Hochschule für öffentliche Verwaltung und

Finanzen Ludwigsburg

Erfolgreiche Krisenkommunikation im Falle eines Ransomware–Angriffes in einer kleineren Kommunalverwaltung

Master-Thesis

zur Erlangung des Grades eines

Master of Arts (M. A.)

im Masterstudiengang Public Management

vorgelegt von

Dominik Morast

Studienjahr 2024 / 2025

Erstgutachterin: Professorin Dr. Gunda Rosenauer

Zweitgutachterin: Susanne Eva Krieg

Abstract

Erfolgreiche Krisenkommunikation ist ein wichtiger Bestandteil des Krisenmanagements. Die vorliegende Master-Thesis beschäftigt sich mit der Krisenkommunikation einer Kommunalverwaltung im Falle eines Ransomware-Angriffes. In den Fokus werden darin Verwaltungen von Kommunen bis ca. 20.000 Einwohnerinnen und Einwohnern genommen. Das Forschungsprojekt verfolgt das Ziel, wesentliche Erkenntnisse zu diesem Thema zu gewinnen und darauf basierend Handlungsempfehlungen abzuleiten. Zur Beantwortung der Forschungsfrage und deren Unterfragen fand eine systematische Literaturrecherche statt. Weiterhin wurden, auf Basis einer qualitativen Untersuchung durch Interviews mit Expertinnen und Experten, relevante Erfolgsfaktoren ermittelt und mögliche Ansatzpunkte aufgezeigt. Daraus werden Empfehlungen zum Gelingen der Kommunikation im Ernstfall abgeleitet.

Inhaltsverzeichnis

Inhaltsverzeichnis III
Abkürzungsverzeichnis V
Abbildungsverzeichnis VI
Verzeichnis der Anlagen VII
1. Einleitung 1
1.1 Ausgangslage und Problemstellung 2
1.2 Ziel der Arbeit und Forschungsfrage 4
1.3 Methodische Vorgehensweise 6
1.4 Aufbau der Arbeit 7
2. Krisen- und Notfallmanagement 8
2.1 Definitionen und Begriffsverständnis von Krise 9
2.2 Elemente des Krisen- und Notfallmanagements 11
2.2.1 Krisenmanagement als iterativer Gesamtprozess 12
2.2.2 Aufbauorganisation zur Krisenbewältigung 15
2.3 Notfallmanagement nach BSI-Standard 200-4 18
3. Krisenkommunikation 20
3.1 Definition 21
3.2 Ziele und Prinzipien von Krisenkommunikation 23
3.3 Relevante Zielgruppen und Kanäle 25
3.3.1 Interne Zielgruppen 26
3.3.2 Externe Zielgruppen 32
3.3.3 Beteiligte im Krisenmanagement 43
3.4 Vorbereitung der Krisenkommunikation 44
4. Zwischenfazit 48
5. Interviews mit Expertinnen und Experten zur Erhebung von Schlüsselfaktoren für eine erfolgreiche Krisenkommunikation 50
5.1 Forschungsmethode 51
5.2 Auswahl und Beschreibung der Expertinnen und Experten 55
5.3 Leitfragen als Grundlage für die Interviews 60
5.4 Analyse der Interviews 61

6. Ergebnisse der qualitativen Befragung 63
6.1 Aufbauorganisation und Zusammenarbeit in der Krise 63
6.1.1 Der Krisenstab als Basis 64
6.1.2 Einbindung aller relevanten Akteure 65
6.1.3 Klare Aufgaben und Rollenverteilung 66
6.2 Kommunikationsverhalten und Kommunikationsfähigkeit 66
6.2.1 Proaktive und transparente Kommunikation 67
6.2.2 Bedeutung von Kompetenzen und Know-How 67
6.3 Erreichen der wichtigsten Zielgruppen 68
6.3.1 Kommunikation mit den Mitarbeitenden 69
6.3.2 Nutzung vorhandener Kommunikationskanäle 69
6.3.3 Website als zentraler Kommunikationskanal nach außen 71
6.4 Vorbereitung auf die Krise 71
6.4.1 Funktionstüchtigkeit der Kommunikationstechnik 72
6.4.2 Organisatorische Vorbereitung auf die Krise 72
6.5 Disponieren der Ressourcen 74
6.5.1 Einsatz der eigenen personellen Ressourcen 74
6.5.2 Unterstützung durch externe Organisationen 74
7. Diskussion und Synthese der Ergebnisse 75
8. Erkenntnisse und Ableitung von Handlungsempfehlungen 84
9. Fazit 87
Literaturverzeichnis 90
Ehrenerklärung 98
Anlagen .....

Abkürzungsverzeichnis

Abb.	Abbildung
Abs.	Absatz
Art.	Artikel
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BCM	Business Continuity Management
BSI	Bundesamt für Sicherheit in der Informationstechnik
bzw.	beziehungsweise
ca.	circa
CSBW	Cybersicherheitsagentur Baden-Württemberg
CSG	Gesetz für die Cybersicherheit in Baden-Württemberg
dt.	deutsch
DSGVO	Datenschutz-Grundverordnung
GemO	Gemeindeordnung Baden-Württemberg
GG	Grundgesetz
ggf.	gegebenenfalls
i.S.	im Sinne
i.S.d.	im Sinne des
IT	Informationstechnologie
RN	Randnummer
S.	Seite
sog.	sogenannte
Tsd.	Tausend
vgl.	vergleiche
VZÄ	Vollzeitäquivalent
Z.	Zeile
z.T.	zum Teil

Abbildungsverzeichnis

Abbildung 1 Bestandteile des Krisenmanagements nach BMI 13

Abbildung 2 Der Risiko- und Krisenmanagementzyklus nach BBK 14

Abbildung 3 Managementsysteme nach BSI–Standard 200–4 19

Abbildung 4 Risiko- und Krisenkommunikation nach BBK 22

Abbildung 5 Interviewpartnerinnen und Interviewpartner 59

Abbildung 6 Matrix der herausgebildeten Kategorien 63

Abbildung 7 Schadenbewältigungsverlauf nach BSI–Standard 200–4 81

Abbildung 8 Handlungsempfehlungen 87

Verzeichnis der Anlagen

Anlage 1	Muster-Pressemitteilung
Anlage 2	Muster-FAQ für Bevölkerung
Anlage 3	Muster-FAQ für Mitarbeitenden
Anlage 4	Muster-Aushang für Mitarbeitenden
Anlage 5	Muster-Anschreiben nach Art. 34 DSGVO
Anlage 6	Interviewleitfaden Kommune
Anlage 7	Interviewleitfaden externe Organisation

Die folgenden Dokumente sind nur als digitale Anlage beigefügt und nicht in der Druckausgabe enthalten.

Anlage 8	Einverständniserklärung zur Erhebung und Verarbeitung von Interviewdaten
Anlage 9:	Transkription A
Anlage 10:	Transkription B
Anlage 11:	Transkription C
Anlage 12:	Transkription D
Anlage 13:	Transkription E
Anlage 14:	Transkription F

1. Einleitung

In den meisten Unternehmen und (Kommunal-) Verwaltungen dürfte Krisenkommunikation ein Themenfeld sein, das nur ausnahmsweise bespielt wird, da Krisenszenarien dort nicht alltäglich auftreten und daher nicht ständig zu bewältigen sind. Es ist jedoch feststellbar, dass die unterschiedlichsten Ereignisse, wie zum Beispiel kriminelle Handlungen, betriebliche Störungen, Naturereignisse oder Unfälle, geeignet sind, sich zu Krisen zu entwickeln.[1] Die Möglichkeit des Eintritts einer krisenhaften Lage und des damit verbundenen Kommunikationsbedarfs ist vor diesem Hintergrund grundsätzlich auch für Unternehmen und (Kommunal-) Verwaltungen jederzeit gegeben.[2] Eine immer stärker werden Relevanz erhält dabei die zunehmende Bedrohungslage aus dem Cyberraum.[3] Die voranschreitende Digitalisierung bietet nicht nur Chancen, sondern birgt auch neue Gefahren und Risiken.[4] Zusätzliche Angriffsflächen werden geschaffen und neue Notfall- bzw. Krisenszenarien tun sich auf. Ein Cyberangriff, der durch die Verschlüsselung sämtlicher Daten und Server ein Unternehmen oder eine Verwaltung nahezu handlungsunfähig macht, unterzieht die betroffene Organisation einem Stresstest.[5] Er stellt damit die Managementsysteme und die Organisationsstrukturen sowie die handelnden Personen auf eine Belastungsprobe. Das Krisenmanagement und als wichtiger Bestandteil

[1] Trauboth, J. H. (2022): Grundlagen für professionelles Krisenmanagement in einer sich verändernden Welt, 2022, S. 26; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 6.

[2] Vgl. hierzu auch Bachmann, S.; Ternès von Hattburg, A. (2021): Effiziente Krisenkommunikation - transparent und authentisch, S. 1; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 2.

[3] BSI: Die Lage der IT-Sicherheit in Deutschland 2023, S. 68, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html (16.11.2024); CSBW: Jahresbericht 2023, S. 10, https://www.cybersicherheit-bw.de/jahresbericht-2023 (16.11.2024); BSI-Standard 200 - 4 Business Continuity Management, S. 13, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html (16.11.2024); Kulow, A. - C. (2022): Informations- und Cybersicherheit, S. 343 f..

[4] BSI: Die Lage der IT-Sicherheit in Deutschland 2023, S. 3; CSBW: Jahresbericht 2023, S. 12.

[5] BSI: Die Lage der IT-Sicherheit in Deutschland 2023, S. 67; CSBW: Jahresbericht 2023, S. 36.

davon die Krisenkommunikation sind dabei stark gefordert.[6] Aufgrund der zunehmenden Bedrohungslage und den immer häufiger auch auf Kommunalverwaltungen stattfindenden Cyberangriffen, ist die Thematik präsenter denn je.[7]

1.1 Ausgangslage und Problemstellung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt in seinem Bericht „Die Lage der IT–Sicherheit in Deutschland 2023“ die Situation während des Berichtszeitraumes[8] als „angespannt bis kritisch“[9] und stuft die Bedrohungslage als „so hoch wie nie zuvor“[10] ein. Die Cybersicherheitsagentur Baden–Württemberg bewertet die Lage ebenso kritisch. In Teilbereichen wird ihrerseits eine erhebliche Steigerung von Cyberattacken festgestellt.[11] Das BSI führt in seinem Bericht weiterhin aus, dass Landes- und Kommunalverwaltungen verstärkt Opfer cyberkrimineller Ransomware–Angriffe[12] geworden sind. Durchschnittlich wurden monatlich zwei Kommunalverwaltungen oder kommunale Betriebe als Opfer von Ransomware–Angriffen bekannt. Damit waren sie dem BSI zufolge überproportional von Ransomware-Angriffen betroffen.[13] Es ist inzwischen gängige Praxis, dass im Rahmen vorbezeichneter Cyberattacken nicht nur zentrale Server verschlüsselt werden und dadurch die betroffene Verwaltung z.T. handlungsunfähig wird, sondern auch Daten von Bürgerinnen und Bürgern gestohlen und teilweise auch auf Leak–Seiten illegal publiziert werden.[14] Veröffentlicht werden teils komplette Verzeichnisse mit Akten von Einzelpersonen. Die im behördlichen IT-Netz-

---

[6] CSBW: Jahresbericht 2023, S. 36 f.; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 234 f.; Merten, K. (2013): Krise, Krisenmanagement und Krisenkommunikation, S. 159.

[7] BSI: Die Lage der IT-Sicherheit in Deutschland 2023, S. 68; CSBW: Jahresbericht 2023, S. 9; BSI-Standard 200-4 Business Continuity Management, S. 13.

[8] Berichtszeitraum: 01. Juni 2022 bis 30. Juni 2023

[9] BSI: Die Lage der IT-Sicherheit in Deutschland 2023, S. 11.

[10] BSI: Die Lage der IT-Sicherheit in Deutschland 2023, S. 11.

[11] CSBW: Jahresbericht 2023, S. 10; CSBW: Leitfaden zur Cybersicherheit, S. 3, https://www.cybersicherheit-bw.de/fuer-cybersicherheit-sensibilisieren (16.11.2024).

[12] Erläuterungen zu der Angriffsart "Ransomware": BSI: Die Lage der IT-Sicherheit in Deutschland 2023, S. 14.

[13] BSI: Die Lage der IT-Sicherheit in Deutschland 2023, S. 56 Abb. S. 16 u. S. 68.

