darauf ab, dass Behörden und Betreiber kritischer Infrastrukturen ein Stabsmodell verwenden, in dem die Interoperabilität gewährleistet ist. Der erhoffte Mehrwert liegt darin, eine klare Aussage zur Flexibilität und zur möglichen Effizienzsteigerung im Krisenmanagement der kritischen Infrastrukturen (nicht Behördenseite) zu erhalten.

Es wird untersucht, wie die High-Reliability-Organization (HRO)-Theorie im Krisenmanagement angewendet werden kann und welche Maßnahmen für eine erfolgreiche Anwendung erforderlich sind. Der Fokus liegt dabei auf der Untersuchung der Stabsarbeit. Die Arbeit berücksichtigt einen breiten Kontext und analysiert sektorübergreifende Verbesserungsmaßnahmen, um ganzheitliche Ansätze zu fördern.

1.3 Wissenschaftliche Fragestellungen

In diesem Kapitel wird die wissenschaftliche Herangehensweise detailliert beschrieben, um den Prozess des Erkenntnisgewinns transparent und reproduzierbar zu machen. Es werden die Hypothesen und die dazugehörigen Forschungsfragen dargelegt. Darüber hinaus wird die gewählte Methodik der Arbeit beschrieben.

Ein wesentlicher Bestandteil dieses Abschnitts ist die Darstellung der wissenschaftlichen Vorgehensweise, die dieser Arbeit zugrunde liegt. Neben einer Literaturrecherche werden die erarbeiteten Ergebnisse mit Experteninterviews bzw. einer Onlinebefragung von Experten abgeglichen. Dieser Schritt dient dazu, die Ergebnisse zu untermauern oder gegebenenfalls zu relativieren.

1.3.1 Hypothese 1

Die Digitalisierung von Informations- und Kommunikationssystemen in kritischen Infrastrukturen wird die Effizienz bei der Informationsweitergabe und -verarbeitung im Krisenmanagement erheblich steigern.

Um die Hypothese 1 beantworten zu können, wurden Forschungsfragen definiert.

1. Wie kann die Digitalisierung in kritischen Infrastrukturen für das Krisenmanagement genutzt werden, um die Effizienz zu steigern, während gleichzeitig Sicherheitsmaßnahmen ergriffen werden, um sowohl vor technischen Ausfällen als auch Cyberbedrohungen zu schützen?
2. Welche digitalen Technologien und Lösungen sind derzeit in kritischen Infrastrukturen verfügbar und wie werden sie eingesetzt?
3. Welche Erfahrungen haben andere Organisationen bei der Implementierung digitaler Technologien im Krisenmanagement gemacht?

1.3.2 Hypothese 2

Die Anwendung von HRO-Prinzipien in kritischen Infrastrukturen wird die Effizienz des Krisenmanagements steigern und zur effektiven Umsetzung der zuvor erwähnten digitalen Lösungen beitragen.

Um die Hypothese 2 beantworten zu können, wurden Forschungsfragen definiert.

1. Wie können die Prinzipien der Hochzuverlässigen Organisationen (HRO) in kritischen Infrastrukturen gezielt und angepasst implementiert werden, um das Krisenmanagement zu optimieren.
2. Welche konkreten HRO-Prinzipien und -Praktiken sind in anderen Bereichen erfolgreich angewandt worden und könnten in kritischen Infrastrukturen übertragen werden?
3. Wie können HRO-Prinzipien in kritischen Infrastrukturen effektiv implementiert und implementiert werden, um die präventive Krisenbewältigung zu fördern und den Umgang mit unvorhersehbaren Ereignissen zu verbessern?

2 Methodik

In diesen Abschnitt wird die Methode der Erstellung der Masterthesis dargestellt. Die Forschungsfragen wurden teils durch eine umfassende Literaturrecherche und teils durch Befragungen von Expertinnen und Experten der österreichischen kritischen Infrastruktur beantwortet. Die Befragung erfolgte mittels strukturierter Interviews, die sich an Verantwortliche im Krisenmanagement und der Stabsarbeit innerhalb der jeweiligen Organisationen richteten. Ein Online-Fragebogen wurde entwickelt und an Mitglieder von Krisenstäben verteilt. Die Fragen basierten auf Erkenntnissen der Literaturrecherche.

2.1.1 Literaturrecherche

Die Suche nach Literatur erfolgt mithilfe verschiedener akademischer Datenbanken. Bei der Recherche wird das Portal u:search der Universität Wien als Hauptquelle genutzt.

Die Plattform „u:search“ ermöglicht eine elektronische Recherche in lizenzierten oder frei zugänglichen Datenbanken sowie in E-Journal-Kollektionen der Universitätsbibliothek Wien. Dafür steht eine Oberfläche zur Verfügung, mit der Suchabfragen zu Schlagworten erstellt werden. Die Schlagworte können logisch verknüpft werden und die Ergebnisse lassen sich nach bestimmten Feldern ordnen.

Außerdem erlaubt der Dienst „u:access“ einen direkten Zugriff auf von der Universitätsbibliothek Wien lizenzierte elektronische Quellen. Für die Literaturrecherche wurde zunächst das Schneeballsystem angewendet. Dieses Verfahren ermöglicht es, schnell relevante Literatur zu identifizieren.

Die Ergebnisse der Literaturrecherche zeigen, dass die das untersuchende Forschungsfeld nur getrennt voneinander betrachtet wurde. Da nur wenig Literatur zur Stabsarbeit in kritischen Infrastrukturen vorhanden ist, erfolgte eine Annäherung über Umwege. Die Theorie der Höchstzuverlässigkeitsorganisationen ist im direkten Konnex zu kritischen Infrastrukturen in nicht erforscht. Die Annäherung erfolgt über Beispiele der Literatur wo die HRO-Prinzipien ausgeprägt sind.

Die Suchbegriffe ließen sich anhand der Forschungsfragen und der Hypothesen festlegen. Danach wurden Synonyme oder ähnliche Begriffe gesucht. Es war notwendig, eine Begrenzung vorzunehmen, da die Anzahl der gefundenen Publikationen unüberschaubar war.

Viele Veröffentlichungen stellen das Thema der Stabsarbeit in Verbindung mit militärischen oder polizeilichen Einheiten. Der Ausdruck Krisenmanagement hat bis Juli 2024 mehr als 5700 Ergebnisse.

Es wird eine separate Untersuchung der Themen Krisenmanagement und HRO-Theorie durchgeführt, um gemeinsame Aspekte zu betonen. Dadurch kann festgestellt werden, auf welche Weise und in welchen Gebieten die beiden Themen kompatibel sind. Die Erkenntnisse werden anschließend miteinander verknüpft.

Tabelle 1 Beispielhafte Suchbegriffe Literaturrecherche

Thema Krisenmanagement	Thema Höchstzuverlässigkeitsorganisationen
Krisenmanagement Strategie	HRO Theorie AND kritische Infrastruktur
Krisenmanagement AND kritische Infrastrukturen	Best Practice Modelle AND HRO Theorie
Teamarbeit Krisenmanagement	HRO – Training
Ausbildung / Weiterbildung Krisenmanagement	HRO AND Stabsarbeit
Stabsarbeit kritische Infrastrukturen	Organisationsstrukturen in Hochzuverlässigkeitsorganisationen
Digitalisierung AND Stabsarbeit	Faktor Mensch AND kritische Infrastruktur
etc.	etc.

Die Ermittelte Literatur wurde anschließend gesichtet und eine Bewertung hinsichtlich Zitierfähigkeit und -würdigkeit durchgeführt. Quellen, die den wissenschaftlichen Standards entsprechen, werden als zitierwürdige Quellen bezeichnet. Die Eignung hängt von der Qualität und den spezifischen Anforderungen ab. Es kann anhand von Büchern unterschieden werden zwischen wissenschaftlichen Originalwerken und populärwissenschaftlicher oder praxisorientierter Literatur. Im Vergleich zu praxisorientierter Literatur wie Ratgeberbüchern oder Büchern ohne Quellenangaben sind wissenschaftliche Originalarbeiten wie Dissertationen und Habilitationsschriften zitierwürdig, da sie in der Regel die wissenschaftlichen Kriterien erfüllen. Im Gegensatz dazu ist die Zitierfähigkeit die Erreichbarkeit der Quellen. Es ist für eine wissenschaftliche Arbeit unverzichtbar, dass die genutzten Quellen von anderen Forschern abgerufen werden können (vgl. Ebster & Stalzer, 2017, S. 66ff).

2.1.2 Experteninterviews

Ergänzend zu der Literaturrecherche wurden Experteninterviews mit Verantwortlichen aus dem Krisenmanagement der kritischen Infrastruktur durchgeführt. Dabei wurde darauf geachtet, dass mehrerer Sektoren abgebildet werden, um ein breiteres Bild zur Stabsarbeit im Krisenfall zu erhalten. Durch die sektorübergreifende Auswahl an führenden Experten der österreichischen kritischen Infrastruktur ist breites Bild hinsichtlich der Beantwortung der Forschungsfragen möglich. Die Interviews wurden zum Teil in den Büros der Experten und elektronisch durchgeführt.

Für die Durchführung wurde ein Leitfaden (im Anhang) entwickelt, um sicherstellen zu können, dass die Vergleichbarkeit der Antworten gegeben ist und die Teilnehmer dieselben Fragen erhalten. Die Interviews waren auf eine Dauer von rund 45 Minuten ausgelegt. Der Leitfaden für die Interviews wurde auf der Grundlage des Theorieteils

der vorliegenden Arbeit erstellt. Zur Vorbereitung wurde dieser vor dem Interviewtermin an die Teilnehmer via E-Mail versendet.

Das Interview zielt darauf ab, tiefgreifendes Fachwissen, Insiderperspektiven und spezialisierte Meinungen von Personen mit fundiertem Wissen und besonderen Erfahrungen zu gewinnen. Ein Leitfadeninterview ist eine halbstrukturierte Interviewform, die auf einem theoretisch fundierten Leitfaden basiert. Dieser Ansatz erleichtert die Vergleichbarkeit der Interviews und lässt dennoch Raum für spontane Äußerungen. Der Vorteil liegt in der strukturierten, aber flexiblen Durchführungsmöglichkeit (vgl. Berger-Grabner, 2016, S. 141 ff).

Die qualitative Inhaltsanalyse nach Mayring wurde zur Analyse der Interviews verwendet. Diese kann in drei grundlegende Interpretationsformen unterteilt werden: „Zusammenfassung", „Strukturierung" und „Explikation". Diese Analysemethoden sind eigenständige Schritte, die nicht sequenziell durchgeführt werden müssen. Die vorliegende Masterarbeit nutzte die Methode der „Zusammenfassung", bei der der Inhalt der Interviews so verringert wird, dass nur noch die wesentlichen Inhalte zur Beantwortung der Forschungsfrage übrigbleiben. Durch diese Verdichtung entsteht ein überschaubarer Korpus, welcher das Originalmaterial repräsentativ darstellt (vgl. Mayring, 2022, S. 66 ff).

2.1.3 Befragung

Neben den verantwortlichen Experten aus dem Bereich der kritischen Infrastruktur wurde eine Befragung der zugehörigen Mitarbeiter in den Krisenstäben durchgeführt. Hierfür wurde ein Online-Fragebogen entwickelt, der sich an den Fragen der Experteninterviews und an der Literaturrecherche orientierte. Der Fragebogen wurden im Anschluss an die Interviews verteilt.

Die Teilnehmer*innen der Onlinebefragung repräsentieren die unterschiedlichsten Sektoren und Führungsebenen. Hierbei sind alle Ebenen vertreten. Dadurch konnte ein vollständigeres Bild gewonnen werden. Der Link zur Onlinebefragung wurden von den Interviewpartnern an die jeweilige Krisenorganisation weitergeleitet. Dadurch konnte die Fachexpertise aus der kritischen Infrastruktur hinsichtlich der Arbeit im Krisenmanagement befragt werden. Details zur Onlinebefragung werden in Kapitel 9.4 erklärt.

2.1.4 Privacy und Informationssicherheit

Informationssicherheit ist für die Aufrechterhaltung von kritischen Infrastrukturen essentiell. Die Teilnahme an den Interviews und an den Befragungen erfolgte freiwillig. Aufgrund der Sensibilität des Themas wurde ein Interview anonymisiert. Hierbei handelt es sich um einen Teilbereich der österreichischen Energieversorgung. Das Interview ist unter „Expert*in Energieversorgung" geführt.

Die Teilnahme an der Onlinebefragung erfolgte vollständig anonym und freiwillig. Es können keine Rückschlüsse auf die Teilnehmer*innen bzw. deren Organisationen gezogen werden.

Im Zuge der Interviews wurde zu Beginn das Einverständnis der Aufzeichnung sowie der Veröffentlichung abgefragt und deren Bestätigung eingeholt.

3 Kritische Infrastrukturen

3.1 Definition

Die Entstehung und Entwicklung des Konzepts der kritischen Infrastruktur kann historisch auf die strategischen Maßnahmen während des Kalten Krieges zurückgeführt werden, insbesondere auf das in den USA ausgearbeitete "continuity of government-planning". Der Schutz kritischer Infrastrukturen und Institutionen rückte in dieser Zeit in den Vordergrund, getrieben von dem Bedarf an einer robusten Infrastruktur, die einem möglichen feindlichen Angriff standhalten könnte. Im Zuge dessen entwickelten sich Sicherheitstechnologien, die heute die Basis für die Absicherung kritischer betrieblicher Systeme darstellen (vgl Folkers, 2018, S. 135).

In der deutschen "Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)" des Bundesministeriums des Innern wird der Begriff "kritische Infrastruktur" wie folgt definiert:

Kritische Infrastrukturen sind Einrichtungen und Institutionen, die für das staatliche Gemeinwesen von großer Bedeutung sind. Wenn sie nicht funktionieren oder beeinträchtigt werden, würden nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen auftreten.

Diese Definition unterstreicht die essenzielle Rolle, die kritische Infrastrukturen für die Aufrechterhaltung der gesellschaftlichen Funktionen und die Sicherheit des Staates spielen. Der Schutz dieser Infrastrukturen ist daher eine zentrale Aufgabe der staatlichen und unternehmerischen Sicherheitsvorsorge (vgl. Bundesministerium des Innern, 2009, S. 3).

„Kritische Infrastrukturen“ sind nach dem österreichischen Programm zum Schutz kritischer Infrastrukturen (APCIP) Systeme, Anlagen, Prozesse, Netzwerke oder deren Teile, die für die Funktionsweise wichtiger gesellschaftlicher Funktionen unverzichtbar sind. Die Funktionsfähigkeit staatlicher Institutionen oder die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl der Bevölkerung würden durch eine Störung oder Zerstörung dieser Infrastrukturen stark beeinträchtigt. Damit beteiligt sich Österreich am Programm der europäischen Union zum Schutz der kritischen Infrastrukturen. (vgl. BMI, 2015, S. 6).

Das europäische Programm zum Schutz kritischer Infrastrukturen wurde als Reaktion auf die zunehmende Bedrohung durch Terroranschläge entwickelt. Auslöser waren u.a. die Terroranschläge in den USA und Europa sowie die zunehmende Verwundbarkeit wichtiger Infrastrukturen, wie z.B. Energie- und Kommunikationsnetze. Das Programm zielt darauf ab, die Resilienz dieser Infrastrukturen zu stärken, indem Risiken identifiziert und Schutzmaßnahmen verbessert werden. Es betont die Zusammenarbeit zwischen öffentlichen und privaten Akteuren und fördert den Informationsaustausch zur besseren Prävention und Reaktion auf potenzielle Angriffe (vgl. Europäische Kommission, 2004).

Die kritische Infrastruktur ist ein zentrales Element der Daseinsvorsorge, das im historischen Kontext, insbesondere während des Zweiten Weltkriegs, an Bedeutung gewonnen hat. Die Wurzeln des Konzepts der Daseinsvorsorge, das eng mit der Idee

kritischer Infrastrukturen verknüpft ist, lassen sich auf die Arbeiten des deutschen Juristen Ernst Forsthoff zurückführen. Forsthoff erkannte die essenzielle Rolle der Infrastruktur sowohl für militärische Zwecke als auch für das tägliche Leben der Zivilbevölkerung. Die strategische Wichtigkeit von Infrastrukturen wurde insbesondere durch die Praxis des "strategic bombing" im Zweiten Weltkrieg evident, bei der gezielte Luftangriffe auf feindliche Infrastrukturen zur Schwächung der gegnerischen Kriegsführung und zur Unterbindung der lebensnotwendigen Versorgung eingesetzt wurden. Diese historische Entwicklung zeigt die Doppelrolle der Infrastruktur als Unterstützungselement für die industrielle Kriegsführung sowie als unerlässlicher Bestandteil für die Grundversorgung der Bevölkerung. Die daraus resultierende Sichtweise, dass Schutz und Erhaltung der Infrastruktur staatliche Aufgaben sind, hat Forsthoff explizit in seinen Schriften verankert und wurde im Laufe der Zeit zu einem festen Bestandteil staatlicher Sicherheits- und Vorsorgepolitik (vgl. Folkers, 2018, S. 126 ff).

Im Kontext des „strategic bombing" während der Weltkriege entstand die Doktrin, welche das Ziel verfolgte, die Infrastruktur des Feindes gezielt zu attackieren, um dessen kriegswichtige Kapazitäten zu schwächen. Dies manifestierte sich später im Kalten Krieg in der Sorge um die Verwundbarkeit der eigenen Infrastruktur. Hier wurde besonders das sogenannte "vulnerability mapping" angewandt, um durch räumliche Analyse die Anfälligkeiten zu identifizieren. Die Kritikalität von Infrastruktur wurde so nicht nur physisch, sondern auch in räumlicher Hinsicht erfasst, wobei Elemente wie "choke points" und Interdependenzen zwischen Versorgungssystemen betrachtet wurden (vgl. Folkers, 2018, S. 135).

Zum Zeitpunkt der Erstellung der Arbeit sind auf EU-Ebene zwei Richtlinien zum Schutz der kritischen Infrastrukturen veröffentlicht, jedoch noch nicht in nationales Recht umgesetzt. Die NIS-2 (vgl. NIS2-Richtlinie, 2023)wird die Nachfolge Richtlinie zu NIS-1 und die RKE-Richtlinie (vgl. RKE-RL, 2023) wird Teile des europäischen Programms zum Schutz der kritischen Infrastrukturen ablösen. Beide definieren kritische Infrastrukturen als Einrichtungen die Aufrechterhaltung wichtiger gesellschaftlicher und wirtschaftlicher Funktionen entscheidend.

Die RKE-Richtlinie wurde verabschiedet, um die Resilienz kritischer Einrichtungen in der Europäischen Union zu verbessern und die Richtlinie 2008/114/EG zu ersetzen (vgl. RKE-RL, 2023). Diese Richtlinie verfolgt wesentliche Ziele, darunter die Festlegung harmonisierter Mindestanforderungen zur Stärkung der Widerstandsfähigkeit kritischer Infrastrukturen, die Gewährleistung der Sicherheit und Kontinuität wesentlicher Dienste sowie die Förderung der grenzüberschreitenden Zusammenarbeit und Unterstützung. Angesichts wachsender Bedrohungen wie Naturkatastrophen und terroristischen Angriffen sollen die Maßnahmen den Schutz und die Anpassungsfähigkeit dieser Einrichtungen erheblich erhöhen.

Die NIS-2-Richtlinie, zielt darauf ab, ein hohes Maß an Cybersicherheit in der Europäischen Union zu gewährleisten. Sie ersetzt die frühere Richtlinie (EU) 2016/1148 und erweitert deren Geltungsbereich. Die neuen Maßnahmen sollen die Cybersicherheitskapazitäten stärken, Bedrohungen für Netz- und Informationssysteme eindämmen und die Kontinuität wesentlicher Dienste

sicherstellen. Wesentliche Ziele sind die Harmonisierung der Sicherheitsanforderungen, die Förderung der Zusammenarbeit zwischen Mitgliedstaaten und die Aktualisierung der betroffenen Sektoren und Dienste. Dadurch soll die Fragmentierung des Binnenmarktes verringert und die Cyberresilienz erhöht werden (vgl. NIS2-Richtlinie, 2023).

Die Definition und Kategorisierung kritischer Einrichtungen erfolgt gemäß den Richtlinien RKE und NIS2 durch die Mitgliedstaaten der EU. Die NIS2-Richtlinie fokussiert auf die Cybersicherheit und verlangt von Betreibern wesentlicher Dienste und digitalen Dienstleistern, dass sie sich regelmäßig selbst einschätzen und ihre Sicherheitsmaßnahmen kontinuierlich verbessern. Diese Selbsteinschätzung ist ein zentraler Bestandteil der Richtlinie, um sicherzustellen, dass Sicherheitsrisiken proaktiv gemanagt werden (vgl. NIS2-Richtlinie, 2023)

Die Resilienz-Richtlinie hingegen konzentriert sich auf den umfassenden Schutz kritischer Infrastrukturen sowohl vor physischen als auch digitalen Bedrohungen. Hier liegt die Hauptverantwortung bei den Mitgliedstaaten, die nationale Strategien zur Identifizierung und Sicherung dieser Einrichtungen entwickeln und umsetzen müssen. Diese Richtlinie legt weniger Wert auf die Selbsteinschätzung der Betreiber und mehr auf die staatlich getriebene Evaluierung und den Schutz (vgl. RKE-RL, 2023).

Im Vergleich zeigt sich, dass die NIS2-Richtlinie die Betreiber stärker verpflichtet, da sie eine aktive Rolle bei der Selbsteinschätzung und kontinuierlichen Überwachung ihrer Sicherheitsmaßnahmen übernehmen müssen. Diese Selbstverantwortung ist ein integraler Bestandteil der Cybersicherheitsstrategie, die in der NIS2-Richtlinie festgelegt ist. Die Resilienz-Richtlinie ergänzt dies durch einen umfassenderen, staatlich überwachten Schutzansatz, der jedoch weniger auf die direkte Einbindung der Betreiber setzt (vgl. RKE-RL, 2023; NIS2-Richtlinie, 2023)

3.2 Komplexität, Vernetzung und Kritikalität

Das Business Continuity Management (BCM) repräsentiert einen modernen Ansatz, der sich von den historischen staatlichen Sicherheitskonzepten löst und eine zeitgemäße Perspektive auf die Kritikalität von Infrastrukturen bietet. Es adressiert nicht nur die physischen Komponenten, sondern auch die Aufrechterhaltung betrieblicher Funktionen und Abläufe. BCM betont, dass der Schutz kritischer Infrastrukturen nicht mehr nur auf einzelne Institutionen oder staatliche Programme beschränkt ist, sondern sich auf ein Netzwerk von Akteuren erstreckt, die gemeinsam für die Resilienz und das Krisenmanagement zuständig sind. Somit wird die Betrachtung der kritischen Infrastruktur von einer rein institutionellen Perspektive zu einem umfassenderen, netzwerkbasierten Ansatz erweitert, der die zeitliche Dimension von Kritikalität und betrieblicher Kontinuität in den Vordergrund rückt (vgl. Folkers, 2018, S. 134).

In der wissenschaftlichen und anwendungsorientierten Diskussion um die Sicherheit kritischer Infrastrukturen nimmt der Begriff der Kritikalität eine zentrale Stellung ein. Er beschreibt ein skalierbares Maß zur Bewertung und Priorisierung von Geschäftsprozessen und Infrastrukturen hinsichtlich ihrer Bedeutung für die Wertschöpfungskette und die Versorgungssicherheit. Kritikalität wird dabei in

Kategorien eingeordnet, die sich an den Anforderungen für den Wiederaufbau und die Ausfalldauer im Falle eines Schadensereignisses orientieren. Dies ermöglicht es, in Krisenfällen die Verteilung der Ressourcen effektiv zu steuern und die am meisten kritischen Prozesse bevorzugt zu behandeln (vgl Münzberg & Ottenburger, 2018, S. 182 ff).

Die Definition von Kritikalität ist international variabel und richtet sich nach den jeweiligen nationalen Schutzprogrammen für kritische Infrastrukturen. Ein Beispiel dafür ist die Kritikalität in der Schweiz, die die relative Bedeutung eines Versorgungssektors in Bezug auf die Bevölkerung, die Wirtschaft und die bestehenden Abhängigkeiten misst. Im Gegensatz dazu wird Kritikalität in Deutschland als ein relatives Maß dafür definiert, wie wichtig eine Infrastruktur im Hinblick auf die Auswirkungen einer Störung oder eines Funktionsausfalls auf die Versorgungssicherheit der Gesellschaft mit erforderlichen Gütern und Dienstleistungen ist. (vgl. Münzberg & Ottenburger, 2018, S. 182 ff).

Die wissenschaftliche Literatur nutzt den Begriff der Kritikalität vorrangig als Attribut zur Identifizierung und Auswahl von kritischen Infrastrukturen. Dies unterstreicht die Notwendigkeit, Kritikalität sowohl aus einer mikro- als auch aus einer makroökonomischen Perspektive zu betrachten und die Priorisierung von Ressourcen und Maßnahmen nach dem Grad der Kritikalität zu gestalten. Die Kritikalitätsbewertung dient somit als entscheidendes Werkzeug für das Risikomanagement und die Krisenbewältigung in modernen Gesellschaften (vgl. Münzberg & Ottenburger, 2018, S. 182 ff).

Die Komplexität und gesellschaftliche Bedeutung von kritischen Infrastrukturen erforderten eine branchenübergreifende Zusammenarbeit. Die dynamische Gefahrenlage, deren kritische Infrastrukturen ausgesetzt sind, zwingt die Betreiber zu umfassende Zusammenarbeit mit anderen (externen) Stellen. Für die Aufrechterhaltung der (öffentlichen) Versorgung, ist ein effektiver Umgang mit krisenauslösenden Ereignissen notwendig. Das Ziel von Infrastrukturbetreibern ist, im Schadensfall, eine schnelle Wiederherstellung der Funktionsfähigkeit (vgl. Lauwe, 2012, S. 24).

3.3 Einteilung einer Infrastruktur als kritisch

Kritische Infrastrukturen sind für die Aufrechterhaltung des öffentlichen Lebens von wesentlicher Bedeutung. Die Verfügbarkeit der KRITIS stellt wesentliche gesellschaftliche Funktionen sicher. Ein Ausfall kann Versorgungsengpässe bzw. Gefährdungen der öffentlichen Sicherheit nach sich ziehen (vgl. Karsten & Voßschmidt, 2019, S. 21).

Schädigungen bzw. Ausfälle von kritischen Infrastrukturen beeinflussen moderne Gesellschaften negativ. Dadurch entsteht ein öffentliches Interesse das KRITIS ständig verfügbar sind (vgl. Lauwe, 2012, S. 9)

Die hohe Bedeutung für die Gesellschaft erfordert, dass sektoren- und branchenübergreifende Schutzkonzepte erstellt werden. Diese müssen auf die jeweiligen Besonderheiten und vor allem auf die gegenseitigen Beeinflussungen und

Kaskadeneffekte abgestimmt sein (vgl. Lauwe, 2012, S. 9 ff). Der Begriff "kritische Infrastruktur" in der NIS-2-Richtlinie nicht direkt definiert. Dennoch wird durch die Definition und Regulierung von "kritischen Einrichtungen" und deren spezifische Sicherheitsanforderungen ein klares Bild vermittelt. (vgl. NIS2-Richtlinie, 2023).

Objekte, Anlagen, Ausrüstung, Netze oder Systeme oder Teile davon, die für die Erbringung eines wesentlichen Dienstes notwendig sind, werden als kritische Infrastrukturen im Sinne der RKE-Richtlinie bezeichnet. Diese Infrastrukturen sind unverzichtbar für die Erbringung von Dienstleistungen, die für die Erhaltung wesentlicher sozialer Funktionen, wirtschaftlicher Aktivitäten, öffentlicher Gesundheit und Sicherheit sowie für den Schutz der Umwelt von entscheidender Bedeutung sind. (vgl. RKE-RL, 2023).

Eine Infrastruktureinrichtung wird gemäß der Richtlinie des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen als kritisch eingestuft, wenn sie essenzielle Dienstleistungen erbringt, deren Beeinträchtigung erhebliche nachteilige Auswirkungen auf die öffentliche Sicherheit, Gesundheit, Wirtschaft oder das allgemeine Wohlbefinden haben würde, und dabei starke Interdependenzen aufweist. Die Dienstleistungen ist für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Aktivitäten unerlässlich und eine Störungen oder Zerstörungen der Einrichtung würde schwerwiegende Auswirkungen auf andere EU-Mitgliedsstaaten haben (vgl. NIS2-Richtlinie, 2023).

Im Rahmen der Arbeit sind kritische Infrastrukturen demnach Einrichtungen, deren Schutz und Widerstandsfähigkeit aufgrund ihrer essentiellen Rolle für die Gesellschaft und Wirtschaft von höchster Priorität ist. Grundlage ist hierfür das österreichische Programm zum Schutz der kritischen Infrastrukturen.

4 High Reliability Organizations

Laut Fahlbruch, Schöbel und Marold (2012) liegt der Schlüssel für Hochzuverlässigkeitsorganisationen in der Schaffung einer Organisationskultur, die konsequent auf höchste Sicherheit und Fehlertoleranz ausgerichtet ist, wobei die proaktive Identifikation und das Management von Risiken im Mittelpunkt stehen.

High Reliability Organizations (HROs) sind Organisationstypen, die in Hochrisikoumwelten operieren, in denen Fehler dramatische Konsequenzen haben könnten. Sie werden durch ihre Fähigkeit definiert, bei hoher Komplexität und inhärenten Risiken dennoch äußerst zuverlässig zu funktionieren. (vgl. Weick & Sutcliffe, 2007, S. 7).

4.1 Grundlegendes zur Theorie

Die High Reliability Theory beleuchtet die Mechanismen und Organisationsprinzipien, durch welche Organisationen in Hochrisiko-Industrien eine hohe Betriebssicherheit erreichen. Die Theorie geht davon aus, dass solche Organisationen, auch bekannt als High Reliability Organizations (HROs), über Eigenschaften verfügen, die es ihnen ermöglichen, trotz komplexer und gefahrenanfälliger Prozesse eine Kultur der Zuverlässigkeit zu kultivieren. Hierbei spielen ein kontinuierliches Engagement für das Lernen aus Beinahe-Fehlern, eine Präferenz für komplexe statt vereinfachender Interpretationen, Sensibilität für betriebliche Abläufe und das Zulassen von Flexibilität in der Entscheidungsfindung zentrale Rollen. Dies erfordert eine Organisationsstruktur, die Expertenwissen über hierarchische Grenzen hinweg respektiert und eine gemeinschaftliche Ausrichtung auf das Ziel der Fehlervorbeugung und Reaktionsbereitschaft auf unvorhergesehene Ereignisse fördert (vgl. Fahlbruch et al., 2012, S. 24).

High Reliability Organizations (HROs) sind Organisationen, die unter extremen Bedingungen operieren und ein Höchstmaß an Zuverlässigkeit erreichen. Sie werden durch fünf Prinzipien charakterisiert (vgl. Weick & Sutcliffe, 2007, S. 7):

1. **Sensibilität für Betriebsabläufe:** HROs konzentrieren ihre Aufmerksamkeit sowohl auf ihre Fehler als auch auf ihre Erfolge. Dies ermöglicht es ihnen, aus beiden zu lernen und kontinuierliche Verbesserungen vorzunehmen.
2. **Abneigung gegen vereinfachende Interpretationen:** Sie hinterfragen ständig die aktuelle Situation und sind wachsam gegenüber zu einfachen Erklärungen für komplexe Probleme.
3. **Streben nach Flexibilität:** HROs besitzen ein feines Gespür für betriebliche Abläufe und sind bereit, ihre Strukturen und Prozesse anzupassen, wenn sich Bedingungen ändern.
4. **Respekt vor fachlichem Wissen und Können:** Sie lassen Entscheidungsbefugnisse zu den Experten "wandern". Das bedeutet, dass Entscheidungen dort getroffen werden, wo das meiste Wissen über die aktuelle Situation vorhanden ist.

5. **Streben Resilienz:** HROs sind darauf ausgerichtet, Fehler zu erkennen, zu korrigieren und daraus zu lernen, bevor diese zu einer Krise eskalieren können.

Diese fünf Prinzipien erzeugen einen kollektiven Zustand der Achtsamkeit innerhalb der Organisation. Durch diese kontinuierliche Achtsamkeit sind HROs in der Lage, das Unerwartete besser zu bewältigen als andere Organisationen. Sie können schneller auf unvorhergesehene Ereignisse reagieren und sich an neue oder veränderte Bedingungen anpassen. Dadurch sind HROs Vorbilder für alle Organisationen, die zuverlässiger arbeiten möchten (vgl. Weick & Sutcliffe, 2007, S. 7).

4.2 Überblick über Hochzuverlässigkeitsorganisationen

Als Beispiele für solche Organisationen gelten unter anderem Atomkraftwerke, Fluggesellschaften oder Feuerwehrmannschaften, die unter anspruchsvollsten Bedingungen arbeiten und dennoch eine geringe Fehler- und Unfallrate aufweisen (vgl. Weick & Sutcliffe, 2007, S. 7).