[14] Vgl. hierzu auch Stadtverwaltung Schriesheim: Cyberangriff bei der Stadt Schriesheim-Datenverlust leider bestätigt, https://www.schriesheim.de/de/Aktuelles/Stadtnachrichten/Nachricht?view=publish&item=article&id=1141 (16.11.2024).

werk befindliche Schadsoftware hat ferner zum Ziel, sich weiter in der Netzwerkinfrastruktur und damit auch zu anderen, in das Netzwerk eingebundenen Organisationen, auszubreiten.[15] Das BSI berichtet, dass die betroffenen Verwaltungen im Regelfall einige Tage bis zu mehreren Wochen nicht in der Lage waren, die gewohnten Verwaltungsleistungen zu erbringen. Teils litten die Verwaltungen noch Monate nach dem Vorfall unter Beeinträchtigungen.[16]

Die Lageberichte des BSI und der CSBW verdeutlichen eindringlich die Relevanz und Praxisnähe des Szenarios „Ransomware–Angriff" für Kommunalverwaltungen. Die Baden-Württembergischen Gemeindeverwaltungen Schriesheim und Burladingen zählen neben weiteren Gemeinden zu den Opfern entsprechender Vorfälle und haben sich in der Situation wiedergefunden, die (Not-) Lage meistern zu müssen.[17] Die Aufgabe, die technischen Störungen zu beheben, um die Funktionsfähigkeit der Verwaltung wiederherzustellen, ist dabei nur eine der zu bewältigenden Aufgabenstellungen im Ernstfall. Eine besondere Herausforderung stellt die Kommunikation zur Außenwelt, aber auch z.B. zu den Mitarbeiterinnen und Mitarbeitern dar.[18] Folgendermaßen könnte sich das Bild in Schriesheim oder Burladingen dargestellt haben:

Bürgerinnen und Bürger, die dringend eine Verwaltungsleistung (wie z.B. einen Expressreisepass) benötigen, drängen auf Funktionsfähigkeit der Verwaltung und auf Informationen, wann die Leistung erbracht werden kann. Andere Personen sind ggf. verunsichert, weil vielleicht Kreditkartendaten von Hackern gestohlen wurden und verlangen nach zügiger Klärung. Ein weiterer Personenkreis macht sich eventuell noch größere Sorgen und hat Angst, dass essentielle Versorgungsleistungen wie Strom, Wasser und Gas in Kürze nicht mehr zur Verfügung stehen könnten. Die Belegschaft im Rathaus ist sich unsicher, ob sie nach Hause gehen darf. Der

---

[15] BSI: Die Lage der IT-Sicherheit in Deutschland 2023, S. 16.

[16] BSI: Die Lage der IT-Sicherheit in Deutschland 2023, S. 68; Vgl. hierzu auch CSBW: Jahresbericht 2023, S. 10.

[17] Stadtverwaltung Schriesheim: Cyberangriff bei der Stadt Schriesheim - Datenverlust leider bestätigt; B2B - Cyber–Security: Stadtverwaltung Burladingen durch Ransomware lahmgelegt, https://b2b-cyber-security.de/stadtverwaltung-burladingen-durch-ransomware-lahmgelegt/ (16.11.2024).

[18] BSI-Standard 200-4 Business Continuity Management, S. 139 ff.; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 36 ff.; BMI: Leitfaden Krisenkommunikation, S. 3; Kulow, A.-C. (2022): Informations- und Cybersicherheit, S. 365.

gewöhnliche Arbeitsalltag ist ohne IT, Telefon und Internet nicht möglich. Ob sich jemand von der „Rathausspitze“ bei Ihnen meldet, ist unklar. Es stellt sich die Frage: „Wie geht es hier in der Verwaltung jetzt weiter?“ Der ein oder andere Bedienstete ist besorgt, weil er befürchtet, dass private, teils sensible Bilder, die er auf dem Arbeitsrechner verbotenerweise abgelegt hat, von den Kriminellen gestohlen und im Internet oder im Darknet veröffentlicht werden. Einem anderen Teil der Belegschaft drängt sich der Gedanke auf, den Schaden durch das Öffnen einer E-Mail oder eines Links im Internet verursacht zu haben und vermutet, in Regress genommen zu werden. Es herrscht somit nicht nur bei der Bevölkerung, sondern auch intern Unsicherheit. Der Kommunikationsbedarf ist hoch. Schließlich stehen auch Vertreter der Presse, vielleicht zum Teil Radio- oder Fernsehteams, vor der Eingangstür des Rathauses und möchten über das „spektakuläre Ereignis“ berichten. Die Medienvertreter fordern unverzüglich ein Statement des Rathauses zum Vorfall. Die Managementebene zerbricht sich derweil bereits den Kopf, wie sie mit der Situation jetzt umgehen soll. „Wen zuerst informieren? Über welchen Kanal können wir kommunizieren? Geben wir nach außen Infos bekannt oder schweigen wir lieber? Muss der Vorfall nicht der Datenschutzbehörde proaktiv gemeldet werden? Sollten wir das regionale Rechenzentrum informieren, bevor wir über das kommunale Verwaltungsnetz andere Gemeinden gefährden?“

Das skizzierte Bild mag in der Realität etwas anders ausgesehen haben. Dennoch wird deutlich, wie notwendig und wichtig im Ernstfall eine gut funktionierende Kommunikation ist.[19]

1.2 Ziel der Arbeit und Forschungsfrage

An dieser Stelle möchte die vorliegende Master-Thesis ansetzen und Erkenntnisse gewinnen im Hinblick auf Schlüsselfaktoren für eine erfolgreiche Krisenkommunikation im Fall einer typischen Ransomware-Attacke[20], bei der jedoch die kritische Infrastruktur, die der Regulierung des BSI–Gesetzes unterliegen, nicht betroffen ist.

[19] Vgl. hierzu auch BMI: Leitfaden Krisenkommunikation, S. 6; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 1.

[20] Wie in Kap. 1.1 beschrieben; ausführlich BSI: Die Lage der IT-Sicherheit in Deutschland 2023, S. 14 ff..

Der Arbeit liegt die Annahme zu Grunde, dass kleinere Kommunalverwaltungen (ca. 80 - 200 Bedienstete) von Gemeinden bis ca. 20.000 Einwohnerinnen und Einwohnern nur eingeschränkt personelle Ressourcen (maximal 1,00 -1,50 VZÄ) für das Aufgabenspektrum Krisenmanagement und Kommunikation zur Verfügung stehen.

Inzwischen existiert zahlreiche Literatur zum Thema Krisenmanagement und Krisenkommunikation. Die vielfältigen Werke und Leitfäden allein können jedoch im Ernstfall nur eingeschränkt Nutzen bringen. Ob diese überhaupt von Kommunalverwaltungen, idealerweise bereits vor einem Schadensereignis, gelesen und die Theorie sinnvoll in die Praxis umgesetzt wird, ist nicht bekannt. Diese Forschungsarbeit möchte ausdrücklich nicht klären, auf welchem (Umsetzungs-) Stand sich die Kommunen derzeit befinden. Vielmehr steht bei dieser Master-Thesis die Forschungsfrage im Mittelpunkt:

„Welche Schlüsselfaktoren führen zu einer erfolgreichen Krisenkommunikation im Falle eines Ransomware–Angriffes?“

Aus dieser Forschungsfrage ergeben sich folgende Unterfragen:

- Worin liegen die wesentlichen Herausforderungen für kleinere Kommunalverwaltungen im Zuge der Krisenkommunikation im Zusammenhang mit einem Ransomware-Angriff?
- Welche Rolle spielen dabei die vorherrschenden Rahmenbedingungen?
- Welche Ansatzpunkte ergeben sich daraus für kleinere Kommunalverwaltungen für das Gelingen der Krisenkommunikation?

Die Arbeit richtet sich, dem gesetzten Ziel entsprechend, an die kommunale Praxis und dort insbesondere an die Spitzen–Managementebene der Kommunalverwaltungen. Diese trägt die Verantwortung für die sachgemäße Erledigung der Gemeinde-

aufgaben sowie für den ordnungsmäßigen Gang der Verwaltung und regelt die innere Organisation der Gemeindeverwaltung.[21] Darüber hinaus initiiert und steuert sie den Krisen- und Notfallmanagementprozess.[22]

1.3 Methodische Vorgehensweise

Im Rahmen der Master–Thesis findet zum einen eine systematische Literaturrecherche und zum anderen eine empirische Erhebung statt. Anhand einschlägiger Fachliteratur wird zunächst der Stand der Forschung aufgezeigt. Darauf aufbauen und daran anknüpfend folgt der empirische Teil des Forschungsprojekts.

Im empirischen Teil wird eine qualitative Forschung durch eine rekonstruierende Untersuchung in Form von Interviews mit Expertinnen und Experten durchgeführt. Diese Methode eignet sich, um Spezialwissen zu erschließen, persönliche Erfahrungen und Meinungen zu einem speziellen Sachverhalt zu erhalten und daraus Erkenntnisse zu gewinnen.[23]

Zur Datenerhebung bietet sich das leitfadengestützte Interview von Expertinnen und Experten an. Der Leitfaden dient dabei als Gerüst und stellt die Abhandlung aller relevanten Fragen sicher, ohne dass sich die interviewende Person zwingend an die Reihenfolge der zu stellenden Fragen halten muss. Daneben wird eine Vergleichbarkeit der Interviewergebnisse gewährleistet.[24] Es werden sechs Interviews mit sieben Expertinnen und Experten geführt. Dabei sind fünf der sieben interviewten Personen unmittelbar in einer von einer Ransomware – Attacke betroffenen Kommunalverwaltung tätig. Es wird bewusst auch auf Informantinnen und Informanten zurückgegriffen, die einen objektiven Blick „von außen“ einnehmen, aber dennoch die Rahmenbedingungen von Kommunalverwaltung einschätzen können. Dabei wird das Ziel verfolgt, eine möglichst breite Streuung für den Erkenntnisgewinn zu gewährleisten. Im Rahmen der Expertinnen und Expertenauswahl werden

[21] Gemeindeordnung Baden–Württemberg, § 44 Abs. 1.
[22] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 18; BSI-Standard 200-4 Business Continuity Management, S. 52.
[23] Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, S. 11.
[24] Schnell, R.; Hill, P. B.; Esser, E. (2023): Methoden der empirischen Sozialforschung, S. 356.

vorab Auswahlkriterien festgelegt, die die zu befragenden Personen erfüllen müssen. Dadurch wird sichergestellt, dass die aus den Interviews gewonnen Informationen einen gewissen Qualitätsstandard erfüllen und die gewonnenen Erkenntnisse einen belastbaren Mehrwert bringen.[25] Nach der Operationalisierung der Forschungsfrage und der Konzeption des Fragenkataloges wird der erstellte Interviewleitfaden vor der Anwendung durch einen Pretest geprüft. Ein sich ergebender Anpassungsbedarf kann dadurch im Vorfeld der eigentlichen Interviews berücksichtigt und der Leitfaden angepasst werden. Die Interviews werden vom Verfasser in einem persönlichen Gespräch, z.T. auch per Videokonferenz, unter Berücksichtigung der Anonymität durchgeführt. Die Gespräche werden mit Einwilligung der Interviewpartnerinnen und Interviewpartnern aufgezeichnet. Im Anschluss werden die Gespräche transkribiert. In der vorliegenden Forschungsarbeit liegt der Schwerpunkt der Transkription auf dem semantischen Inhalt des Gesprächs. Es werden in Folge dessen die entsprechenden Transkriptionsregeln von Dresing und Pehl befolgt.[26]

Nach der Erhebung des Datenmaterials und dessen Verschriftlichung werden die Daten im Rahmen einer qualitativen Inhaltsanalyse nach Mayring ausgewertet. Dabei werden, ohne vorab Datenmaterial zu reduzieren, über eine induktive Vorgehensweise Kategorien gebildet und definiert, um den Prozess möglichst ergebnisoffen zu gestalten.[27]

1.4 Aufbau der Arbeit

Im ersten Kapitel wurde zunächst die Relevanz des übergeordneten Themas dargelegt. Es folgte ein Problemaufriss, in dem die konkrete Problematik für Kommunalverwaltungen aufgezeigt wurde. Weiterhin fanden eine Eingrenzung und eine Fokussierung der Problemstellung statt. Daran anschließend wurde das Ziel der Arbeit näher erläutert und die zentrale Forschungsfrage formuliert. In dessen Kontext wurde auch die Zielgruppe, also die Adressaten der Master–Thesis, definiert.

[25] Ausführlich hierzu Kapitel 5.2.
[26] Dresing, T.; Pehl, T. (2018): Praxisbuch Interview, Transkription & Analyse, S. 21 f..
[27] Mayring, P. (2022): Qualitative Inhaltsanalyse, S. 85 f..

Schließlich folgten Ausführungen und eine Begründung zu der Auswahl der wissenschaftlichen Methoden.

Mit Kapitel 2 und 3 wird der Master–Thesis, auf Basis einer systematischen Literaturrecherche, ein theoretischer Rahmen gegeben. Das Kapitel 2 widmet sich dabei dem Krisen- und Notfallmanagement, in dessen Kontext die Krisenkommunikation im Ernstfall stattfindet. Kapitel 3 behandelt ausführlich das Thema Krisenkommunikation und beleuchtet deren zentrale Aspekte. In diesem Zusammenhang wird bereits an verschiedenen Stellen ein Bezug zum Notfallszenario „Ransomware–Angriff“ hergestellt. Im Anschluss daran wird in Kapitel 4 ein Zwischenfazit gezogen.

Das Kapitel 5 beschäftigt sich mit der qualitativen Erhebung des empirischen Datenmaterials. Die Methodik und Vorgehensweise zur Datenerhebung, aber auch zur Auswertung der Informationen werden erläutert und begründet. In Kapitel 6 werden die Auswertungsergebnisse der gewonnen Daten dargestellt, bevor sich in Kapitel 7 eine Diskussion und Synthese über die gewonnenen Ergebnisse anschließen. In Kapitel 8 wird dargelegt, welche Erkenntnisse aus dem Forschungsprojekt gewonnen werden konnten und welche Handlungsempfehlungen sich für die kommunale Praxis ableiten lassen. Mit Kapitel 9, dem Fazit, findet die Master–Thesis letztlich ihren Abschluss

2. Krisen- und Notfallmanagement

In diesem Kapitel werden die theoretischen Grundlagen erarbeitet, auf denen im weiteren Verlauf aufgebaut und an denen in den folgenden Kapiteln angeknüpft wird. Es findet zunächst eine Einordnung der Begrifflichkeiten Krisen- und Notfallmanagement statt, bevor sich eine intensive Auseinandersetzung mit dem Thema Krisenkommunikation anschließt. Weiterhin findet eine Abgrenzung von Begriffsdefinitionen statt. Es ist beispielsweise zu klären, inwieweit im Rahmen dieser Arbeit eine scharfe Unterscheidung zwischen Krise und Notfall erforderlich und sinnvoll ist.

2.1 Definitionen und Begriffsverständnis von Krise

Ehekrise, Wirtschaftskrise, Flüchtlingskrise, Umweltkrise, Wohnungskrise - der Begriff „Krise“ findet sich im allgemeinen Sprachgebrauch sehr häufig wieder. Eine klare, eindeutige und allumfassende Definition des Krisenbegriffs scheint es jedoch nicht zu geben.[28] Der Duden versteht unter Krise „eine schwierige Lage, Situation, Zeit (die den Höhe- und Wendepunkt einer gefährlichen Entwicklung darstellt); Schwierigkeit, kritische Situation; Zeit der Gefährdung, des Gefährdetseins; kritischer Wendepunkt bei einem Krankheitsverlauf; Krisis“[29] Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) definiert Krise als eine „vom Normalzustand abweichende Situation mit dem Potenzial für oder mit bereits eingetretenen Schäden an Schutzgütern, die mit der normalen Ablauf- und Aufbauorganisation nicht mehr bewältigt werden kann, so dass eine ‚Besondere Aufbauorganisation‘ (BAO) erforderlich ist.“[30]

In Anbetracht der Tatsache, dass sich die vorliegende Arbeit mit der Kommunikation im Falle einer Ransomware–Attacke beschäftigt, ist die vom BSI gefasste Bedeutung des Krisenbegriffs grundsätzlich von gesteigertem Interesse. Das BSI definiert Krise im Sinne des BSI-Standards 200-4 Business Continuity Management folgendermaßen: „Als Krise im Sinne dieses Standards wird ein Schadensereignis bezeichnet, das sich in erheblicher Weise negativ auf die Institution auswirkt und dessen Auswirkungen auf die Institution nicht im Normalbetrieb bewältigt werden können. Im Gegensatz zu einem Notfall liegen zur Bewältigung einer Krise jedoch keine spezifischen Notfallpläne vor. Vorhandene Notfallpläne können nicht oder nur bedingt adaptiert werden oder greifen schlicht nicht. Innerhalb der Institution wird die Krise durch eingeleitete Maßnahmen der BAO (Besondere Aufbauorganisation) bewältigt“[31] Die DIN Norm DIN EN ISO 22361:2023-2 Krisenmanagement

[28] Vgl. auch Trauboth, J. H. (2022): Grundlagen für professionelles Krisenmanagement in einer sich verändernden Welt, S. 22; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 5.
[29] Duden: Krise, https://www.duden.de/rechtschreibung/Krise (16.11.2024).
[30] BBK: Krise, https://www.bbk.bund.de/SharedDocs/Glossareintraege/DE/K/krise.html (16.11.2024).
[31] BSI-Standard 200-4 Business Continuity Management, S. 21.

führt zum Begriff Krise unter 3.2 der Norm aus: „Unübliche(s) oder außergewöhnliche(s) Ereignis oder Situation, das/die eine Organisation (3.13) oder Gemeinschaft bedroht und eine strategische, anpassungsfähige und schnelle Reaktion erfordert, um die Existenzfähigkeit und Integrität der Organisation oder Gemeinschaft zu erhalten.“ Unter Anmerkung 3 zum Begriff fügt die Norm hinzu, dass aufgrund des Wesens einer Krise zusätzlich zu den erprobten Plänen und Verfahren ein flexibler und dynamischer Ansatz erforderlich sei.[32]

Zieht man die Kernaussagen des BBK, des BSI und der DIN Norm heran, kommt man zum Ergebnis, dass eine Krise immer dann vorliegt, wenn über die alltäglichen Mittel und Maßnahmen hinaus weitere Schritte erforderlich werden, um die negativen Folgen einer sich zuspitzenden Gefährdungs- oder Schadenslage abzuwehren.[33] Das BSI führt als Abgrenzungsmerkmal zu einem Notfall an, dass bei einer Krise (im Vergleich zum Notfall) keine Notfall- bzw. Krisenpläne genutzt werden können. Besonders zu beachten ist jedoch in diesem Kontext, dass vom BSI der Begriff „Notfall- und Krisenkommunikation“ im Glossar zum BSI–Standard 200-4 zusammengefasst, als eine Begrifflichkeit erläutert wird. Es wird dort explizit darauf hingewiesen, dass (Kommunikations-) Vorsorgemaßnahmen im Ernstfall eingesetzt werden können.[34] Daraus lässt sich schließen, dass das BSI zunächst keine Unterscheidung zwischen Krise und Notfall im Hinblick auf die Kommunikation vorsieht. In Kapitel 3.1 wird diese Thematik näher erörtert.

Weiterhin gilt es, eine Abgrenzung zwischen Krise und Katastrophe vorzunehmen. Im Vergleich zur Krise bestehen zum Katastrophenbegriff länderspezifische gesetzliche Regelungen. § 1 Absatz 2 Landeskatastrophenschutzgesetz Baden–Württemberg definiert den Begriff folgendermaßen: „Katastrophe im Sinne dieses Gesetzes ist ein Geschehen, das Leben oder Gesundheit zahlreicher Menschen oder Tiere, die Umwelt, erhebliche Sachwerte oder die lebensnotwendige Versorgung der Bevölkerung in so ungewöhnlichem Maße gefährdet oder schädigt, dass es geboten

[32] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 9.
[33] Vgl. auch Trauboth, J. H. (2022): Grundlagen für professionelles Krisenmanagement in einer sich verändernden Welt, S. 22.
[34] BSI: Glossar zum BSI–Standard 200-4 Business Continuity Management, Notfall- und Krisenkommunikation.

erscheint, ein zu seiner Abwehr und Bekämpfung erforderliches Zusammenwirken von Behörden, Stellen und Organisationen unter die einheitliche Leitung der Katastrophenschutzbehörde zu stellen.“

In den gesetzlichen Regelungen der anderen Bundesländer finden sich ähnliche Formulierungen.[35] Von einer Katastrophe kann in Folge der Regelungen bei einem Ereignis mit ungewöhnlich hohem Gefährdungs- oder Schädigungspotenzial gesprochen werden. Eine Krise und eine Katastrophe können damit in einer wechselseitigen Beziehung zueinander stehen oder sogar gleichzeitig vorliegen, müssen dies aber nicht zwingend.[36] Den gesetzlichen Regelungen kann entnommen werden, dass der Gesetzgeber für den Fall der Katastrophe die lokalen Handlungsmöglichkeiten nicht für ausreichend erachtet. Bei einer Krise ist dies nicht unbedingt der Fall. Insofern wird die Katastrophe z.T. auch als nächste Eskalationsstufe der Krise bezeichnet.[37]

Unter Berücksichtigung vorgenannter Ausführungen kann ein Ransomware–Angriff auf eine kleinere Kommunalverwaltung zunächst als Notfall im Sinne des BSI–Standards 200-4 eingestuft werden, denn Notfallpläne, Notfallhandbücher, die im Rahmen des Notfallmanagements erarbeitet wurden, könnten zur Bewältigung der Situation herangezogen werden. Darüber hinaus ist das Szenario auch unter den Krisenbegriff des Duden, des BBK und der DIN ISO 22361:2023-2 zu subsumieren, weil die außergewöhnliche, kritische Lage mit den „Bordmitteln“ nicht mehr zu meistern ist. Eine Katastrophe im Sinne der gesetzlichen Regelungen liegt bei einem Cyberangriff, der sich bei einer kleineren Kommunalverwaltung ereignet und sich „nur“ auf deren IT–Infrastruktur erstreckt, nicht vor.

2.2 Elemente des Krisen- und Notfallmanagements

Auf Basis der vorgenommen Begriffsdefinitionen und der Einordnung eines Ransomware–Angriffs als Notfall im Sinne des BSI–Standards 200–4 und als Krise

[35] Vgl. z.B. Hessisches Gesetz über den Brandschutz, die Allgemeine Hilfe und den Katastrophenschutz, § 24; Gesetz über den Brandschutz, die Hilfeleistung und den Katastrophenschutz Nordrhein–Westfalen, § 1 Abs. 2 Nr. 2.

[36] Vgl. Trauboth, J. H. (2022): Grundlagen für professionelles Krisenmanagement in einer sich verändernden Welt, S. 22.

[37] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 6 f.

im Sinne des BBK und der DIN ISO 22361:2023–2 kann nun tiefer in die Materie des Krisen- und Notfallmanagements eingetaucht werden. Wodurch sich Krisen- und Notfallmanagement auszeichnet, welche Aufgaben wahrgenommen und welche Ziele verfolgt werden, wird in den nächsten Abschnitten zusammengetragen und erörtert.

Gemäß der vorbezeichneten DIN Norm sorgt das Krisenmanagement für koordinierte Maßnahmen zur Führung, Lenkung und Steuerung einer Organisation im Hinblick auf Krisen.[38] Das BBK führt zum Krisenmanagement aus, dass dieses die konzeptionellen, organisatorischen und verfahrensmäßigen Rahmenbedingungen schafft, um im Krisenfall schnellstmöglich in den Normalzustand zurückzukehren.[39] Das Krisenmanagement umfasst dabei Maßnahmen, die zur Vorbereitung und Bewältigung von Krisen dienen, aber auch zur Vermeidung einer Ausweitung der Krise sowie zur Nachbereitung von Krisen behilflich sind.[40] Töpfer fast unter Krisenmanagement „das vorausschauende und koordinierte Handeln und Verhalten, das der Problematik und Dringlichkeit der Situation Rechnung trägt und die erkannte oder bereits eingetretene Bedrohung möglichst umfassend beseitigen sowie den früheren positiven Zustand wiederherstellen bzw. fortführen will“ zusammen. Daneben weist er darauf hin, dass aus der Krisensituation für die Zukunft Lehren gezogen werden sollen.[41] Die jeweiligen Inhalte der Definitionen ähneln sich stark. Vordergründig hat Krisenmanagement damit das übergeordnete Ziel, Krisen zu vermeiden oder schnellstmöglich und umfassend zu bewältigen.

2.2.1 Krisenmanagement als iterativer Gesamtprozess

Bei genauerer Analyse lässt sich feststellen, dass das Krisenmanagement mehrere Phasen umfasst. Das BMI beschreibt drei Phasen.[42]

---

[38] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 9.
[39] BBK: Krisenmanagement, https://www.bbk.bund.de/DE/Themen/Krisenmanagement/krisenmanagement_node.html (16.11.2024).
[40] BBK: Krisenmanagement.
[41] Töpfer, A. (2013): Die Managementperspektive im Krisenmanagement - Welche Rolle spielt das Management bei der Bewältigung von Krisensituationen, S. 239 f..
[42] BMI: Schutz Kritischer Infrastrukturen-Risiko- und Krisenmanagement, S. 5 f., https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis-leitfaden.html (16.11.2024).

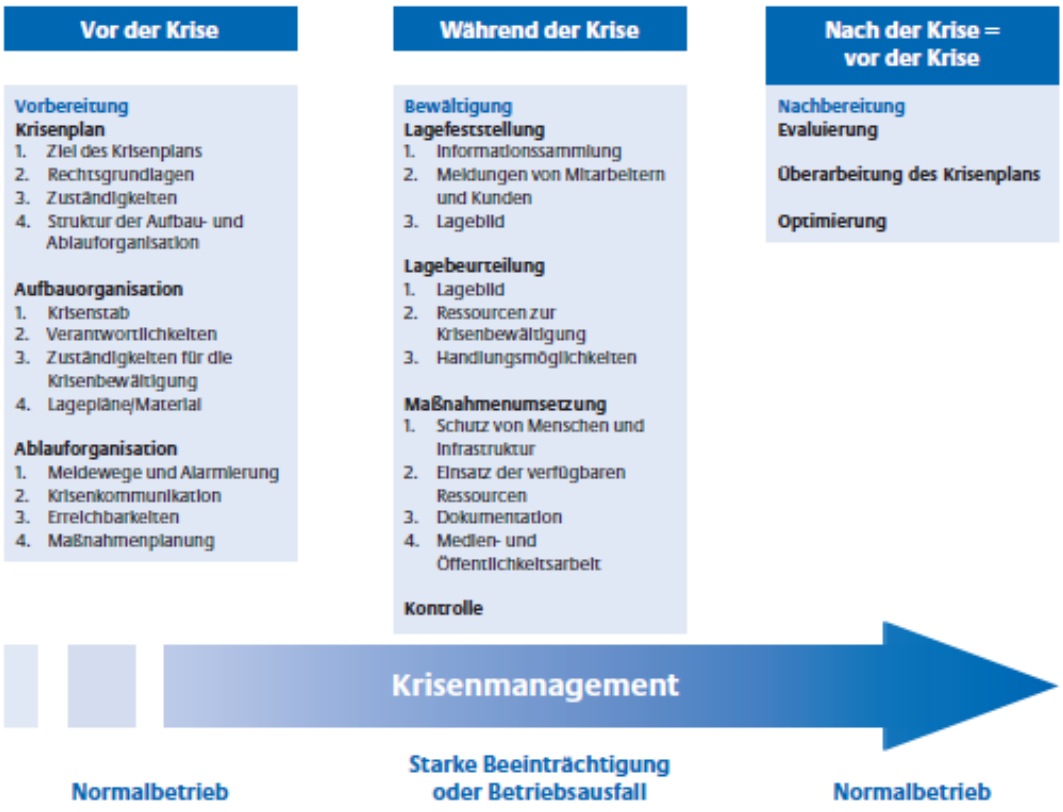

Abbildung 1: Bestandteile des Krisenmanagement nach BMI[43]

Das BBK definiert in seinem Risiko- und Krisenmanagementzyklus vier Abschnitte. Mit Ausnahme geringfügiger Abweichung gleichen sich die Tätigkeiten, die während der jeweiligen Phasen zu erledigen sind, sehr stark. Das BBK gibt den einzelnen Abschnitten folgende Bezeichnungen: Die Präventionsphase, die auch das Risikomanagement umfasst. Die Vorbereitungsphase, die Bewältigungsphase und die Nachbereitungsphase.[44]

[43] BMI: Schutz Kritischer Infrastrukturen - Risiko- und Krisenmanagement, S. 23.
[44] BBK: Krisenmanagement ist ein Zyklus, https://www.bbk.bund.de/DE/Themen/Krisenmanagement/KMZirkel/KMZirkel_node.html (16.11.2024); vgl. hierzu auch BMI: Leitfaden Krisenkommunikation, S. 6 f..