In der wissenschaftlichen Auseinandersetzung mit HRO wird deutlich, dass solche Organisationen trotz ihrer Heterogenität – zu denen unter anderem Fluggesellschaften, Flugsicherungssysteme, Atomkraftwerke, Notfallmedizin sowie Brandbekämpfungseinheiten zählen – eine fundamentale Anforderung teilen: die Notwendigkeit, zuverlässige Leistungen in Umfeldern zu erbringen, die von hoher Komplexität und potenziellen katastrophalen Fehlern geprägt sind. Untersuchungen zeigen, dass diese Organisationen nicht nur durch ihre strukturellen Eigenschaften beeindruckend sind, sondern auch durch eine Denk- und Handlungsweise, die sie von konventionellen Organisationen unterscheidet. Ein Schlüsselelement ihrer Arbeitsweise ist die konsequente Fokussierung auf Zuverlässigkeit und die Konzentration auf Fehler. HROs illustrieren die Wichtigkeit von Zuverlässigkeit als eine Kernkomponente organisationaler Exzellenz, insbesondere in Bereichen, wo das Potenzial für katastrophale Fehler besteht und Spitzenleistungen von essenzieller Bedeutung sind (vgl. Weick & Sutcliffe, 2007, S. 9).

4.3 Prinzipien

HRO tendieren dazu, auf unerwartete Ereignisse nicht hilflos zu reagieren; sie bewahren eine robuste mentale Haltung, die von der kontinuierlichen Interpretation von Zusammenhängen und der ständigen Aktualisierung von Wissen geprägt ist. HROs unterscheiden sich von anderen Organisationen dadurch, dass sie in der Lage sind, die wichtigsten Probleme sowie potenzielle Gegenmaßnahmen zu identifizieren. Sie reagieren auf schwache Signale stark, indem sie diese frühzeitig erkennen und ihnen entschieden entgegentreten. Der Schlüssel zu ihrem Erfolg liegt in der konstanten Wachsamkeit und Anpassungsfähigkeit, die sie in die Lage versetzt, das Unerwartete zu antizipieren und potenzielle Katastrophen abzuwenden (vgl. Weick & Sutcliffe, 2007, S. 15).

4.3.1 Prinzip 1 – Konzentration auf Fehler

In HRO liegt ein besonderes Augenmerk auf der Konzentration auf Fehler, was maßgeblich zu ihrer Fähigkeit beiträgt, Katastrophen zu vermeiden. Jeder Fehler wird als ein Symptom dafür betrachtet, dass im System etwas nicht in Ordnung ist und potenziell ernsthafte Konsequenzen haben könnte, wenn mehrere kleine Fehler in einem unglücklichen Moment zusammenkommen (vgl. Weick & Sutcliffe, 2007, S. 23).

HROs fördern aktiv eine Kultur, in der Mitarbeiter dazu ermutigt werden, Fehler zu melden. Sie analysieren Fehler gründlich und lernen daraus, um Wiederholungen zu vermeiden. Dabei achten sie besonders auf die potenziellen Gefahren von Selbstzufriedenheit, Nachlässigkeit und dem Abgleiten in Routine, die als Bedrohung für die Sicherheitsstandards und den langfristigen Erfolg gesehen werden (vgl. Weick & Sutcliffe, 2007, S. 15).

4.3.2 Prinzip 2 – Abneigung gegen Vereinfachungen

Weick und Sutcliffe betonen, dass Erwartungen die Welt vereinfachen und Beobachter von Hinweisen ablenken, die diesen Erwartungen widersprechen und auf unerwartete Probleme hinweisen. Diese Vereinfachungen können kritische Warnzeichen übersehen lassen. Zur Vermeidung dieses Phänomens empfiehlt es sich, ständig auf den Kontext sowie auf Kategorien und Erwartungen zu achten. Dies führt zu einer differenzierteren Anschauungsbild und einem umfassenderen Verständnis potenzieller Folgen (vgl. Weick & Sutcliffe, 2007, S. 73).

HROs konzentrieren sich darauf, Vereinfachungen zu verkomplizieren und sich intensiv mit ihren Fehlern auseinanderzusetzen, anstatt sich ausschließlich auf Erfolge zu fokussieren. Dies erfordert, die eigenen Kategorien ständig zu hinterfragen und nicht in vereinfachte Schubladen wie „Herstellen oder Kaufen“, „Freund oder Feind“ oder „Gewinn oder Verlust“ zu stecken (vgl. Weick & Sutcliffe, 2007, S. 73).

Die ständige Reflexion und Fehleranalyse tragen dazu bei, Risiken frühzeitig zu erkennen und Vorsichtsmaßnahmen zu ergreifen (vgl. Weick & Sutcliffe, 2007, S. 73).

Vereinfachende Sichtweisen führen zu blinden Flecken in der Wahrnehmung. HROs vermeiden dies durch erhebliche Anstrengungen, ihre Vereinfachungen sorgfältig zu überprüfen, was einen achtsamen Umgang mit dem Unerwarteten fördert. Eine zentrale Devise lautet: "Man benötigt Vielfalt, um Vielfalt zu beherrschen." In einem

komplexen Umfeld sind vielfältige Sensoren notwendig, um die Gegebenheiten zu erkennen. Einfache Erwartungen führen zu einfachen Wahrnehmungen, die nur einen Bruchteil des tatsächlich Vorhandenen erfassen (vgl. Weick & Sutcliffe, 2007, S. 76).

Beispielsweise kann ein Kommandant einer Flugzeugstaffel, der alle Flugzeugtypen geflogen hat, eher erkennen, wenn eine Maschine schlecht funktioniert, als jemand mit weniger Erfahrung. Ähnlich verfügt ein Finanzspezialist, der mit verschiedenen Krediten gearbeitet hat, über ein komplexeres Sensorium als ein Kreditberater, der nur gute Kreditgeschäfte kennt. Ein Topmanagement-Team mit vielfältigen Aufgabenbereichen besitzt ein feineres Wahrnehmungsinstrumentarium als ein homogenes Team aus Betriebswirten, Juristen oder Ingenieuren (vgl. Weick & Sutcliffe, 2007, S. 73).

4.3.3 Prinzip 3 – Sensibilität für betriebliche Abläufe

Ein wesentliches Merkmal von hochzuverlässigen Organisationen (HROs) ist ihre Sensibilität für betriebliche Abläufe, die sich durch eine konsequente Beschäftigung mit dem Unerwarteten auszeichnet. Überraschende Ereignisse entstehen oft durch sogenannte "latente Fehler", also Lücken in den Abwehrmechanismen und Sicherheitsvorkehrungen eines Systems. Diese Lücken, die in Bereichen wie Supervision, Fehlermeldungen, sicherheitstechnischen Verfahren, Sicherheitstraining, Sicherheitsinstruktionen und Gefahrenermittlung auftreten, werden oft erst nach einem Unfall erkannt. Doch die normalen betrieblichen Abläufe können solche Mängel aufdecken und so Hinweise auf potenzielle Probleme geben, bevor es zu Unfällen kommt (vgl. Weick & Sutcliffe, 2007, S. 25).

HROs zeichnen sich durch ein entwickeltes Gespür für Anomalien aus und führen kontinuierlich Anpassungen durch, um Fehler frühzeitig zu erkennen und zu beheben. Dabei wird die praktische Arbeit und die situationsbezogene Handlungsweise betont. Mitarbeiter in HROs haben keine Angst, Anomalien anzusprechen, wodurch ein System geschaffen wird, das flexibel und anpassungsfähig bleibt. Ein enger Zusammenhang zwischen der Sensibilität für betriebliche Abläufe und der Qualität der zwischenmenschlichen Beziehungen trägt wesentlich zur erfolgreichen Fehlerprävention bei (vgl. Weick & Sutcliffe, 2007, S. 26).

Organisationen mit hoher Zuverlässigkeit zeichnen sich durch besondere Ansätze in Hierarchie, Führung und dem Verständnis betrieblicher Abläufe aus. Der Fokus liegt auf der ganzheitlichen Wahrnehmung der Betriebssituation. Diese umfassende Aufmerksamkeit ermöglicht es, unerwartete Ereignisse frühzeitig zu erkennen und zu verhindern, dass das System an seine Belastungsgrenze gerät (vgl. Weick & Sutcliffe, 2007, S. 78).

Starre Hierarchien und schwerfällige Bürokratien werden vermieden, indem alle Beschäftigten detailliert über den aktuellen Stand informiert und für alle erforderlichen Aktivitäten bereitgehalten werden. Dadurch behalten mehr Menschen einen Gesamtüberblick (vgl. Weick & Sutcliffe, 2007, S. 78).

4.3.4 Prinzip 4 – Streben nach Flexibilität

HROs konzentrieren sie sich auf vorausschauendes Handeln, Lernen aus Fehlern und größtmögliche Flexibilität. Diese Flexibilität beinhaltet die Fähigkeit, Fehler frühzeitig zu identifizieren und das System mithilfe improvisierter Verfahren am Laufen zu halten. HROs entwickeln Fähigkeiten, um unvermeidliche Irrtümer zu entdecken, zu begrenzen und sich schnell davon zu erholen (vgl. Weick & Sutcliffe, 2007, S. 27).

HROs lassen sich durch Fehler nicht lähmen, sondern lernen daraus und passen sich an. Sie setzen auf Mitarbeiter mit umfangreicher Erfahrung, Kombinationsfähigkeit und guter Ausbildung, die mental Ernstfälle simulieren und ihre "Feuerwehr-Fähigkeiten" regelmäßig üben. Flexibilität erfordert ein tiefes Verständnis der Technik, des Systems, der handelnden Personen und der eigenen Ressourcen. (vgl. Weick & Sutcliffe, 2007, S. 27).

Die Fähigkeit, das Unerwartete zu managen, erfordert sowohl Antizipation als auch Reaktionsfähigkeit. Organisationen müssen nicht nur vorhersagen, was geschehen könnte, sondern auch darauf vorbereitet sein, unvorhergesehene Ereignisse zu bewältigen. Diese doppelte Perspektive kombiniert strategische Planung mit operativer Flexibilität. HROs fördern diese Sensibilität durch ständige Überwachung, Anpassung und offene Kommunikation, was zur allgemeinen Betriebssicherheit und Effizienz beiträgt (vgl. Weick & Sutcliffe, 2007, S. 82).

Die Flexibilität ist ein zentrales Merkmal von HROs, das entscheidend zur Krisenbewältigung und zum Umgang mit unerwarteten Ereignissen beiträgt. Gene Rochlin fand heraus, dass Krisen auf Flugzeugträgern oft durch informelle Netzwerke eingedämmt werden. Wenn Ereignisse den Normalbetrieb überschreiten, bilden erfahrene Mitarbeiter ad hoc Netzwerke, um eigenverantwortlich Problemlösungen zu finden. Diese Netzwerke haben keinen formalen Status und lösen sich nach der Krise wieder auf, ermöglichen aber ein schnelles Bündeln von Fachkenntnissen (vgl. Weick & Sutcliffe, 2007, S. 86).

Dadurch erweitert sich das Wissens- und Handlungsspektrum der Organisation. Durch flexible Kriseninterventionen können Systeme mit unvermeidlichen Unsicherheiten und Wissenslücken umgehen. Generalisierte, nicht gebundene Ressourcen tragen ebenfalls entscheidend zur Flexibilität bei (vgl. Weick & Sutcliffe, 2007, S. 86)

Flexibilität erfordert, dass alle Mitarbeiter lernen, betriebliche Abläufe, mögliche Störungen und Gegenmaßnahmen zu verstehen und im Voraus zu planen. Schulungen sind darauf ausgerichtet, Szenarien zu durchspielen und die Fähigkeit zu entwickeln, erfolgreich auf unvorhersehbare Ereignisse zu reagieren (vgl. Weick & Sutcliffe, 2007, S. 85).

4.3.5 Prinzip 5 – Respekt vor fachlichem Wissen und Können

HROs haben mehrere betriebliche Verfahrensweisen eingeführt, die auf Respekt vor Fachkenntnis beruhen. HROs weisen das Problem nicht einfach einem Experten zu und gehen dann zur Tagesordnung über. In HROs gibt hierarchische Strukturen wie in

vielen großen Organisationen, jedoch begegnen die Mitarbeiter mit Respekt gegenüber Wissen und Erfahrung (vgl. Weick & Sutcliffe, 2007, S. 88).

HROs reagieren flexibel auf Veränderungen und legen Wert auf die Frage, wessen Urteil zählt, um betriebliche Abläufe anzupassen und Probleme frühzeitig zu erkennen. In einer hierarchischen Struktur werden wichtige Entscheidungen oft von Führungskräften getroffen, die sich durch Auswahlprozesse qualifiziert haben. In HROs jedoch bestimmt nicht nur der Status, sondern auch das Know-how, wer Entscheidungen trifft (vgl. Weick & Sutcliffe, 2007, S. 89).

Effiziente HROs haben eine Entscheidungsstruktur, bei der wichtige Entscheidungsträger aktiv an vielen Auswahlprozessen teilnehmen können. Diese Kombination aus Hierarchie und Spezialisierung bedeutet, dass die Zuständigkeit für Entscheidungen dynamisch bleibt und sich an das jeweilige Fachwissen anpasst (vgl. Weick & Sutcliffe, 2007, S. 89)

5 Krisenmanagement

In diesem Kapitel werden die, für die Arbeit notwendigen, theoretischen Grundlagen zum Krisenmanagement und die dazugehörigen Definitionen dargestellt. Im Zuge der Recherche wurden viele, teils unterschiedliche, Definitionen des Krisenmanagements betrachtet. Für die Arbeit wird die normative Grundlage als state of the art herangezogen.

5.1 Definitionen

5.1.1 Krise

Eine Krise, gemäß Duden, bezeichnet eine schwierige Lage, Situation oder Zeit, die den Höhe- und Wendepunkt einer gefährlichen Entwicklung darstellt. Sie umfasst Schwierigkeiten oder kritische Situationen, die eine Zeit der Gefährdung oder des Gefährdet seins kennzeichnen. Krisen können in verschiedenen Kontexten auftreten, beispielsweise als finanzielle, seelische oder wirtschaftliche Krisen, und erfordern oft entscheidende Maßnahmen zur Überwindung oder Bewältigung. Der Begriff wird auch in der Medizin verwendet, um einen kritischen Wendepunkt bei einem Krankheitsverlauf zu beschreiben. Die Herkunft des Wortes "Krise" lässt sich auf das griechische "krísis" zurückführen, was Entscheidung oder entscheidende Wendung bedeutet, und wurde durch das französische "crise" in der allgemeinen Bedeutung beeinflusst (vgl. Dudenredaktion, 2024).

Gemäß der neuesten Krisenmanagement-Norm EN ISO 22361:2022 wird eine Krise als ein ungewöhnliches oder außergewöhnliches Ereignis beschrieben, das eine potenzielle Bedrohung für Organisationen oder Gemeinschaften darstellt. Eine prompte Reaktion auf ein solches Ereignis ist essentiell, um die Handlungskompetenz und Funktionsfähigkeit der betroffenen Organisation oder Gemeinschaft sicherzustellen bzw. zu erhalten (vgl. ISO 22361, 2022, S. 9).

Eine themenverwandte Norm, die ÖNORM S 2412 aus dem Jahr 2017, charakterisiert eine Krise als eine Situation, die aufgrund der Unzulänglichkeit regulärer Strukturen und Prozesse innerhalb einer Organisation außergewöhnliche Maßnahmen verlangt, wodurch die Notwendigkeit einer Stabsarbeit entsteht (vgl. ÖNORM S 2412, 2017, S. 6).

Im Sinne einer Norm zu Begriffsbestimmungen aus dem Bereich Sicherheit und Resilienz ist eine Krise ein instabiler Zustand, in welchem die Gefahr einer plötzlichen oder markanten Veränderung besteht. Diese Situation erfordert sofortige Aufmerksamkeit und das Ergreifen von Maßnahmen, um Menschenleben, Werte, Eigentum und die Umwelt zu bewahren und zu schützen (vgl. ISO 22300, 2021, S. 14).

Krisen zeichnen sich durch drei Hauptmerkmale aus: ihre unerwartete Natur, ihren bedeutenden Einfluss oder Schaden und ihre zeitliche Begrenzung. Die zeitliche Begrenzung von Krisen impliziert, dass sie vorübergehender Natur sind und durch angemessene Vorbereitung und Management bewältigt werden können (vgl. Timtschenko, 2021, S. 51).

Krisensituationen können unterschiedlich sein, sowohl in ihrer Entwicklung als auch in der Geschwindigkeit ihres Auftretens. Eine Pandemie beispielsweise kündigt sich oft frühzeitig durch ihre Ausbreitung in anderen Ländern an, während ein Feuer innerhalb kurzer Zeit ernsthafte Gefahren für Menschen und Strukturen darstellen kann. In solchen akuten Krisenfällen sind sofortige Maßnahmen erforderlich, die von der Rettung und Erstversorgung von Opfern bis zur Erfassung und Analyse der Situation reichen (vgl. Frodl, 2022, S. 6)

Krisen sind, gemäß dem deutschen Wirtschaftsgrundschutz, durch einen hohen Handlungs- und Entscheidungsdruck gekennzeichnet, der oft auf einer unvollständigen oder mehrdeutigen Informationslage basiert. Sie ziehen ein großes Medieninteresse und öffentliche Aufmerksamkeit auf sich und können ohne geeignete Bewältigungsmechanismen schnell zu einer existenziellen Bedrohung für die gesamte Institution werden. Die genauen Auswirkungen einer Krise sind anfangs schwer zu beurteilen, was die Notwendigkeit besonderer Strukturen zur Krisenbewältigung unterstreicht. Diese Strukturen müssen flexible, kreative, strategische und kontinuierliche Reaktionsmöglichkeiten bieten, um den Herausforderungen einer Krise effektiv begegnen zu können (vgl. Bundesamt für Verfassungsschutz, 2017, S. 3).

5.1.2 Krisenmanagement

Krisenmanagement ist, im Sinne der Begriffsbestimmungen der Normenreihe Sicherheit und Resilienz, ein ganzheitlicher Managementprozess, der darauf abzielt, mögliche negative Auswirkungen zu identifizieren, die eine Organisation bedrohen könnten. Es beinhaltet die Entwicklung eines Rahmens zur Resilienz, welcher der Organisation ermöglicht, effektiv auf Bedrohungen zu reagieren. Dies soll die Interessen der Stakeholder schützen und sicherstellen, dass das Ansehen, die Marke und die wertschöpfenden Aktivitäten der Organisation bewahrt bleiben, sowie die Betriebsfähigkeit effektiv wiederhergestellt wird. Krisenmanagement schließt auch die Handhabung von Notfallvorsorge, Schadensminderung im Falle eines Vorfalls und die Aufrechterhaltung der Betriebsfähigkeit durch regelmäßige Schulungen, Tests und Überprüfungen mit ein, um die Aktualität und Angemessenheit der Notfallpläne sicherzustellen (vgl. ISO 22300, 2021, S. 15).

Das Krisenmanagement übernimmt die Koordination, Steuerung und Führung einer Organisation für die Dauer einer Krise (vgl. ISO 22361, 2022, S. 9) und stellt somit die Gesamtheit aller Maßnahmen zur Bewältigung von Krisen sicher (vgl. ÖNORM S 2304, 2018, S. 13).

Das Krisenmanagement zielt, nach dem deutschen Wirtschaftsgrundschutz, auf den Umgang mit kritischen Vorfällen ab, die existenzgefährdende oder strategische Auswirkungen haben können. Es stellt die höchste Eskalationsebene in einer Institution dar und unterscheidet sich von anderen reaktiven Strukturen wie dem Notfallmanagement oder der Geschäftsfortführungsplanung. Krisenmanagement erfordert eine spezielle Organisationsform und eigene Dokumentation, um den institutionsübergreifenden Herausforderungen gerecht zu werden. Die Leitung einer Institution ist für die Etablierung des Krisenmanagements verantwortlich und kann eine spezifische Rolle für dessen Umsetzung und Aufrechterhaltung benennen. Die

Bewältigung komplexer Szenarien erfordert häufig eine enge Zusammenarbeit zwischen Krisen- und Notfallmanagement, wobei die entwickelten Verfahren und Strukturen aufeinander abgestimmt sind (vgl. Bundesamt für Verfassungsschutz, 2017, S. 4).

5.2 Ziel von Krisenmanagement

Schawel und Billing definieren Unternehmenskrisen als signifikante Bedrohungen für die Überlebensfähigkeit von Unternehmen. Krisenmanagement umfasst demnach die Prävention, Erkennung, Diagnose und Behebung dieser Krisen, um eine Insolvenz abzuwenden. Die Autoren betonen die Wichtigkeit eines frühzeitigen Eingreifens und die Notwendigkeit der Anwendung dieser Praktiken in allen Unternehmen. Sie unterstreichen die Bedeutung von systematischem Risikomanagement, Krisen-Frühwarnsystemen, der frühzeitigen Krisenidentifikation und -diagnose sowie effektiven Krisenbekämpfungsmaßnahmen, um das unternehmerische Überleben zu sichern (vgl. Schawel & Billing, 2018, S. 191 ff).

Die ÖNORM D 4902:2021 stellt die gestiegene Bedeutung kritischer Infrastrukturen. Das Krisenmanagement nach dieser Norm wird als ein proaktives und reaktives Instrument definiert, das darauf ausgerichtet ist, Organisationen gegenüber unerwarteten und schwerwiegenden Ereignissen widerstandsfähig zu machen. Es wird besonders hervorgehoben, dass in Fällen von Störungen und Notfällen die unverzügliche Wiederherstellung der Betriebsfunktionen im Fokus steht, um die Wertschöpfungskette zügig wiederherzustellen und eine kontinuierliche Leistungserbringung zu garantieren. In diesem Sinne avanciert das Krisenmanagement zu einem unerlässlichen Bestandteil organisatorischer Resilienz und einer nachhaltigen Sicherung der Unternehmenswerte (vgl. ÖNORM D 4902-3, 2021, S. 3).

Die Führungsprozesse des Krisenmanagements müssen ad hoc aktiviert werden, um die Krise zu bewältigen, mögliche Weiterentwicklungen zu bewerten und entsprechende Gegenmaßnahmen zu planen und umzusetzen. Der Erfolg dieser Maßnahmen wird kontrolliert, mit dem Ziel, zur Normalsituation zurückzukehren oder den Betrieb unter veränderten Bedingungen fortzusetzen. Dabei wird eine Krise erst ab einem bestimmten Punkt als solche erkannt, und das Krisenmanagement setzt per Definition ein, um präventiv im Sinne der Schadensbegrenzung zu wirken und die Organisation auf die krisenbedingte Ausnahmesituation vorzubereiten (vgl. Frodl, 2022, S. 5 ff).

Das Krisenmanagement in Unternehmen kennzeichnet sich durch einen bewussten Bruch mit den üblichen Alltagsstrukturen, um effektiv auf Krisensituationen reagieren zu können. In den Anfangsphasen einer Krise neigt die Führungsstruktur dazu, stärker hierarchisch zu sein, folgt also einem „Command and Control“-Ansatz. Dieser Ansatz zielt darauf ab, schnell Entscheidungen zu treffen, die auf guter Information basieren, und alle verfügbaren Ressourcen zielgerichtet einzusetzen. Um dies zu erreichen, wird interdisziplinär vorgegangen, indem Experten aus allen relevanten Disziplinen zusammengebracht werden. Trotz der hierarchischen Ausrichtung wird durch diesen interdisziplinären Ansatz auch Kreativität gefördert, um innovative und

unkonventionelle Lösungen für die auftretenden Probleme zu finden (vgl. Rühl, 2021, S. 80).

5.3 Resilienz und Flexibilität im Krisenmanagement

Ein resilientes operatives Krisenmanagementsystem kennzeichnet sich durch seine Anpassungsfähigkeit und Reaktionsstärke in Krisensituationen. Es stützt sich auf standardisierte Vorgehensweisen, wie Standard Operation Procedures, die allerdings flexibel an die Dynamik realer Einsatzlagen angepasst werden müssen. Wesentlich dabei ist, dass im Krisenfall Kreativität, Improvisationsvermögen und Inkompetenzkompensation unter extremem Druck entscheidend für das Management sind. Die Grundprinzipien eines resilienten Systems beinhalten die kollektive Lagefeststellung, in der die beteiligten Einheiten ein Ereignis erkennen und registrieren, gefolgt von einem gemeinsamen Austausch zur Lagebeurteilung, um ein kohärentes Lagebild und eine koordinierte Reaktion zu gewährleisten. Entscheidend ist, dass Vertrauen, Transparenz und Mut als Grundpfeiler des Informationsaustauschs etabliert sind. Erfolg im Krisenmanagement hängt also nicht nur von den Handlungen selbst, sondern vor allem von deren effektiven Auswirkungen ab. Ein effektives Krisenmanagement wird an der schnellen Wahrnehmung einer Krise, dem Verständnis der Situation durch die Responder, der richtigen Entscheidungsfindung, der koordinierten Kommunikation und klar definierten Verantwortlichkeiten sowie der Bereitschaft, aus der Krise zu lernen, gemessen (vgl. Karsten & Voßschmidt, 2019, S. 161 ff)

6 Faktor Mensch im Krisenmanagement

Alle physischen, psychischen und sozialen Merkmale des Menschen werden als menschliche Faktoren (Human Factors) bezeichnet, sofern sie das Verhalten in und mit soziotechnischen Systemen beeinflussen oder davon beeinflusst werden. Es handelt sich dabei um Personen, Gruppen oder Organisationen (Badke-Schaub et al., 2012, S. 4).

Human Factors untersucht das Verhältnis von Mensch und Technik interdisziplinär. Sie integriert Erkenntnisse aus verschiedenen Disziplinen, um die Interaktion zu optimieren, mit Fokus auf kognitiven, motivationalen und emotionalen Leistungen, nicht nur auf physischen Eigenschaften (vgl. Badke-Schaub et al., 2012, S. 8).

Der Sinn dieser Theorien liegt darin, die Mensch-Technik-Interaktion durch fundierte wissenschaftliche Ansätze zu optimieren, um sowohl die Effizienz als auch das Wohlbefinden der beteiligten Menschen zu verbessern (vgl. Badke-Schaub et al., 2012, S. 10).

6.1 Handlungsmuster

Das Linda-Experiment von Kahneman und Tversky zeigt den Konjunktionsfehlschluss, bei dem Menschen detaillierte Szenarien als wahrscheinlicher einschätzen als allgemeine, obwohl das statistisch falsch ist. Diese Fehleinschätzung entsteht durch den Einfluss von Stereotypen und Kohärenz auf intuitive Urteile. Das Phänomen unterstreicht die Notwendigkeit, kritisches und analytisches Denken zu fördern, um Fehlurteile zu vermeiden und fundierte Entscheidungen zu treffen. (vgl. Rascher & Schröder, 2017, S. 182 ff).

Die Handlungsmuster und Rahmenbedingungen, unter denen Menschen arbeiten und Entscheidungen treffen, sind stark von Stress und Selbstüberschätzung beeinflusst. Stress hat weitreichende Auswirkungen auf die Informationsverarbeitung und Entscheidungsfindung. Unter hohem Stress neigen Menschen dazu, Informationen weniger effizient zu verarbeiten und ihre Aufnahmefähigkeit ist eingeschränkt (vgl. Rascher & Schröder, 2017, S. 185). Dem entgegen wirken programmierte Entscheidungen, auch bekannt als Wenn-Dann-Regeln. Sie sind entscheidend für die Beschleunigung und Effizienz von Entscheidungsprozessen in klar definierten Situationen. Sie basieren auf einer sorgfältigen Analyse und Klassifizierung der Ausgangssituation und der kontinuierlichen Anpassung der Handlungsoptionen. Diese Regeln sind besonders nützlich in stressreichen und dynamischen Situationen, wie etwa bei polizeilichen Einsätzen, da sie strukturierte und methodische Leitlinien bieten, die Fehler minimieren und die Effizienz erhöhen. In der Stabsarbeit sind sie unerlässlich, um schnelle und präzise Lösungen in komplexen Szenarien zu gewährleisten (vgl. Zinke & Hofinger, 2022, S. 169).

Stabsmitglieder ohne Erfahrung empfinden neue Aufgaben als unsicher und nutzen daher oft unpassende Denk- und Handlungsmuster. Menschen organisieren ihre Erfahrungen in kognitive Schemata und mentale Modelle, die effizientes Arbeiten ermöglichen. Fehlende Routinen führen zu Unsicherheit. Neue Mitglieder müssen durch reflektiertes Handeln neue Muster entwickeln, wobei Wissen über stabsinterne

Prozesse entscheidend ist. Die Bildung neuer Schemata ist anspruchsvoll und erfordert Anpassung an spezifische Abläufe. Solche Muster sind notwendig, um Routine, Sicherheit und effektive Reaktionen auf Herausforderungen zu gewährleisten (vgl. Künzer et al., 2022, S. 194).

Es ist notwendig, Rahmenbedingungen zu schaffen, die Stress und Selbstüberschätzung minimieren. Dazu gehören die Förderung realistischer Selbsteinschätzung durch Bildung und Training sowie ein Arbeitsumfeld mit einem angemessenen Erregungsniveau. Dies fördert Kreativität, Zufriedenheit und kompetente Problemlösung, während fundierte Entscheidungen und weniger Fehler ermöglicht werden. Die Berücksichtigung dieser Faktoren optimiert die Leistungsfähigkeit und Entscheidungsfindung. (vgl. Rascher & Schröder, 2017, S. 186).

6.2 Wie trifft der Mensch Entscheidungen

Das Handeln in komplexen Situationen wird als permanentes, paralleles Zusammenspiel ähnlicher Prozesse dargestellt. Die Funktion "Handlungsplan umsetzen" steuert das Verhalten basierend auf dem Vergleich der aktuellen Handlungen mit den erwarteten Effekten. Dabei werden die Funktionen "Lage bewerten und analysieren" sowie "Handlungswissen aktivieren" integriert, um Zielsysteme zu erzeugen. Die Handlungsplanung wird kontinuierlich durch die Ergebnisse des Handelns angepasst (vgl. Hacker & Weth, 2012, S. 92).

Klassische rationale Entscheidungen, die auf vollständigen Informationen und zweckrationalen Regeln beruhen, sind in komplexen Situationen oft nicht praktikabel. Der Mangel an sicheren Informationen erfordert improvisatorische und wissensbasierte Formen der Handlungssteuerung. Diese sind oft die einzige Alternative, bergen jedoch Risiken (vgl. Hacker & Weth, 2012, S. 92). Es wird erwartet, dass sowohl Menschen als auch Maschinen Entscheidungen optimal treffen, insbesondere in verantwortungsvollen beruflichen Positionen. Die Forschung befasst sich mit den Anforderungen an solche Entscheidungen und deren Umsetzung in der Praxis, wobei das Konzept der „High Reliability“ eine zentrale Rolle spielt (vgl. Blanz, 2017, S. 12 ff).

Eine wirksame Entscheidung besteht aus drei Schritten: Erstens, das Problem erkennen und gezielt analysieren. Zweitens, einen strukturierten Entscheidungsprozess anwenden. Drittens, Denkfehler vermeiden durch einen klaren und logischen Denkprozess. Diese Schritte gewährleisten fundierte und durchdachte Entscheidungen (vgl. Höbel et al., 2022, S. 193).

Bei der Bewertung von Handlungsalternativen sind verschiedene Entscheidungsarten relevant. Valenzbedingte Entscheidungen priorisieren den Wert einer Alternative, während bei chancenbedingten Entscheidungen die Wahrscheinlichkeit des Erfolgs im Vordergrund steht. Lagebedingte Entscheidungen integrieren sowohl Werte als auch Wahrscheinlichkeiten (vgl. Hacker & Weth, 2012, S. 96).

Für effektive Problemlösung und Entscheidungsfindung sollten Bedingungen geschaffen werden, die das Denken unterstützen. Dies umfasst das Minimieren von Störfaktoren wie Multitasking oder Ablenkungen (vgl. Höbel et al., 2022, S. 193).

6.3 Umgang mit Fehler

Es gibt viele Definitionen und Ansätze in der Wissenschaft, jedoch keinen Konsens. Die verschiedenen Definitionen spiegeln unterschiedliche Perspektiven wider, bleiben aber im Kern bei der Abweichung vom gewünschten oder als richtig angesehenen Verhalten (vgl. Hofinger, 2012, S. 40).

Bei einem Fehler handelt es sich um eine Abweichung von einem als angemessen betrachteten Verhalten oder einem angestrebten Handlungsziel, das der Handelnde hätte durchführen oder erreichen können. In dieser Definition wird hervorgehoben, dass Fehler mit dem menschlichen Handeln zusammenhängen. Maschinen haben keinen Fehler im Sinne des Menschen; sie können nur falsch eingesetzt, fehlerhaft programmiert oder fehlerhaft verwendet werden. (vgl. Hofinger, 2012, S. 40).

In komplexen Situationen kann ein Fehler oft erst im Nachhinein erkannt werden. Beispielsweise kann das Abweichen von Standardprozeduren, das ein Flugzeug rettet, als Flexibilität statt als Fehler gelten. Handlungen werden häufig erst rückblickend als Fehler eingestuft. Daher ist es sinnvoller, von riskanten Handlungen zu sprechen, die negativ beurteilt werden, wenn das geschätzte Sicherheitsrisiko vom tatsächlichen abweicht. In komplexen Situationen können solche Abweichungen helfen, Fehlerursachen besser zu verstehen und zu verhindern (vgl. Hacker & Weth, 2012, S. 92).