Abbildung 2: Der Risiko- und Krisenmanagementzyklus nach BBK[45]

In den einzelnen Phasen stehen unterschiedliche Ziele und Aufgaben im Mittelpunkt des Krisenmanagements. In der Präventionsphase gilt es, potenzielle Risiken zu erkennen, zu analysieren und zu behandeln.[46] Während der Vorbereitungszeitraum zur Bereitstellung von Ressourcen, Optimierung der Notfallplanung und Prozesse sowie zur Übung etwaiger Vorfälle genutzt werden sollte, muss im Ernstfall zur Bewältigung der Krisenstab einberufen und geführt werden, die Bevölkerung gewarnt und die Institution operativ tätig werden.[47] Die Phase nach einer Krise kann und sollte genutzt werden, um die getroffenen Maßnahmen zu evaluieren, Erkenntnisse zu gewinnen und diese umzusetzen. Das Krisenmanagement stellt damit ein iterativer Gesamtprozess dar.[48] Insbesondere das Managementsystem des BSI–

[45] BBK: Krisenmanagement ist ein Zyklus.
[46] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 15; BBK: Krisenmanagement ist ein Zyklus; BMI: Schutz Kritischer Infrastrukturen - Risiko- und Krisenmanagement, S. 14.
[47] BBK: Krisenmanagement ist ein Zyklus; BMI: Schutz Kritischer Infrastrukturen - Risiko- und Krisenmanagement, S. 23.
[48] BMI: Leitfaden Krisenkommunikation, S. 6 f., https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/leitfaden-krisenkommunikation.html (16.11.2024); BBK: Krisenmanagement ist ein Zyklus.

Standard 200-4 ist an den PDCA-Zyklus von William Edwards Deming angelehnt.[49] Es ist bereits an dieser Stelle der Arbeit festzustellen, dass „Kommunikation“ in jeder Phase des Gesamtprozesses ein bedeutsames Teilelement des Krisenmanagements ist.[50]

Ein weiterer wesentlicher Aspekt des Krisenmanagements liegt in der Sicherstellung einer funktionierenden Aufbau- und Ablauforganisation. Diese Aufgabe nimmt in verschiedenen der vorgenannten Phasen eine zentrale Stellung ein.[51] Insbesondere die Planung und Einrichtung einer besonderen Aufbauorganisation zur Krisenbewältigung ist integraler Bestandteil des Notfall- und Krisenmanagements.[52] Sowohl für Krisenszenarien im Sinne des BBK und der einschlägigen DIN Norm als auch für Notfälle im Sinne des BSI–Standards 200-4 ist explizit eine von der gewöhnlichen Aufbauorganisation abweichende Struktur vorgesehen, um den besonderen Anforderungen der Situation gerecht zu werden.[53] Auch das Arbeitspapier des BSI „Erste Hilfe bei einem schweren IT–Sicherheitsvorfall“ rät im Ernstfall dazu „frühzeitig relevante interne Stellen einzubinden, zum Beispiel in Form eines Krisenstabes.“[54]

2.2.2 Aufbauorganisation zur Krisenbewältigung

Stabsarbeit findet in vielen Bereichen statt. Hierbei kann es sich um Einsatzorganisationen (Feuerwehr, Rettungsdienst, Polizei) oder Verwaltungen, Wirtschaftskonzerne sowie beispielsweise Krankenhäusern und Kirchen handeln. Entsprechend der unterschiedlichen Bereiche, in denen Stäbe eingesetzt werden, existieren unterschiedliche Stabsdefinitionen. Gemeinsam ist den einzelnen Definitionen, dass eine leitende Person eine Unterstützung durch mehrere andere Personen erfährt, in dem

[49] Vgl. hierzu auch BSI-Standard 200-4 Business Continuity Management, S. 25.
[50] Vgl. z.B. Abbildungen S. 13 u. 14
[51] BSI-Standard 200-4 Business Continuity Management, S. 97.
[52] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 24 f.; BSI-Standard 200-4 Business Continuity Management, S. 97 f..
[53] BBK: Krisenmanagement; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 24 f.; BSI-Standard 200-4 Business Continuity Management, S. 97 f..
[54] BSI: Erste Hilfe bei einem schweren IT- Sicherheitsvorfall (Version 1.2.), S. 9, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.html (16.11.2024).

ihr die Gruppe beratend zur Seite steht und die Gruppe ihr inhaltlich sowie organisatorisch zuarbeitet.[55] Aufgrund der vielfältigen Einsatzgebiete unterscheiden sich die jeweiligen Stabsformen je nach Branche, bzw. Organisation. Stäbe sind entsprechend unterschiedlich ausgestaltet. Der (Verwaltungs-) Krisenstab ist eine besondere, anlassbezogene Aufbauorganisation innerhalb einer Behörde.[56] Er setzt sich üblicherweise aus der Stabsleitung und Vertreterinnen und Vertretern aus den im Krisenfall wichtigen Bereichen zusammen.[57] Es ist für das jeweilige Krisenszenario im Einzelfall zu entscheiden, welche Funktionen unter Berücksichtigung der speziellen Anforderung, der vorhandenen Ressourcen und der gesetzlichen Bestimmungen besetzt werden.[58] Im Falle eines schwerwiegenden Cyberangriffes empfiehlt das BSI in seinem entsprechenden Arbeitspapier neben der Leitungsebene als Stabsleitung, die Einbindung der IT–Leitung, Juristen, Presse- und Öffentlichkeitsarbeit, Datenschutzbeauftragte und den Personalrat.[59] Der BSI–Standard 200–4 sieht grundsätzlich in dem Kernteam des Stabs, unabhängig vom konkreten Notfallszenario, auch Vertreter der Gebäudeverwaltung und des Bereichs Personal vor.[60] Auch die allgemein für Krisenereignisse konzipierte DIN Norm sieht zahlreiche Verwaltungsbereiche im Stab, zum Teil optional, vertreten, z.B. auch Personal u. Finanzen, darüber hinaus Protokollführer, administrative Unterstützung und zusätzliche Spezialisten.[61] Der Bereich Kommunikation wird im Zusammenhang mit der Besetzung eines Krisenstabes im Gegensatz zu optionalen Bereichen ausnahmslos als fester Bestandteil vorgesehen.[62] Auch die baden–württembergische Verwaltungsvorschrift der Landesregierung und der Ministerien zur Bildung von Stäben bei außergewöhnlichen Ereignissen und Katastrophen (VwV Stabsarbeit)

---

[55] Spielvogel, C. (2018): Stabsorganisation, S. 80; Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 11; Heimann, R.; Hofinger, G. (2022): Stabsarbeit - Konzept und Formen der Umsetzung, S. 3 f.; Künzer, L.; Hofinger, G.; Mähler, M. (2022): Psychologische Einflussfaktoren auf Stabsarbeit, S. 193.

[56] Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 6 f.

[57] Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 10; Gißler, D. (2019): Erfolg der Stabsarbeit, S. 34 f.; Gahlen, M. (2022): Aufgaben und Strukturen von Verwaltungsstäben, S. 71 f.; DIN EN ISO 22361:2023 – 2 Krisenmanagement, S. 24 f..

[58] Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 6.

[59] BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 9.

[60] BSI-Standard 200-4 Business Continuity Management, S. 101.

[61] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 24 f..

[62] BSI-Standard 200-4 Business Continuity Management, S. 101; BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 9; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 25.

vom 07.05.2024 deklariert nach Ziffer 3.2.3.4 die Bevölkerungsinformation und Medienarbeit (BuMA) als Mitglieder der Koordinierungsgruppe des Verwaltungsstabes, die bei Einberufung des Stabes i.d.R. sofort zu beteiligen sind.

Stabsarbeit weist teilweise Gemeinsamkeiten mit gewöhnlicher Teamarbeit auf.[63] Die Tatsache, dass die gesamte Gruppe ein gemeinsames Ziel verfolgt, die Mitglieder aus unterschiedlichen Funktionsbereichen oder Organisationseinheiten stammen, deren Fähigkeiten sich ergänzen sollen und eine Vernetzung untereinander stattfindet, verdeutlichen dies.[64] Auch wenn Gemeinsamkeiten mit einer üblichen Arbeit in Teams bestehen, zeichnet sich Stabsarbeit durch besondere Merkmale aus. In Bezug auf den Autonomiegrad und der Hierarchie ist feststellbar, dass Stäbe in der Regel eine hierarchische Führungsstruktur aufweisen und die Autonomie der Stabsmitglieder beschränkt ist.[65] Der jeweiligen Stabsleitung kommt damit eine besondere Rolle zu.[66] Die Stabsleitung steht im Zentrum des Stabes und trägt die Führungs- und Handlungsverantwortung.[67] Sie regelt die Zuständigkeiten und Verantwortlichkeiten innerhalb des Stabes. Darüber hinaus ist sie für die internen Abläufe des Stabes und die erzielten Ergebnisse verantwortlich. Daneben trifft die Stabsleitung die wichtigsten Entscheidungen und legt die Ziele fest.[68] Der Erfolg der Arbeit in Stabsform hängt von verschiedenen Aspekten ab. Das Einhalten förderlicher Verhaltensweisen beim Führen eines Krisenstabes ist dabei ein entscheidender Faktor.[69] Die Berücksichtigung spezieller Grundsätze und Leitlinien haben besonderen Einfluss auf den Erfolg der Stabsarbeit und des Krisenmanagements.[70] Auf Einzelheiten wird in dieser Master–Thesis nicht eingegangen.

---

[63] Gißler, D. (2019): Führung und Stabsarbeit trainieren, S. 48 f.; Gißler, D. (2019): Erfolg der Stabsarbeit, S. 46 f.; Künzer, L.; Hofinger, G.; Mähler, M. (2022): Psychologische Einflussfaktoren auf Stabsarbeit, S. 196 f.

[64] Heimann, R.; Hofinger, G. (2022): Stabsarbeit - Konzept und Formen der Umsetzung, S. 7.

[65] Gißler, D. (2019): Erfolg der Stabsarbeit, S. 33; Heimann, R.; Hofinger, G. (2022): Stabsarbeit - Konzept und Formen der Umsetzung, S. 7; Heimann, R. (2022): Historie von Stäben, S. 15 ff.-

[66] Spielvogel, C. (2018): Stabsorganisation, S. 80.

[67] Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 11.

[68] Spielvogel, C. (2018): Stabsorganisation, S. 80; Gahlen, M. (2022): Aufgaben und Strukturen von Verwaltungsstäben, S. 71.

[69] Gißler, D. (2019): Führung und Stabsarbeit trainieren, S. 12.

[70] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 15 f.; Bedé, A. (2022): Grundsätze und Leitlinien zum Führen von (Unternehmens-) Krisenstäben, S. 131 ff..

2.3 Notfallmanagement nach BSI-Standard 200-4

In den vorangegangenen Unterkapiteln wurde dargelegt, welche Funktion das Krisenmanagement innehat und welche Ziele vom Krisenmanagement verfolgt werden. Es wurde aufgezeigt, dass das Krisenmanagement verschiedene Phasen umfasst. Jeder Abschnitt bringt dabei spezielle Aufgabenstellungen mit sich. Entsprechend des Prinzips „Nach der Krise ist vor der Krise“ bilden die Phasen in ihrer Gesamtheit einen iterativen Gesamtprozess. Ein weiterer wesentlicher Aspekt des Krisenmanagements, die Anpassung der Aufbauorganisation an die besondere Situation, wurde beleuchtet. Auf die speziellen Eigenheiten der Stabsarbeit wurde in diesem Zusammenhang eingegangen. Damit wurden, ohne sich inhaltlich in Details zu verlieren, die „Basics“ des Krisenmanagements dargestellt. Auf dieser Grundlage wird nun in Kapitel 2.3 erörtert, inwieweit der BSI–Standard 200-4 Business Continuity Management als Spezialregelwerk im Zusammenhang mit einer Ransomware–Attacke zu betrachten ist.

Der BSI-Standard 200-4 trägt die Überschrift „Business Continuity Management“ (BCM). Er löste im Jahr 2022 seinen Vorgänger, BSI–Standard 100-4 mit dem Namen „Notfallmanagement“, ab. Der BSI–Standard 200-4 richtet sich grundsätzlich an alle Institutionen und damit auch an Kommunalverwaltungen jeder Größe.[71] Durch die Anwendung des Regelwerks sollen Institutionen in die Lage versetzt werden, gegen verschiedene Ausfälle des Geschäftsbetriebes umfassend vorzusorgen bzw. angemessene Möglichkeiten zur Geschäftsfortführung im Schadensfall vorzubereiten. Im Vordergrund eines BCMs steht somit, zu gewährleisten, dass der Geschäftsbetrieb, selbst bei erheblichen Schadensereignissen, nicht unterbrochen wird oder nach einem Ausfall in angemessener Zeit auf einem definierten Mindestniveau fortgeführt werden kann.[72] Die Hauptintention liegt damit bei der Sicherstellung, dass die Leistungsfähigkeit der Institution nicht beeinträchtigt wird. Das BCM ist damit ein eigenständiges Managementsystem neben dem Krisenmanagement, auch wenn es Überschneidungen gibt.

[71] BSI-Standard 200-4 Business Continuity Management, S. 13.
[72] Roselieb, F. (2022): Grundlagen des Business Continuity Managements, S. 14; BSI-Standard 200-4 Business Continuity Management, S. 14.

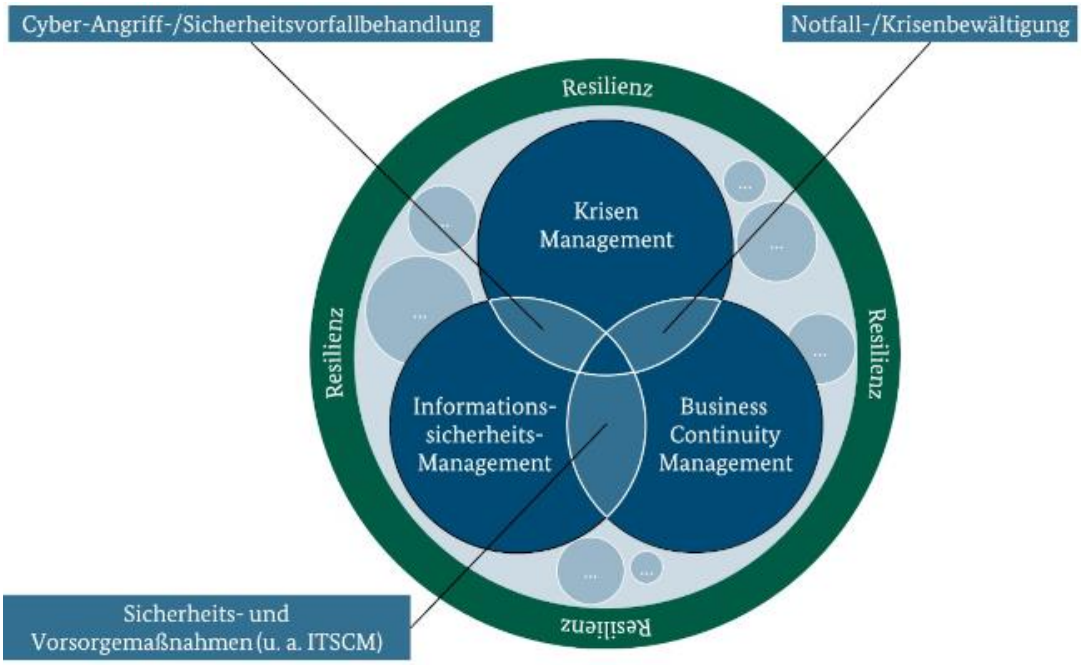

Abbildung 3: Managementsysteme nach BSI–Standard 200-4[73]

Der inhaltliche Schwerpunkt des BSI–Standards 200-4 ähnelt bei genauerer Betrachtung der DIN-Norm für Business Continuity Management, der DIN EN ISO 22301:2019. Entsprechend der Zielsetzung des Standards, befasst sich dieser zu einem erheblichen Maß mit dem grundlegenden Aufbau eines BCMs, mit der Identifikation der wichtigsten Geschäftsprozesse einer Institution und der Entwicklung von Kontinuitätsstrategien. Nichtsdestotrotz ist darüber hinaus z.B. integraler Bestandteil des BSI–Standard 200-4, die Einrichtung einer besonderen Aufbauorganisation zur Bewältigung des Notfalls.[74] Auch befindet sich in dem Standard eine Anleitung zur Notfall- und Krisenkommunikation.[75] In dem Werk selbst wird angeführt, dass durch den Standard die Institutionen grundsätzlich in die Lage versetzt werden „alle Arten von Notfällen erfolgreich und auch Krisen zumindest rudimentär zu bewältigen, da die organisatorischen Vorrausetzungen zur Bewältigung für Notfälle und Krisen nahezu identisch sind.“[76]

[73] BSI-Standard 200-4 Business Continuity Management, S. 15
[74] BSI-Standard 200-4 Business Continuity Management, S. 97 ff..
[75] BSI-Standard 200-4 Business Continuity Management, S. 139 ff..
[76] BSI-Standard 200-4 Business Continuity Management, S. 15.

Vor der dargestellten Sachlage kann im Ergebnis festgestellt werden, dass der BSI–Standard 200-4 Überschneidungen mit Synergiepotenzialen zum Krisenmanagement aufweist, das Konzept jedoch im Kern darauf zugeschnitten ist, die Organisation gegen Betriebsunterbrechungen durch Notfallvorsorge widerstandsfähiger zu machen, bei Ausfällen eine effektive Notfallreaktion zu gewährleisten und die Geschäftsprozesse im Ernstfall wiederherzustellen. Vor diesem Hintergrund ist der BSI–Standard 200-4 nicht als Spezialanleitung für die allgemeine Bewältigung von Krisen- und Notfällen im Zusammenhang mit IT–Ausfällen zu betrachten. Vielmehr ist er als spezielle Handlungsanleitung in Bezug auf die Sicherstellung des Geschäftsbetriebs zu verstehen, z.B. bei einer Ransomware–Attacke. Infolgedessen stellt er eine Ergänzung des allgemeinen Krisen- und Notfallmanagements dar. Wie wichtig jedoch die Entwicklung von Kontinuitätsstrategien einzelner kritische Geschäftsprozesse für die technische Sicherstellung der Krisenkommunikation ist, wird im weiteren Verlauf dieser Arbeit noch deutlich erkennbar. Auf die Verzahnung der Managementsysteme und die Abhängigkeiten von verschiedenen Geschäftsprozessen sei bereits an dieser Stelle hingewiesen.

3. Krisenkommunikation

Nach dem in Kapitel 2 die Grundlagen des Krisenmanagements erarbeitet und erläutert wurden, widmet sich dieses Kapitel nun der Krisenkommunikation, die einen zentralen Bestandteil des Krisenmanagements darstellt.[77] Es werden auf theoretischer Ebene die einzelnen Bestandteile der Krisenkommunikation behandelt und darüber hinaus an verschiedenen Stellen ein Bezug zum Szenario „Ransomware–Angriff auf eine kleinere Kommunalverwaltung“ hergestellt. Daneben wird die Frage geklärt, was unter „erfolgreicher“ Krisenkommunikation zu verstehen ist. Im Anschluss erfolgt ein Zwischenfazit, bevor sich in Kapitel 5 der empirische Teil des Forschungsprojektes anschließt.

[77] BMI: Leitfaden Krisenkommunikation, S. 6; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 235.

3.1 Definition

In Kapitel 2 wurde die Begrifflichkeit Krise näher definiert und erläutert. An dieser Stelle wird erörtert, was unter Krisenkommunikation zu verstehen ist. Das BBK bezeichnet Krisenkommunikation „als den Austausch von Informationen und Meinungen während einer Krise zur Verhinderung oder Begrenzung von Schäden an einem Schutzgut.“[78] Die DIN Norm DIN EN ISO 22361:2022 Krisenmanagement definiert Krisenkommunikation als „interne und externe Kommunikation zur Bereitstellung von Informationen, Aktualisierungen und Anweisungen für interne und externe interessierte Parteien.“[79] Der BSI–Standard 200-4 fasst die Begriffe Notfall- und Krisenkommunikation zusammen und beschreibt diese als „Tätigkeiten, die vor oder während einer Krise oder einem Notfall und gegebenenfalls auch nach deren Bewältigung ausgeführt werden, um relevante Informationen zu sammeln, zu verifizieren sowie zielgruppengerecht nach innen und außen zu kommunizieren.“[80] Die Kerninhalte der drei vorgenannten Definitionen von Krisen- bzw. Notfallkommunikation dienen als Basis für die weitere Abhandlung in dieser Arbeit.

In einem ersten Schritt wird deutlich, dass es - zumindest für das Szenario „Ransomware-Angriff“ - dahingestellt bleiben kann, ob es sich bei der Kommunikationsform um Notfall- oder Krisenkommunikation handelt. Der BSI–Standard 200-4 differenziert diesbezüglich nicht. Ungeachtet der Definitionen des BSI–Standards 200-4 wurde bereits in Kapitel 2 festgestellt, dass per Begriffsdefinition des BBKs und der einschlägigen DIN-Norm ein Ransomware–Angriff tendenziell als Krise einzustufen ist und damit auch (als logische Konsequenz) das Erfordernis von Krisenkommunikation vorliegt. Die Problemstellung, dass die jeweiligen Begrifflichkeiten von Krise und Notfall nicht deckungsgleich verwendet werden, ist damit gelöst.

[78] BBK: Krisenkommunikation, https://www.bbk.bund.de/SharedDocs/Glossareintraege/DE/K/krisenkommunikation.html (16.11.2024).
[79] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 10.
[80] BSI: Glossar zum BSI–Standard 200-4 Business Continuity Management, Notfall- und Krisenkommunikation

Eng verwandt mit der Krisenkommunikation ist die Risikokommunikation.[81] Obgleich beide Kommunikationsformen auf identischen Grundsätzen basieren, liegt ein entscheidender Unterschied in der zeitlichen Dimension.[82] Risikokommunikation dient vordringlich dem Zweck, präventiv vor möglichen Gefahren zu warnen und Aufklärungsarbeit zu leisten, bevor eine konkrete Krise abzusehen ist. Sie erfolgt somit im Idealfall anlassunabhängig.[83] Dadurch kann sichergestellt werden, dass z.T. zeitaufwändige Vorsorgemaßnahmen rechtzeitig umgesetzt werden können und die Bevölkerung im Ernstfall besser geschützt ist.[84]

Abbildung 4: Risiko- und Krisenkommunikation nach BBK[85]

Auch wenn eine langfristige und kontinuierlich stattfindende Risikokommunikation grundsätzlich ein Erfolgsfaktor für eine - im konkreten Schadensfall - praktizierte Krisenkommunikation darstellt,[86] wird diese im Rahmen der vorliegenden Master–Thesis nicht näher beleuchtet.

[81] BBK: Risikokommunikation, S. 29, https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/Risikomanagement/handbuch-risikokommunikation.pdf?__blob=publicationFile&v=5 (16.11.2024); BMI: Leitfaden Krisenkommunikation, S. 12.
[82] BBK: Risikokommunikation, S. 29; BMI: Leitfaden Krisenkommunikation, S. 12.
[83] BBK: Risikokommunikation, S. 9 u. S. 28; BMI: Leitfaden Krisenkommunikation, S. 12.
[84] BBK: Risikokommunikation, S. 9; BMI: Leitfaden Krisenkommunikation, S. 12; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 239 f..
[85] BBK: Risikokommunikation, S. 30.
[86] BBK: Risikokommunikation, S. 28; BMI: Leitfaden Krisenkommunikation, S. 12.

3.2 Ziele und Prinzipien von Krisenkommunikation

Wie anhand des im Einleitungskapitel skizzierten Bildes[87] deutlich geworden ist, herrscht bei Krisen und krisenhaften Lagen -intern wie extern- ein großer Informationsbedarf.[88] In dieser Situation ist es daher notwendig, alle identifizierten Zielgruppen möglichst schnell, bedarfsgerecht, wahrheitsgemäß und widerspruchsfrei zu informieren.[89] Diese Grundsätze gelten jedoch nicht uneingeschränkt. Im Einzelfall ist zu prüfen, ob ein differenzierteres Vorgehen erforderlich ist.[90]

Ein grundsätzliches Ziel von (Behörden-) Kommunikation ist der Aufbau von Vertrauen in Behörden.[91] Darüber hinaus soll die Glaubwürdigkeit von Behörden gesteigert werden.[92] Dies gilt sowohl in Bezug auf die externe als auch auf die interne Krisenkommunikation.[93] Die Krisenkommunikation muss sicherstellen, dass das z.B. im Zuge der Risikokommunikation hergestellte Vertrauen und die aufgebaute Glaubwürdigkeit in der Krisensituation bestehen bleiben.[94] Dies kann durch Offenheit, Transparenz und aktiver Kommunikation erlangt werden.[95] Eine abgestimmte Kommunikationslinie mit anderen von der Krise betroffenen Behörden ist unbedingt erforderlich.[96] Im Szenario Ransomware–Angriff könnten dies beispielsweise

---

[87] Kapitel 1.1
[88] Vgl. hierzu auch Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 234.
[89] DIN EN ISO 22361:2023 – 2 Krisenmanagement, S. 39; BMI: Leitfaden Krisenkommunikation, S. 13; Bachmann, S.; Ternès von Hattburg, A. (2021): Effiziente Krisenkommunikation-transparent und authentisch, S. 8; Riecken, M. (2013): Erfolgskritische Faktoren der angewandten Krisenkommunikation, S. 326 ff..
[90] Merten, K. (2013): Krise, Krisenmanagement und Krisenkommunikation, S. 164 f..
[91] BMI: Leitfaden Krisenkommunikation, S. 13; Hoffjann, O. (2013): Kommunikative Grenzen des Krisenmanagements, S. 414.
[92] BBK: Risikokommunikation, S. 26; BMI: Leitfaden Krisenkommunikation, S. 13; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 10.
[93] Heide, M. (2021): Interne Krisenkommunikation: eine Möglichkeit für Kommunikatoren, strategische Werte nachzuweisen, S. 568; BMI: Leitfaden Krisenkommunikation, S. 18.
[94] BMI: Leitfaden Krisenkommunikation, S. 13; vgl. hierzu auch Schmitt-Geiger, A. (2013): Litigation - PR: Strategische Rechtskommunikation bei Unternehmenskrisen, S. 307.
[95] BBK: Risikokommunikation, S. 26; BSI: Erste Hilfe bei einem schweren IT- Sicherheitsvorfall (Version 1.2.), S. 24; BMI: Leitfaden Krisenkommunikation, S. 13; Schmitt-Geiger, A. (2013): Litigation - PR: Strategische Rechtskommunikation bei Unternehmenskrisen, S. 313.
[96] BMI: Leitfaden Krisenkommunikation, S. 13; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 31; Merten, K. (2013): Krise, Krisenmanagement und Krisenkommunikation, S. 165.

die Strafverfolgungsbehörden, die CSBW, die Komm.ONE und der Landesbeauftragte für Datenschutz und Informationsfreiheit sein.[97] Um zu vermeiden, dass ein Informationsvakuum entsteht, das von anderen Akteuren genutzt werden könnte, um die Deutungshoheit in einer krisenhaften Lage zu erlangen, ist ein rechtzeitiges Agieren der Behörde unerlässlich.[98] Die Meinungshoheit inne zu haben, ist im Ernstfall von wesentlicher Bedeutung.[99] Vor diesem Hintergrund muss im Rahmen der Krisenkommunikation gut überlegt sein, ob ein „Schweigen in der Krise“ eine zielführende Option darstellt.[100]

Von einer erfolgreichen Krisenkommunikation kann in Folge voranstehender Ausführungen dann gesprochen werden, wenn es gelingt, die relevanten Zielgruppen mit den an sie adressierten Botschaften bedarfsgerecht zu erreichen und im Rahmen der Kommunikation dem Sender vertraut und er als glaubwürdig eingestuft wird. Erfolgreiche Krisenkommunikation zeichnet sich weiterhin dadurch aus, wenn die Behörde im Verlauf der krisenhaften Lage bewerkstelligen kann, stets die Deutungshoheit über die Situation innezuhaben.