Fehler entstehen durch interne und externe Ursachen. Interne Faktoren umfassen physiologische und biologische Aspekte wie Müdigkeit, Ablenkung durch Lärm und gesundheitliche Beeinträchtigungen. Diese variieren individuell und beeinflussen die Fehleranfälligkeit (vgl. Hofinger, 2012, S. 55). Das Schutzempfinden ist zentral für die Bewältigung komplexer Situationen in Stäben. Stabsmitglieder benötigen Kompetenzen wie situative Wahrnehmung, Stressbewältigung und emotionale Belastbarkeit, um effektiv auf Herausforderungen zu reagieren. Strategische Flexibilität und Vertrauen ins Team sind entscheidend, um unerwartete Ereignisse zu meistern und eine konstruktive Arbeitsatmosphäre zu bewahren (vgl. Strohschneider, 2022, S. 23)

Externe Ursachen schließen Organisationsfaktoren wie Sicherheitskultur, Zielprioritäten und Arbeitsumgebung ein. Dazu gehören auch Lärm, Arbeitszeiten, Ausstattung sowie die Komplexität der Aufgaben und Arbeitslast (vgl. Hofinger, 2012, S. 56).

6.4 Abgrenzung zum Begriff Katastrophe

Eine Katastrophe, im Sinne des Duden, bezeichnet ein schweres Unglück oder ein Naturereignis mit verheerenden Folgen und findet Anwendung in Beschreibungen von Ereignissen mit tiefgreifend negativen Auswirkungen, wie etwa furchtbare, unvorhergesehene oder wirtschaftliche Katastrophen, sowie in politischen Kontexten. In der Literaturwissenschaft wird der Ausdruck spezifisch für eine entscheidende Wendung zum Schlimmen, vor allem als Schlusshandlung im antiken Drama, verwendet. Die etymologische Wurzel des Wortes liegt im lateinischen "catastropha", abgeleitet vom griechischen "katastrophé", was Umkehr oder Wendung bedeutet. Als

feminines Substantiv in der deutschen Sprache umfasst "Katastrophe" eine breite Palette dramatischer Ereignisse oder Wendepunkte (Duden, 2024).

In Österreich wird eine Katastrophe administrativ definiert als ein Ereignis, das Leben oder Gesundheit von vielen Menschen, die Umwelt oder bedeutende Sachwerte in außergewöhnlichem Maße gefährdet oder schädigt und dessen Abwehr oder Bekämpfung einen koordinierten Einsatz notwendiger Kräfte und Mittel durch eine Behörde erfordert (vgl. Jachs, 2011, S. 74).

Es konzentrieren sich damit administrative Katastrophendefinitionen auf das Ereignis selbst, das außergewöhnliche behördliche Hilfsmaßnahmen auslöst, basierend auf dem Schadensausmaß und der Notwendigkeit spezifischer Gefahrenabwehr. Im Unterschied zum amerikanischen System, das eine formelle Ausrufung der Katastrophe für Bundesunterstützung vorsieht, gibt es in Österreich keine solche Prozedur, wobei der Fokus auf der Anpassung der Führungsstruktur und Rechtsvorschriften liegt (vgl. Jachs, 2011, S. 74).

Eine Katastrophe, im Sinne der Definition der vereinten Nationen (UNDRR), ist eine ernsthafte Störung der Funktionsfähigkeit einer Gemeinschaft oder Gesellschaft, verursacht durch gefährliche Ereignisse, die aufgrund von Exposition, Verwundbarkeit und begrenzter Bewältigungskapazität zu menschlichen, materiellen, wirtschaftlichen und umweltbedingten Verlusten führen. Die Auswirkungen können sofort und lokalisiert sein, tendieren jedoch dazu, weitreichend und langanhaltend zu sein, was oft externe Hilfe erforderlich macht. Katastrophenschäden und -auswirkungen umfassen die Zerstörung von Vermögen, die Unterbrechung von Dienstleistungen und Lebensgrundlagen sowie negative Effekte auf das menschliche Wohlbefinden. Katastrophen werden in langsam eintretende, wie Dürren, und plötzlich eintretende, wie Erdbeben, unterteilt. Die Bewältigung dieser Ereignisse kann nationale oder internationale Unterstützung erfordern (UNDRR, 2009).

7 Stabsarbeit

Unter Stabsarbeit wird im Sinne der SKKM-Richtlinie des österreichischen Innenministeriums das standardisierte Zusammenwirken einer arbeitsteilig organisierten Personengruppe, bezeichnet als Stab, verstanden. Der Hauptzweck dieser Organisation ist die Unterstützung und Beratung des Einsatzleiters bei der Erledigung seiner Führungsaufgaben. Dies umfasst die Handhabung von Führungsmitteln für die Informationsgewinnung und -verarbeitung, die kontinuierliche Lagebewertung und -darstellung, die Erarbeitung von Entscheidungsvorschlägen sowie die Umsetzung der Entscheidungen des Einsatzleiters. Die Stabsarbeit dient primär der Entlastung des Einsatzleiters von administrativen Aufgaben und der Sicherstellung einer effizienten, kontinuierlichen Arbeitsweise unter Einsatzbedingungen, wobei besonders auf die Erhaltung der Leistungsfähigkeit geachtet wird (vgl. BMI, Staatliches Krisen- und Katastrophenschutzmanagement, 2006, S. 35).

7.1 Grundlagen der Stabsarbeit

Stabsarbeit ist ein vorübergehendes Unterstützungselement, das dazu dient, den Linienvorgesetzten zu beraten und zu unterstützen, häufig in Verbindung mit einem Fachstab. Dazu gehören reine Fachstäbe, die nur aus Fachkräften bestehen, sowie dauerhaft eingerichtete Stabsabteilungen in alltäglichen Organisationen. Ein Stab wird speziell auf Führungsebenen eingerichtet, auf denen die Anforderungen so umfangreich sind, dass die Entscheidungsträger die anfallenden Aufgaben allein weder überblicken noch bewältigen können. Die Bildung von Stäben findet demnach statt, wenn ein erhöhter Koordinationsbedarf besteht, beispielsweise durch den Einsatz von viel Personal oder spezieller Technik, wenn Zuständigkeitsgrenzen überschritten werden, das Informationsaufkommen für eine einzelne Person zu hoch ist, Spezialistenwissen schnell und effizient für Entscheidungsprozesse benötigt wird, lokale Ressourcen nicht ausreichen und somit übergreifend organisiert werden müssen oder wenn die Menge der eingesetzten Ressourcen und die Vielzahl der beteiligten Stellen eine einheitliche Führung erfordern (vgl. Heimann & Hofinger, 2022a, S. 5).

Stabsarbeit kennzeichnet die kooperative Bearbeitung von Aufgaben, ähnlich der Teamarbeit, mit besonderen Eigenschaften. Während Teamarbeit das Zusammenkommen von Personen aus verschiedenen Bereichen mit komplementären Fähigkeiten für ein Ziel umfasst, zeichnet sich Stabsarbeit durch eine hierarchische Struktur und beschränkte Autonomie aus, fokussiert auf Einzelaufgaben mit Schnittstellenbewusstsein. Sie ist zeitlich begrenzt und zielorientiert, mit klar definierten Rollen und physischen Grenzen innerhalb der Organisation, die für effiziente Zusammenarbeit gezielt überschritten werden. Stäbe sind oft homogen und nutzen eine einheitliche Fachsprache, können aber für spezifische Aufgaben heterogen zusammengestellt werden, um verschiedene Perspektiven zu integrieren. Virtuelle Teams und IT-Vernetzung spielen eine wichtige Rolle für flexible, standortunabhängige Stabsarbeit (vgl. Heimann & Hofinger, 2022a, S. 6 ff).

Die Bildung eines Führungsstabes wird durch die Notwendigkeit eines schnellen Informationsflusses oder der Verarbeitung einer großen Menge und Vielfalt an Informationen motiviert. Grundlegend für die Arbeit eines Stabes ist, dass die Kompetenz mehrerer Akteure die Entscheidungsfindung verbessert, indem sie dem Entscheidungsträger eine breitere Wissensbasis bietet und die Fehlerwahrscheinlichkeit durch kollektive Überprüfung verringert. Die Effektivität eines Führungsstabes resultiert nicht nur aus der Summe der Beiträge einzelner Mitglieder, sondern zielt darauf ab, rationale Entscheidungen zu treffen, die weitgehend unabhängig von den individuellen Fähigkeiten der Beteiligten sind (vgl. Weitkunat, 2020, S. 269).

Die Stabsarbeit ist ein wesentliches Führungsinstrument sowohl im öffentlichen als auch im privaten Sektor zur Bewältigung von Notfällen, Krisen und Katastrophen. Trotz ihrer zentralen Rolle stellen aktuelle Rahmenbedingungen und die interorganisationale Zusammenarbeit Herausforderungen dar, wie zuletzt die Flutkatastrophe 2021 in Deutschland verdeutlichte. Um die gesellschaftliche Resilienz zu stärken, ist eine dringende Weiterentwicklung der Stabsarbeit notwendig. Das Ziel ist es, leistungsfähige und durchhaltefähige Stäbe zu schaffen, die quer durch verschiedene Bereiche und auf unterschiedlichen Ebenen effizient funktionieren können (vgl. Bayer et al., 2022, Kapitel Einleitung).

7.2 SKKM Modell

Die Fachgruppe Ausbildung des Staatlichen Krisen- und Katastrophenschutzmanagements (SKKM) arbeitete an der Richtlinie für das Führen im Katastropheneinsatz mit Experten aus den Bereichen der Behörden, der Einsatz-, Hilfs- und Rettungsorganisationen zusammen. Um eine bundesweite Vereinheitlichung und integrierte Einsatzführung im Katastrophenfall zu erreichen, hatte diese Richtlinie vor allem das Ziel, eine einheitliche Grundlage für die vom SKKM initiierte Führungs- und Stabsausbildung zu etablieren. Die Richtlinie wurde von Experten aus den Bereichen der Behörden, Einsatz-, Hilfs- und Rettungsorganisationen sowie der Fachgruppe Ausbildung des SKKM erarbeitet. Darüber hinaus haben die im SKKM-Koordinationsausschuss vertretenen Behörden sowie Einsatz-, Hilfs- und Rettungsorganisationen erklärt, ihre bestehenden Handbücher, Ausbildungsbehelfe und sonstigen schriftlichen Grundlagen zum Thema „Führen im Katastropheneinsatz“ an diese Richtlinie anzupassen, soweit dies die Besonderheiten der jeweiligen Einrichtungen zulassen (vgl. BMI, Staatliches Krisen- und Katastrophenschutzmanagement, 2006, S. 5).

Das SKKM wurde mit Ministeratsbeschluss vom Jänner 2004 neuorganisiert. Die wichtigste Änderung bestand darin, dass die Koordination des Krisenmanagements und der internationalen Katastrophenhilfe vom Bundeskanzleramt auf das Innenministerium übertragen wurde. Dies führte zur Vereinigung aller zentralen Koordinationszuständigkeiten für den Bevölkerungsschutz auf Bundesebene (vgl. BMI - Ministerratsbeschluss (SKKM), 2004).

.

Ein bedeutender Schritt war die Einrichtung eines Koordinationsausschusses für Angelegenheiten des SKKM beim Innenministerium, der die Grundsatzplanung und Abstimmung der Maßnahmen aller Bundesministerien und Länder übernimmt. Dieser Ausschuss fördert den Informationsaustausch und koordiniert die Maßnahmen im Krisenfall.

Die Aufgabenverteilung zwischen Bund und Ländern wurde neu geordnet, um eine klare Kompetenzverteilung und effiziente Zusammenarbeit zu gewährleisten. Die Bundeswarnzentrale wurde zu einer modernen Einsatzzentrale ausgebaut, die für das überregionale Informations- und Ressourcenmanagement zuständig ist und stärker mit den Leiteinrichtungen der Bundesländer vernetzt wurde (vgl. BMI - Ministerratsbeschluss (SKKM), 2004).

Diese Maßnahmen zielten darauf ab, die Koordinations- und Planungskompetenz des Bundes zu stärken, die Effizienz der Krisenbewältigung zu erhöhen und eine zeitgemäße Anpassung an neue sicherheitspolitische Herausforderungen sicherzustellen (vgl. BMI - Ministerratsbeschluss (SKKM), 2004).

7.3 Krisensicherheitsgesetz

Der bisherige rechtliche Rahmen für staatliches Krisen- und Katastrophenschutzmanagement basiert weitgehend auf den Ministerratsbeschluss aus dem Jahr 2004. Angesichts der Entwicklungen und Herausforderungen in der jüngeren Vergangenheit, insbesondere der Covid-19-Pandemie, hat die Bundesregierung erkannt, dass es neben vorhandenen Stärken auch erhebliches Verbesserungspotenzial im Krisenmanagement gibt (vgl. Katharina Schmögl, 2023, S. 85).

Auf Grundlage des Bundeskrisensicherheitsgesetzes wird im Bundesministerium für Inneres ein Bundeslagezentrum eingerichtet. Es hat die Aufgabe, die Bundesministerien bei Krisen und Katastrophen zu unterstützen, indem es technische und sicherheitsrelevante Standards einhält und den Betrieb sicherstellt. Es ist für die Informationssammlung, Beobachtung, Analyse und Bewertung aktueller Entwicklungen verantwortlich und arbeitet mit Vertretern der Länder, dem Österreichischen Städtebund, dem Österreichischen Gemeindebund und Einsatzorganisationen zusammen. Zusätzlich unterstützt es die Fachgremien und das Koordinationsgremium bei administrativen Belangen und fungiert als Kontaktstelle für Länder, Städte, Gemeinden, Betreiber kritischer Infrastrukturen und Nichtregierungsorganisationen (vgl. Bundes-Krisensicherheitsgesetz (B-KSG), 2023).

Die Mitglieder der Bundesregierung sind verpflichtet, in ihrem jeweiligen Wirkungsbereich die strukturellen Voraussetzungen für ein effektives Krisenmanagement zu schaffen. Dies umfasst die Durchführung erforderlicher Schulungen, die Festlegung von Erreichbarkeiten, die Aufstellung und regelmäßige Überprüfung von Krisenplänen sowie die Sicherstellung der Erbringung notwendiger Leistungen für die Bevölkerung im Krisenfall. Darüber hinaus müssen sie ein System zur Qualitätssicherung der Krisenvorsorgemaßnahmen einrichten. Sie haben dafür zu sorgen, dass Hilfsmittel und systemrelevante Güter jederzeit einsatzbereit sind und eine zentrale Kontaktstelle für das Bundeslagezentrum benennen. Bei spezifischen

Maßnahmen zur Krisenbewältigung ist besonders auf die Bedürfnisse vulnerabler Gruppen zu achten (vgl. Bundes-Krisensicherheitsgesetz (B-KSG), 2023)

Bis zur Einrichtung des Bundeslagezentrums übernimmt eine Organisationseinheit des Innenministeriums dessen Aufgaben. Die Ausschreibung der Regierungsberaterstellen ist bereits vor Inkrafttreten zulässig. Der Bundeskanzler trifft die erforderlichen organisatorischen und personellen Maßnahmen ab dem Tag der Kundmachung des Gesetzes. Für die Vollziehung des Gesetzes sind die Bundesregierung, der Bundeskanzler, der Innenminister und die zuständigen Bundesminister verantwortlich, jeweils für die in ihren Wirkungsbereichen definierten Aufgaben (vgl. Bundes-Krisensicherheitsgesetz (B-KSG), 2023).

7.4 Strukturmodell

Das Stabsmodell, nach SKKM-Richtlinie, besteht aus einer Führungs- und einer Fachgruppe. Wobei beide Gruppen dem Leiter der Stabsarbeit unterstellt sind. Die Führungsgruppe ist standardisiert aufgestellt, die Fachgruppe kann an die Bedürfnisse angepasst werden (vgl. BMI, Staatliches Krisen- und Katastrophenschutzmanagement, 2006, S. 38).

Die zum Führen erforderlichen Informationen werden in arbeitsteiliger Weise nach Aufgabenfeldern geordnet und Sachgebieten zugewiesen (vgl. BMI, Staatliches Krisen- und Katastrophenschutzmanagement, 2006, S. 40).

Die zur Führungsgruppe zusammengefassten Sachgebiete erfüllen drei wesentliche Grundfunktionen: Einsatz, Einsatzunterstützung und Führungsunterstützung. Die Grundfunktion Einsatz wird durch die Sachgebiete 2 und 3 abgedeckt, die Einsatzunterstützung durch die Sachgebiete 1 und 4, und die Führungsunterstützung durch die Sachgebiete 5 und 6 (vgl. BMI, Staatliches Krisen- und Katastrophenschutzmanagement, 2006, S. 40).

Diese Struktur ermöglicht eine klare Aufgabenverteilung und effiziente Bearbeitung der anfallenden Aufgaben im Krisen- und Katastrophenmanagement. Die Notwendigkeit dieser Gliederung liegt in der Sicherstellung einer geordneten und effektiven Informationsverarbeitung, die für eine erfolgreiche Einsatzführung unabdingbar ist. Durch die arbeitsteilige Organisation der Sachgebiete wird gewährleistet, dass alle relevanten Aspekte eines Einsatzes abgedeckt und koordiniert werden können, was die Effizienz und Reaktionsfähigkeit im Krisenfall erheblich verbessert (vgl. BMI, Staatliches Krisen- und Katastrophenschutzmanagement, 2006, S. 40).

7.5 Interoperabilität durch SKKM

Durch die Anwendung der Richtlinie soll die Interoperabilität zwischen den handelnden Stellen sichergestellt werden. Ziel der Richtlinie ist es, bei den betroffenen Behörden, Einsatzorganisationen und Einrichtungen eine notwendige Vereinheitlichung im Führungsbereich sicherzustellen (vgl. BMI, Staatliches Krisen- und Katastrophenschutzmanagement, 2006, S. 5).

7.6 Digitalisierung

Digitalisierung beschreibt die Umwandlung von Prozessen, Objekten und Ereignissen durch die Nutzung digitaler Technologien. Im Kern geht es um die zunehmende Implementierung und Nutzung von Computern, Algorithmen und Netzwerken, die traditionelle, oft analoge Verfahren ersetzen. Dieser Prozess der digitalen Transformation umfasst eine Vielzahl von Aspekten, darunter die Automatisierung von Geschäftsprozessen, die Entwicklung neuer digitaler Plattformen und die Schaffung innovativer Produkte und Dienstleistungen (vgl. Stahl & Staab, 2019, S. 22).

Im historischen Kontext ähnelt die Digitalisierung früheren industriellen Revolutionen, die grundlegende Veränderungen in Wirtschaft und Gesellschaft bewirkten. Ein wesentliches Merkmal der Digitalisierung ist die schnelle und umfassende Natur der Veränderungen. Diese Transformation wird oft als disruptiv bezeichnet, da sie bestehende Geschäftsmodelle infrage stellt und neue Möglichkeiten eröffnet. Die digitale Revolution wird durch die massive Nutzung von Informations- und Kommunikationstechnologien getragen, die nahezu alle Lebensbereiche durchdringen (vgl. Stahl & Staab, 2019, S. 23)

7.6.1 Begriffsdefinition bzw. -eingrenzung

Der Begriff Digitalisierung umfasst nicht nur technische Innovationen, sondern auch deren tiefgreifende gesellschaftliche und wirtschaftliche Auswirkungen. Diese Veränderungen sind mit Hoffnungen auf Fortschritt und Wachstum, aber auch mit Ängsten und Widerständen verbunden. Ein umfassendes Verständnis der Digitalisierung erfordert daher eine interdisziplinäre Perspektive, die technologische, wirtschaftliche und soziale Dimensionen integriert (vgl. Stahl & Staab, 2019, S. 23).

Insgesamt ist die Digitalisierung ein komplexes und dynamisches Phänomen, das die Art und Weise, der Zusammenarbeit und des täglichen Lebens, grundlegend verändert. Ihre Bedeutung wird durch die allgegenwärtige Präsenz digitaler Technologien in unserem Alltag unterstrichen, von der Nutzung mobiler Endgeräte bis hin zu digitalen Plattformen für Kommunikation und Handel. Diese digitale Transformation wird auch in Zukunft eine treibende Kraft für Innovation und gesellschaftlichen Wandel bleiben (vgl. Stahl & Staab, 2019, S. 23 ff).

7.6.2 Digitalisierung in der Stabsarbeit

Führungsstäbe, die nur analoge Techniken zur Visualisierung, Kommunikation und Dokumentation nutzen, sind heute nicht mehr realistisch. Moderne Führungsstäbe verwenden elektronische Dokumentations- und Lagedarstellungssysteme sowie komplexe EDV-Systeme, Big-Data-Anwendungen und soziale Medien (vgl. Heimann,

2022a, S. 12). Die Notwendigkeit des Einsatzes neuer Technologien und digitaler Werkzeuge sowie die Vermeidung von Fehlhandlungen durch digitale Tools sind zentrale Aspekte der Stabsarbeit. Digitale Methoden und Werkzeuge, die Prozesse in Führung, Aus- und Fortbildung, Informationsmanagement und Organisation unterstützen, sind unerlässlich. Diese Technologien minimieren Fehlhandlungen in Führungsszenarien, präzisieren die Planungs- und Entscheidungsfindung und steigern die Effizienz. Der Einsatz digitaler Tools trägt somit zur Optimierung und Professionalisierung der Stabsarbeit bei (vgl. Heimann, 2022a, S. 19).

Bis zum Jahr 2020 wurde die Stabsarbeit größtenteils in physischer Präsenz durchgeführt. Der Übergang zu virtuellen Meetings oder Videokonferenzen war selten und meist nur in speziellen Fällen vorhanden. Erst durch die COVID-19-Pandemie und die damit einhergehenden strengen Hygieneregeln und die Gefahr von Infektionen war es notwendig, auf digitale Lösungen umzusteigen. Dies führte dazu, dass Videokonferenzen und hybride Arbeitsmodelle zur Norm wurden, obwohl es vorher erhebliche rechtliche und kulturelle Vorbehalte gegen solche Formen der Zusammenarbeit gab(vgl. Heimann & Hofinger, 2022b, S. 299).

Die Pandemie zwang viele Stabsmitglieder ins Homeoffice, was neue Herausforderungen bei Vertraulichkeit, störungsfreiem Arbeiten und technischer Infrastruktur brachte. Diese Probleme betonten die Notwendigkeit, digitale Fähigkeiten und Homeoffice-Bedingungen zu verbessern, um effektive Stabsarbeit zu ermöglichen (vgl. Heimann & Hofinger, 2022b, S. 305). Das Hauptproblem virtueller Führung liegt in der Distanz und den fehlenden persönlichen Kontakten zwischen Führungskräften und Mitarbeitern. Diese Distanz beeinträchtigt die Effektivität der Führung und erschwert den Aufbau von sozialen Beziehungen und Vertrauen, was zu Passivität und Leistungsrückgang führen kann (vgl. Lippold, 2019, S. 36)

Digitale Systeme in der Stabsarbeit nehmen keine Bewertung vor. Die Entscheidung trifft der Mensch/Stab (vgl. Heimann, 2022b, S. 328).

8 Empirische Untersuchung

In diesem Kapitel wird die empirische Untersuchung dargestellt. Im Zuge der Mastersthesis wurden Experteninterviews sowie eine Onlinebefragung von Expertinnen und Experten aus dem Krisenmanagement der kritischen Infrastruktur durchgeführt. Die Ergebnisse aus Interviews und Befragung wurden aufbereitet. Am Ende des Kapitels werden die Ergebnisse miteinander verknüpft.

8.1 Experteninterviews

In diesem Kapitel werden die Zusammenfassungen der Experteninterviews dargestellt. Die Interviews wurden im zwischen April und Mai 2024 durchgeführt. Die Experten erklärten sich bereit und einverstanden im Zuge der Masterthesis genannt zu werden. Für die Durchführung der Experteninterviews wurden individuelle Termine mit jeder Expertin und jedem Experten vereinbart. Die Interviews fanden unabhängig voneinander statt. Durch die separate Terminierung und Durchführung konnte sichergestellt werden, dass die Expertinnen und Experten ihre Perspektiven und Erfahrungen ohne äußere Einflüsse oder Beeinflussung durch andere Teilnehmende darlegen konnten.

8.2 Die Experten

In diesem Kapitel werden die Interviewpartner kurz vorgestellt. Die Informationen stammen aus den geführten Interviews von den Experten selbst.

8.2.1 Florian Schwarz

Florian Schwarz ist ein Fachmann im Bereich Krisenmanagement und Resilienz, der sowohl eine militärische als auch zivile Expertise aufweist. Nach zehn Jahren militärischer Laufbahn, einschließlich Ausbildungsphasen an der Militärakademie in Österreich und an der Militärakademie in den USA in West Point, sowie mehreren Auslandseinsätzen im Kosovo und Mali, verließ er das Militär, um seine Karriere in der zivilen Beratungsbranche zu starten. Seitdem hat er sich weiterqualifiziert, unter anderem mit einem Master in Führung von Organisationen und einem weiteren in integriertem Sicherheitsmanagement. Zusätzlich ist er zertifizierter Business Continuity Instructor.

Seit 2020 ist Schwarz als Senior-BCM Consultant tätig. Er betreut umfangreiche Projekte im Bereich Krisenmanagement, Resilienz, Objektschutz und Softwareentwicklung, wobei er ein besonderes Augenmerk auf die kritische Infrastruktur in den Sektoren Energie, Finanz- und Versicherungsdienstleistungen sowie im Gesundheitswesen legt. Sein breites Wissensspektrum und seine praktischen Erfahrungen ermöglichen ihm eine sektorübergreifende Beratungstätigkeit, in der er innovative Lösungen für komplexe Probleme entwickelt.

8.2.2 Michal Cieslik

Michal Cieslik ist Chief Security Officer der Wiener Linien. Er bringt eine umfangreiche berufliche Erfahrung mit, die durch seine mehrjährige Tätigkeit bei den Wiener Linien und seine frühere Laufbahn als Berufsoffizier beim österreichischen Bundesheer geprägt ist. In seiner militärischen Karriere spezialisierte er sich auf ABC-Abwehr und

war anschließend beim Heeresnachrichtenamt tätig. Seine Expertise und sein Verständnis für Sicherheits- und Verteidigungsstrategien, insbesondere in kritischen Infrastrukturen, bilden die Grundlage für seine Rolle in der Steuerung und Entwicklung von Sicherheitsstrategien für den öffentlichen Verkehrssektor.

8.2.3 Günter Rattei

Günter Rattei leitet seit Mai 2023 die Abteilung für Krisenmanagement und Business Continuity Management bei der ASFINAG, wo er seit 2004 in verschiedenen leitenden Positionen tätig ist. Er besitzt umfassende Erfahrung in der Entwicklung und Umsetzung von Krisenstrategien und nutzt digitale Technologien zur Effizienzsteigerung in Krisensituationen. Unter seiner Führung wurden bei ASFINAG ein detailliertes Krisenhandbuch implementiert. Rattei fördert die kontinuierliche Verbesserung und Anpassung von Krisenplänen und kooperiert eng mit anderen kritischen Infrastrukturen und Behörden, um die Resilienz und Sicherheit der österreichischen Verkehrsinfrastruktur zu gewährleisten.

8.2.4 Experten Energiewirtschaft AUT

Die Kernaussagen des Interviews aus der vorliegenden Masterarbeit beleuchten die Praktiken und Grundprinzipien des Krisenmanagements einer Organisation im Energiebereich, unter der Leitung eines langjährigen Experten mit umfangreicher Erfahrung in verschiedenen Führungsrollen seit Mitte der 1990er Jahre. Aufgrund der Offenheit und der teilweisen sensiblen Inhalte wurde zum Beginn des Interviews auf die Notwendigkeit der Anonymisierung geben. Aufgrund der Inhalte für die vorliegende Arbeit wurde dem Wunsch nachgekommen.

8.2.5 Roland Pachtner

Roland Pachtner beginnt mit seiner Tätigkeit am Flughafen im Jahr 1997, zunächst als Feuerwehrmann im Schichtdienst. Wechselte später in den Verwaltungsbereich, wurde stellvertretender Kommandant und übernahm 2012 die Rolle des Feuerwehrkommandanten sowie die Leitung der Abteilung für Emergency. In dieser Funktion verantwortet er die Bereiche Feuerwehr, Rettungsdienst und die neu hinzugekommene Intendanz. Zu seinen Aufgaben zählen Wartungs- und Reparaturarbeiten auf der Airside, wie Fugensanierung und Zaunreparaturen. Pachtner betont seine Rolle als Brandschutzbeauftragter der Flughafen Wien AG und erwähnt, dass das Thema Krisenmanagement seit zwei Jahren zu seinen Zuständigkeiten gehört, nachdem es zuvor in anderen Abteilungen weniger erfolgreich behandelt wurde. Insgesamt führt er ein Team von 130 Mitarbeitern.

8.2.6 Manuel Schwarzeneker

Manuel Schwarzeneker ist stellvertretender Abteilungsleiter in der Pensionsversicherung in der Hauptstelle in Wien. Er verfügt über einen fundierten fachlichen Hintergrund in Wirtschaft, Psychologie, Coaching und Organisationsentwicklung sowie umfangreiche Erfahrungen im Krisenmanagement. Diese Expertise wurde durch seine Tätigkeit als Milizoffizier beim Bundesheer ergänzt. Seit Dezember 2023 ist er für das Krisenmanagement verantwortlich, ein Bereich, den er ursprünglich mit zwei weiteren Kollegen aufgebaut hat. Heute betreut er etwa 7000

Mitarbeiter und ist hauptverantwortlich für die Umsetzung und Weiterentwicklung der Krisenmanagementstrategien in seiner Organisation. Seine umfassende Erfahrung und sein tiefgehendes Wissen machen ihn zu einem wertvollen Ansprechpartner in Fragen der Flexibilität und Anpassungsfähigkeit im Krisenmanagement, insbesondere im Umgang mit kritischen Infrastrukturen und digitalen Herausforderungen.

8.2.7 Interview Florian Schwarz

Schwarz betont die Bedeutung der Unternehmensgröße und der internen Expertise für die Implementierung flexibler Krisenstabsmodelle. Insbesondere kritisiert er das in Österreich verbreitete SKKM-Modell für seine mangelnde Anpassungsfähigkeit an moderne Anforderungen, wie die Notwendigkeit der Einbindung von IT-Abteilungen aufgrund zunehmender IT-Risiken.

Ein weiterer zentraler Punkt des Interviews ist die Nutzung digitaler Technologien zur Verbesserung der Krisenkommunikation und -dokumentation. Schwarz beschreibt, wie moderne Technologien, wie Alarmierungssysteme und digitale Krisenmanagementsysteme, zur Effizienzsteigerung beitragen, indem sie eine bessere Dokumentation und Interoperabilität ermöglichen.

Schwarz hebt auch die Wichtigkeit der Einbindung aller relevanten Stakeholder in das Krisenmanagement hervor. Er argumentiert, dass die interne und externe Stakeholder-Einbindung, besonders durch Schulungen und Übungen, wesentlich zur Verbesserung der Krisenstabsarbeit beiträgt.

Ein weiteres Thema ist die psychische und physische Belastung von Mitarbeitern in Krisensituationen. Er empfiehlt, betroffene Mitarbeiter aus dem Krisenstab auszuschließen und die Nutzung von Unterstützungsangeboten durch das Unternehmen zu fördern.

Zuletzt werden die regulatorischen und gesetzlichen Anforderungen an das Krisenmanagement angesprochen. Schwarz weist auf die Notwendigkeit hin, gesetzliche Vorgaben konsequent umzusetzen und gleichzeitig die eigenen Krisenmanagementpraktiken kontinuierlich zu verbessern.

8.2.8 Interview Michal Cieslik

Cieslik betont die fundamentale Bedeutung von Flexibilität und Anpassungsfähigkeit, die als Eckpfeiler eines effizienten und resilienzorientierten Krisenmanagementsystems fungieren. Diese Prinzipien erlauben es, spezifische Herausforderungen agil und zielgerichtet anzugehen, indem der Krisenstab dynamisch und bedarfsgerecht zusammengestellt wird.

Die Struktur des Krisenstabes reflektiert diese Flexibilität deutlich. Anstelle einer starren Rollenzuweisung, die in vielen herkömmlichen Krisenmanagementansätzen vorherrscht, priorisiert die Wiener Linien ein Modell, das eine hohe personelle Variabilität und Fachexpertise in den Vordergrund stellt. Jedes Mitglied wird entsprechend seiner speziellen Fachkenntnisse und der aktuellen Anforderungen der Krisensituation ausgewählt. Diese strategische Flexibilität ist entscheidend, um auf die vielschichtigen Herausforderungen eines urbanen Verkehrssystems effektiv reagieren zu können.

Ein weiterer wichtiger Aspekt des Interviews ist die Rolle digitaler Technologien im Krisenmanagement. Diese Technologien werden primär zur schnellen Alarmierung und effizienten Kommunikation eingesetzt, was eine sofortige Reaktionsfähigkeit des Krisenstabs ermöglicht. Für die Lagedarstellung wählt das Krisenmanagement der Wiener Linien jedoch bewusst einfache und klare Mittel wie Papier und Stift, um Zeitverlust durch die Erstellung aufwendiger digitaler Präsentationen zu vermeiden und um die Konzentration auf wesentliche Entscheidungsprozesse zu erleichtern.

Zusätzlich wird die kontinuierliche Verbesserung durch regelmäßige Debriefings und den Einsatz des PDCA-Zyklus (Plan-Do-Check-Act) betont, welche systematische Auswertungen von Übungen und realen Einsätzen fördern. Diese Vorgehensweise unterstützt eine ständige Optimierung der Prozesse und eine schnelle Integration von Erkenntnissen in das Krisenmanagement-Handbuch der Organisation.

Die Implementierung der Prinzipien der Hochzuverlässigkeitsorganisationen (HRO) wird als essenziell für das Krisenmanagement beschrieben. Diese Prinzipien, insbesondere die Sensibilität für betriebliche Abläufe und die schnelle Reaktionsfähigkeit auf unerwartete Ereignisse, sind kritisch für die Aufrechterhaltung der Betriebsfähigkeit unter Krisenbedingungen. Durch eine proaktive statt nur reaktiver Herangehensweise unterstützen diese HRO-Prinzipien das Krisenmanagement darin, effektiv zu handeln.

In Bezug auf zukünftige Herausforderungen wird die Notwendigkeit einer verbesserten Informationsgewinnung und -teilung hervorgehoben. Cieslik betont die Bedeutung interorganisationaler Kooperationen und fortschrittlicher Kommunikationstechnologien, um einen Informationsvorsprung zu erzielen, der präzisere und schnellere Entscheidungen in Krisensituationen ermöglicht.

Abschließend vermittelt das Interview mit Michael Cieslik, wie durch die Kombination aus strategischer Flexibilität, der gezielten Nutzung digitaler Technologien, einer Kultur der kontinuierlichen Verbesserung und einer starken Ausrichtung auf HRO-Prinzipien ein hochwirksames Krisenmanagement in einem Sektor kritischer Infrastruktur gestaltet werden kann. Diese Elemente stärken wesentlich die Resilienz urbaner Verkehrssysteme gegenüber einer Vielzahl von Bedrohungsszenarien.

8.2.9 Interview Günter Rattei

Seit den frühen 2000er Jahren implementiert die ASFINAG ein Krisenmanagement, das fortlaufend aktualisiert und den modernen Anforderungen angepasst wird. Es existiert ein Krisenhandbuch, das grundlegende Strukturen festlegt und rund 30 spezifische Szenarien für den Krisenfall definiert. Diese Strukturen befinden sich in einem kontinuierlichen Überarbeitungsprozess, um bestimmte Funktionen des traditionellen Krisenmanagements zu konsolidieren und die Effizienz zu steigern.

Digitale Technologien nehmen eine zentrale Rolle im Krisenmanagement der ASFINAG ein. Die Entwicklung hat sich von einem überwiegend papierbasierten System zu einer hochintegrierten digitalen Plattform entwickelt, die auf Microsoft Teams basiert. Dieses System ermöglicht eine effektive und effiziente Kommunikation und Koordination zwischen den Mitarbeitern, unabhängig von deren physischen Standorten. Die digitale Transformation wurde durch die praktischen Erfahrungen

und Lernprozesse während der COVID-19-Pandemie erheblich beschleunigt und hat zu einer nahezu vollständigen Digitalisierung des Krisenmanagements geführt.

Neben der digitalen Umwandlung wird das Krisenmanagement der ASFINAG durch regelmäßige praktische Übungen und die Einführung einer speziellen Alarmierungssoftware weiter optimiert. Diese regelmäßigen Übungen sind entscheidend, um die Reaktionsgeschwindigkeit und die Effizienz der Krisenstäbe kontinuierlich zu verbessern, und sie werden von externen Beratern evaluiert, um konstruktives Feedback für zukünftige Verbesserungen zu gewinnen.

Die Einhaltung gesetzlicher und regulatorischer Vorgaben nimmt einen hohen Stellenwert ein, da die ASFINAG als staatlicher Betreiber kritischer Infrastrukturen fungiert. Die sorgfältige Beachtung und Umsetzung von Gesetzen und Richtlinien, wie beispielsweise der NIS-Richtlinie, ist für die Organisation von hoher Bedeutung, um Compliance und rechtliche Sicherheit zu gewährleisten.

Die interne Kommunikation innerhalb des Krisenmanagements wird durch eine Reduktion der beteiligten Personen und den gezielten Einsatz von Teams und spezifischen Kommunikationstechnologien strategisch verbessert. Dabei wird besonderer Wert auf die Berücksichtigung kultureller und regionaler Unterschiede innerhalb Österreichs gelegt, um die Kommunikationseffizienz zu maximieren und Missverständnisse zu vermeiden.

Abschließend wird die psychische und physische Belastung der Mitarbeiter während und nach Krisensituationen intensiv thematisiert. Seit der Corona-Pandemie bietet die ASFINAG umfassende psychologische Unterstützung für alle Mitarbeiter an, um die psychische Widerstandsfähigkeit des Personals zu stärken und die langfristige Leistungsfähigkeit des Krisenmanagements zu sichern. Diese Maßnahmen sind ein zentraler Bestandteil der Personalstrategie, um sicherzustellen, dass das Team auch unter extremen Bedingungen effektiv funktionieren kann.

8.2.10 Interview Experte Energiewirtschaft (AUT)

Der Experte unterstreicht die Bedeutung eines stabilen, standardisierten Organisationskerns, der es ermöglicht, in Krisenzeiten effektiv eine große Menge an Informationen schnell zu verarbeiten. Hierfür werden zwei primäre Stabsmodelle eingesetzt: ein vollständig besetzter Stab sowie ein stark reduzierter Stab. Diese Modelle können je nach der spezifischen Situation und den Anforderungen der Krise flexibel angepasst werden.

Ein wesentlicher Diskussionspunkt im Interview ist die Notwendigkeit von Anpassungsfähigkeit und Flexibilität im Krisenmanagement. Der Experte betont, dass durch einfache und standardisierte Modelle die schnelle Reaktionsfähigkeit von Organisationen unterstützt wird. Die Ausbildung der Krisenmanagementteams wird als kritisch für die effektive Reaktion auf Krisen angesehen. Es wird hervorgehoben, dass die Verwendung von Rollenblättern und Checklisten, die keine festen Szenarien vorgeben, sondern als flexible Handlungsleitlinien in Krisensituationen dienen, zentral für die Effizienz der Stabsarbeit ist.

Digitale Technologien spielen eine zunehmend wichtige Rolle im Krisenmanagement. Der Interviewte stellt fest, dass technologische Lösungen, insbesondere speziell entwickelte Software für Krisenmanagement und regelmäßige Lageberichte, die Kommunikation und Informationsverteilung wesentlich effizienter gestalten. Diese Technologien haben nicht nur die Reaktionsfähigkeit verbessert, sondern auch die Prozesse optimiert, indem sie eine kontinuierliche und schnelle Informationsverteilung ermöglichen.

Ein weiterer wichtiger Aspekt, der im Interview diskutiert wird, ist das Management von Stakeholdern, insbesondere in Krisenzeiten. Der Experte erläutert einen systematischen Ansatz, bei dem jede Unternehmenseinheit spezifische Richtlinien für die Kommunikation mit Stakeholdern besitzt. Diese Richtlinien ermöglichen eine schnelle und koordinierte Verbreitung von Informationen und stellen sicher, dass alle relevanten Parteien effizient informiert werden.

Zusätzlich werden Feedback und Verbesserungen, die aus regelmäßigen Krisenübungen gewonnen werden, als essenziell für die kontinuierliche Verbesserung der Krisenmanagementpraktiken angesehen. Diese Übungen ermöglichen es der Organisation, die Effektivität der umgesetzten Maßnahmen regelmäßig zu bewerten und anzupassen.

Zusammenfassend hebt das Interview die zentrale Bedeutung einer soliden Ausbildung, standardisierter Prozesse und der Anpassungsfähigkeit im Krisenmanagement hervor. Diese Elemente fördern die organisatorische Flexibilität und ermöglichen eine effektive Reaktion in Krisensituationen. Die Integration von Digitalisierung und ein strategisch durchdachtes Stakeholdermanagement sind entscheidend für die moderne Krisenbewältigung. Diese Faktoren spielen eine entscheidende Rolle in der Entwicklung und Umsetzung von effektiven Krisenmanagementstrategien in kritischen Infrastruktursektoren.

8.2.11 Interview Roland Pachtner

Pachtner hebt hervor, dass die Einführung eines umfassenden Krisenmanagements eine wesentliche Neuerung in seiner Abteilung darstellte, welche zuvor keine strukturierte Handhabung solcher Situationen kannte. Er illustriert den sorgfältigen Prozess des Aufbaus eines Krisenmanagementsystems, das auf den langjährigen Erfahrungen der Feuerwehr aufbaut und regelmäßig aktualisiert wird. Ein zentrales Element dabei ist das Krisenhandbuch, welches nun für alle Unternehmensbereiche gültig ist und klare Anweisungen für den Aufbau der Krisenorganisation und die Bildung eines Krisenstabs enthält.

Ein wesentlicher Aspekt des neu gestalteten Krisenmanagements ist die Orientierung an dem SKKM-Modell (Staatliches Krisen- und Katastrophenmanagement), welches in Österreich weit verbreitet ist und als Grundlage für die Strukturierung des Krisenmanagements am Flughafen dient. Pachtner betont die Wichtigkeit der Anpassung dieses Modells an die spezifischen Bedürfnisse und Gegebenheiten des Flughafens, was durch die Zusammenarbeit mit externen Beratungsfirmen unterstützt wird, die ein modifiziertes Modell vorgeschlagen haben, das kompakter ist und digitale Möglichkeiten integriert.

Die Digitalisierung spielt eine zunehmend wichtige Rolle im Krisenmanagement. Obwohl Pachtner eine Präferenz für traditionelle Methoden wie Papier und Bleistift äußert, erkennt er den Nutzen digitaler Technologien zur Steigerung der Effizienz, insbesondere im Bereich der Alarmierung und Kommunikation. Der Einsatz digitaler Tools beginnt mit einfachen Alarmierungssystemen und erstreckt sich bis zu umfassenden Informationssystemen, die eine effiziente Informationsverteilung und Teilnahme an Krisenmeetings ermöglichen.

Des weiteren wird die Einbindung von internen und externen Stakeholdern als entscheidend für ein wirksames Krisenmanagement hervorgehoben. Pachtner beschreibt, wie die Flughafen Wien AG durch die aktive Integration von relevanten Geschäftsbereichen und die Zusammenarbeit mit Schlüsselkunden wie Fluglinien, Polizei und anderen Organisationen eine robuste Vernetzung und Koordination in Krisensituationen sicherstellt.

Die kontinuierliche Verbesserung der Krisenmanagementfähigkeiten durch Schulungen und regelmäßige Übungen wird als essenziell betrachtet. Pachtner misst den Erfolg dieser Maßnahmen an der positiven Rückmeldung der Mitarbeiter, die sich nach den Schulungen sicherer in ihren Rollen fühlen und die Abläufe und Strukturen des Krisenmanagements besser verstehen.

Schließlich wird die psychologische Unterstützung für die Mitarbeiter als ein kritischer Aspekt betont. Pachtner erläutert, dass umfassende Betreuungsangebote vorhanden sind, die Mitarbeiter*innen helfen, sowohl berufliche als auch private Herausforderungen zu bewältigen. Diese Unterstützung ist integraler Bestandteil des Krisenmanagements, um sicherzustellen, dass die Mitarbeiter im Ernstfall effektiv und ohne übermäßige Angst handeln können.

Das Interview mit Roland Pachtner bietet Einblicke in die Implementierung eines effektiven und strukturierten Krisenmanagements am Flughafen Wien. Er erklärt, wie ein an das österreichische SKKM-Modell angelehntes Krisenmanagement entwickelt wurde, das speziell auf die Bedürfnisse des Flughafens zugeschnitten und durch digitale Technologien ergänzt wurde, um Effizienz und Reaktionsfähigkeit zu steigern. Diese Maßnahmen zeigen, dass das Krisenmanagement sowohl auf bewährten Modellen basiert als auch innovative Ansätze integriert, um internationale Standards zu erfüllen.

8.2.12 Interview Manuel Schwarzeneker

Im Interview erläutert Schwarzeneker die wesentlichen Aspekte des Krisenmanagements und die Anpassungsfähigkeit der Organisation. Er beschreibt, dass das Krisenmanagementsystem zwar feste Prozesse und Anforderungen enthält, jedoch flexibel genug ist, um auf verschiedene Szenarien angemessen reagieren zu können. Die COVID-19-Pandemie habe gezeigt, dass das System schnell auf neue Herausforderungen reagieren kann.

Das Krisenmanagementsystem basiert auf den Vorgaben der Sozialversicherung und den Sicherheitsrichtlinien des Dachverbands. Es orientierte sich ursprünglich am SKKM-Modell, wurde jedoch aufgrund der Erfahrungen aus der Pandemie angepasst.

In der Hauptstelle und der Landesstelle wurden neue Modelle etabliert, die spezifische Rollen wie „Personal“ und „Lage“ definieren.

Digitale Technologien werden derzeit im Krisenmanagement nicht eingesetzt, Stattdessen werden klassische Methoden mit Papier und Stift verwendet.

Um die Effizienz der Stabsarbeit zu verbessern, wurde der Krisenstab neu strukturiert und verschlankt, wobei einige Rollen redundant besetzt wurden, um flexible Unterstützung zu gewährleisten. Der Erfolg dieser Maßnahmen wird durch Feedbackschleifen, einschließlich Rückmeldungen von BC Consulting und einer Übung im April, bewertet.

Bezüglich der Prinzipien hochzuverlässiger Organisationen (HRO) gibt Schwarzeneker an, dass diese Prinzipien teilweise unbewusst umgesetzt werden. Dazu zählen Sensibilität für betriebliche Abläufe, Abneigung gegen Vereinfachung, Streben nach Flexibilität und Respekt vor der Expertise. Er betont die Notwendigkeit von Redundanzen und die Entwicklung von Notfallplänen, insbesondere im Hinblick auf potenzielle Blackout-Szenarien.

Die Einbindung von Stakeholdern in die Krisenstabsarbeit erfolgt über die Selbstverwaltungsstruktur der Sozialversicherung, die Arbeitgeber und Arbeitnehmer umfasst. Externe Beratung und Zusammenarbeit mit anderen Institutionen, wie Krankenhäusern und Rettungsorganisationen, sind ebenfalls wesentliche Bestandteile.

Feedback wird systematisch durch intensive Feedbackschleifen nach Schulungen und Übungen gesammelt und in die Verbesserung der Notfallpläne integriert. Die Organisation setzt auf kontinuierliches Lernen und Verbessern, um die Effizienz des Krisenmanagements zu steigern.

Im Bereich der Cybersicherheit wird auf Papierform gesetzt, um unabhängig von IT-Systemen zu bleiben. Ein IT-Notfallteam und ein Chief Information Security Officer sorgen für die Abdeckung von Cyber-Themen und die Entwicklung geordneter Strategien für Cyberszenarien.

Gesetzliche Anforderungen und regulative Vorgaben werden durch die Sicherheitsrichtlinie der Sozialversicherung vorgegeben und kontinuierlich an neue Gesetze angepasst, wie beispielsweise die Umsetzung von NIS-2.

Die Kommunikation und Teamarbeit im Krisenstab funktionieren gut, wobei Informationen offen und schnell geteilt werden. Psychische und physische Belastungen der Mitarbeiterinnen und Mitarbeiter werden durch eine betriebliche Arbeitspsychologin und die Möglichkeit zur Rücksprache mit dem Krisenstab oder Leitungsstab gemonitort und bewältigt.

Schwarzeneker sieht Blackout-Szenarien und den Klimawandel als große Herausforderungen für das zukünftige Krisenmanagement. Insbesondere exponierte Lagen der Rehazentren und potenzielle Kundenkonflikte in der Landesstelle Wien werden als spezifische Risiken identifiziert. Ein neuer Einsatzstab für die Landesstelle Wien soll gezielt auf diese Herausforderungen vorbereitet werden.

8.3 Diskussion der Interviews

In diesem Kapitel werden die Ergebnisse der Interviews und des Onlinefragebogens zusammengefasst, interpretiert und gegenübergestellt. Durch die Verbindung von Interviews und Befragung wurde ein umfassendes Bild aus dem Bereich des Krisenmanagements innerhalb kritischer Infrastrukturen erstellt.

Im Zentrum der Diskussion stehen die zentralen Themen und Forschungsfragen dieser Arbeit: die Struktur und Flexibilität des Krisenmanagements, die Integration digitaler Technologien, die Einbindung von Stakeholdern sowie die Bewältigung von physischen und psychischen Belastungen der Mitarbeiter. Besonders wird darauf eingegangen, wie die Prinzipien der Hochzuverlässigkeitsorganisationen (HRO) in der Praxis angewendet werden und welche Herausforderungen und Chancen sich dabei ergeben.

Ein weiterer wichtiger Aspekt der Diskussion ist die Rolle der Digitalisierung im Krisenmanagement. Es wird untersucht, wie digitale Technologien die Effizienz und Reaktionsfähigkeit verbessern und welche Lösungen bereits erfolgreich implementiert wurden. Zudem wird analysiert, wie gesetzliche Anforderungen und Normen in den Organisationen umgesetzt und überwacht werden, um Compliance und Resilienz zu gewährleisten.

Die Diskussion reflektiert nicht nur die gewonnenen Erkenntnisse, sondern zeigt auch mögliche Implikationen für die Praxis auf. Handlungsempfehlungen für die Zukunft des Krisenmanagements werden aufgezeigt, basierend auf den vielfältigen Erfahrungen und Einsichten der befragten Experten. Ziel ist es, durch die kritische Auseinandersetzung mit den Interviews wertvolle Beiträge zur Weiterentwicklung des Krisenmanagements in kritischen Infrastrukturen zu leisten.

Ein zentraler Aspekt, der in allen Interviews hervorgehoben wird, ist die Notwendigkeit einer klar definierten Struktur innerhalb des Krisenmanagements. Alle befragten Experten betonen die Bedeutung einer präzisen Festlegung von Rollen und Verantwortlichkeiten, um im Krisenfall schnell und effizient handeln zu können. Dabei spielt die Einrichtung eines Krisenstabs eine wesentliche Rolle, der aus Mitgliedern verschiedener Abteilungen besteht. Dieser interdisziplinäre Ansatz gewährleistet, dass unterschiedliche Perspektiven und Fachkenntnisse in die Entscheidungsprozesse einfließen, wodurch eine umfassende Bewältigung der Krise ermöglicht wird.

Ein weiterer gemeinsamer Punkt ist die Betonung der Flexibilität und Anpassungsfähigkeit der Krisenmanagementsysteme. Alle Experten hoben hervor, dass feste Strukturen wichtig sind, das System jedoch in der Lage sein muss, sich schnell an neue Informationen und veränderte Bedingungen anzupassen. Dies erfordert regelmäßige Überprüfungen und Aktualisierungen der bestehenden Prozesse und Protokolle. Die Fähigkeit zur Improvisation und zur schnellen Entscheidungsfindung wurde als entscheidend für den Erfolg in Krisensituationen angesehen.

In den meisten befragten Organisationen ist die HRO-Theorie bekannt und wird als wertvolles Instrument zur Verbesserung der Krisenbewältigung angesehen.

Insbesondere die Prinzipien der Fehlervermeidung, Fehlertoleranz und die Schaffung einer Kultur der Achtsamkeit. Einige Organisationen haben Maßnahmen implementiert, um diese Prinzipien zu fördern. Beispielsweise berichteten Experten, dass regelmäßige Schulungen und Übungen durchgeführt werden, um Mitarbeiter für potenzielle Fehlerquellen zu sensibilisieren und eine offene Fehlerkultur zu etablieren. Diese Schulungen zielen darauf ab, die Aufmerksamkeit auf Details zu lenken und Mitarbeiter zu ermutigen, Fehler frühzeitig zu erkennen und zu melden.

Ein weiterer zentraler Aspekt der HRO-Theorie, der in den Interviews angesprochen wurde, ist die Resilienz und Anpassungsfähigkeit der Organisationen. Die HRO-Theorie betont die Notwendigkeit, flexibel auf unvorhergesehene Ereignisse reagieren zu können und kontinuierlich aus Erfahrungen zu lernen. Viele Organisationen haben diese Prinzipien erkannt und in ihre Krisenmanagementprozesse integriert. Nach Übungen und realen Einsätzen finden Nachbesprechungen und Evaluierungen, gemeinsam mit Beobachtern, statt, um Lehren zu ziehen und Verbesserungen vorzunehmen. Diese Praxis der kontinuierlichen Verbesserung ist ein wesentliches Element der HRO-Theorie und wird in den meisten befragten Organisationen angewendet.

Zusammenfassend lässt sich feststellen, dass die HRO-Theorie und ihre Prinzipien in den meisten befragten Organisationen bekannt sind. Die Umsetzung und Integration dieser Prinzipien variiert stark und erfolgt unbewusst.

Die Wichtigkeit der Einbindung von Stakeholdern wird von allen befragten Experten bestätigt.

Sie betonen, dass die Zusammenarbeit mit externen und internen Stakeholdern entscheidend für eine effektive Krisenbewältigung ist. Stakeholder umfassen eine Vielzahl von Akteuren, darunter Behörden, andere Unternehmen, Notfallorganisationen und die Öffentlichkeit.

Die systematische Einbindung von Stakeholdern variiert jedoch zwischen den Organisationen. Während einige Organisationen, wie der Flughafen Wien und Teile der Energiebranche formalisierte Schulungsprogramme und regelmäßige Übungen zur Einbindung von Stakeholdern durchführen, ist dies bei anderen Organisationen weniger systemisch ausgeprägt. In der Pensionsversicherung beispielsweise wird die Zusammenarbeit mit Stakeholdern als wichtig erkannt, jedoch erfolgt die Einbindung oft informeller und weniger systematisch. Hier liegt der Fokus eher auf der praktischen Zusammenarbeit im Rahmen von Krisenereignissen, ohne dass spezifische Schulungsprogramme zur Stakeholder-Einbindung existieren.

Ein weiterer zentraler Punkt, der in den Interviews hervorgehoben wird, ist die Rolle der Kommunikation. Effektive Kommunikation mit Stakeholdern wird als wesentlich für das Krisenmanagement angesehen. Viele Organisationen haben Kommunikationspläne entwickelt, um sicherzustellen, dass im Krisenfall alle relevanten Informationen schnell und klar übermittelt werden.

Zusammenfassend lässt sich feststellen, dass die Einbindung von Stakeholdern im Krisenmanagement von allen befragten Organisationen als wichtig anerkannt wird. Die Ansätze und Praktiken variieren jedoch erheblich. Während einige Organisationen

formalisierte Systeme und Schulungsprogramme zur Einbindung von Stakeholdern implementiert haben, setzen andere auf informellere und weniger systematische Ansätze. Diese Unterschiede verdeutlichen die Notwendigkeit, die Prinzipien der Stakeholder-Einbindung an die spezifischen Bedingungen und Anforderungen jeder Organisation anzupassen, um eine effektive und nachhaltige Krisenbewältigung zu gewährleisten.

Ein zentrales Thema, das von den meisten Experten angesprochen wurde, ist die wachsende Bedeutung der Cybersicherheit im Krisenmanagement. Alle befragten Organisationen erkennen die Notwendigkeit an, sich gegen digitale Bedrohungen abzusichern.

Die Organisationen haben spezifische Maßnahmen implementiert, um ihre digitalen Infrastrukturen zu schützen und auf Cyberangriffe vorbereitet zu sein. Die Schulungen umfassen sowohl theoretische als auch praktische Komponenten, um sicherzustellen, dass die Prinzipien der Cybersicherheit nicht nur verstanden, sondern auch effektiv angewendet werden können.

Ein weiterer zentraler Aspekt, der in den Interviews hervorgehoben wurde, ist die Rolle der kontinuierlichen Verbesserung und Anpassung der Cybersicherheitsstrategien. Die Organisationen erkennen die Notwendigkeit, ihre Cybersicherheitsmaßnahmen regelmäßig zu überprüfen und anzupassen, um neuen Bedrohungen und Entwicklungen im digitalen Bereich gerecht zu werden.

Die Unterschiede in der Umsetzung der Cybersicherheitsstrategien sind auf die spezifischen Bedingungen der jeweiligen Organisationen zurückzuführen.

Im Zuge der Interviews stellten die Experten unterschiedliche Methoden zur Lageführung im Krisenstab dar.

Eine Variante der Lageführung im Krisenstab erfolgt durch ein strukturiertes und hierarchisches System, das auf digitale Technologien setzt. Digitale Kommunikationsplattformen und Echtzeitüberwachungssysteme ermöglichen eine schnelle und effiziente Verteilung von Informationen sowie eine koordinierte Reaktion auf Krisensituationen. Regelmäßige Schulungen und Übungen stellen sicher, dass alle Mitglieder des Krisenstabs die Systeme effektiv nutzen können. Diese Variante zeichnet sich durch klar definierte Rollen und Verantwortlichkeiten aus, was eine effiziente Entscheidungsfindung unterstützt.

Eine weitere Variante nutzt digitale Überwachungssysteme und Datenanalyse-Tools, die eine kontinuierliche Überwachung der Netzwerke und Anlagen ermöglichen. Hier erfolgt die Lageführung durch eine zentrale Leitstelle, die alle relevanten Informationen sammelt und analysiert. Regelmäßige Schulungen im Umgang mit diesen Tools sind entscheidend, um sicherzustellen, dass die Mitarbeiter die Technologien effektiv nutzen können. Digitale Kommunikationsplattformen werden ebenfalls eingesetzt, um die Koordination und den Informationsaustausch zwischen verschiedenen Abteilungen und externen Partnern zu erleichtern.

Eine dritte Variante zeigt einen eher traditionellen Ansatz auf Papier, unterstützt durch grundlegende digitale Werkzeuge wie E-Mail und einfache Datenbanken. Obwohl die

Prinzipien der Digitalisierung bekannt sind, wird weniger auf spezialisierte digitale Technologien zurückgegriffen. Die Lageführung basiert auf etablierten Protokollen und Verfahren, die durch regelmäßige, jedoch weniger formalisierte Schulungen unterstützt werden. Die Zusammenarbeit im Krisenstab erfolgt durch regelmäßige Meetings und den Austausch von Informationen über konventionelle Kommunikationswege.

Eine weitere Variante ist die Kombination aus digitaler und traditioneller Lageführung. Hier werden sowohl fortschrittliche digitale Überwachungssysteme als auch traditionelle Kommunikationsmittel verwendet. Diese Hybridstrategie ermöglicht eine flexible und vielseitige Reaktion auf Krisensituationen. Schulungen und Übungen sind darauf ausgelegt, die Mitarbeiter sowohl im Umgang mit modernen Technologien als auch mit traditionellen Methoden zu schulen.

Die Experteninterviews zeigen eine Vielzahl von Ansätzen und Herausforderungen im zukünftigen Krisenmanagement, wobei die Digitalisierung und die damit verbundenen Cyberbedrohungen als eine der größten Herausforderungen hervorgehoben wurden. Die Experten betonen die Notwendigkeit, digitale Sicherheitsmaßnahmen zu verstärken und die Mitarbeiter im Umgang mit neuen Technologien zu schulen. Die Prinzipien der Cybersecurity werden in den meisten Organisationen anerkannt, doch die kontinuierliche Schulung und Verbesserung der Fähigkeiten in diesem Bereich bleiben entscheidende Faktoren.

Ein weiteres gemeinsames Thema in den Interviews ist die Notwendigkeit, die Resilienz der Organisationen zu stärken. Die Experten betonen, dass die Fähigkeit, sich schnell von Krisen zu erholen und die Geschäftskontinuität aufrechtzuerhalten, immer wichtiger wird. Dies erfordert nicht nur robuste Krisenmanagementpläne, sondern auch die kontinuierliche Schulung und Anpassung dieser Pläne an neue Bedrohungen. Regelmäßige Übungen und Schulungen werden genutzt, um die Mitarbeiter auf verschiedene Krisenszenarien vorzubereiten und die organisatorische Resilienz zu erhöhen.

Der Experte aus der Energiebranche hob hervor, dass die Integration erneuerbarer Energien und die damit verbundenen technischen und logistischen Herausforderungen eine bedeutende zukünftige Aufgabe darstellen. Hier wird die Notwendigkeit betont, innovative Technologien zu implementieren und die Mitarbeiter kontinuierlich weiterzubilden, um die Stabilität und Sicherheit des Energienetzes zu gewährleisten.

Ein weiterer trennender Faktor ist der Grad der formalen Strukturierung und der Einsatz von Technologien in den jeweiligen Krisenmanagementsystemen. Während einige Organisationen auf hochstrukturierte und technologiebasierte Ansätze setzen, nutzen andere eher traditionelle Methoden und weniger spezialisierte digitale Werkzeuge. Diese Unterschiede verdeutlichen die Notwendigkeit, die Krisenmanagementstrategien an die spezifischen Bedingungen und Ressourcen der jeweiligen Organisationen anzupassen.

Zusammenfassend lässt sich feststellen, dass die zukünftigen Herausforderungen im Krisenmanagement von allen befragten Organisationen erkannt werden. Die Ansätze

zur Bewältigung dieser Herausforderungen variieren jedoch erheblich. Während einige Organisationen umfassende Schulungsprogramme und formalisierte Protokolle implementiert haben, setzen andere auf weniger strukturierte Ansätze. Diese Unterschiede unterstreichen die Notwendigkeit, die Prinzipien des Krisenmanagements an die spezifischen Bedingungen und Anforderungen jeder Organisation anzupassen, um eine effektive und nachhaltige Bewältigung zukünftiger Krisensituationen zu gewährleisten.

8.4 Ergebnis der Onlinebefragung

Neben den Experteninterviews wurde eine Onlinebefragung von Krisenstabsmitgliedern durchgeführt. Hierfür wurden die Interviewpartner gebeten den Link zur Umfrage an ihre Kolleginnen und Kollegen weiterzuleiten. Von potenziell knapp 180 Personen nahmen 66 Personen an der Onlinebefragung teil. Die Ergebnisse sind prozentuell aufgeschlüsselt. Der Fragebogen befindet sich im Anhang.

8.4.1 Grundlegende Allgemeine Fragen zur Teilnehmer*in

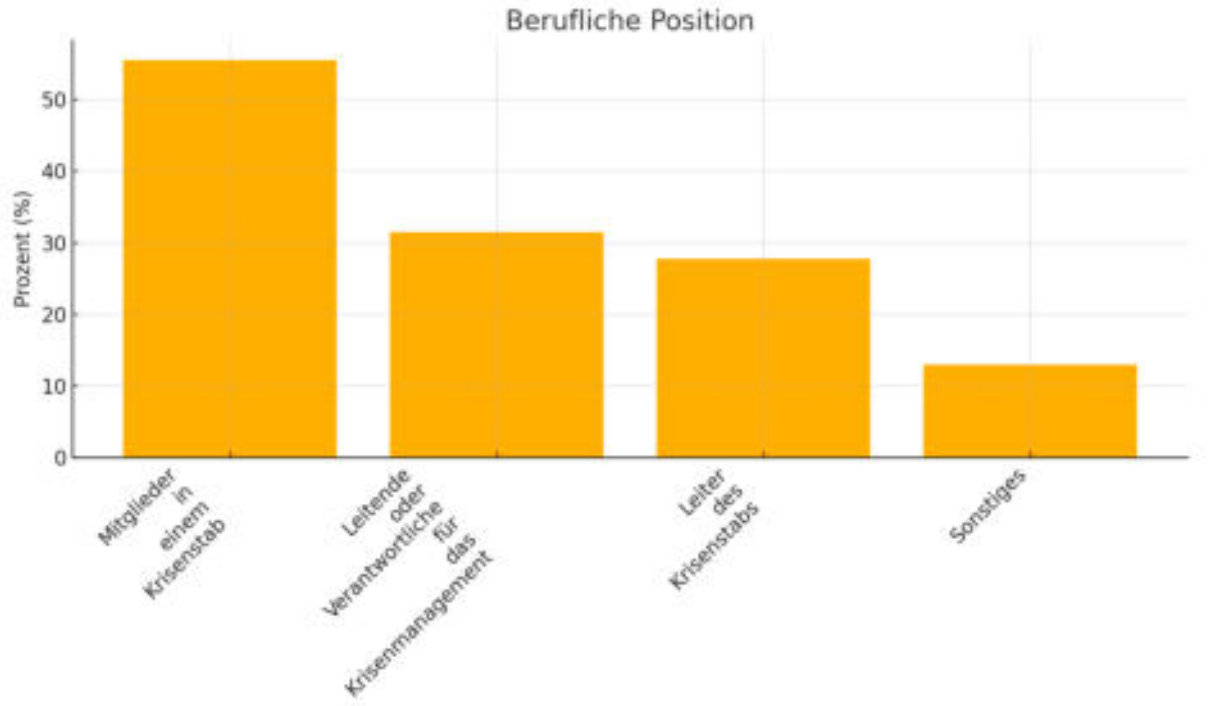


Abbildung 1: Auswertung berufliche Position der Teilnehmer*innen

Unter den knapp 12% der Kategorie fanden sich (interne) Berater, Organisationsmitarbeiter*innen, Bezirksrettungskommandant, Mitglieder und Unterstützende Mitarbeiter*innen im Krisenstab. Es ist davon auszugehen, dass die Kategorisierung Mitglied im Krisenstab nicht für alle Teilnehmer*innen klar und verständlich war. 27,69% gaben an Verantwortlich für das Krisenmanagement zu sein, 24,62% üben die Funktion Leitung Krisenmanagement und 60% der Teilnehmer*innen sind klassische Mitglieder in Krisenstäben.