Eine schlechte Kommunikation kann wiederum dazu führen, dass sich die Krisensituation verschlimmert oder gar eine Krise erst durch die missglückte Kommunikation hervorgerufen wird.[101]

Um erfolgreich in der Krise zu kommunizieren ist es vorteilhaft, sich an grundsätzliche Prinzipien der Krisenkommunikation zu halten.[102] Hierzu zählt das Prinzip

---

[97] BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 23.

[98] Bachmann, S.; Ternès von Hattburg, A. (2021): Effiziente Krisenkommunikation- transparent und authentisch, S. 54; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 37; Merten, K. (2013): Krise, Krisenmanagement und Krisenkommunikation, S. 165.

[99] BMI: Leitfaden Krisenkommunikation, S. 13; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 235; Bachmann, S.; Ternès von Hattburg, A. (2021): Effiziente Krisenkommunikation- transparent und authentisch, S. 5; Merten, K. (2013): Krise, Krisenmanagement und Krisenkommunikation, S. 166.

[100] Vgl. hierzu auch Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 235; Riecken, M. (2013): Erfolgskritische Faktoren der angewandten Krisenkommunikation, S. 323 f.; BSI: Erste Hilfe bei einem schweren IT- Sicherheitsvorfall (Version 1.2.), S. 10.

[101] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 1 f., 15; Merten, K. (2013): Krise, Krisenmanagement und Krisenkommunikation, S. 168; Riecken, M. (2013): Erfolgskritische Faktoren der angewandten Krisenkommunikation, S. 329.

[102] BMI: Leitfaden Krisenkommunikation, S. 15; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 39 f..

der Schnelligkeit (aktiv, frühzeitig),[103] der Wahrhaftigkeit (sachlich, transparent, wahr),[104] der Verständlichkeit (kurz, einfach, unkompliziert, bildhaft)[105] und der Konsistenz (einheitlich, koordiniert, kontinuierlich)[106].

Im Falle eines Ransomware–Angriffs werden sich unmittelbar nach dem Schadensereignis je nach Betroffenengruppe, wie in Kapitel 1.1 aufgezeigt, unterschiedliche Fragestellungen ergeben. Diese sollten - sowohl in zeitlicher als auch in inhaltlicher Hinsicht - zufriedenstellend beantworten werden, um als vertrauensvoller und glaubwürdiger Kommunikator wahrgenommen zu werden, der transparent und unverzüglich informiert.[107]

3.3 Relevante Zielgruppen und Kanäle

In diesem Kapitel wird sich die Master–Thesis der Beantwortung der Frage nähern, wie erfolgreiche Krisenkommunikation gelingen kann. Im ersten Schritt beschäftigt sich die Arbeit damit, die relevanten Zielgruppen zu identifizieren. Die Identifikation der Zielgruppen und im weiteren Verlauf die gezielte Ansprache über einen „funktionierenden“ Kanal ist in der Praxis häufig herausfordernd. Gleichwohl kommt der passgenauen Stakeholder-Kommunikation eine Schlüsselstellung zu.[108]

Der Leitfaden Krisenkommunikation des Bundesinnenministeriums geht prinzipiell von drei übergeordneten Ziel- bzw. Interessensgruppen aus. Er differenziert zwischen externen und internen Zielgruppen und fasst eine weitere Gruppe als „Beteiligte im Krisenmanagement“ zusammen.[109] Die DIN Norm DIN EN ISO 22361:2023 ebenso wie der BSI–Standard 200-4 gehen grundsätzlich von interner

[103] DIN EN ISO 22361:2023 – 2 Krisenmanagement, S. 39; BMI: Leitfaden Krisenkommunikation, S. 15; Merten, K. (2013): Krise, Krisenmanagement und Krisenkommunikation, S. 166.
[104] DIN EN ISO 22361:2023 – 2 Krisenmanagement, S. 39 f.; BMI: Leitfaden Krisenkommunikation, S. 15; Merten, K. (2013): Krise, Krisenmanagement und Krisenkommunikation, S. 167.
[105] BMI: Leitfaden Krisenkommunikation, S. 15; DIN EN ISO 22361:2023 – 2 Krisenmanagement, S. 41.
[106] DIN EN ISO 22361:2023 – 2 Krisenmanagement, S. 39 f.; BMI: Leitfaden Krisenkommunikation, S. 15; Merten, K. (2013): Krise, Krisenmanagement und Krisenkommunikation, S. 166 f..
[107] Vgl. hierzu auch Bachmann, S.; Ternès von Hattburg, A. (2021): Effiziente Krisenkommunikation- transparent und authentisch, S. 72 u. S. 79.
[108] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 244; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 14; BMI: Leitfaden Krisenkommunikation, S. 17.
[109] BMI: Leitfaden Krisenkommunikation, S. 17.

und externer Kommunikation aus, ohne detailliert einzelne Zielgruppen zu beschreiben.[110] Allerdings empfehlen die vorgenannten Werke die Berücksichtigung aller relevanten Zielgruppen in der Kommunikation.[111] Der groben Untergliederung des Bundesinnenministeriums in drei Ziel- bzw. Interessensgruppen wird sich angeschlossen. Die Aufsplittung ist nachvollziehbar und einer gewissen Logik folgend. Die Unterscheidung im Vorfeld zwischen „Freund“ und „Feind“ wird im Hinblick auf das genauer zu betrachtende Notfallszenario nicht als zwingend erforderlich erachtet.[112] Ungeachtet der Stakeholder-Identifikation, kommt es maßgeblich auf die adäquate Ansprache und die Übermittlung einer passenden Botschaft an.[113] Dies spricht für eine sorgfältige Analyse der Interessengruppen. Das Kriterium „zielgruppengerecht“ ist dann erfüllt, wenn die Zielgruppe über das gewählte Medium tatsächlich erreicht wird und die Empfänger auch motiviert werden können, die übermittelte Botschaft aufzunehmen, die Botschaft korrekt verstanden wird und schließlich die Zielgruppe auf die Botschaft eine Reaktion zeigt.[114]

3.3.1 Interne Zielgruppen

Zu den internen Zielgruppen zählen insbesondere die Mitarbeiterinnen und Mitarbeiter der Institution. Darüber hinaus jedoch auch z.B. interne Gremien. Bei einer Kommunalverwaltung gehört hierzu auch der Gemeinderat, als Teil der Verwaltung und Hauptorgan der Gemeinde.[115] Zu einem internen Gremium kann jedoch auch der Krisenstab gezählt werden, wenn dieser zur Bewältigung der Lage eingesetzt wird. Aufgrund der Bedeutsamkeit der Kommunikation innerhalb des Krisenstabes, erfolgt am Ende dieses Kapitels ein spezieller Abschnitt zu dieser Thematik.

---

[110] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 36; BSI-Standard 200-4 Business Continuity Management, S. 139 ff..
[111] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 37; BSI-Standard 200-4 Business Continuity Management, S. 139 ff.
[112] Vgl. hierzu Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 244; zum Nutzen von "Verbündeten" Bachmann, S.; Ternès von Hattburg, A. (2021): Effiziente Krisenkommunikation- transparent und authentisch, S. 79.
[113] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 244 f..
[114] BMI: Leitfaden Krisenkommunikation, S. 17.
[115] Vgl. Gemeindeordnung Baden–Württemberg, § 23 u. § 24 Absatz 1 Satz 1.

Gerade die eigenen Mitarbeiterinnen und Mitarbeiter werden im Zusammenhang mit Krisenkommunikation oftmals nicht ausreichend berücksichtigt.[116] Die Kommunikation mit dieser Gruppe ist jedoch sehr wichtig und sollte bereits vor der Krise stattfinden, so dass in der Krisensituation bereits ein Vertrauensverhältnis besteht.[117] Loyale Mitarbeiterinnen und Mitarbeiter, die in einer guten Beziehung zu ihrem Arbeitgeber stehen, können in der Krise zu wertvollen Botschafterinnen und Botschafter für die Einrichtung werden.[118] Vor der Krise sollte Klarheit darüber geschaffen werden, welche Ziele im Ernstfall im Rahmen der internen Kommunikation verfolgt werden.[119] Für die erfolgreiche Kommunikation mit internen Zielgruppen, müssen rechtzeitig die erforderlichen Strukturen etabliert und die notwenigen Rahmenbedingungen geschaffen werden.[120] Zu klären und festzulegen ist, wie, wann und wo die Belegschaft Informationen erhält.[121] Es gilt für den Krisenfall konkrete Sprachregelungen zu treffen, Handlungsempfehlungen zu erarbeiten und ggf. Dienstanweisungen vorzubereiten.[122] Entsprechend sollte ein Kommunikationskonzept geplant werden.[123] Zur Gewährleistung einer vertrauensvollen Kommunikation ist sicherzustellen, dass die internen Zielgruppen mindestens zeitgleich mit anderen Empfängern Informationen erhalten.[124]

---

[116] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 17; Heide, M. (2021): Interne Krisenkommunikation: eine Möglichkeit für Kommunikatoren, strategische Werte nachzuweisen, S. 565.

[117] Heide, M. (2021): Interne Krisenkommunikation: eine Möglichkeit für Kommunikatoren, strategische Werte nachzuweisen, S. 568; Schmitt-Geiger, A. (2013): Litigation-PR: Strategische Rechtskommunikation bei Unternehmenskrisen, S. 313.

[118] BMI: Leitfaden Krisenkommunikation, S. 18; Heide, M. (2021): Interne Krisenkommunikation: eine Möglichkeit für Kommunikatoren, strategische Werte nachzuweisen, S. 572; Schmitt-Geiger, A. (2013): Litigation-PR: Strategische Rechtskommunikation bei Unternehmenskrisen, S. 313.

[119] Heide, M. (2021): Interne Krisenkommunikation: eine Möglichkeit für Kommunikatoren, strategische Werte nachzuweisen, S. 572.

[120] BSI-Standard 200-4 Business Continuity Management, S. 139 f.; BMI: Leitfaden Krisenkommunikation, S. 18.

[121] Heide, M. (2021): Interne Krisenkommunikation: eine Möglichkeit für Kommunikatoren, strategische Werte nachzuweisen, S. 575 ff.; BMI: Leitfaden Krisenkommunikation, S. 18; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 23 f..

[122] BSI-Standard 200-4 Business Continuity Management, S. 139 f.; BMI: Leitfaden Krisenkommunikation, S. 18.

[123] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 36; BMI: Leitfaden Krisenkommunikation, S. 25.

[124] BSI-Standard 200-4 Business Continuity Management, S. 141; BSI: Erste Hilfe bei einem schweren IT- Sicherheitsvorfall (Version 1.2.), S. 10; Heide, M. (2021): Interne Krisenkommunikation: eine Möglichkeit für Kommunikatoren, strategische Werte nachzuweisen, S. 576;

Im Zusammenhang mit einem Ransomware–Angriff auf eine kleinere Kommunalverwaltung, der die Verfügbarkeit der technischen Infrastruktur stark beschränkt und der mit einem Diebstahl von Daten und deren Veröffentlichung einhergeht, sind neben den vorgenannten Gesichtspunkten folgende Aspekte zu berücksichtigen:

Es könnte eine starke Verunsicherung bei der Belegschaft vorherrschen, weil der Schaden durch einen selbst ausgelöst worden sein könnte (z.B. durch Öffnen einer Datei oder eines Internet–Links). Darüber hinaus könnte der Datenabzug und dessen etwaige Veröffentlichung zu Unsicherheiten bei der Belegschaft führen, insbesondere wenn sensible, ggf. private Daten im Vorhinein gespeichert wurden.[125] Bei der Belegschaft (insbesondere bei Personen mit IT-gestütztem Arbeitsplatz) könnte, aufgrund der Tatsache, dass die IT-Infrastruktur nicht zur Verfügung steht und dadurch die geschuldete Arbeit nicht verrichtet werden kann, sehr schnell ein Informationsbedarf zum weiteren Vorgehen in Bezug auf die geschuldete Arbeitsleistung entstehen.[126]

Personen, die bei der Bewältigung der krisenhaften Lage eingesetzt werden sollen, können durch die technischen Einschränkungen ggf. nicht alarmiert werden.[127]

Der Gemeinderat ist grundsätzlich Teil der Verwaltung und Hauptorgan der Gemeinde. Die Mitglieder des Gemeinderates sind ehrenamtlich tätige, (kommunal-) politische Akteure unterschiedlichster politischer Couleur und vertreten die Bürgerinnen und Bürger.[128] Dadurch sind Sie z.T. erste Ansprechstellen für die Einwohnerinnen und Einwohner einer Gemeinde, insbesondere wenn es um das Anbringen von Mängeln in Bezug auf kommunale Leistungen geht.[129] Im Kontext eines fol-

Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 111; BMI: Leitfaden Krisenkommunikation, S. 18.