8.4.2 Alter

Das Durchschnittsalter der Befragten liegt bei 44,37 Jahren mit einer Standardabweichung von 8,74 Jahren. Das Alter reicht von 28 bis 67 Jahren, wobei das untere Quartil bei 38,75 Jahren und das obere Quartil bei 52 Jahren liegt.

Abbildung 2 Auswertung der Sektoren der Teilnehmer*innen

38,89% der Befragten arbeiten im Energiesektor, 20,37% im Gesundheitswesen und ebenfalls 20,37% im Bereich Transport und Verkehr. Weitere 14,81% gehören zu Staat,Verwaltung, während kleinere Anteile in den Sektoren Abwasser und Trinkwasser, Finanzen und Banken sowie digitale Infrastruktur tätig sind.

8.4.3 Digitale Lösungen im Krisenmanagement

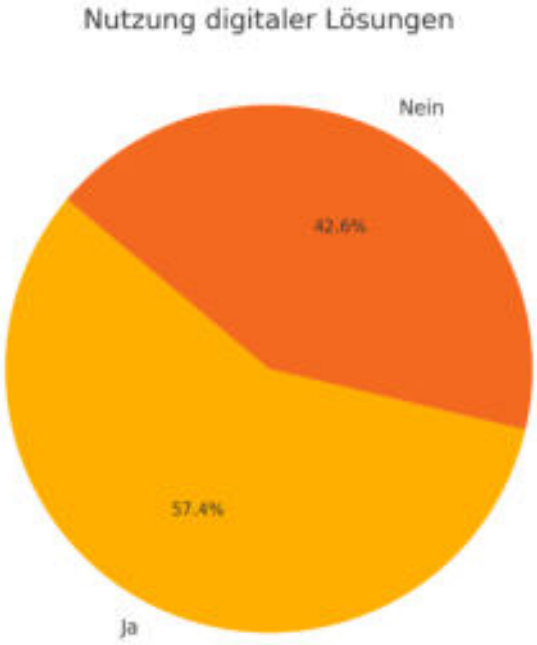


Abbildung 3 Auswertung Nutzung von digitalen Lösungen im Krisenmanagement

57,41% der Befragten geben an, dass ihr Krisenstab digitale Lösungen zur Lageführung nutzt, während 42,59% dies nicht tun.

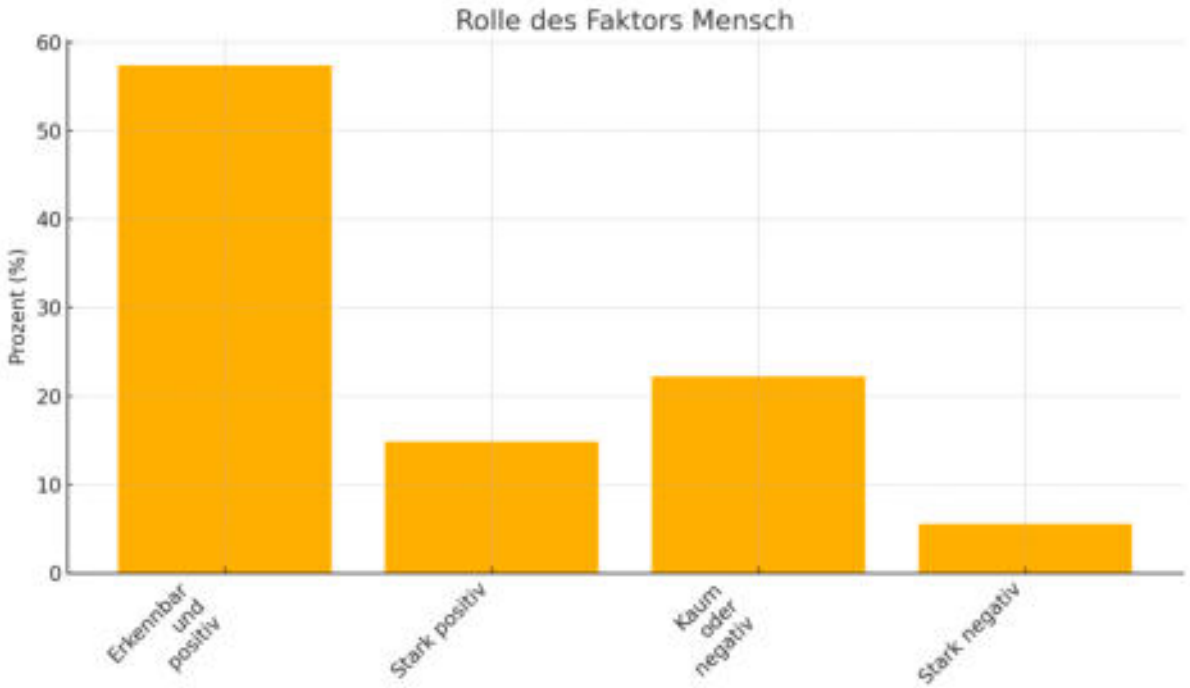


Abbildung 4 Auswertung Rolle Faktor Mensch im Krisenmanagement

Durch die Digitalisierung hat sich die Rolle des Faktors Mensch im Krisenstab bei 57,41% der Befragten erkennbar und positiv verändert. 14,81% berichten von einer

starken positiven Veränderung, während 22,22% kaum oder negative Veränderungen wahrnehmen. 5,56% sehen eine starke negative Veränderung.

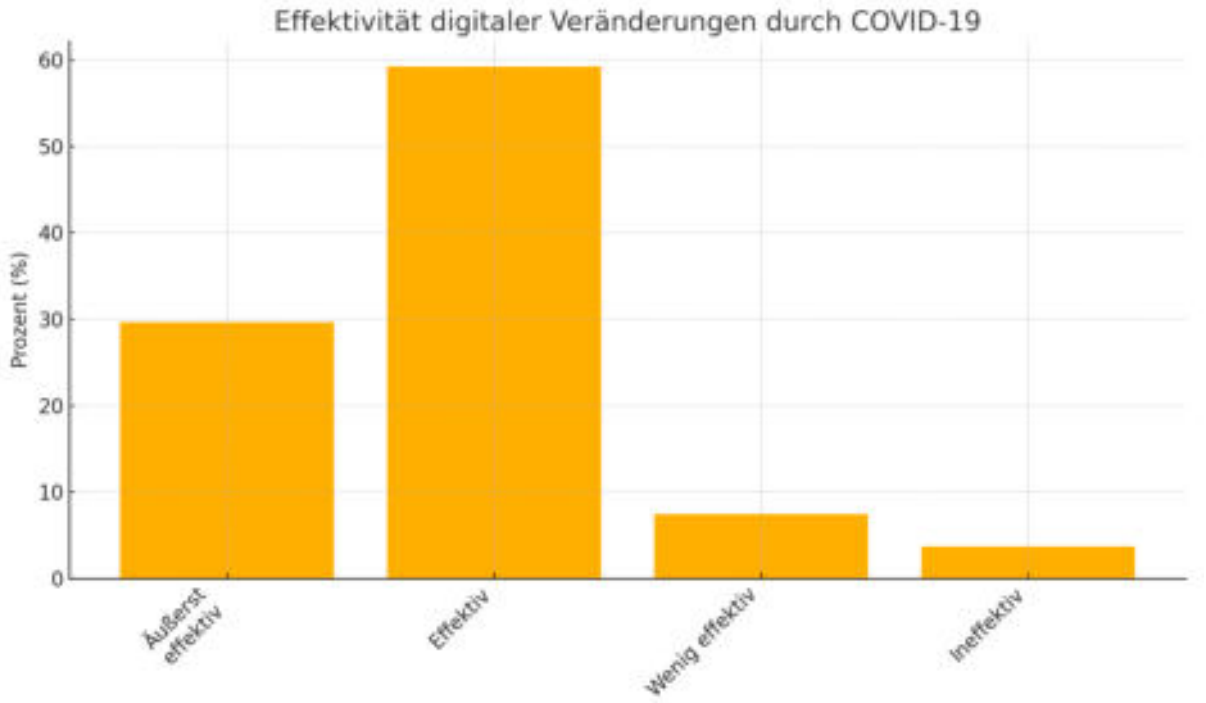


Abbildung 5 Auswertung Effektivität digitaler Veränderungen

29,63% der Befragten bewerten die durch COVID-19 initiierten digitalen Veränderungen als äußerst effektiv. 59,26% sehen die Veränderungen als effektiv an, 7,41% als wenig effektiv, und 3,70% empfinden sie als ineffektiv.

Abbildung 6 Auswertung hinsichtlich organisatorischer Faktoren

16,67% der Befragten sehen keine organisatorischen Hindernisse für die Digitalisierung. 38,89% empfinden nur geringfügige Hindernisse, die leicht überwindbar sind, während ebenfalls 38,89% signifikante Hindernisse wahrnehmen. 5,56% sehen erhebliche Hindernisse, die die Digitalisierung verhindern.

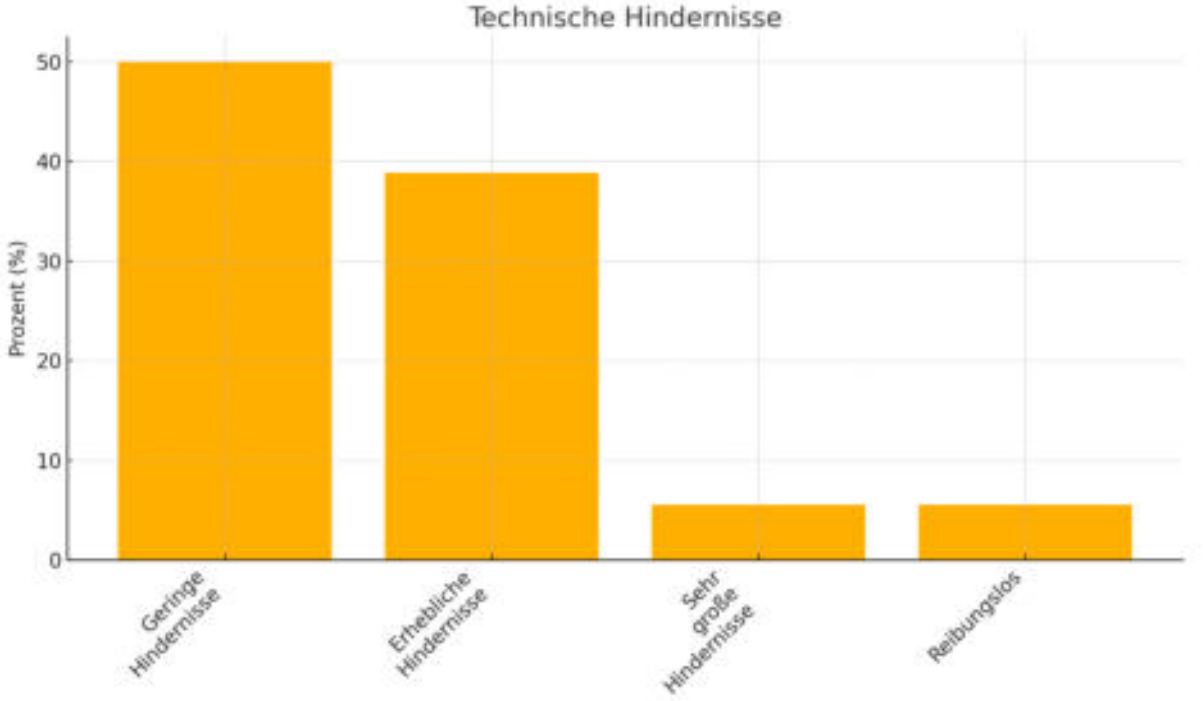


Abbildung 7 Auswertung hinsichtlich technischer Faktoren

50,00% der Befragten berichten von geringen technischen Hindernissen bei der Einführung digitaler Führungs- und Führungsunterstützungssysteme. 38,89% sehen erhebliche technische Hindernisse, und 5,56% erkennen sehr große Hindernisse. Weitere 5,56% erleben eine reibungslose Einführung.

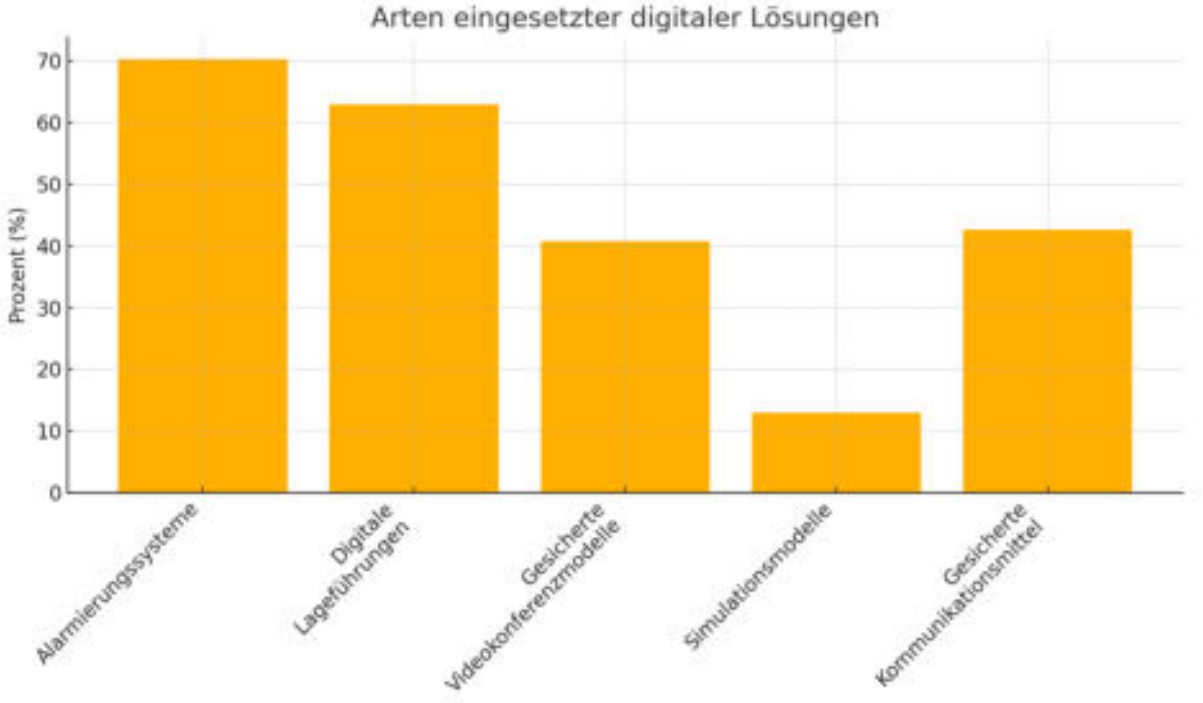


Abbildung 8 Auswertung der verwendeten technologischen Systeme

70,37% der Befragten nutzen Alarmierungssysteme, 62,96% digitale Lageführungen und 40,74% eigene, gesicherte Videokonferenzmodelle. Simulationsmodelle für die Entscheidungsunterstützung werden von 12,96% verwendet, und 42,59% setzen gesicherte und ausfallsichere Kommunikationsmittel ein.

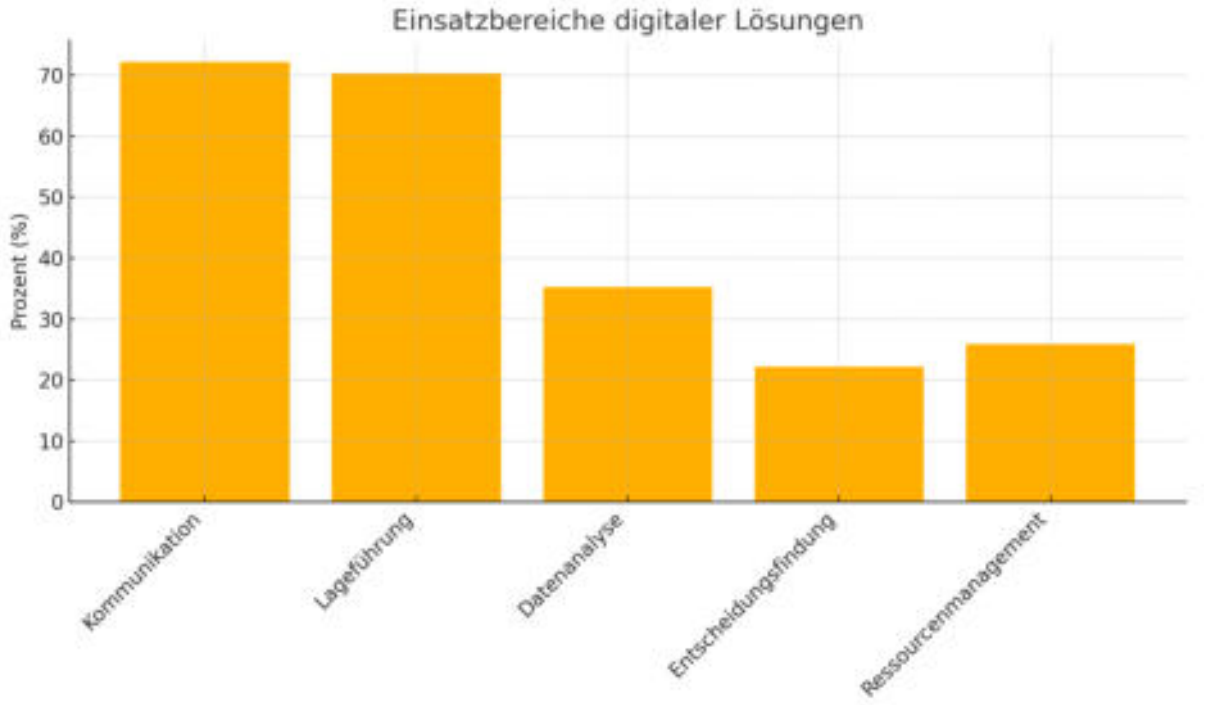


Abbildung 9 Auswertung hinsichtlich Einsatzbereiche digitaler Lösungen

Digitale Lösungen werden hauptsächlich in den Bereichen Kommunikation (72,22%), Lageführung (70,37%), und Datenanalyse (35,19%) eingesetzt. Entscheidungsfindung (22,22%) und Ressourcenmanagement (25,93%) sind ebenfalls relevante Einsatzbereiche.

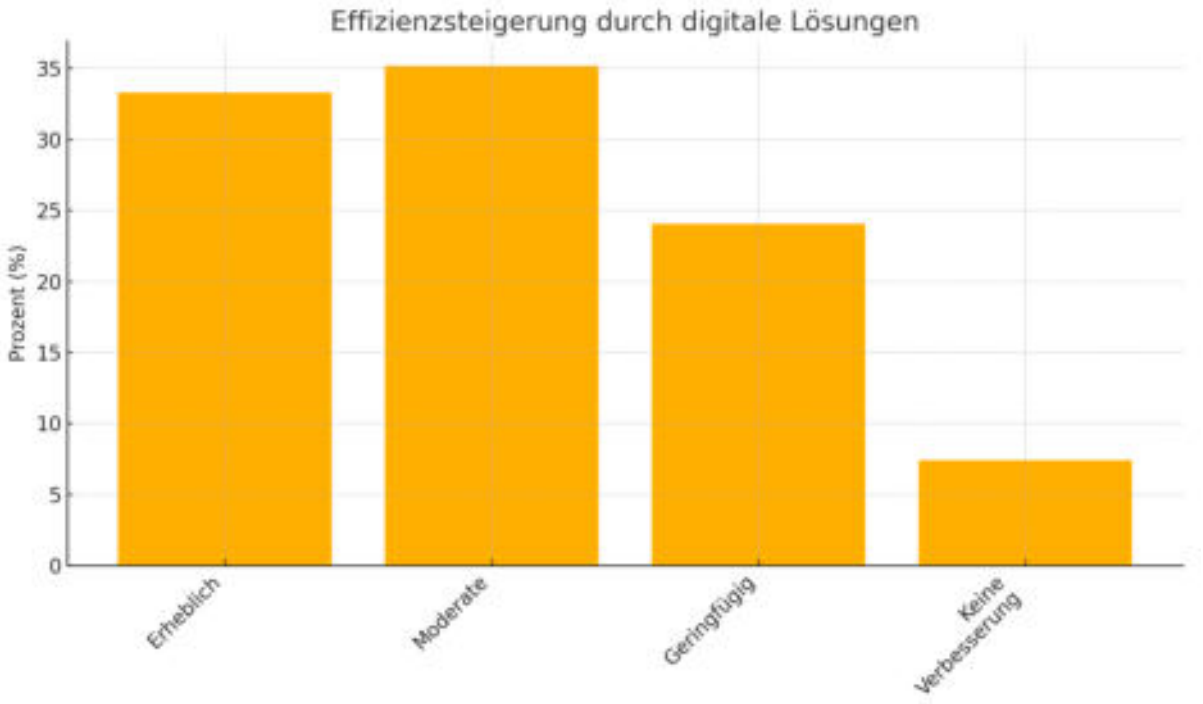


Abbildung 10 Auswertung Verbesserung der Effizenz

33,33% der Befragten geben an, dass digitale Lösungen die Effizienz des Krisenmanagements erheblich gesteigert haben. 35,19% sehen eine moderate Steigerung, während 24,07% nur eine geringfügige Verbesserung wahrnehmen. 7,41% berichten von keiner Verbesserung oder einer Verschlechterung.

8.4.4 Cybersecurity und Informationssicherheit

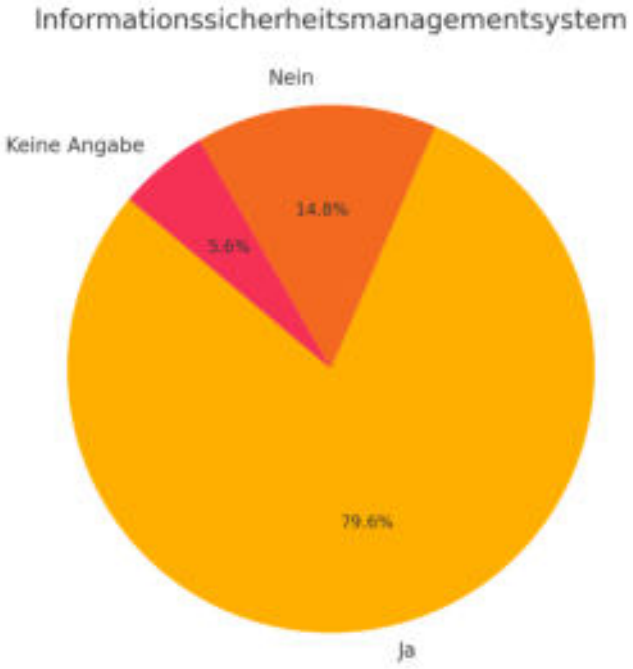


Abbildung 11 Auswertung hinsichtlich Informationssicherheitsmanagementeysteme

79,63% der Organisationen der Befragten betreiben ein Informationssicherheitsmanagementsystem, wie z.B. ISO 27001. 14,81% haben kein solches System, und 5,56% machten keine Angabe.

Abbildung 12 Auswertung Schulungen zu Cybersicherheit

79,63% der Befragten wurden in Bezug auf Cybersicherheit/Informationssicherheit geschult. 20,37% gaben an, keine entsprechende Schulung erhalten zu haben.

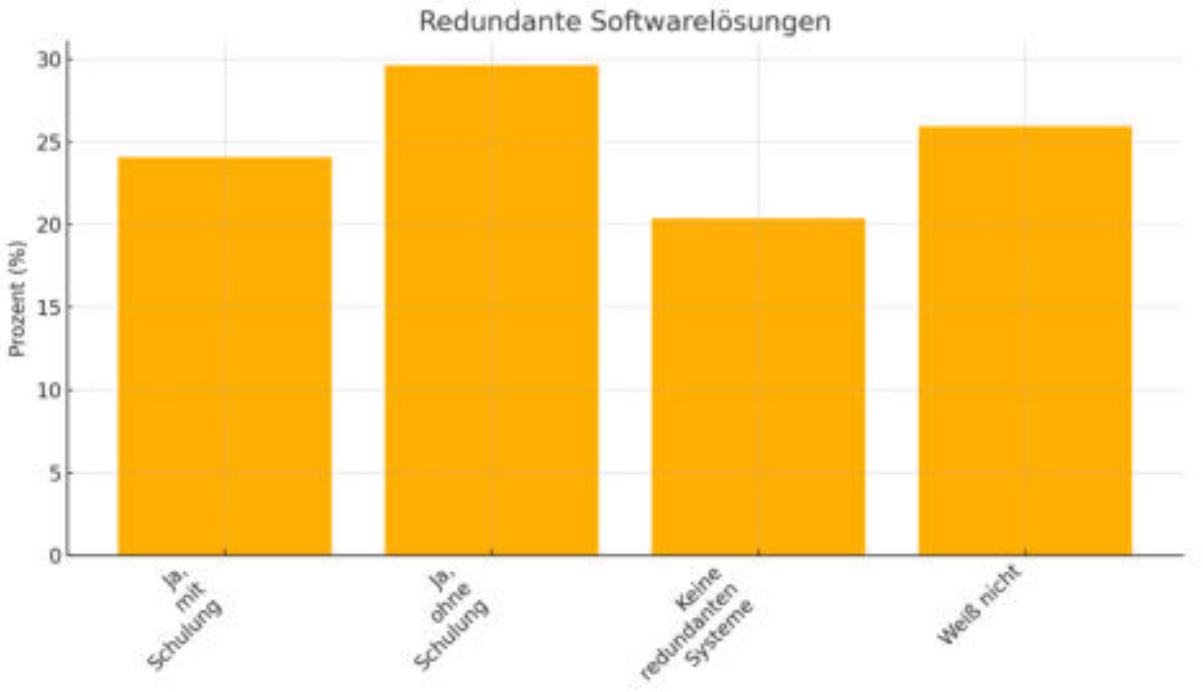


Abbildung 13 Auswertung Redundanz von Softwarelösungen

24,07% der Befragten arbeiten mit redundanten Softwarelösungen und sind darauf geschult, während 29,63% die Softwarelösungen ohne Schulung nutzen. 20,37% haben keine redundanten Systeme, und 25,93% wissen es nicht.

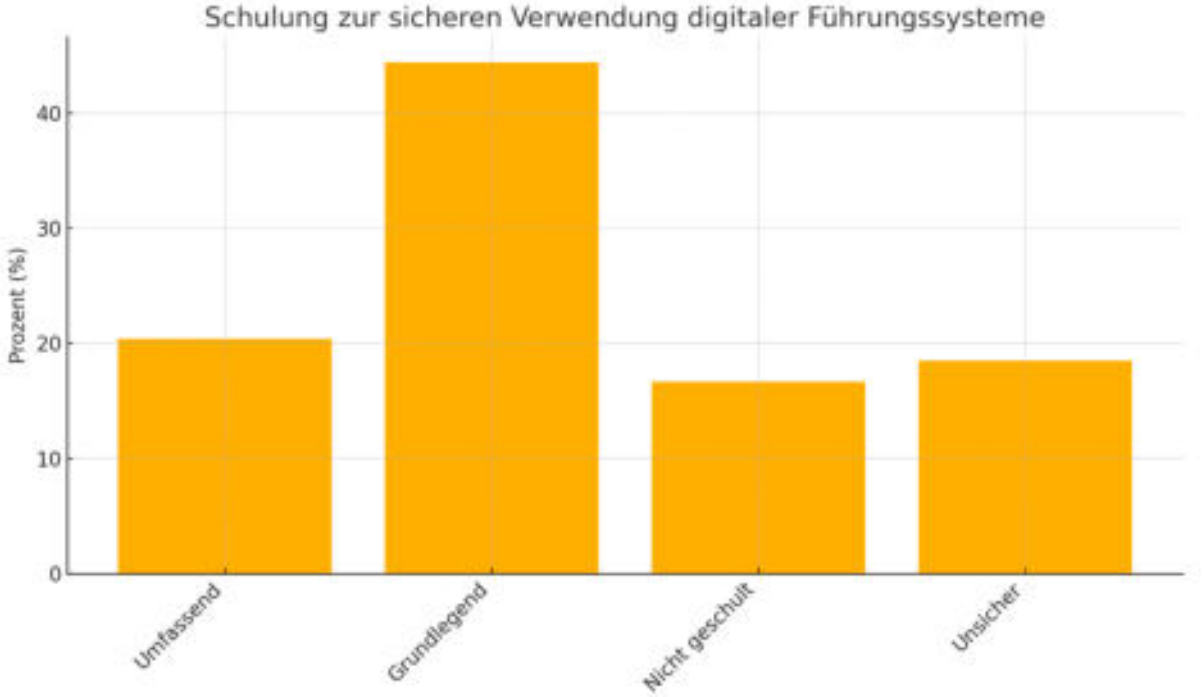


Abbildung 14 Auswertung Schulung zur sicheren Verwendung digitaler Führungssysteme

20,37% der Befragten wurden umfassend in der sicheren Nutzung digitaler Führungssysteme geschult, einschließlich IT-Sicherheitsaspekten. 44,44% erhielten eine grundlegende Schulung ohne spezifische IT-Sicherheitsaspekte. 16,67% wurden nicht geschult, und 18,52% sind sich unsicher.

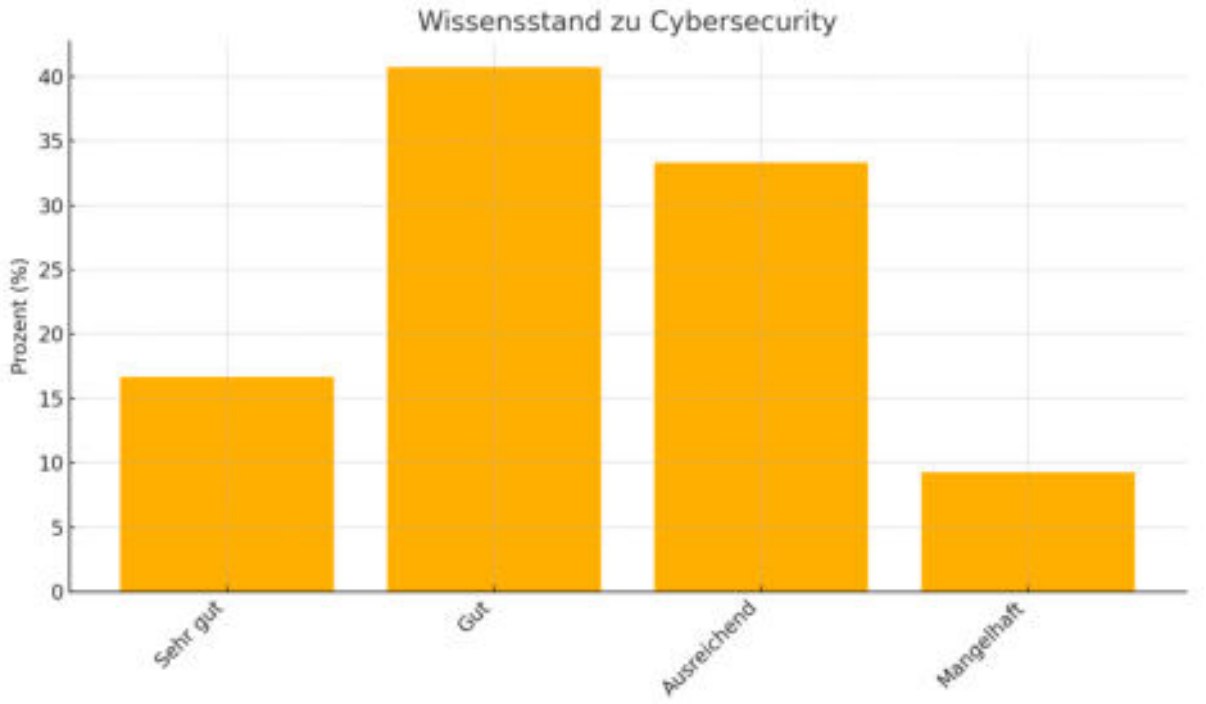


Abbildung 15 Auswertung hinsichtlich Wissen zu Cybersecurity

16,67% der Befragten bewerten ihren Wissensstand als sehr gut, 40,74% als gut, 33,33% als ausreichend und 9,26% als mangelhaft.

8.4.6 HRO-Theorie und Flexibilität

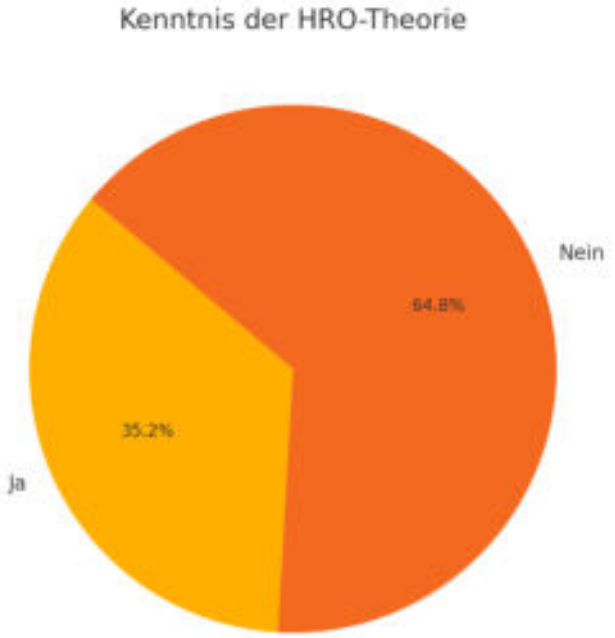


Abbildung 16 Auswertung hinsichtlich Kenntnis der HRO Theorie

35,19% der Befragten ist die Theorie der Hochzuverlässigkeitsorganisationen bekannt. 64,81% kennen diese Theorie nicht.

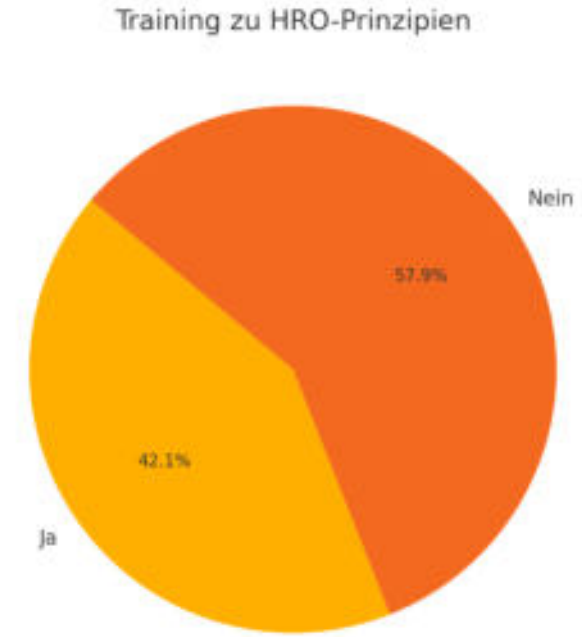


Abbildung 17 Auswertung hinsichtlich Training zu HRO Prinzipien

42,11% der Befragten haben ein Training zu den Grundprinzipien der HRO-Theorie absolviert, während 57,89% dies nicht getan haben. Diese Frage wurde nur jene

Teilnehmer*innen angezeigt, welche Kenntnisse der HRO-Theorie mit „ja“ beantwortet haben.

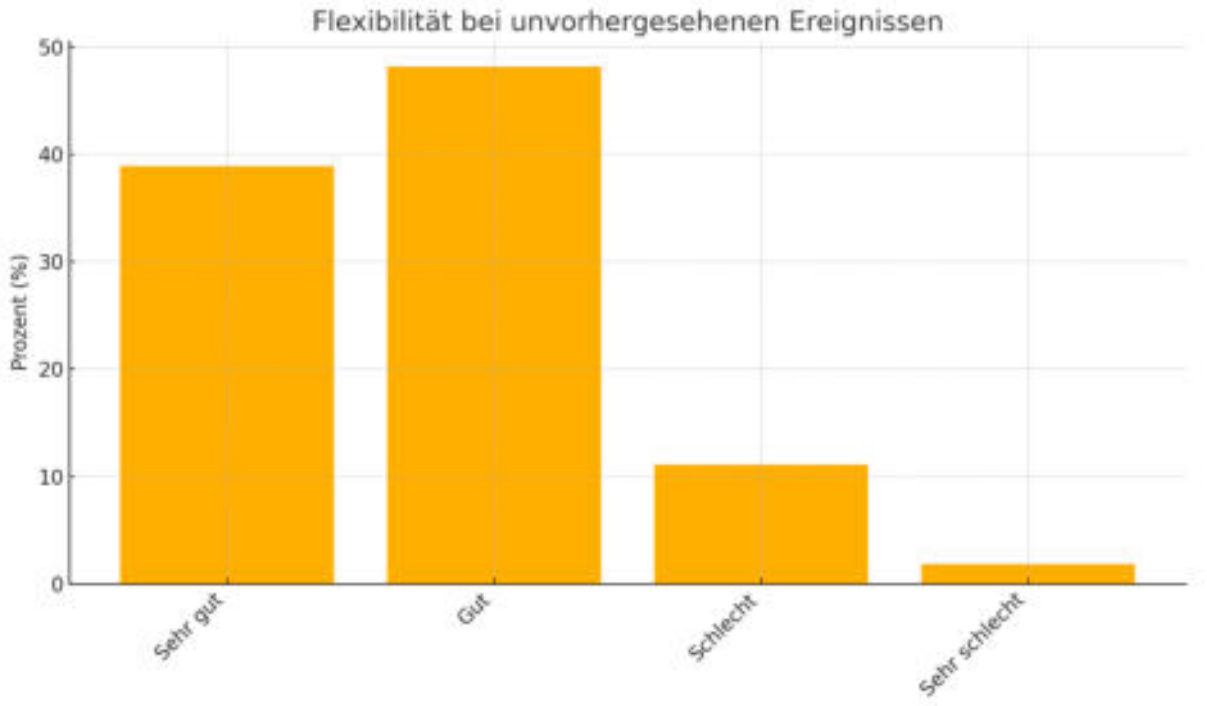


Abbildung 18 Auswertung hinsichtlich Flexibilität hinsichtlich bei unvorhergesehenen Ereignissen

38,89% der Befragten bewerten die Flexibilität ihrer Organisation in solchen Fällen als sehr gut, 48,15% als gut, 11,11% als schlecht und 1,85% als sehr schlecht.

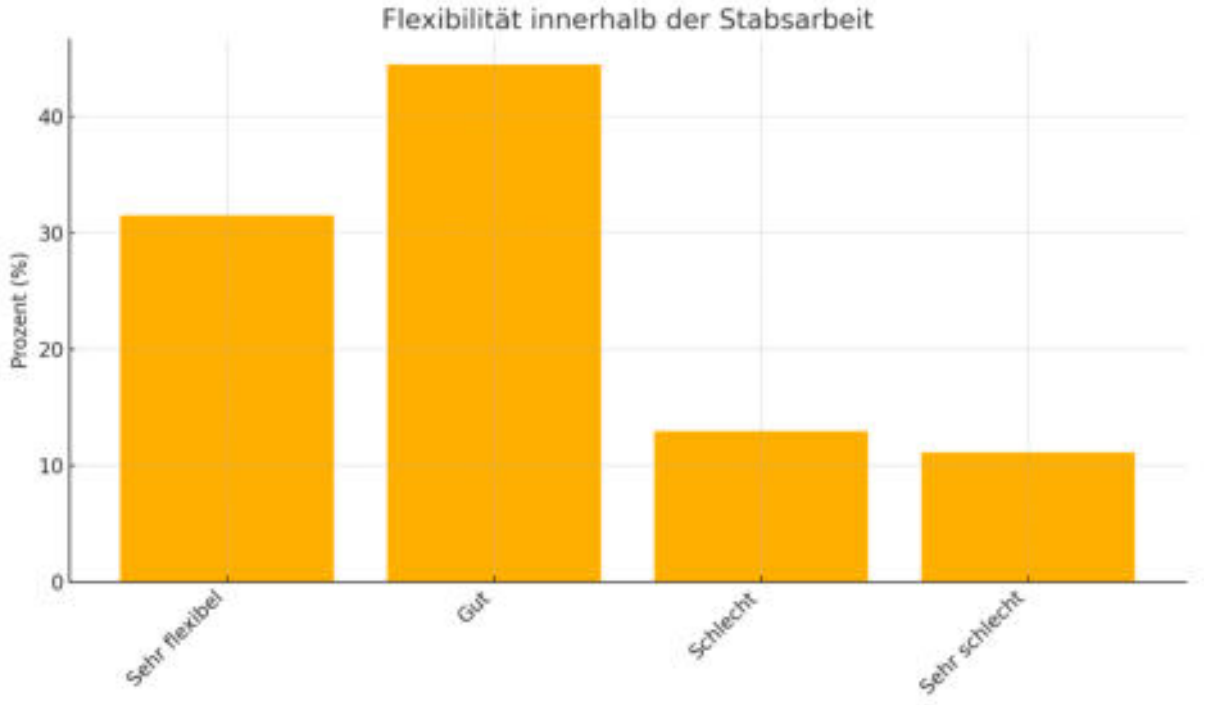


Abbildung 19 Auswertung hinsichtlich Flexibilität innerhalb der Stabsarbeit

31,48% der Befragten sehen ihre Organisation innerhalb der Stabsarbeit als sehr flexibel, 44,44% als gut, 12,96% als schlecht und 11,11% als sehr schlecht.

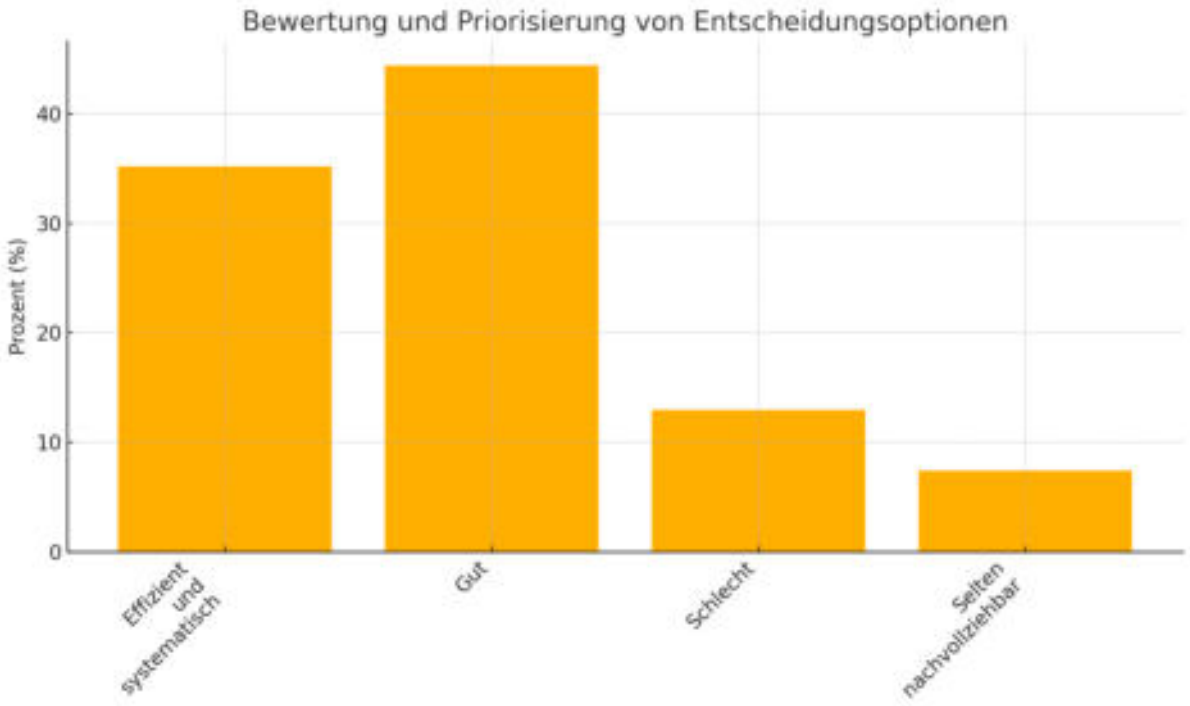


Abbildung 20 Auswertung hinsichtlich Priorisierung der Entscheidungen im Krisenstab

35,19% der Befragten geben an, dass Entscheidungen in ihrem Krisenstab effizient und systematisch priorisiert werden. 44,44% bewerten die Priorisierung als gut, 12,96% als schlecht und 7,41% als selten nachvollziehbar.

8.4.7 Erfolgsmessung und Fehlermanagement

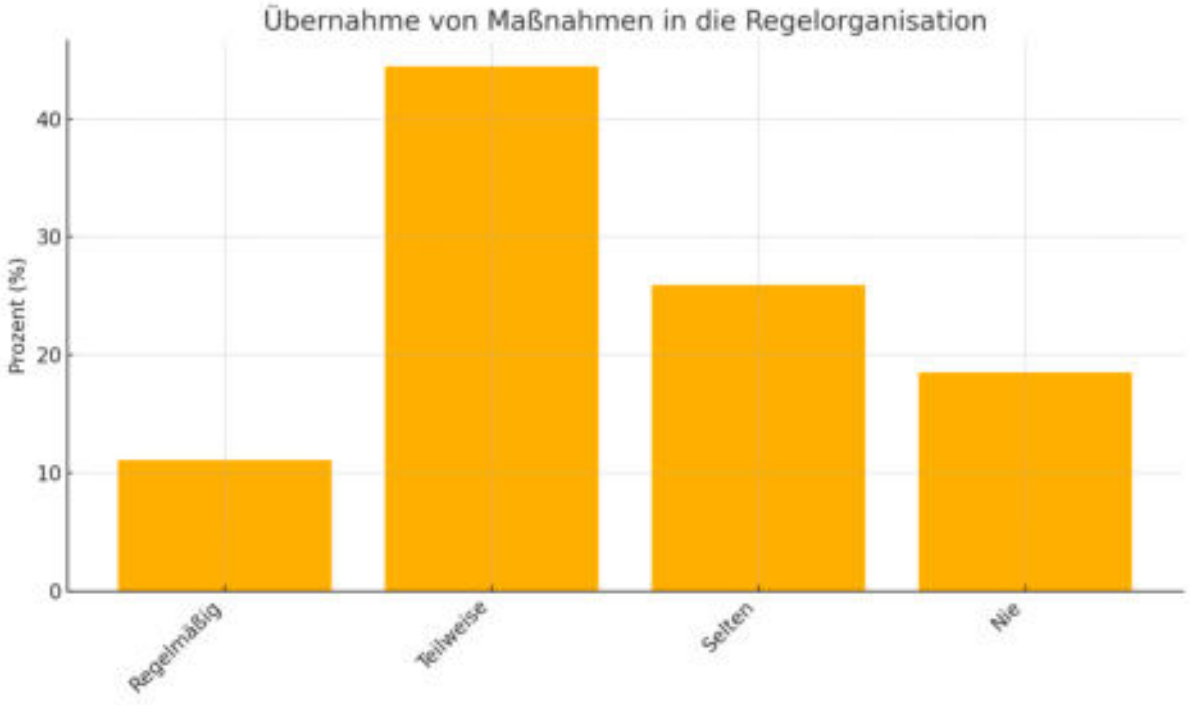


Abbildung 21 Auswertung Übernahme von Maßnahmen in die Regelorganisation

11,11% der Befragten berichten, dass Maßnahmen regelmäßig in die Regelorganisation übernommen werden. 44,44% geben an, dass dies teilweise geschieht, 25,93% selten und 18,52% nie.

Abbildung 22 Auswertung hinsichtlich Erfolgsmessung des Krisenmanagements

44,44% der Befragten messen den Erfolg ihres Krisenmanagements durch Feedback und Bewertungen von Stakeholdern. 25,93% nutzen Nachbereitungsberichte, 18,52% führen regelmäßige Überprüfungen und Audits durch, und 1,85% verwenden spezifische Leistungsindikatoren. Weitere 44,44% sind sich der Methoden zur Erfolgsmessung nicht sicher.

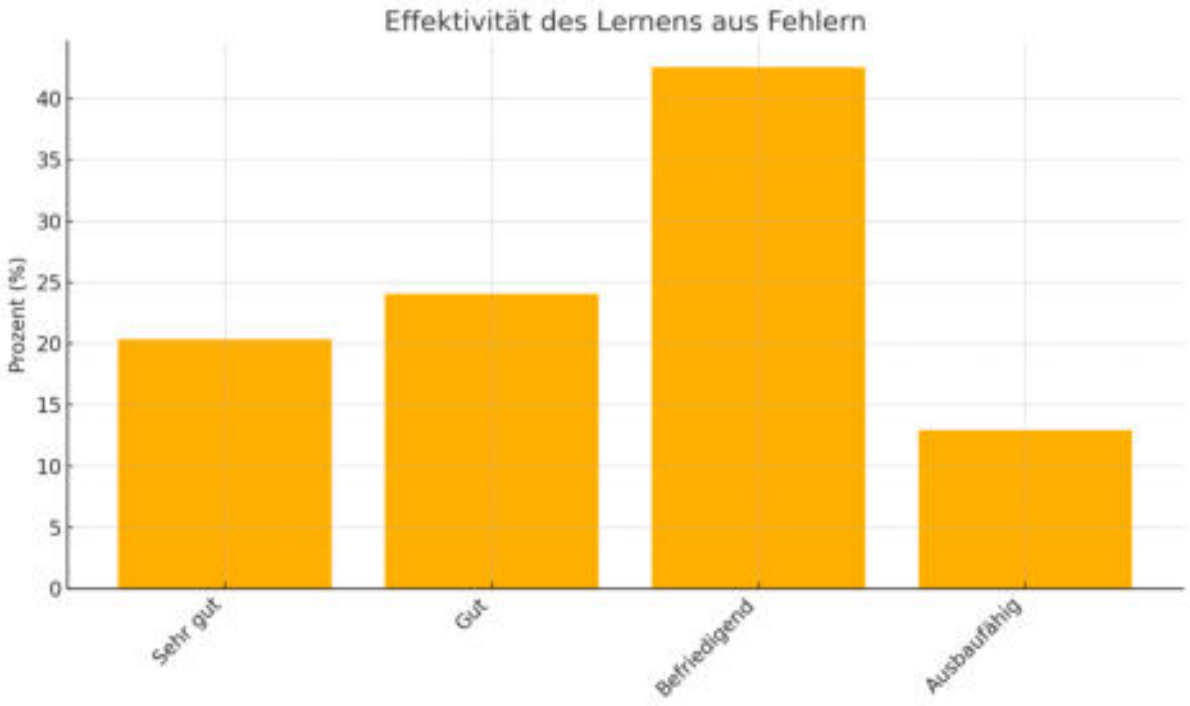


Abbildung 23 Auswertung hinsichtlich Effektivität bzgl. lernen aus Fehlern

20,37% der Befragten bewerten das Lernen aus Fehlern in ihrer Organisation als sehr gut, 24,07% als gut, 42,59% als befriedigend und 12,96% als ausbaufähig.

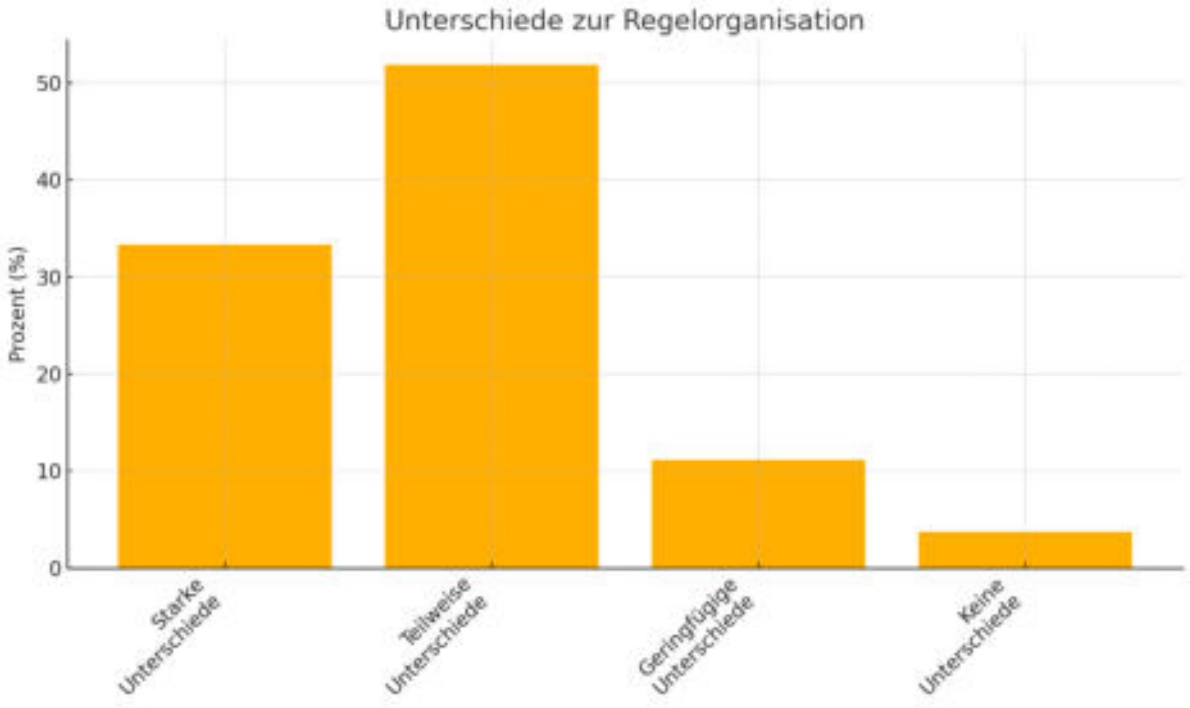


Abbildung 24 Auswertung hinsichtlich unterschiedlicher Arbeitsweisen

33,33% der Befragten sehen starke Unterschiede zwischen der Arbeit im Krisenmanagement und der Regelorganisation. 51,85% erkennen teilweise Unterschiede, 11,11% geringfügige Unterschiede, und 3,70% keinen Unterschied.

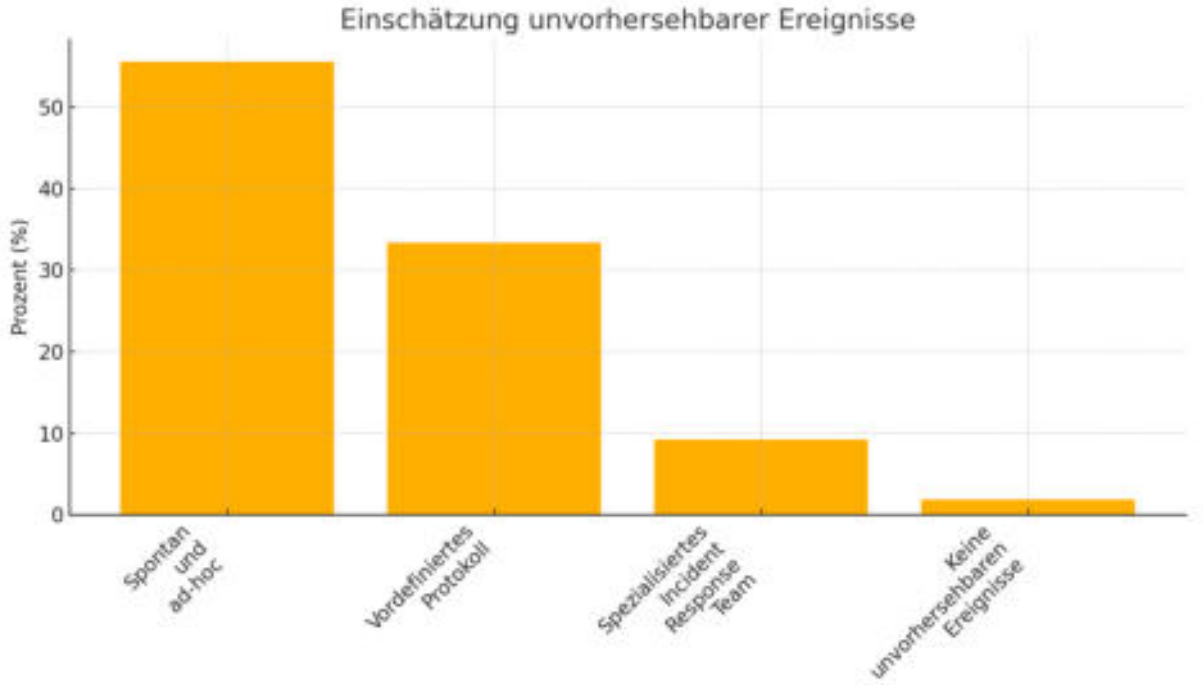


Abbildung 25 Auswertung Einschätzung unvorhersehbarer Ereignisse

55,56% der Befragten geben an, dass die erste Einschätzung unvorhersehbarer Ereignisse spontan und ad-hoc erfolgt. 33,33% folgen einem vordefinierten Protokoll, 9,26% verlassen sich auf ein spezialisiertes Incident Response Team, und 1,85% glauben, dass keine unvorhersehbaren Ereignisse eintreten können.

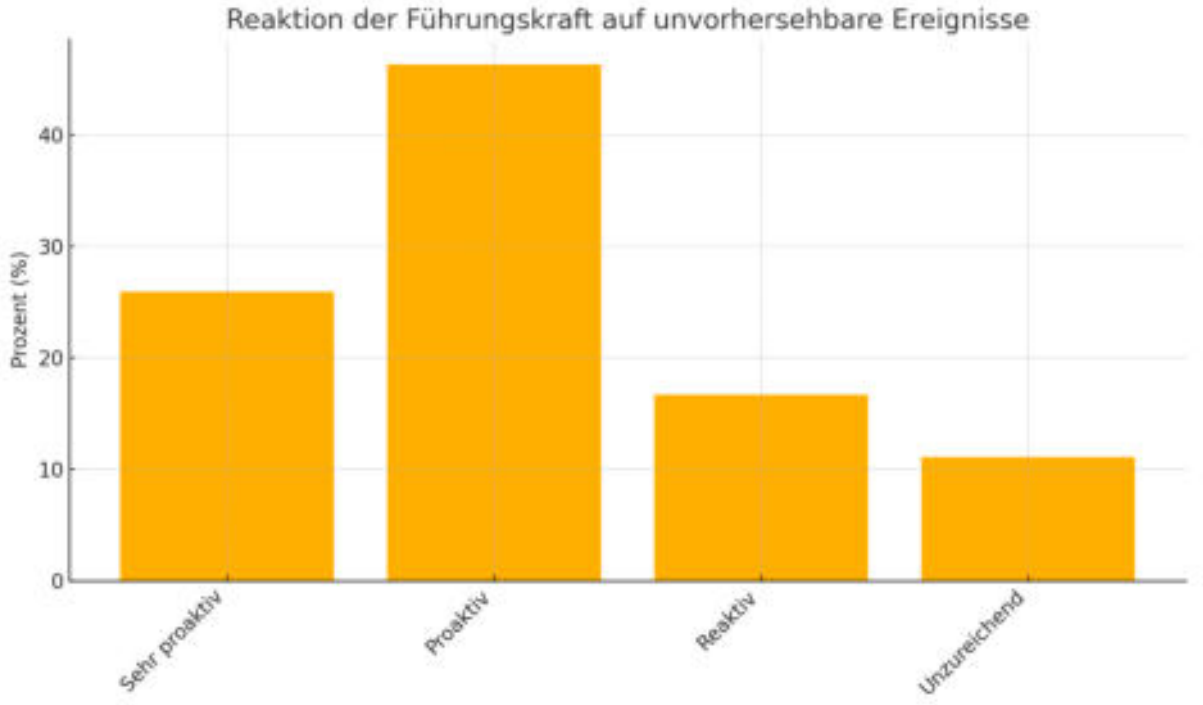


Abbildung 26 Auswertung Reaktion der Führungskräfte

25,93% der Befragten bewerten die Reaktion ihrer Führungskraft auf unvorhersehbare Ereignisse als sehr proaktiv. 46,30% sehen sie als proaktiv, 16,67% als reaktiv und 11,11% als unzureichend.

8.5 Interpretation der Onlinebefragung

Ein zentraler Aspekt der Umfrage ist die Nutzung digitaler Lösungen im Krisenmanagement. Mehr als die Hälfte der Befragten (57,41%) gibt an, dass ihr Krisenstab digitale Lösungen zur Lageführung nutzt. Dies zeigt, dass die Digitalisierung in vielen Krisenstäben bereits integriert ist und als Mittel zur Steigerung der Effizienz und Verbesserung der Entscheidungsfindung angesehen wird. Diese Beobachtung unterstützt die Hypothese der vorliegenden Masterarbeit, dass die Digitalisierung von Informations- und Kommunikationssystemen die Effizienz bei der Informationsweitergabe und -verarbeitung im Krisenmanagement erheblich steigern kann.

Die Wahrnehmung der Rolle des Faktors Mensch im digitalen Zeitalter ist ebenfalls ein wichtiges Ergebnis der Umfrage. Die Mehrheit der Befragten (57,41%) sieht eine erkennbare und positive Veränderung durch die Digitalisierung, während 14,81% eine starke positive Veränderung wahrnehmen. Dies bestätigt, dass digitale Technologien nicht nur die Effizienz steigern, sondern auch die Rolle des Menschen im Krisenmanagement positiv beeinflussen können. Gleichzeitig gibt es jedoch auch eine Gruppe von Befragten (22,22%), die kaum oder negative Veränderungen wahrnimmt, und 5,56% sehen eine starke negative Veränderung. Dies deutet auf Herausforderungen bei der Integration und Akzeptanz digitaler Lösungen hin, was ein wichtiger Aspekt für die weitere Forschung und Praxis ist.

Die durch COVID-19 initiierten digitalen Veränderungen werden von einer großen Mehrheit der Befragten als effektiv (59,26%) oder äußerst effektiv (29,63%) bewertet. Dies unterstreicht die Rolle der Pandemie als Katalysator für die Digitalisierung und die Anpassungsfähigkeit der Organisationen in Krisensituationen. Nur ein kleiner Teil der Befragten (7,41%) empfindet die Veränderungen, als wenig effektiv, was auf spezifische Herausforderungen in bestimmten Bereichen hinweisen könnte.

Organisatorische und technische Hindernisse bei der Einführung digitaler Lösungen sind ein weiteres zentrales Thema der Umfrage. Signifikante Hindernisse werden von 38,89% der Befragten sowohl in organisatorischer als auch in technischer Hinsicht gesehen. Diese Hindernisse stellen wichtige Barrieren dar, die überwunden werden müssen, um die volle Wirksamkeit digitaler Lösungen zu gewährleisten. Dies unterstreicht die Notwendigkeit, nicht nur technologische, sondern auch organisatorische Rahmenbedingungen zu verbessern, um die Effizienz des Krisenmanagements zu steigern.

Die Flexibilität der Organisationen bei unvorhergesehenen Ereignissen wird von 48,15% der Befragten als gut und von 38,89% als sehr gut eingeschätzt. Diese positive Einschätzung zeigt, dass viele Organisationen in der Lage sind, sich schnell und effektiv an neue Situationen anzupassen. Dies ist besonders wichtig im Kontext der HRO-Prinzipien, die in meiner Masterarbeit untersucht werden, da Flexibilität ein Schlüsselmerkmal hochzuverlässiger Organisationen ist.

Fehlermanagement ist ein weiterer wichtiger Aspekt, der in der Umfrage behandelt wird. Die Mehrheit der Befragten sieht positive Veränderungen in der Rolle des Menschen durch die Digitalisierung, was darauf hindeutet, dass digitale Lösungen dazu beitragen können, menschliche Fehler zu minimieren. Dies ist ein zentrales Anliegen der HRO-Theorie, die in meiner Arbeit ausführlich behandelt wird, und unterstützt die Annahme, dass eine verbesserte Fehlerkultur und die Integration von Technologie entscheidend für die Effizienzsteigerung im Krisenmanagement sind.

Schließlich zeigt die Umfrage, dass das Wissensmanagement und die Schulung zu Cybersicherheit in vielen Organisationen gut verankert sind. Ein Großteil der Befragten (79,63%) gibt an, dass sie in Bezug auf Cybersicherheit geschult wurden, und ebenso viele Organisationen betreiben ein Informationssicherheitsmanagementsystem. Dies ist entscheidend, um die Resilienz und Sicherheit in kritischen Infrastrukturen zu gewährleisten und unterstützt die These, dass kontinuierliches Lernen und Wissensmanagement integrale Bestandteile eines effektiven Krisenmanagements sind.

Es muss jedoch angemerkt werden, dass durch den Fragebogen schwer zu untersuchen ist, wie stark vorgegebene Regelwerke und strukturelle Rahmenbedingungen die Stabsarbeit beeinflussen. Diese Aspekte können durch ergänzende qualitative Methoden wie Interviews besser beleuchtet werden. Daher ist es wichtig, die Ergebnisse der Umfrage mit den Erkenntnissen aus den Interviews zu ergänzen, um ein umfassenderes Bild zu erhalten.

Zusammenfassend zeigen die Umfrageergebnisse, dass die Digitalisierung und die Anwendung der HRO-Prinzipien im Krisenmanagement bereits positive Effekte haben, es jedoch weiterhin Herausforderungen gibt, insbesondere in Bezug auf die Integration und Akzeptanz digitaler Lösungen sowie die Beseitigung organisatorischer und technischer Hindernisse. Diese Erkenntnisse sind essenziell für die Optimierung der Stabsarbeit in kritischen Infrastrukturen und unterstreichen die Relevanz meiner Masterarbeit, die sich mit der Flexibilität, dem Fehlermanagement und dem Wissensmanagement im Kontext des Krisenmanagements beschäftigt.