[125] Heide, M. (2021): Interne Krisenkommunikation: eine Möglichkeit für Kommunikatoren, strategische Werte nachzuweisen, S. 575.

[126] Heide, M. (2021): Interne Krisenkommunikation: eine Möglichkeit für Kommunikatoren, strategische Werte nachzuweisen, S. 575 u. S. 578.

[127] BSI: Die Lage der IT- Sicherheit in Deutschland 2023, S. 16.

[128] Gemeindeordnung Baden–Württemberg, § 24 Abs. 1.

[129] Vgl. hierzu auch Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 28 f..

genschweren Cyberangriffs auf die Verwaltung ist der Gemeinderat daher ein wichtiger interner Stakeholder mit Schnittstellencharakter zu externen Interessengruppen.

Aus den vorbezeichneten, sich speziell aus der Situation eines Ransomware–Angriffs ergebenden Aspekten, können individuelle Ziele für die Kommunikation mit internen Zielgruppen abgeleitet werden. Beispielsweise könnte neben der Übermittlung von Handlungsanweisungen und Sachstandsmitteilung an die Belegschaft auch der Fokus auf die Reduzierung der Verunsicherung gelegt werden.[130] Dabei ist von Bedeutung, dass bereits im Vorfeld eine Analyse und Reflexion stattfindet, im Rahmen derer die Informationsbedürfnisse und Erwartungshaltungen eruiert werden. Das Anspruchsniveau zu definieren, ist ein zentraler Schritt, bevor klare Kommunikationsziele festgelegt werden.[131]

Besonderer Beachtung ist im Kontext des Notfallszenarios der Fragestellung zu widmen, wie die internen Zielgruppen mit Informationen versorgt werden können.[132] Eventuell sind etablierte und üblicherweise verlässliche Kommunikationskanäle - die idealerweise auch in der Krise genutzt werden könnten - nicht verfügbar.[133] Die Verschlüsselung von Servern könnte zum kompletten Ausfall der kommunalen IT-Infrastruktur führen, so dass die Nutzung bzw. der Zugriff auf das Mailsystem, des Intranets und sogar der Telefonanlage nicht möglich ist. Ungeachtet der o.g. inhaltlichen Fragestellungen sollte daher im Vorhinein zum einen geklärt und festgelegt werden auf welchem Weg die Informationen zur Verfügung gestellt werden und zum anderen die technischen und organisatorischen Rahmenbedingungen für die Informationsversorgung geschaffen werden.[134] Im Idealfall wird im Rahmen der Notfallplanung im Sinne des BSI–Standards 200-4 eine Kontinuitätsstrategie für die Gewährleistung des kritischen Geschäftsprozesses „Interne

---

[130] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 8 f.; Heide, M. (2021): Interne Krisenkommunikation: eine Möglichkeit für Kommunikatoren, strategische Werte nachzuweisen, S. 574.

[131] Heide, M. (2021): Interne Krisenkommunikation: eine Möglichkeit für Kommunikatoren, strategische Werte nachzuweisen, S. 572; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 37.

[132] BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 10.

[133] BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 10.

[134] BSI-Standard 200-4 Business Continuity Management, S. 140; BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 10.

(Krisen-) Kommunikation“ festgehalten und im Schadensfall entsprechende Maßnahmen umgesetzt.[135] Einzelheiten sollten im entsprechenden Notfallhandbuch festgehalten werden.[136] Grundsätzlich kann die Mitarbeiterinformation im Notfall auch über gut sichtbare Aushänge, bestehende Chatgruppen oder die Führungskräfte erfolgen.[137]

Weiterhin ist festzuhalten, dass der Gemeinderat ein wichtiger Stakeholder einer Kommunalverwaltung ist. Im Rahmen der Master–Thesis wird auf die (kommunalrechtliche) Einbindung des Gemeinderates zur Durchführung von Beratungen und Herbeiführung von Entscheidungen i.S.d. § 24 I, 37 GemO nicht näher eingegangen. Als Hauptorgan der Gemeinde sollte dieser im Notfall jedoch nicht nachrangig mit Informationen versorgt werden.[138] Auf die Informationsrechte nach § 24 III u. IV GemO wird an dieser Stelle hingewiesen.

Zur Bewältigung einer Krise oder eines Notfalls wird regelmäßig eine besondere Aufbauorganisation eingesetzt.[139] Auf die Kommunikation und Kultur im (Krisen-) Stab wird aufgrund der gesteigerten Bedeutung des Stabs für die Krisen- bzw. Notfallbewältigung im Folgenden eingegangen. In Kapitel 2.2.2 wurde bereits dargelegt, dass der Stab ein Gremium ist, welches der Beratung und der Unterstützung dient. Eine gut funktionierende Kommunikation ist daher ein wichtiger Faktor für eine erfolgreiche Stabsarbeit.[140] Kommunikationsfehler können in Krisensituationen zu nicht unerheblichen Schwierigkeiten führen.[141]

Die Sicherstellung eines offenen, zuverlässigen und verständlichen Austausches ist von großer Bedeutung.[142] Eine Nachricht muss akustisch störungsfrei übermittelt

---

[135] BSI-Standard 200-4 Business Continuity Management, S. 84 ff..
[136] BSI-Standard 200-4 Business Continuity Management, S. 86 f..
[137] BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 10.
[138] Vgl. hierzu auch Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 111.
[139] Vgl. Kapitel 2.2.2.
[140] Gißler, D. (2019): Führung und Stabsarbeit trainieren, S. 46.
[141] Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 68; Gißler, D. (2019): Erfolg der Stabsarbeit, S. 49; Hofinger, G. (2022): Sprachliche Kommunikation im Stab - Grundsätze des Sprechens und Schreibens, S. 343; Künzer, L.; Hofinger, G.; Mähler, M. (2022): Psychologische Einflussfaktoren auf Stabsarbeit, S. 197.
[142] Gißler, D. (2019): Führung und Stabsarbeit trainieren, S. 46; Hofinger, G. u. a. (2021): Stabsarbeit aus Sicht der Human Factors-Psychologie, S. 197.

und vom Empfänger aufgenommen werden können.[143] Daneben muss die Botschaft, die überbracht werden soll, vom Empfänger richtig verstanden werden. Fehlinterpretationen sind unbedingt zu vermeiden, denn diese behindern die weitere Kommunikation und führen gegebenenfalls zu Missverständnissen.[144] Vor diesem Hintergrund sollten eindeutige Nachrichten überbracht werden, die im Idealfall kein Raum für Fehlinterpretationen lassen. Darüber hinaus sollte im Rahmen der Stabsarbeit nicht davon ausgegangen werden, dass Ziele, Intentionen, Absichten bekannt sind. Scheinbar selbstverständliche Dinge sollten immer auch explizit ausgesprochen werden.[145]

Unabhängig davon, dass Nachrichten vom Empfänger korrekt verstanden und verarbeitet werden, gilt es, eine offene und konstruktive Gesprächskultur zu erreichen.[146] Trauen sich die Stabsmitglieder aufgrund hierarchischer Beziehungen oder aufgrund zwischenmenschlicher Spannungen nicht, ihre Gedanken, Ideen und gegebenenfalls Bedenken einzubringen, ist dies für die erfolgreiche Arbeit eines Beratungs- und Unterstützungsgremiums nicht förderlich.[147] Es gilt vor diesem Hintergrund eine tragfähige Arbeitsbeziehung, die auf Respekt und Akzeptanz beruht, zu schaffen.[148] Beim gegenseitigen Austausch empfiehlt es sich, einen konstruktiven Umgang zu pflegen und seine Wahrnehmungen dem Gegenüber wertungsfrei mitzuteilen. Das Einhalten von Feedbackregeln sollte beachtet werden.[149] Um als Gruppe erfolgreich im Stab zusammenarbeiten zu können, ist es unerlässlich, dass die Stabsmitglieder ein gut funktionierendes Team darstellen. Die Stärkung von förderlichen Gruppenprozessen für gute Teamarbeit ist in diesem Zusammenhang von gesteigertem Stellenwert.[150]

---

[143] Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 69.
[144] Gißler, D. (2019): Erfolg der Stabsarbeit, S. 49; Hofinger, G. (2022): Sprachliche Kommunikation im Stab - Grundsätze des Sprechens und Schreibens, S. 344.
[145] Hofinger, G. u. a. (2021): Stabsarbeit aus Sicht der Human Factors - Psychologie, S. 198; Hofinger, G. (2022): Sprachliche Kommunikation im Stab - Grundsätze des Sprechens und Schreibens, S. 346.
[146] Gißler, D. (2019): Führung und Stabsarbeit trainieren, S. 48 ff.; Bedé, A. (2022): Grundsätze und Leitlinien zum Führen von (Unternehmens-) Krisenstäben, S. 134.
[147] Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 70.
[148] Hofinger, G. (2022): Sprachliche Kommunikation im Stab - Grundsätze des Sprechens und Schreibens, S. 347.
[149] Gißler, D. (2019): Führung und Stabsarbeit trainieren, S. 51.
[150] Gißler, D. (2019): Erfolg der Stabsarbeit, S. 47.

Die Führungskultur ist ein wichtiger Faktor in Bezug auf die gesamte Kultur des Stabes und wird im besonderen Maße durch die Stabsleitung geprägt.[151] Die Stabsleitung sollte die Meinungen der anderen Mitglieder aktiv einfordern und die eigene Meinung erst zum Schluss äußern.[152] Der Stab wird seiner Rolle als Beratungs- und Unterstützungsgremium nur gerecht, wenn die Person, die letztendlich verantwortlich zu entscheiden hat, sich auch beraten lässt und dies auch signalisiert.[153] Der Führungsstil sollte aufgabenorientiert sein und die Führungskraft sollte - je nach Situation - einen autoritären bis kooperativen Stil verfolgen. Die Stabsleitung muss die Kompetenz besitzen, die Notwendigkeit für die situative Veränderung des Führungsstils zu erkennen und den Wechsel beherrschen.[154] Um den Stab als Team zu führen und eine entsprechende Teamkultur zu fördern, muss die Leitung über ein Höchstmaß an sozialer Kompetenz verfügen.[155]

Auch im Zusammenhang mit der im Notfall stattfindenden Stabsarbeit muss auf die dann vorherrschenden eingeschränkten Rahmenbedingen Rücksicht genommen werden. Damit die kommunikativen Herausforderungen der Stabsarbeit gemeistert werden können, müssen organisatorische und technische Grundvoraussetzungen erfüllt sein.[156] Dieser Aspekt ist bei der Krisen- bzw. Notfallplanung zu berücksichtigen und in einem Notfallkonzept aufzunehmen.[157]

3.3.2 Externe Zielgruppen

Der Kreis der externen Zielgruppen ist groß und vielfältig. Hinzuzuzählen sind z.B. die Bürgerinnen und Bürger, Betroffene, Dienstleister und Medien. Jede einzelne Zielgruppe nimmt dabei einen anderen Blickwinkel ein, verfolgte individuelle Ziele

[151] Gißler, D. (2019): Führung und Stabsarbeit trainieren, S. 52.
[152] Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 70; Bedé, A. (2022): Grundsätze und Leitlinien zum Führen von (Unternehmens-) Krisenstäben, S. 135.
[153] Bedé, A. (2022): Grundsätze und Leitlinien zum Führen von (Unternehmens-) Krisenstäben, S. 134.
[154] Gißler, D. (2019): Führung und Stabsarbeit trainieren, S. 52.
[155] Spielvogel, C. (2018): Stabsorganisation, S. 80; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 30.
[156] BSI-Standard 200-4 Business Continuity Management, S. 134 ff.; Heimann, R.; Gahlen, M. (2022): Räume für Verwaltungsstäbe, S. 249 ff.; Hofinger, G. (2022): Kommunikationsmittel in Verwaltungs- und Unternehmensstäben, S. 291.
[157] BSI-Standard 200-4 Business Continuity Management, S. 85 ff..

und verfügt über eine eigene Anspruchshaltung.[158] Infolgedessen erfolgt im weiteren Verlauf eine Untergliederung der einzelnen externen Interessensgruppen.