9 Zusammenfassung

In diesem Kapitel werden die Ergebnisse aus Onlinebefragung und Experteninterviews abgleichend interpretiert. Nach der zusammenfassenden Interpretation erfolgt die Beantwortung der Forschungsfragen und die Verifizierung der Hypothesen.

9.1 Abgleichende Interpretation der Untersuchungsergebnisse

Flexibilität von Organisationsstrukturen und Prozessen ist ein zentrales Element für erfolgreiches Krisenmanagement (vgl. Interview Cieslik). Flexibilität ermöglicht es den Stabsmitgliedern, schnell und präzise auf unerwartete Veränderungen und Herausforderungen zu reagieren, besonders in dynamischen Krisensituationen. Starre und unflexible Strukturen führen zu Verzögerungen und ineffizienten Entscheidungsprozessen. Interviews zeigen, dass flexible Organisationsstrukturen, die improvisierte und innovative Lösungen erlauben, wesentlich effektiver sind als traditionelle Modelle (vgl. Interview Cieslik und Interview Rattei). Das SKKM-Modell wird oft als zu starr und unflexibel kritisiert und benötigt Modernisierungen, um die Reaktionsfähigkeit und Anpassungsfähigkeit der Krisenstäbe zu verbessern (vgl. Interview Cieslik, Interview Rattei und Interview Schwarz).

Fehlermanagement ist in Stresssituationen, unter hohem Zeitdruck und bei Ermüdung ein zentraler Aspekt. Hochzuverlässigkeitsorganisationen (HRO) bieten wertvolle Ansätze zur Minimierung von Fehlern durch eine Kultur der Fehlerfreundlichkeit und systematische Fehlervermeidungsstrategien. Die Anwendung von HRO-Prinzipien kann die Fehlerquote in Krisenstäben signifikant reduzieren. Umfassende Trainingsprogramme stärken die Resilienz der Stabsmitglieder und bereiten sie auf den Umgang mit komplexen und stressigen Situationen vor.

Wissensmanagement ist ein kritischer Faktor für die Effizienz von Entscheidungsprozessen. Digitalisierung verbessert das Wissensmanagement durch schnellere und präzisere Verarbeitung und Verteilung von Informationen, was die Entscheidungsfindung beschleunigt. Organisationen, die digitale Technologien in ihre Stabsarbeit integriert haben, berichten von effizienteren und koordinierteren Reaktionen auf Krisensituationen. Traditionelle Methoden wie Papier und Bleistift sind demnach zeitaufwendiger und fehleranfälliger. Die Befragungsergebnisse unterstreichen die Notwendigkeit der Integration digitaler Werkzeuge, um die Effizienz in der Stabsarbeit zu steigern und den modernen Herausforderungen des Krisenmanagements gerecht zu werden.

Die Ergebnisse der Interviews und Befragungen zeigen die Notwendigkeit einer flexiblen und anpassungsfähigen Organisationsstruktur. Das SKKM-Modell muss überarbeitet werden, um flexiblere Strukturen und Prozesse zu integrieren. Die Implementierung umfassender Fehlermanagementstrategien durch die Anwendung von HRO-Prinzipien ist entscheidend (vgl. Interview Cieslik und Interview Rattei). Die Digitalisierung der Stabsarbeit erhöht die Effizienz der Informationsverarbeitung und -verteilung und verbessert die Gesamtleistung des Krisenmanagements (vgl. Interview Schwarz, Interview Experten Energie AUT und Interview Rattei).

9.2 Überprüfung Hypothese 1 inkl. zugehörigen Forschungsfragen

Die Hypothese 1 besagt, dass die Digitalisierung von Informations- und Kommunikationssystemen in kritischen Infrastrukturen die Effizienz bei der Informationsweitergabe und -verarbeitung im Krisenmanagement erheblich steigern wird. Um diese Hypothese zu überprüfen, wurden mehrere Forschungsfragen gestellt. Nach der Analyse der Ergebnisse aus den Experteninterviews und der Onlinebefragung kann die Hypothese weitgehend verifiziert werden, obwohl es auch Herausforderungen gibt.

> **Wie kann die Digitalisierung in kritischen Infrastrukturen für das Krisenmanagement genutzt werden, um die Effizienz zu steigern, während gleichzeitig Sicherheitsmaßnahmen ergriffen werden, um sowohl vor technischen Ausfällen als auch Cyberbedrohungen zu schützen?**

Die Digitalisierung in kritischen Infrastrukturen kann die Effizienz im Krisenmanagement durch den Einsatz digitaler Kommunikationsplattformen und Echtzeitüberwachungssysteme erheblich steigern. Diese Technologien ermöglichen eine schnelle und effiziente Verteilung von Informationen und eine koordinierte Reaktion auf Krisensituationen. Die Ergebnisse zeigen, dass digitale Lösungen in vielen Organisationen bereits integriert sind, wobei 57,41% der befragten Krisenstäbe digitale Lösungen zur Lageführung nutzen. Zudem berichten viele Befragte von einer positiven Veränderung der Rolle des Menschen im Krisenmanagement durch die Digitalisierung, was darauf hindeutet, dass digitale Technologien die menschliche Komponente ergänzen und unterstützen können. Sicherheitsmaßnahmen umfassen die Implementierung von Cybersicherheitsstrategien, regelmäßige Schulungen und Übungen sowie die Nutzung von Informationssicherheitsmanagementsystemen wie ISO 27001. Diese Maßnahmen tragen dazu bei, sowohl technische Ausfälle als auch Cyberbedrohungen zu minimieren.

> **Welche digitalen Technologien und Lösungen sind derzeit in kritischen Infrastrukturen verfügbar und wie werden sie eingesetzt?**

Zu den derzeit verfügbaren digitalen Technologien und Lösungen in kritischen Infrastrukturen gehören Alarmierungssysteme, digitale Lageführungen, gesicherte Videokonferenzmodelle, Simulationsmodelle zur Entscheidungsunterstützung sowie gesicherte und ausfallsichere Kommunikationsmittel. Diese Technologien werden hauptsächlich in den Bereichen Kommunikation, Lageführung und Datenanalyse eingesetzt. Alarmierungssysteme und digitale Lageführungen sind die am häufigsten genutzten Technologien, was darauf hinweist, dass diese Tools als wesentlich für die Koordination und Informationsverarbeitung in Krisensituationen angesehen werden. Die Implementierung und Nutzung dieser Technologien variieren jedoch je nach Organisation und spezifischen Anforderungen.

> **Welche Erfahrungen haben andere Organisationen bei der Implementierung digitaler Technologien im Krisenmanagement gemacht?**

Die Erfahrungen anderer Organisationen bei der Implementierung digitaler Technologien im Krisenmanagement sind gemischt. Einige Organisationen berichten von erheblichen Effizienzsteigerungen und einer verbesserten Entscheidungsfindung durch digitale Lösungen. So geben 33,33% der Befragten an, dass digitale Lösungen die Effizienz des Krisenmanagements erheblich gesteigert haben. Gleichzeitig gibt es jedoch auch Herausforderungen, insbesondere organisatorische und technische Hindernisse. Signifikante Hindernisse wurden von 38,89% der Befragten sowohl in organisatorischer als auch in technischer Hinsicht gesehen. Diese Hindernisse müssen überwunden werden, um die volle Wirksamkeit digitaler Lösungen zu gewährleisten. Zudem variiert die Akzeptanz und Integration digitaler Lösungen zwischen den Organisationen, was auf die Notwendigkeit einer Anpassung der Technologien und Schulungsprogramme an die spezifischen Bedürfnisse und Bedingungen jeder Organisation hinweist.

Die Hypothese 1, dass die Digitalisierung von Informations- und Kommunikationssystemen in kritischen Infrastrukturen die Effizienz bei der Informationsweitergabe und -verarbeitung im Krisenmanagement erheblich steigern wird, kann weitgehend verifiziert werden. Die Ergebnisse der Umfrage und Interviews zeigen, dass digitale Technologien bereits in vielen Organisationen erfolgreich eingesetzt werden und positive Effekte auf die Effizienz und Entscheidungsfindung im Krisenmanagement haben. Gleichzeitig gibt es jedoch Herausforderungen bei der Integration und Akzeptanz dieser Technologien sowie organisatorische und technische Hindernisse, die angegangen werden müssen. Insgesamt unterstützen die Erkenntnisse die Hypothese, weisen aber auch auf Bereiche hin, die verbessert werden müssen, um die volle Wirksamkeit der Digitalisierung im Krisenmanagement zu gewährleisten.

9.3 Überprüfung Hypothese 2 inkl. zugehörigen Forschungsfragen

Die Hypothese 2 besagt, dass die Anwendung von HRO-Prinzipien in kritischen Infrastrukturen die Effizienz des Krisenmanagements steigern und zur effektiven Umsetzung der digitalen Lösungen beitragen wird. Nach der Analyse der Ergebnisse aus den Experteninterviews und der Onlinebefragung kann die Hypothese größtenteils verifiziert werden, obwohl es Unterschiede in der Implementierung und Herausforderungen bei der kontinuierlichen Anwendung der Prinzipien gibt.

> **Wie können die Prinzipien der Hochzuverlässigen Organisationen (HRO) in kritischen Infrastrukturen gezielt und angepasst implementiert werden, um das Krisenmanagement zu optimieren?**

Die Interviews zeigten, dass die HRO-Prinzipien in den meisten befragten Organisationen bekannt sind und als wertvolles Instrument zur Verbesserung der Krisenbewältigung angesehen werden. Insbesondere die Prinzipien der Fehlervermeidung, Fehlertoleranz und die Schaffung einer Kultur der Achtsamkeit wurden hervorgehoben. Einige Organisationen haben Maßnahmen implementiert, um diese Prinzipien zu fördern, beispielsweise durch regelmäßige Schulungen und Übungen, die darauf abzielen, Mitarbeiter für potenzielle Fehlerquellen zu

sensibilisieren und eine offene Fehlerkultur zu etablieren. Diese Schulungen zielen darauf ab, die Aufmerksamkeit auf Details zu lenken und Mitarbeiter zu ermutigen, Fehler frühzeitig zu erkennen und zu melden.

> **Welche konkreten HRO-Prinzipien und -Praktiken sind in anderen Bereichen erfolgreich angewandt worden und könnten in kritischen Infrastrukturen übertragen werden?**

Die Diskussion der Interviews zeigte, dass die Prinzipien der Hochzuverlässigkeitsorganisationen (HRO) in verschiedenen Bereichen erfolgreich angewandt wurden und in kritischen Infrastrukturen übertragen werden können. Zum Beispiel betonen die befragten Experten die Bedeutung einer klar definierten Struktur innerhalb des Krisenmanagements, einschließlich der präzisen Festlegung von Rollen und Verantwortlichkeiten. Regelmäßige Überprüfungen und Aktualisierungen der bestehenden Prozesse und Protokolle sind notwendig, um sicherzustellen, dass das System flexibel und anpassungsfähig bleibt. Die Fähigkeit zur Improvisation und zur schnellen Entscheidungsfindung wurde als entscheidend für den Erfolg in Krisensituationen angesehen.

> **Wie können HRO-Prinzipien in kritischen Infrastrukturen effektiv implementiert werden, um die präventive Krisenbewältigung zu fördern und den Umgang mit unvorhersehbaren Ereignissen zu verbessern?**

Die Interviews ergaben, dass die HRO-Prinzipien, insbesondere die Resilienz und Anpassungsfähigkeit der Organisationen, in den meisten befragten Organisationen bekannt sind und teilweise angewandt werden. Viele Organisationen haben erkannt, dass sie flexibel auf unvorhergesehene Ereignisse reagieren und kontinuierlich aus Erfahrungen lernen müssen. Nach Übungen und realen Einsätzen finden Nachbesprechungen und Evaluierungen statt, um Lehren zu ziehen und Verbesserungen vorzunehmen. Diese Praxis der kontinuierlichen Verbesserung ist ein wesentliches Element der HRO-Theorie und wird in den meisten befragten Organisationen angewendet.

Die Hypothese 2, dass die Anwendung von HRO-Prinzipien in kritischen Infrastrukturen die Effizienz des Krisenmanagements steigern und zur effektiven Umsetzung der digitalen Lösungen beitragen wird, kann größtenteils verifiziert werden. Die Ergebnisse der Umfrage und Interviews zeigen, dass HRO-Prinzipien in vielen Organisationen bekannt sind und teilweise angewandt werden. Die Implementierung dieser Prinzipien hat positive Auswirkungen auf die Effizienz und Reaktionsfähigkeit im Krisenmanagement, wie die Betonung auf Fehlervermeidung und die Schaffung einer Kultur der Achtsamkeit zeigen. Gleichzeitig gibt es Herausforderungen bei der umfassenden Integration und kontinuierlichen Anwendung dieser Prinzipien, die angegangen werden müssen, um die volle Wirksamkeit zu gewährleisten. Insgesamt unterstützen die Erkenntnisse die Hypothese, weisen aber auch auf die Notwendigkeit einer gezielten und angepassten Implementierung der HRO-Prinzipien hin, um die präventive Krisenbewältigung zu fördern und den Umgang mit unvorhersehbaren Ereignissen zu verbessern.

10 Ausblick und mögliche Perspektiven

Auf Grundlage dieser Erkenntnisse lassen sich mehrere vielversprechende Ansätze für zukünftige Forschungsarbeiten identifizieren, die das Potenzial haben, die Effizienz und Effektivität des Krisenmanagements weiter zu verbessern.

Ein möglicher Ausblick für zukünftige Forschung besteht in der detaillierten Untersuchung der Implementierung und Wirkung hybrider Stabsmodelle, die sowohl traditionelle als auch digitale Methoden integrieren. Die Ergebnisse dieser Arbeit zeigen, dass viele Organisationen bereits digitale Lösungen erfolgreich einsetzen, gleichzeitig aber auch auf bewährte traditionelle Methoden zurückgreifen. Es wäre wichtig, die spezifischen Vorteile und Herausforderungen solcher hybriden Modelle systematisch zu analysieren, um Best Practices zu identifizieren und Empfehlungen für eine optimierte Integration zu entwickeln.

Ein weiterer Forschungsbereich könnte die tiefere Analyse der Flexibilität und Anpassungsfähigkeit von Krisenmanagementsystemen sein. Die Interviews und Umfrageergebnisse heben die Bedeutung dieser Aspekte hervor, jedoch bleibt unklar, welche spezifischen Maßnahmen und Strukturen die größte Wirkung entfalten. Zukünftige Studien könnten hier experimentelle Ansätze verfolgen, um verschiedene Flexibilitätsstrategien in kontrollierten Krisenszenarien zu testen und ihre Effektivität zu messen.

- Detaillierte Untersuchung der Implementierung und Wirkung hybrider Stabsmodelle, die sowohl traditionelle als auch digitale Methoden integrieren.
- Analyse der spezifischen Vorteile und Herausforderungen hybrider Krisenmanagementmodelle zur Identifikation von Best Practices und Empfehlungen.
- Tiefere Analyse der Flexibilität und Anpassungsfähigkeit von Krisenmanagementsystemen, einschließlich experimenteller Ansätze zur Messung der Effektivität verschiedener Flexibilitätsstrategien.
- Vergleich der Wirksamkeit verschiedener Schulungsansätze und -methoden im Wissensmanagement, insbesondere im Bereich Cybersicherheit.
- Erforschung der Integration und Umsetzung gesetzlicher Rahmenbedingungen und Normen im Krisenmanagement sowie deren Einfluss auf die Resilienz und Compliance von Organisationen.
- Analyse der Rolle digitaler Technologien bei der Effizienzsteigerung und Verbesserung der Entscheidungsfindung im Krisenmanagement.
- Untersuchung der Auswirkungen der Digitalisierung auf die organisatorische Resilienz und die Fähigkeit zur schnellen Anpassung an neue Bedrohungen.
- Entwicklung von Maßnahmen zur kontinuierlichen Verbesserung der Cybersicherheitsstrategien in kritischen Infrastrukturen.
- Analyse der Anwendung und Wirksamkeit der HRO-Prinzipien (Hochzuverlässigkeitsorganisationen) in verschiedenen Organisationen.

- Untersuchung, wie HRO-Prinzipien, wie Fehlervermeidung, Fehlertoleranz und Achtsamkeit, in Schulungs- und Übungsprogramme integriert werden können.
- Erforschung der langfristigen Auswirkungen der HRO-Prinzipien auf die Resilienz und Anpassungsfähigkeit von Organisationen im Krisenmanagement.
- Entwicklung und Bewertung von HRO-basierten Methoden zur Verbesserung der organisationalen Resilienz und Fehlerkultur.
- Überprüfung und Überarbeitung des starren SKKM-Modells zur Anpassung an moderne Krisenszenarien und Anforderungen.
- Analyse der Auswirkungen digitaler und hybrider Ansätze auf die Effizienz des SKKM-Modells.
- Entwicklung von Empfehlungen zur Anpassung des SKKM-Modells unter Berücksichtigung aktueller technischer und organisatorischer Entwicklungen im Krisenmanagement.

Auf Grundlage der gewonnenen Erkenntnisse lassen sich Ansätze für zukünftige Forschung im Krisenmanagement identifizieren, die Effizienz und Effektivität weiter verbessern könnten.

Ein Fokus könnte auf der Untersuchung hybrider Stabsmodelle liegen, die traditionelle und digitale Methoden integrieren. Diese Arbeit zeigt, dass viele Organisationen bereits digitale Lösungen nutzen, aber auch traditionelle Methoden schätzen. Die Vorteile und Herausforderungen solcher hybriden Modelle sollten systematisch analysiert werden, um Best Practices zu identifizieren.

Die Wirksamkeit verschiedener Schulungsansätze, besonders im Bereich Cybersicherheit, und die Integration gesetzlicher Rahmenbedingungen im Krisenmanagement sollten weiter untersucht werden. Ebenso wichtig ist die Rolle digitaler Technologien bei der Effizienzsteigerung und Entscheidungsfindung sowie deren Einfluss auf die organisatorische Resilienz.

Langfristig könnten Maßnahmen zur Verbesserung der Cybersicherheitsstrategien und die Anwendung der HRO-Prinzipien (Hochzuverlässigkeitsorganisationen) in Organisationen weiter erforscht werden. Die Anpassung des starren SKKM-Modells an moderne Anforderungen und die Entwicklung von Empfehlungen zur Integration digitaler Ansätze sind weitere wichtige Forschungsfelder.

11 Literaturverzeichnis

BADKE-SCHAUB P. HOFINGER G. UND LAUCHE K. (2012): Human Factors - In P. BADKE-SCHAUB, G. HOFINGER, UND K. LAUCHE (HRSG.), Human Factors (S. 3–20) Springer Berlin Heidelberg; - Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-19886-1_1

BAYER F. FIEDRICH F. GIßLER D. HOFINGER G. KARSTEN A. LAMERS C. UND ARBEITSGRUPPE STABSARBEIT (2022): *Thesen zur Zukunft der Stabsarbeit*. https://doi.org/10.13140/RG.2.2.13949.64488

BERGER-GRABNER D. (2016): Wissenschaftliches Arbeiten in den Wirtschafts- und Sozialwissenschaften Springer Fachmedien Wiesbaden; - Wiesbaden. https://doi.org/10.1007/978-3-658-13078-7

BLANZ B. M. (2017): High-Reliability-Entscheidungen Springer Fachmedien Wiesbaden; - Wiesbaden. https://doi.org/10.1007/978-3-658-16738-7

BMI (2015): Österreichisches Programm zum Schutz der kritischen Infrastrukturen (Ö. BUNDESKANZLERAMT, HRSG.) BMI. https://www.bmi.gv.at/505/start.aspx

BMI, STAATLICHES KRISEN- UND KATASTROPHENSCHUTZMANAGEMENT (2006): Richtlinie für das Führen im Katastropheneinsatz - SKKM Richtlinie.

BUNDESAMT FÜR VERFASSUNGSSCHUTZ (HRSG.) (2017): Wirtschaftsgrundschutz - Baustein ÜA4 Krisenmanagement. https://www.wirtschaftsschutz.info/DE/Veroeffentlichungen/Wirtschaftsgrundschutz/Bausteine/Krisenmanagement.pdf%3F__blob%3DpublicationFile%26v%3D2

BUNDESMINISTERIUM DES INNERN (2009): Nationale Strategie zum Schutz Kritischer Infrastrukturen www.bmi.bund.de. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=3

Neuorganisation des Staatlichen Krisen- und Katastrophenschutzmanagements sowie der internationalen Katastrophenhilfe (SKKM), Pub. L. No. GZ 66.000/939-II/4/03 (2004). https://www.bmi.gv.at/204/SKKM/files/001_Ministerratsbeschluss.pdf

Bundesgesetz über die Sicherstellung der staatlichen Resilienz und Koordination in Krisen (Bundes-Krisensicherheitsgesetz – B-KSG), Pub. L. No. Bundesgesetzblatt I Nr. 89/2023 (2023). https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20012321

CHRISTIAN SCHULDT (o. J.): Trendguide Digitalisierung (Trendguide Digitalisierung, S. 105) Zukunftsinstitut GmbH; - Frankfurt am Main. Abgerufen 21. Juli 2024, von https://www.wko.at/oe/epu/2022-09-27-wko-trendguide-digitalisierung-doppelseiten-web.pdf

DUDEN (2024): Duden - In Duden. https://www.duden.de/rechtschreibung/Katastrophe

DUDENREDAKTION (2024): Krise - In Duden - Die deutsche Rechtschreibung - Berlin. https://www.duden.de/suchen/dudenonline/Krise

EBSTER C. UND STALZER L. (2017): Wissenschaftliches Arbeiten für Wirtschafts- und Sozialwissenschaftler (5., überarbeitete und erweiterte Auflage) facultas; - Wien.

Mitteilung der Kommission an den Rat und das Europäische Parlament - Eine europäische Strategie zur Förderung von Technologien für die sichere Informationsgesellschaft - „Ein Dialog für mehr Vertrauen und Sicherheit“, Pub. L. No. KOM(2004) 702 endgültig (2004).

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, Pub. L. No. 2022/2557 (2023). https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2557#d1e650-164-1

Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS2-Richtlinie), Pub. L. No. 2022/2555 (2023), Diese Richtlinie ersetzt die Richtlinie (EU) 2016/1148 und führt neue Maßnahmen ein, um die Cybersicherheit in der Union zu verbessern. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02022L2555-20221227&qid=1721592204313

FAHLBRUCH B. SCHÖBEL M. UND MAROLD J. (2012): Sicherheit - In P. BADKE-SCHAUB, G. HOFINGER, UND K. LAUCHE (HRSG.), Human Factors (S. 21–38) Springer Berlin Heidelberg; - Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-19886-1_2

FOLKERS A. (2018): Was ist kritisch an Kritischer Infrastruktur? Kriegswichtigkeit, Lebenswichtigkeit, Systemwichtigkeit und die Infrastrukturen der Kritik - In J. I. ENGELS UND A. NORDMANN (HRSG.), Science Studies (1. Aufl., S. 123–154) transcript Verlag; - Bielefeld, Germany. https://doi.org/10.14361/9783839442074-005

FRODL A. (2022): Stabilität und Sicherheit: Worauf kommt es an, um Risiken und Krisen erfolgreich zu widerstehen? - In A. FRODL, Krisenmanagement für Gesundheitseinrichtungen (S. 1–18) Springer Fachmedien Wiesbaden; - Wiesbaden. https://doi.org/10.1007/978-3-658-36374-1_1

HACKER W. UND WETH R. V. D. (2012): Denken – Entscheiden – Handeln - In P. BADKE-SCHAUB, G. HOFINGER, UND K. LAUCHE (HRSG.), Human Factors (S. 83–99) Springer Berlin Heidelberg; - Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-19886-1_5

HEIMANN R. (2022a): Polizeiliche Stabsarbeit – Erfordernisse für die Zukunft - In D. WEHE UND H. SILLER (HRSG.), Handbuch Polizeimanagement (S. 1–23) Springer Fachmedien Wiesbaden; - Wiesbaden. https://doi.org/10.1007/978-3-658-34394-1_103-1

HEIMANN R. (2022b): Software zum Informations- und Kommunikationsmanagement in Stäben - In G. HOFINGER UND R. HEIMANN (HRSG.), Handbuch Stabsarbeit (S. 327–335) Springer Berlin Heidelberg; - Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-63035-8_40

HEIMANN R. UND HOFINGER G. (2022a): Stabsarbeit – Konzept und Formen der Umsetzung - In G. HOFINGER UND R. HEIMANN (HRSG.), Handbuch Stabsarbeit (S. 3–10) Springer Berlin Heidelberg; - Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-63035-8_1

HEIMANN R. UND HOFINGER G. (2022b): Video- und Webkonferenzen im Stab - In G. HOFINGER UND R. HEIMANN (HRSG.), Handbuch Stabsarbeit (S. 299–307) Springer Berlin Heidelberg; - Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-63035-8_37

HÖBEL P. KULOW A.-C. MARQUARDSEN N. MEURER F. UND WALDSCHMIDT F. C. (2022): Krisenmanagement in Unternehmen und öffentlichen Einrichtungen: professionelle Prävention und Reaktion bei sicherheitsrelevanten Bedrohungen von innen und außen (J. H. TRAUBOTH, HRSG.; 2., überarbeitete und erweiterte Auflage) Richard Boorberg Verlag; - Stuttgart München Hannover Berlin Weimar Dresden.

HOFINGER G. (2012): Fehler und Unfälle - In P. BADKE-SCHAUB, G. HOFINGER, UND K. LAUCHE (HRSG.), Human Factors (S. 39–60) Springer Berlin Heidelberg; - Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-19886-1_3

ISO 22300 (2021): Sicherheit und Resilienz - Vokabular Austrian Standards International.

ISO 22361 (2022): Sicherheit und Resilienz - Krisenmanagement - Leitlinien Austrian Standards International.

JACHS S. (2011): Einführung in das Katastrophenmanagement Verl. tredition; - Hamburg.

KARSTEN, A. H., UND VOßSCHMIDT, S. (HRSG.) (2019): Resilienz und kritische Infrastrukturen: Aufrechterhaltung von Versorgungsstrukturen im Krisenfall (1. Auflage) Verlag W. Kohlhammer; - Stuttgart.

KATHARINA SCHMÖGL (2023): Gebündelte Kompetenz bei Krisen - In Öffentliche Sicherheit, *9*–

10, 85–86.

KÜNZER L. HOFINGER G. UND MÄHLER M. (2022): Psychologische Einflussfaktoren auf Stabsarbeit - In G. HOFINGER UND R. HEIMANN (HRSG.), Handbuch Stabsarbeit (S. 193–199) Springer Berlin Heidelberg; - Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-63035-8_24

LAUWE P. (2012): Schutzkonzepte Kritischer Infrastrukturen im Bevölkerungsschutz: Ziele, Zielgruppen, Bestandteile und Umsetzung im BBK (BUNDESAMT FÜR BEVÖLKERUNGSSCHUTZ UND KATASTROPHENHILFE, HRSG.) - Bonn.

LIPPOLD D. (2019): Führungskultur im Wandel: Klassische und moderne Führungsansätze im Zeitalter der Digitalisierung Springer Fachmedien Wiesbaden; - Wiesbaden. https://doi.org/10.1007/978-3-658-25855-9

MAYRING P. (2022): Qualitative Inhaltsanalyse: Grundlagen und Techniken (13., überarbeitete Auflage) Beltz; - Weinheim Basel.

MÜNZBERG T. UND OTTENBURGER S. S. (2018): Schutz Kritischer Infrastrukturen: Kritikalität Als Entscheidungsmaß Zur Abwehr Von Gefahr Am Beispiel Stromausfall - In J. I. ENGELS UND A. NORDMANN (HRSG.), Science Studies (1. Aufl., S. 179–214) transcript Verlag; - Bielefeld, Germany. https://doi.org/10.14361/9783839442074-007

ÖNORM D 4902-3 (2021): Risikomanagement für Organisationen und Systeme - Leitfaden Austrian Standards International.

ÖNORM S 2304 (2018): Integriertes Katastrophenmanagement - Bennung und Definitionen Austrian Standards International.

ÖNORM S 2412 (2017): Security Management System - Bennenung und Definitionen Austrian Standards International.

RASCHER S. UND SCHRÖDER R. (2017): Die Gestaltung einer konstruktiven Fehlerkultur als Führungsaufgabe in High Reliability Organizations (HRO) am Beispiel der zivilen Luftfahrt - In C. VON AU (HRSG.), Struktur und Kultur einer Leadership-Organisation (S. 177–200) Springer Fachmedien Wiesbaden; - Wiesbaden. https://doi.org/10.1007/978-3-658-12554-7_10

RÜHL U. (2021): Quick Guide Erfolgreiches Business-Continuity-Management: Wie Sie Geschäftsunterbrechungen überleben und gestärkt in die Zukunft gehen Springer Berlin Heidelberg; - Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-63791-3

SCHAWEL C. UND BILLING F. (2018): Krisenmanagement: (Strategische Managementkonzepte) - In C. SCHAWEL UND F. BILLING, Top 100 Management Tools (S. 191–193) Springer Fachmedien Wiesbaden; - Wiesbaden. https://doi.org/10.1007/978-3-658-18917-4_50

STAHL R. UND STAAB P. (2019): Was ist Digitalisierung? - In R. STAHL UND P. STAAB, Don't worry, be digital (S. 21–24) Springer Berlin Heidelberg; - Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-59324-0_6

STROHSCHNEIDER S. (2022): Die Kunst der Stabsarbeit – Ein Essay - In G. HOFINGER UND R. HEIMANN (HRSG.), Handbuch Stabsarbeit (S. 21–26) Springer Berlin Heidelberg; - Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-63035-8_3

TIMTSCHENKO F. (2021): Professionelles Sicherheitsmanagement für Unternehmen: Leitfaden für erfolgreiche Corporate Security Springer Fachmedien Wiesbaden; - Wiesbaden. https://doi.org/10.1007/978-3-658-35047-5

UNDRR (2009): UNDRR - Terminology.

WEICK K. E. UND SUTCLIFFE K. M. (2007): Das unerwartete Managen: wie Unternehmen aus Extremsituationen lernen (2. Aufl) Klett-Cotta; - Stuttgart.

WEITKUNAT G. (2020): Der Rationalitätsmythos der Stabsarbeit - In C. BARTHEL (HRSG.), Managementmoden in der Verwaltung (S. 267–284) Springer Fachmedien Wiesbaden; - Wiesbaden. https://doi.org/10.1007/978-3-658-26530-4_12

ZINKE R. UND HOFINGER G. (2022): Lagebesprechungen und gemeinsame mentale Modelle - In G. HOFINGER UND R. HEIMANN (HRSG.), Handbuch Stabsarbeit (S. 159–166) Springer Berlin Heidelberg; - Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-63035-8_20

12 Kurzfassung

Diese Masterarbeit untersucht die Bedeutung der Flexibilität von Krisenstäben für die effektive Bewältigung von Krisensituationen und betont die Notwendigkeit einer hohen Verfügbarkeit kritischer Infrastrukturen. In Krisenzeiten erfordert die Handlungsfähigkeit von Krisenstäben eine hohe Anpassungsfähigkeit und Flexibilität, um schnell und effektiv auf sich ändernde Bedingungen und unerwartete Ereignisse reagieren zu können. Ein zentrales Element der Krisenbewältigung ist die Hochverfügbarkeit kritischer Infrastrukturen, die für die Aufrechterhaltung wesentlicher gesellschaftlicher Funktionen unerlässlich sind.

Die Arbeit analysiert die Anwendung von Prinzipien hochzuverlässiger Organisationen im Kontext des Krisenmanagements. Diese Organisationen zeichnen sich durch ihre Fähigkeit aus, auch in hochkomplexen und risikoreichen Umgebungen zuverlässig zu funktionieren. Die Prinzipien der HRO-Theorie, wie das Streben nach Flexibilität, die Konzentration auf Fehler und der Respekt vor fachlichem Wissen, werden auf ihre Anwendbarkeit und ihren Nutzen für die Arbeit von Krisenstäben untersucht.

Die Ergebnisse zeigen die Notwendigkeit einer strukturierten und kontinuierlichen Weiterentwicklung von Krisenmanagementpraktiken, insbesondere durch die Integration digitaler Lösungen und die Förderung einer Kultur der Flexibilität und Lernbereitschaft.

13 Abstract

This master's thesis examines the significance of the flexibility of crisis teams for the effective management of crisis situations and emphasizes the necessity of high availability of critical infrastructures. During crises, the operational capability of crisis teams requires a high degree of adaptability and flexibility to respond quickly and effectively to changing conditions and unexpected events. A central element of crisis management is the high availability of critical infrastructures, which are essential for maintaining key societal functions.

The thesis analyzes the application of principles of High Reliability Organizations (HRO) in the context of crisis management. These organizations are characterized by their ability to function reliably even in highly complex and high-risk environments. The principles of HRO theory, such as the pursuit of flexibility, a focus on errors, and respect for professional expertise, are examined for their applicability and usefulness for the work of crisis teams.

The empirical investigation includes expert interviews and an online survey of professionals in crisis management. The results show that the deliberate implementation of HRO principles in crisis teams can significantly improve the efficiency and effectiveness of crisis management. Furthermore, it becomes clear that the digitalization of information and communication systems in critical infrastructures not only enhances efficiency in information processing and dissemination but also increases security.

The findings underscore the necessity for a structured and continuous development of crisis management practices, particularly through the integration of digital solutions and the promotion of a culture of flexibility and willingness to learn. The thesis provides valuable insights and concrete recommendations for optimizing the work of crisis teams and contributes to improving the resilience and high availability of critical infrastructures.

14 Anhang

14.1 Beschreibung Online-Befragung

Umfrage zur Untersuchung der Flexibilität, Digitalisierung und Effizienz im Krisenmanagement kritischer Infrastrukturen.

Ich heiße Michael Meier, bin im Krisenmanagement kritischer Infrastrukturen tätig und studiere derzeit berufsbegleitend an der Universität Wien. Im Rahmen meiner Masterarbeit im Studiengang Risikoprävention und Katastrophenmanagement untersuche ich die Effizienz des Krisenmanagements bei kritischen Infrastrukturen.

Zu diesem Zweck führe ich eine Online-Umfrage durch, die wichtige Erkenntnisse über die gegenwärtigen Herausforderungen in diesem Bereich liefern soll. Die Befragung zielt darauf ab, ein tieferes Verständnis für die Effektivität von Krisenmanagementstrategien zu entwickeln und Wege zu finden, wie diese verbessert werden können, um die Widerstandsfähigkeit kritischer Infrastrukturen zu stärken.

Ich lade Sie herzlich ein, an dieser Umfrage teilzunehmen, die etwa 10 bis 15 Minuten Ihrer Zeit in Anspruch nehmen wird. Ihre Teilnahme ist freiwillig und erfolgt vollständig anonym. Rückschlüsse auf Ihre Person sind nicht möglich. Die Ergebnisse der Umfrage werden in meiner Masterarbeit in aggregierter Form veröffentlicht und leisten einen wertvollen Beitrag zur Forschung im Bereich des Krisenmanagements in kritischen Infrastrukturen.

Bitte folgen Sie diesem Link, um den Fragebogen zu öffnen: https://der-meier.at/kritis_umfrage

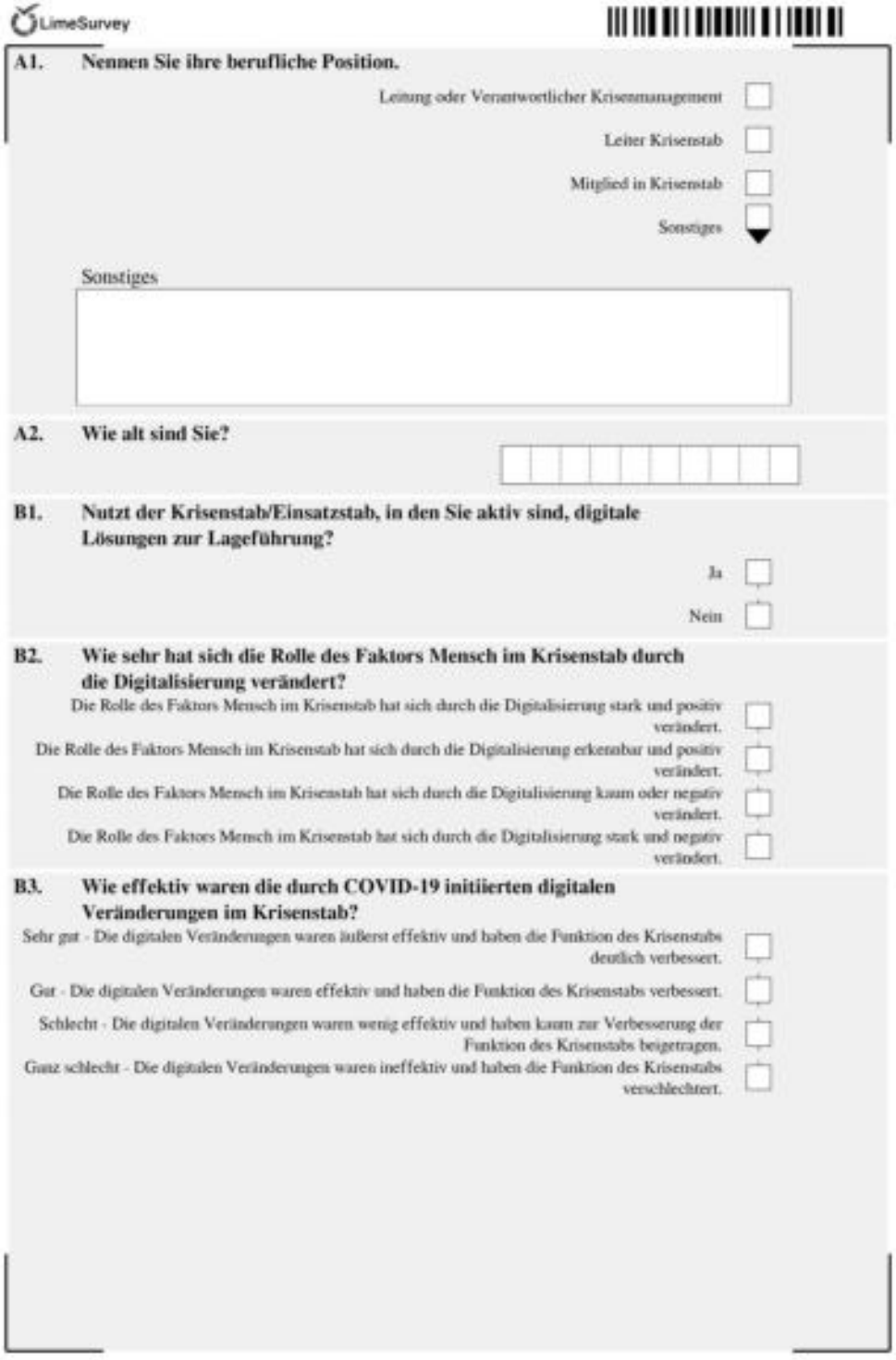
Für Fragen oder Anregungen stehe ich Ihnen gerne via E-Mail zur Verfügung. Ihre Unterstützung ermöglicht es, wertvollen Input aus der Praxis in die Arbeit einfließen zu lassen, wodurch bedeutende Erkenntnisse gewonnen werden können.

Ich danke Ihnen herzlich für Ihre Mitarbeit. Gerne können Sie diese Nachricht an weitere Expertinnen und Experten im Bereich des Krisenmanagements und kritischer Infrastrukturen weiterleiten. Falls Sie Interesse an den Ergebnissen meiner Arbeit haben, kontaktieren Sie mich bitte per E-Mail (mike@der-meier.at), damit ich mich bei Ihnen melden kann.

Vielen Dank für Ihre Unterstützung.

Michael Meier

Onlinefragebogen



LimeSurvey

A1. Nennen Sie ihre berufliche Position.

- [ ] Leitung oder Verantwortlicher Krisenmanagement
- [ ] Leiter Krisenstab
- [ ] Mitglied in Krisenstab
- [ ] Sonstiges

Sonstiges

A2. Wie alt sind Sie?

B1. Nutzt der Krisenstab/Einsatzstab, in den Sie aktiv sind, digitale Lösungen zur Lageführung?

- [ ] Ja
- [ ] Nein

B2. Wie sehr hat sich die Rolle des Faktors Mensch im Krisenstab durch die Digitalisierung verändert?

- [ ] Die Rolle des Faktors Mensch im Krisenstab hat sich durch die Digitalisierung stark und positiv verändert.
- [ ] Die Rolle des Faktors Mensch im Krisenstab hat sich durch die Digitalisierung erkennbar und positiv verändert.
- [ ] Die Rolle des Faktors Mensch im Krisenstab hat sich durch die Digitalisierung kaum oder negativ verändert.
- [ ] Die Rolle des Faktors Mensch im Krisenstab hat sich durch die Digitalisierung stark und negativ verändert.

B3. Wie effektiv waren die durch COVID-19 initiierten digitalen Veränderungen im Krisenstab?

- [ ] Sehr gut - Die digitalen Veränderungen waren äußerst effektiv und haben die Funktion des Krisenstabs deutlich verbessert.
- [ ] Gut - Die digitalen Veränderungen waren effektiv und haben die Funktion des Krisenstabs verbessert.
- [ ] Schlecht - Die digitalen Veränderungen waren wenig effektiv und haben kaum zur Verbesserung der Funktion des Krisenstabs beigetragen.
- [ ] Ganz schlecht - Die digitalen Veränderungen waren ineffektiv und haben die Funktion des Krisenstabs verschlechtert.

LimeSurvey

B4. Inwiefern stellen organisatorische Faktoren ein Hindernis für die Digitalisierung hinsichtlich Führungs- und Führungsunterstützungssysteme im Krisenstab dar?

- Sehr gut - Organisatorische Faktoren stellen kein Hindernis für die Digitalisierung dar und fördern sogar die Implementierung von digitalen Führungs- und Führungsunterstützungssystemen. ☐
- Gut - Organisatorische Faktoren stellen nur geringfügige Hindernisse für die Digitalisierung dar, die leicht überwindbar sind. ☐
- Schlecht - Organisatorische Faktoren stellen signifikante Hindernisse für die Digitalisierung dar und erschweren die Implementierung von digitalen Führungs- und Führungsunterstützungssystemen. ☐
- Ganz schlecht - Organisatorische Faktoren stellen erhebliche Hindernisse für die Digitalisierung dar und verhindern effektiv die Implementierung von digitalen Führungs- und Führungsunterstützungssystemen. ☐

B5. Welche technischen Hindernisse sehen Sie bei der Einführung von digitalen Mitteln (Führungs- bzw. Führungsunterstützungssysteme) im Krisenmanagement?

- Die Einführung von digitalen Führungs- und Führungsunterstützungssystemen verläuft reibungslos. ☐
- Geringe technische Hindernisse, die schnell und effizient gelöst werden können und die Einführung nicht wesentlich beeinträchtigen. ☐
- Erhebliche technische Hindernisse, die die Einführung von digitalen Führungs- und Führungsunterstützungssystemen deutlich erschweren. ☐
- Sehr große technische Hindernisse, die die Einführung von digitalen Führungs- und Führungsunterstützungssystemen erheblich behindern oder sogar verhindern. ☐

B6. Nennen Sie die Art der eingesetzten digitalen Lösungen in Ihrem Wirkungsbereich.

- Alarmierungssystem (Notfallmanagementsoftware, Benachrichtungen etc.) ☐
- digitale Lageführung ☐
- Simulationsmodelle für die Entscheidungsunterstützung ☐
- Echtzeit Überwachungs- und Visualisierungssysteme ☐
- Datenbank- und Analysemodelle zur Visualisierung ☐
- eigene (gesicherte) Videokonferenzmodelle ☐
- gesicherte und Ausfallsichere Kommunikationsmittel ☐
- Sonstiges ☐

Sonstiges

B7. In welchen Einsatzbereichen werden digitale Lösungen, Werkzeuge und/oder Mittel eingesetzt?

- Kommunikation ☐
- Entscheidungsfindung ☐
- Datenanalyse ☐

LimeSurvey

Ressourcenmanagement ☐

Lageführung ☐

Keine digitalen Lösungen ☐

B8. Steigert der Einsatz von digitalen Lösungen die Effizienz des Krisenmanagements?

Der Einsatz digitaler Lösungen hat die Effizienz des Krisenmanagements erheblich gesteigert. ☐

Der Einsatz digitaler Lösungen hat die Effizienz des Krisenmanagements moderat gesteigert. ☐

Der Einsatz digitaler Lösungen hat nur geringfügig zur Effizienz des Krisenmanagements beigetragen. ☐

Der Einsatz digitaler Lösungen hat die Effizienz des Krisenmanagements nicht verbessert oder sogar verschlechtert. ☐

C1. Betreibt Ihre Organisation ein Informationssicherheitsmanagementsystem (z. B. ISO 27001)?

Ja ☐

Nein ☐

C2. Wurden Sie in Bezug auf Cybersicherheit/Informationssicherheit geschult?

Ja ☐

Nein ☐

C3. Sind die Softwarelösungen für die Arbeit im Krisenstab redundant ausgeführt bzw. gibt es definierte Rückfallebenen?

Ja, die Softwarelösungen sind redundant ausgeführt, es gibt definierte Rückfallebenen und ich bin darauf geschult worden. ☐

Ja, die Softwarelösungen sind redundant ausgeführt und es gibt definierte Rückfallebenen, aber ich bin nicht darauf geschult worden. ☐

Nein, die Softwarelösungen sind nicht redundant ausgeführt und es gibt keine definierten Rückfallebenen. ☐

Ich weiß nicht, ob die Softwarelösungen redundant ausgeführt sind oder ob es definierte Rückfallebenen gibt. ☐

C4. Wurden Sie bezüglich der sicheren und vertraulichen Verwendung der digitalen Führungssysteme geschult?

Ja, ich wurde umfassend geschult, einschließlich IT-Sicherheitsaspekten und Maßnahmen bei Systemausfällen. ☐

Ja, ich wurde grundlegend geschult, jedoch ohne spezifische Schulung zu IT-Sicherheitsaspekten. ☐

Nein, ich wurde nicht bezüglich der sicheren und vertraulichen Verwendung geschult. ☐

Ich bin mir nicht sicher oder weiß nicht, ob eine solche Schulung stattgefunden hat. ☐

LimeSurvey

C5. Wie bewerten Sie Ihren Wissensstand hinsichtlich Cybersecurity?

- Sehr gut - Ich habe umfassendes Wissen und bin sehr sicher im Umgang mit Cybersecurity-Themen. ☐
- Gut - Ich habe ein gutes Grundverständnis von Cybersecurity und kann die meisten relevanten Probleme erkennen und adressieren. ☐
- Ausreichend - Mein Wissen über Cybersecurity ist begrenzt; ich kenne einige Grundlagen, fühle mich aber nicht in allen Situationen sicher. ☐
- Mangelhaft - Ich habe wenig bis gar kein Wissen über Cybersecurity und fühle mich in diesem Bereich unsicher. ☐

D1. Ist Ihnen die Theorie der Hochzuverlässigkeitsorganisationen (High Reliability Organization) im Allgemeinen bekannt?

- Ja ☐
- Nein ☐

D2. Haben Sie bereits ein Training bezüglich der Grundprinzipien der HRO-Theorie absolviert?

Diese umfassen wichtige Aspekte wie die kontinuierliche Auseinandersetzung mit potenziellen Fehlern, das Vermeiden von zu simplen Interpretationen und eine ausgeprägte Aufmerksamkeit für laufende Betriebsabläufe. Solche Kenntnisse sind besonders relevant, um die Fähigkeiten im Risiko- und Krisenmanagement bei kritischen Infrastrukturen einschätzen zu können. Rufen Sie sich hier die bekannten 5 Prinzipien in Erinnerung (Konzentration auf Fehler, Abneigung gegen Vereinfachung, Sensibilität für betriebliche Abläufe, Streben nach Resilienz, Respekt vor fachlichem Wissen / Fähigkeiten)

- Ja ☐
- Nein ☐

D3. Wie bewerten Sie die Flexibilität Ihrer Organisation hinsichtlich unvorhergesehener Ereignisse/Not- bzw. Störfälle?

- Sehr gut - Unsere Organisation reagiert sehr schnell und effektiv auf unvorhergesehene Ereignisse und Notfälle. ☐
- Gut - Unsere Organisation reagiert angemessen und zumeist effektiv auf unvorhergesehene Ereignisse und Notfälle. ☐
- Schlecht - Unsere Organisation reagiert oft zögerlich oder ineffektiv auf unvorhergesehene Ereignisse und Notfälle. ☐
- Sehr schlecht - Unsere Organisation ist nicht in der Lage, angemessen auf unvorhergesehene Ereignisse und Notfälle zu reagieren. ☐

D4. Wie bewerten Sie die Flexibilität Ihrer Organisation innerhalb der Stabsarbeit?

- Sehr gut - Unsere Organisation zeigt innerhalb der Stabsarbeit hohe Flexibilität und kann sich schnell an veränderte Bedingungen anpassen. ☐
- Gut - Unsere Organisation zeigt eine angemessene Flexibilität in der Stabsarbeit, wobei gelegentliche Anpassungen effektiv durchgeführt werden. ☐
- Schlecht - Anpassungen an veränderte Bedingungen erfolgen oft verzögert oder sind ineffektiv. ☐
- Sehr schlecht - Anpassungen an neue Situationen sind unzureichend oder unterbleiben. ☐

LimeSurvey

D5. Wie erfolgt die Bewertung und Priorisierung von Entscheidungsoptionen in Ihrem Krisenstab?

- Sehr gut - Entscheidungen werden effizient und systematisch priorisiert, wobei Fachexpertise maßgeblich genutzt wird. ☐
- Gut - Entscheidungen werden meist angemessen bewertet und priorisiert, mit guter Einbindung der Fachexpertise. ☐
- Schlecht - Entscheidungen werden oft zentralisiert getroffen, wobei die Fachexpertise nur teilweise berücksichtigt wird. ☐
- Fachexpertise wird selten oder nicht nachvollziehbar berücksichtigt. ☐

E1. Werden Maßnahmen, Findings, Learnings der Stabsarbeit/Krisenmanagement in die Regelorganisation übernommen?

- Ja, regelmäßig - Alle relevanten Ergebnisse werden systematisch in die Regelorganisation übernommen. ☐
- Teilweise - Einige, aber nicht alle relevanten Ergebnisse werden in die Regelorganisation übernommen. ☐
- Selten - Nur gelegentlich werden Erkenntnisse in die Regelorganisation übernommen. ☐
- Nein, nie - Ergebnisse aus der Stabsarbeit werden nicht in die Regelorganisation übernommen. ☐

E2. Wie wird der Erfolg des Krisenmanagements/der Stabsarbeit gemessen?

- Durch spezifische Leistungsindikatoren (KPIs): Der Erfolg wird anhand festgelegter Indikatoren wie Reaktionszeit, Anzahl gelöster Krisen und Budgeteinhaltung gemessen. ☐
- Mittels Feedback und Bewertungen von beteiligten Stakeholdern: Erfolgsmessung erfolgt durch Auswertung des Feedbacks von internen und externen Stakeholdern. ☐
- Durch regelmäßige Überprüfungen und Audits: Erfolg wird durch interne Überprüfungen und externe Audits bewertet. ☐
- Anhand der Analyse von Nachbereitungsberichten: Der Erfolg wird durch die Analyse von After-Action-Reports und Lessons-Learned bewertet. ☐
- Ich bin mir nicht sicher oder kenne die Methoden nicht, die verwendet werden: Unbekannt, welche Methoden zur Erfolgsmessung eingesetzt werden. ☐

E3. Wie bewerten Sie selbst die Effektivität hinsichtlich „Lernen aus Fehlern" in Ihrer Organisation?

- Sehr gut - wir haben ein starkes Bewusstsein und Ressourcen, die konsequent zur Verbesserung eingesetzt werden. ☐
- Gut - Wir lernen häufig aus Fehlern, unterstützt durch vorhandene Ressourcen und ein vorhandenes Bewusstsein, jedoch könnte der kontinuierliche Verbesserungsprozess weiter ausgebaut werden. ☐
- Befriedigend - Das Lernen aus Fehlern findet statt, aber es fehlen oft die Ressourcen oder das systematische Vorgehen für einen kontinuierlichen Verbesserungsprozess. ☐
- Ausbaufähig - Es besteht ein Bewusstsein für die Notwendigkeit des Lernens aus Fehlern, jedoch mangelt es an einem etablierten KVP-System und den notwendigen Ressourcen, um dieses effektiv umzusetzen. ☐

E4. Unterscheidet sich die Arbeit im Krisenmanagement/Stabsarbeit gegenüber der Arbeitsweise aus der Regelorganisation?

- Stark unterschiedlich - Die Arbeitsweise im Krisenmanagement/Stabsarbeit ist vollkommen anders als in der Regelorganisation und erfordert spezielle Fähigkeiten und Prozesse. ☐
- Teilweise unterschiedlich - Es gibt einige deutliche Unterschiede in der Arbeitsweise zwischen Krisenmanagement/Stabsarbeit und der Regelorganisation, obwohl einige Gemeinsamkeiten bestehen. ☐
- Geringfügig unterschiedlich - Die Arbeitsweise im Krisenmanagement/Stabsarbeit ist der Regelorganisation ähnlich, mit nur geringen Unterschieden. ☐
- Kein Unterschied - Die Arbeitsweise im Krisenmanagement/Stabsarbeit entspricht der in der Regelorganisation. ☐

LimeSurvey

E5. Wie erfolgt die erste Einschätzung unvorhersehbarer Ereignisse in Ihrem Krisenmanagement?

- Spontan und ad-hoc - Die erste Einschätzung erfolgt spontan und ohne vorher festgelegte Richtlinien oder Protokolle. ☐
- Nach einem vordefinierten Protokoll - Wir folgen einem klar definierten Protokoll oder Richtlinien, die speziell für unvorhersehbare Ereignisse entwickelt wurden. ☐
- Durch ein spezialisiertes Incident Response Team - Ein spezialisiertes Team, das für solche Fälle ausgebildet ist, übernimmt die erste Einschätzung. ☐
- Gar nicht - In unserer Organisation gehen wir davon aus, dass keine unvorhersehbaren Ereignisse eintreten können. ☐

E6. Wie reagiert Ihre Führungskraft, in der Regelorganisation, auf unvorhersehbare Ereignisse?

- Sehr proaktiv - Unsere Führungskraft reagiert sofort und effektiv, um die Situation zu managen. ☐
- Proaktiv - Reaktion erfolgt schnell mit aktiver Lösungssuche. ☐
- Reaktiv - Unsere Führungskraft reagiert erst nachdem sich Probleme entwickelt haben. ☐
- Unzureichend - Die Reaktion ist verzögert oder ineffektiv. ☐

F1. Zu welchen Sektor der kritischen Infrastruktur zählt Ihre Organisation?

- Staat und Verwaltung ☐
- Weltraum ☐
- IT Service und Management ☐
- Digitale Infrastruktur ☐
- Abwasser und Trinkwasser ☐
- Gesundheit ☐
- Finanzen und Banken ☐
- Transport und Verkehr ☐
- Energie ☐
- Forschung ☐
- Lebensmittel ☐

LimeSurvey

Vielen Dank, dass Sie sich die Zeit genommen haben, an der Umfrage teilzunehmen! Ihr Beitrag ist für die Verbesserung des Krisenmanagements in kritischen Infrastrukturen äußerst wertvoll.

Falls Sie Interesse an den Ergebnissen der Umfrage und weiteren Informationen zu meiner Arbeit haben, senden Sie mir bitte eine E-Mail. Bitte beachten Sie, dass keine automatische Benachrichtigung über die Ergebnisse vorgesehen ist.

Folgen Sie mir auch gerne in den sozialen Netzwerken.

Nochmals vielen Dank für Ihre Mitarbeit und Ihr Interesse!

14.2 Leitfaden Experteninterview

1 Allgemeines zu Arbeit

Die Master-Thesis konzentriert sich auf die Optimierung der Stabsarbeit in Krisensituationen, insbesondere in Bezug auf kritische Infrastrukturen. Ziel ist eine ganzheitliche Untersuchung durchzuführen, die Flexibilität, mögliche Digitalisierungsmöglichkeiten und Effizienz in den Mittelpunkt stellt. Dabei stehen die Verbesserung der Krisenbewältigung und die Anwendung von Hochzuverlässigen Organisationen (high reliability organization)-Ansätzen (HRO-Theorie) im Fokus.

Inhaltlich wird sich die Arbeit mit folgenden Themen befassen:

- Flexibilität und menschliche Fehler in der Stabsarbeit: Untersuchung der Organisationsstruktur von Stäben und Maßnahmen zur Minimierung menschlicher Fehler unter Stress, Zeitdruck und Ermüdung.
- Vorbereitung der Stabsmitglieder: Entwicklung von Ansätzen zur besseren Vorbereitung von Stabsmitgliedern auf komplexe Ereignisse
- Evaluierung von Stabsarbeit in kritischen Infrastrukturen: Eine Analyse zur Effektivität von Stabsstrukturen und -prozessen in kritischen Infrastrukturen, einschließlich der Anwendung der HRO-Theorie zur Verbesserung der Krisenbewältigung.
- Digitalisierung und Effizienz in Stabsarbeit: Die Integration von digitalen Werkzeugen und Organisationsstrukturen zur Steigerung der Effizienz in der Stabsarbeit.

1.1 Kurzdarstellung High Reliability Theory

Die HRO-Theorie, oder Theorie der Hochzuverlässigkeitsorganisationen, ist ein Konzept, das erklärt, wie manche Organisationen es schaffen, unter extrem schwierigen Umständen fast fehlerfrei zu arbeiten. Es sind zumeist Organisationen, wo jeder kleine Fehler zu ernsten Problemen führen kann. Solche Organisationen müssen also sehr zuverlässig sein.

Die HRO-Theorie besagt, dass diese Organisationen bestimmte Eigenschaften haben, die sie besonders gut machen in dem, was sie tun. Sie sind zum Beispiel sehr aufmerksam auf mögliche Probleme, bevor diese auftreten, sie lernen ständig dazu und können sich gut anpassen, wenn sich die Situation ändert. Sie haben auch eine Kultur, in der Sicherheit an erster Stelle steht, und wo alle Mitarbeiter sich trauen, Bedenken zu äußern, wenn ihnen etwas auffällt, das nicht ganz richtig ist.

Das Besondere an diesen Organisationen ist nicht nur, dass sie Fehler vermeiden, sondern auch, dass sie ständig bereit sind, aus Situationen zu lernen und sich zu verbessern. Dadurch schaffen sie es, auch in stressigen und unvorhersehbaren Situationen gut zu funktionieren.

1.2 HRO Prinzipen

Sensibilität für betriebliche Abläufe: HROs zeichnen sich durch eine kontinuierliche Fokussierung auf die Feinheiten der operativen Abläufe aus. Diese Praxis ermöglicht es ihnen, Abweichungen von Normprozessen frühzeitig zu erkennen und präventive Maßnahmen zu ergreifen. Es herrscht ein ständiger Zustand der Wachsamkeit, wobei operatives Feedback systematisch in den Entscheidungsfindungsprozess eingebettet wird.

Abneigung gegen Vereinfachung: HROs hinterfragen aktiv die Validität ihrer eigenen Wissensstrukturen und widerstehen der Versuchung, komplexe Situationen zu simplifizieren. Durch die Befürwortung einer differenzierten Betrachtung von Ereignissen und Signalen streben sie nach einem umfassenden und nuancierten Verständnis operativer Gegebenheiten.

Streben nach Flexibilität: Die Anpassungsfähigkeit an unvorhergesehene und sich dynamisch verändernde Bedingungen ist ein Schlüsselaspekt von HROs. Diese Flexibilität manifestiert sich in der Fähigkeit, Hierarchien temporär außer Kraft zu setzen, um Expertise und Entscheidungskompetenzen dorthin zu verlagern, wo sie im Hinblick auf eine konkrete Problemstellung am meisten benötigt werden.

Respekt vor Expertise: HROs charakterisiert ein hierarchieübergreifender Respekt vor Fachwissen und Kompetenz. Entscheidungen werden auf der Grundlage von Expertise und nicht nach Rang getroffen, wobei operative Teams befugt sind, diejenigen mit der größten Sachkenntnis zur Leitung von Prozessen zu ermächtigen.

Streben nach Resilienz: Dieses Prinzip reflektiert das Bestreben, die Fähigkeit zur Erholung und Restitution nach Störereignissen zu maximieren. Es impliziert den Aufbau von Redundanzen und die Entwicklung von Notfallplänen sowie die Kultivierung einer Organisationskultur, die kontinuierliches Lernen und die Verbesserung von Sicherheitsmaßnahmen fördert.

1.3 Einleitung

- Begrüßung und Vorstellung.
- Kurze Erläuterung des Forschungsprojekts und des Zwecks des Interviews.
- Bestätigung der Vertraulichkeit und ggf Anonymität der Informationen.
- Zustimmung zur Aufzeichnung des Gesprächs erbitten.
- Geschätzte Dauer des Interviews mitteilen.

1.3.1 Warm-Up-Fragen

1. **Einleitung:** Könnten Sie bitte Ihren beruflichen Hintergrund beschreiben und wie Sie in den Bereich Krisenmanagement speziell für kritische Infrastrukturen gekommen sind?

2 Hauptteil

1. **Flexibilität und Anpassungsfähigkeit:** Wie implementiert Ihre Organisation Anpassungsfähigkeit in das Krisenmanagement für kritische Infrastrukturen?
2. **Digitalisierung:** Welche Rolle spielen digitale Technologien im Krisenmanagement Ihrer Organisation, und wie verbessern sie die Reaktionsfähigkeit in Krisensituationen?
3. **Effizienz der Stabsarbeit:** Welche Maßnahmen wurden ergriffen, um die Effizienz der Stabsarbeit zu verbessern, und wie wird deren Erfolg bewertet?
4. **Anwendung der HRO-Theorie:** Inwiefern werden Konzepte und Prinzipien der Hochzuverlässigen Organisationen im Krisenmanagement Ihrer Organisation berücksichtigt?
5. **Gemeinschaft und Stakeholder-Einbindung:** Können Sie den Prozess der Einbindung von Gemeinschaften und Stakeholdern beschreiben und wie deren Feedback in die Krisenmanagementpläne einfließt?*
6. **Feedback und kontinuierliche Verbesserung:** Wie wird Feedback aus Krisenmanagementübungen gesammelt und genutzt, um Prozesse kontinuierlich zu verbessern?
7. **Digitale und Cybersicherheit:** Welche spezifischen Strategien verfolgt Ihre Organisation, um die digitale und Cybersicherheit im Krisenmanagement zu stärken?
8. **Gesetzliche Anforderungen:** Wie werden gesetzliche und regulatorische Anforderungen in die Krisenmanagementstrategie Ihrer Organisation integriert?
9. **Kommunikation und Teamarbeit:** Können Sie Maßnahmen oder Techniken nennen, die zur Verbesserung der Kommunikation und Teamarbeit im Krisenmanagement geführt haben?
10. **Psychische und physische Belastung:** Wie werden psychische und physische Belastungen von Mitarbeitenden während und nach Krisensituationen adressiert?

Abschlussfragen

11. Gibt es ein spezifisches Beispiel oder eine Situation, die Sie hervorheben möchten, um die Wirksamkeit Ihres Krisenmanagements zu illustrieren?
12. Welche Schlüsselbereiche sehen Sie als zukünftige Herausforderungen oder Verbesserungsmöglichkeiten im Krisenmanagement für kritische Infrastrukturen?

Leitfaden Experten Interview

3 Abschluss

- Dank an den Experten für die Teilnahme.
- Information über die nächsten Schritte und wie die Ergebnisse verwendet werden.
- Möglichkeit für den Experten, weitere Gedanken oder Fragen zu äußern.

Dieser Leitfaden ist darauf ausgelegt, ein tiefes Verständnis für effizientes Krisenmanagement in kritischen Infrastrukturen zu erlangen, indem er spezifische Aspekte wie Flexibilität, Digitalisierung und HRO-Theorie beleuchtet.

Leitfaden Experten Interview

4 Einverständniserklärung zur Verarbeitung persönlicher Daten im Rahmen der Masterarbeit

Titel der Masterarbeit:	Effizientes Krisenmanagement in kritischen Infrastrukturen
Name des Forschenden:	Michael Meier
Institution:	
Telefon:	
E-Mail:	mike@der-meier.at

Sehr geehrte(r) [Name des/der Experten/Expertin],

im Rahmen meiner Masterarbeit mit dem Schwerpunkt auf die Optimierung von Stabsarbeit in Krisensituationen bei kritischen Infrastrukturen führe ich ein Experteninterview durch. Ihre spezialisierten Kenntnisse und Erfahrungen im Bereich der kritischen Infrastruktur sind für das Verständnis und die tiefergehende Analyse der Thematik unverzichtbar.

Hiermit ersuche ich um Ihr Einverständnis, dass die während des Interviews gesammelten Informationen ausschließlich für akademische Zwecke im Kontext der oben genannten Masterarbeit verarbeitet werden dürfen. Dies beinhaltet:

- Die Aufzeichnung des Interviews.
- Die Transkription und Analyse des aufgezeichneten Gesprächs.
- Die Sicherstellung der Vertraulichkeit und den Schutz Ihrer persönlichen Daten gemäß den geltenden Datenschutzrichtlinien.

Bitte bekunden Sie Ihr Einverständnis zur Teilnahme an diesem Forschungsvorhaben durch Unterzeichnung dieser Erklärung. Sie haben das Recht, Ihre Zustimmung jederzeit zu widerrufen.

Ich bedanke mich herzlich für Ihre Unterstützung und wertvollen Beiträge zu meiner Forschungsarbeit.

Mit besten Grüßen,

Michael Meier

Leitfaden Experten Interview

4.1 Zustimmung:

Ich, bestätige hiermit meine freiwillige Zustimmung zur Verarbeitung meiner persönlichen Daten wie oben beschrieben und zur Verwendung im Rahmen der Masterarbeit von Herrn Michael Meier.

Sind Sie damit einverstanden, dass ich Ihren Namen in der Ausarbeitung verwende, oder möchten Sie anonym bleiben?"

Name veröffentlichen	**Nur anonymisiert werden**
☐ ja, darf veröffentlicht werden	☐ nein, nur anonymisiert

Ort, Datum: _____

Unterschrift: _____

Leitfaden Experten Interview