Eine eigene Stellung im Zusammenhang mit der Krisenkommunikation nehmen die öffentlich-rechtlichen und privaten Medien ein. Entsprechend § 3 Landespressegesetz erfüllt die Presse eine öffentliche Aufgabe, wenn sie in Angelegenheiten von öffentlichem Interesse Nachrichten beschafft und verbreitet, Stellung nimmt, Kritik übt oder auf andere Weise an der Meinungsbildung mitwirkt. Ein besonderer Auskunftsanspruch ergibt sich aus § 4 Landespressegesetz, der die Behörden gesetzlich dazu verpflichtet, den Vertretern der Presse die der Erfüllung ihrer Aufgaben dienende Auskünfte zu erteilen. Die an die Medien erteilten Auskünfte werden von diesen an deren Konsumenten über verschiedene Kanäle weitergeben. Die Medien orientieren sich daher bei ihren Beiträgen an den Interessen der Leserinnen und Leser, Hörerinnen und Hörer sowie Zuschauerinnen und Zuschauern.[159] Die Medien versuchen z.T. Krisen in einen engen Zusammenhang mit Personen zu bringen, Emotionen in den Vordergrund zu stellen, die Situation zu vereinfachen oder zuzuspitzen.[160] Eine Krise kann auch eine sehr hohe Anzahl an Medienanfragen mit sich bringen.[161] Dies kann zu einer besonderen Herausforderung für die betroffene Behörde werden.[162] Je nach Phase schwankt der Informationsbedarf der Medien und die Intensität der Berichterstattung.[163] Insbesondere zu Beginn einer krisenhaften Lage ist der Informationsbedarf hoch.[164] Häufig erfolgt die erste Meldung eines Krisenereignisses über die Medien.[165] Es empfiehlt sich daher i.d.R. offensiv die Medien über das Ereignis zu informieren.[166] Dadurch kann die Grundlage für eine

---

[158] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 14; BMI: Leitfaden Krisenkommunikation, S. 19; BSI-Standard 200-4 Business Continuity Management, S. 140 ff..
[159] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 16; BMI: Leitfaden Krisenkommunikation, S. 19; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 307 f..
[160] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 16; Merten, K. (2013): Krise, Krisenmanagement und Krisenkommunikation, S. 164.
[161] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 154.
[162] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 306 ff..
[163] BMI: Leitfaden Krisenkommunikation, S. 20; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 14.
[164] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 16.
[165] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 16.; BMI: Leitfaden Krisenkommunikation, S. 20.
[166] BMI: Leitfaden Krisenkommunikation, S. 20; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 253.

schnelle, wahrheitsgemäße und transparente Kommunikation geschaffen werden.[167] Eine proaktive Vorgehensweise ermöglicht den konkreten Zeitpunkt der Information und die Inhalte sowie Tonalität zumindest teilweise zu steuern.[168] Im Leitfaden Krisenkommunikation des BMI wird zur Bedeutung der Medienberichterstattung zusammenfassend festgestellt: „Die Wahrnehmung der Krise und die Bewertung des Krisenmanagements durch die Öffentlichkeit sind in beachtlichem Umfang von der Medienberichterstattung und darauf aufbauenden privaten Veröffentlichungen im Internet und in sozialen Medien abhängig.“[169]

Aus dieser Feststellung resultiert die Erkenntnis, dass in der Krise die Medien in Bezug auf die Reputation der Verwaltung eine wesentliche Rolle einnehmen. Für eine erfolgreiche Krisenkommunikation ist diesem Sachverhalt angemessen Rechnung zu tragen. Im Idealfall gelingt eine Medienberichterstattung, die sich mit den Primär-Informationen und Botschaften der Behörde deckt, welche über die eigenen Kanäle publiziert werden.[170] Die Zusammenarbeit mit den Medien kann daher auch eine Gelegenheit darstellen, um gezielt und strukturiert Nachrichten an relevante Zielgruppen zu übermitteln. Dies kann dabei unterstützen, der Verbreitung von Falschinformationen und Gerüchten entgegenzuwirken.[171]

Es wird aus den Ausführungen deutlich, dass die Zusammenarbeit mit den Medien eine gewisse Vorbereitung erfordert.[172] Damit im Notfall das Zusammenspiel gelingt, ist ein bereits funktionierendes Netzwerk mit den relevanten Medienvertretern vorhanden, auf das zurückgegriffen werden kann.[173] Im Vorhinein ist auch zu klären und festzulegen, welche Person die Schnittstellenfunktion zu den Medien

---

[167] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 123.
[168] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 253; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 37; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 123.
[169] BMI: Leitfaden Krisenkommunikation, S. 20.
[170] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 37.
[171] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 123; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 37.
[172] Vgl. hierzu auch BSI-Standard 200-4 Business Continuity Management, S. 139 ff.; BMI: Leitfaden Krisenkommunikation, S. 15 u. S. 25.
[173] BMI: Leitfaden Krisenkommunikation, S. 20; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 113.

einnimmt.[174] Auf eine angemessene Eignung und Befähigung der in dieser Funktion eingesetzten Personen sollte dabei Wert gelegt werden.[175] Idealerweise kann im Ernstfall auf bereits im Vorhinein erstelle Muster, Entwürfe u.ä. als Hilfsmittel zurückgegriffen werden.[176]

Wie bereits dargelegt, sollte bereits in der Vorbereitungsphase des Krisenmanagements geplant werden, wie der Kontakt und der Austausch mit den Medien im Falle eines Ransomware–Angriffes erfolgen soll. Klassische Kanäle wie die Pressemitteilung, die Pressemappe, die Pressekonferenz kommen dabei ebenso in Frage, wie das zur Verfügung stellen von Footage–Material.[177] In der Krise ist die klassische Pressemitteilung noch immer ein Hauptwerkzeug.[178] Im Einzelfall müssen die jeweiligen Vor- und Nachteile der einzelnen Optionen abgewogen werden. Die Funktionen und Ziele der Krisenkommunikation[179] sollten bei der Auswahl der eingesetzten Instrumente nicht aus dem Blick verloren werden. Die Festlegungen sind idealerweise in einem Kommunikationsplan festzuhalten.[180] Nicht außer Acht gelassen werden dürfen die technischen Beeinträchtigungen, die im Zusammenhang mit einer Ransomware–Attacke einhergehen. Diese bestehen nämlich (je nach konkreter Schadenslage) ggf. auch im Hinblick auf die Korrespondenz mit den Medien. Für das Notfallszenario sollte daher im Vorfeld eine entsprechende Kontinuitätsstrategie i.S.d. BSI–Standards 200-4 entwickelt und in einem Notfallhandbuch festgehalten werden.[181]

---

[174] BSI-Standard 200-4 Business Continuity Management, S. 142; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 38; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 155; BMI: Leitfaden Krisenkommunikation, S. 20.

[175] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 38; BMI: Leitfaden Krisenkommunikation, S. 20.

[176] BMI: Leitfaden Krisenkommunikation, S. 20; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 36.

[177] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 252 ff..

[178] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 122 f.; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 252.

[179] Siehe Kapitel 3.2.

[180] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 36 f.; BMI: Leitfaden Krisenkommunikation, S. 26.

[181] Vgl. Ausführungen in Kapitel 3.3.1.

Ein wichtiger Aspekt der Medienarbeit liegt im Medienmonitoring.[182] Im Zusammenhang mit Krisen und Notfällen kann eine kritische Berichterstattung seitens der Medien stattfinden. Insbesondere durch Soziale Medien kann sich diese sehr schnell verbreiten und einen „Shitstorm“ nach sich ziehen.[183] Wenn durch die Behörde oder einen externen Dienstleister kein Monitoring stattfindet und somit nicht bekannt ist, wie aktuell über sie selbst oder das krisenhafte Ereignis informiert und kommuniziert wird, kann sie nicht gegensteuern. Infolgedessen ist es empfehlenswert, im Krisen- bzw. Notfall - ggf. sogar dauerhaft zur Früherkennung von sich medial zuspitzenden Themen -[184] die Medien und deren Berichterstattung stetig zu beobachten.[185]

Eine weitere bedeutende externe Zielgruppe stellen die Bürgerinnen und Bürger dar. Die Bürgerschaft wiederum setzt sich aus unterschiedlichen Gruppen zusammen und ist damit ein heterogenes Gebilde mit unterschiedlichen kommunikativen Bedürfnissen und Ansprüchen.[186] Dementsprechend müssen die Informationen aufbereitet und zielgruppenspezifisch zur Verfügung gestellt werden. Es kommt dabei stark auf die konkrete Krisensituation an, wie die Informationen aufbereitet werden und über welchen Kanal kommuniziert wird.[187] Im Regelfall möchte die nicht unmittelbar von dem Schadensereignis betroffene Bevölkerung eine Information über den aktuellen Sachstand der Lage und sich ein aktuelles Bild davon machen, in wie weit die Situation unter Kontrolle ist.[188] Im Falle eines Ransomware–Angriffes auf die lokale Kommunalverwaltung, ist die breite Bevölkerung zunächst „nur“ insoweit tangiert, als dass sie aufgrund der technischen Einschränkungen bei der Be-

[182] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 37 f.; BSI-Standard 200-4 Business Continuity Management, S. 142 f.; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 276 ff.; BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 24.
[183] Bachmann, S.; Ternès von Hattburg, A. (2021): Effiziente Krisenkommunikation- transparent und authentisch, S. 30 f.; BSI-Standard 200-4 Business Continuity Management, S. 143.
[184] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 276 f.; Bachmann, S.; Ternès von Hattburg, A. (2021): Effiziente Krisenkommunikation- transparent und authentisch, S. 55.
[185] BSI-Standard 200-4 Business Continuity Management, S. 143; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 38; BMI: Leitfaden Krisenkommunikation, 20, 23; Schmitt-Geiger, A. (2013): Litigation-PR: Strategische Rechtskommunikation bei Unternehmenskrisen, S. 311 f..
[186] BMI: Leitfaden Krisenkommunikation, S. 21.
[187] BMI: Leitfaden Krisenkommunikation, S. 21.
[188] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 15.

hörde die Leistungen der Verwaltung ggf. nicht in Anspruch nehmen kann und Personen ggf. zu dem Kreis derjenigen zählen, dessen Daten gestohlen und möglicherweise veröffentlicht werden.[189] Eine detaillierte Untersuchung der kommunikativen Bedürfnisse der Bevölkerung speziell für das Notfallszenario „Ransomware–Angriff auf die örtliche Kommunalverwaltung“ kann im Rahmen dieser Master–Thesis nicht geleistet werden. Insofern wird im Rahmen dieses Projekts für das Notfallszenario unterstellt, dass das Leben und die Gesundheit der Bevölkerung durch das Schadensereignis nicht unmittelbar bedroht ist und sich der Informationsbedarf und der Informationsanspruch auf einem beschränkten Niveau befindet. Konkret wird unterstellt, dass bedarfsgerecht an die Bevölkerung kommuniziert wird, wenn folgende Fragestellungen abgehandelt werden: „Was ist passiert? Warum kam es zu dem Schadensereignis? Welche Auswirkungen hat das Geschehnis auf die Bevölkerung? Wie schnell kann die Krise mit ihren Auswirkungen bewältigt werden? Was wird zur Bewältigung getan? Wie ist diesbezüglich der aktuelle Stand und was sind die nächsten Schritte?“[190]

Grundsätzlich kann die Behörde auf verschiedene Möglichkeiten zurückgreifen, um mit der Bevölkerung zu kommunizieren. Der Weg über die Berichterstattung der Medienlandschaft wurde bereits dargelegt. Im Zusammenhang mit der Krisenkommunikation bringen eigene Kanäle den Vorteil mit sich, dass diese durch die Behörde selbst bespielt und kontrolliert werden.[191] Zu den eigenen Medien zählen zum Beispiel die Gemeinde-Website, das „eigene Amtsblatt“[192] sowie eigene Druckerzeugnisse (z.B. Flyer, Broschüren und Plakate). In einer Krise kommt aber grundsätzlich auch der Einsatz von Sirenen, Lautsprecherdurchsagen und Ansprachen in Sammelstellen in Betracht.[193] Darüber hinaus können Bürgeransprechstellen oder Bürgertelefone („Bürgerhotline“) nützliche Dienste erweisen.[194] Nachfolgend wird

---

[189] In Kapitel 1.2. wurde bereits angemerkt, dass die vorliegende Master-Thesis eine Ransomware-Attacke zugrunde legt, bei der die kritische Infrastruktur, die der Regulierung des BSI–Gesetzes unterliegen, nicht betroffen ist.

[190] Vgl. hierzu auch BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 24.

[191] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 251.

[192] Gemeindeordnung Baden–Württemberg, § 20 Abs. 3.

[193] BMI: Leitfaden Krisenkommunikation, S. 21.

[194] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 261; BMI: Leitfaden Krisenkommunikation, S. 21.

auf einzelne Optionen, mit Berücksichtigung des Notfallszenarios „Ransomware–Angriff“ näher eingegangen.

Die Website ist in einer krisenhaften Lage eine der ersten und zentralsten Anlaufstellen für diverse Interessengruppen, wie Medien, Betroffene oder die Bevölkerung.[195] Auf der eigenen Website Informationen bereitzustellen, kann zu einer Entlastung der Pressestelle beitragen.[196] Darüber hinaus bietet die Kommunikation über die eigene Website den Vorteil, dass die Inhalte vollständig der eigenen Kontrolle unterliegen.[197] Idealerweise werden für das Notfallszenario vorbereitete Seiten, die im Ernstfall nur noch aktiviert und ergänzt werden müssen, vorgehalten.[198] FAQs, die im Krisenverlauf regelmäßig aktualisiert werden, können dabei einen großen Mehrwert bringen.[199] Die „Darksites“, mit ersten Informationen sollten bei einer Krise schnell ohne größeren Aufwand aktivierbar und nutzbar sein.[200] Dafür sind entsprechende technische und organisatorische Voraussetzungen zu schaffen. Hat man sich jedoch auf das spezielle Notfallszenario im Hinblick auf die Internetpräsenz vorbereitet, so stellt diese das „wertvollste Kommunikationsmittel schlechthin“[201] dar. Sofern die Behörde selbst auf Social-Media-Kanälen aktiv ist, kann dies genutzt werden, um auf die Behördenwebsite als tieferen, offiziellen Informationskanal zu verweisen und ggf. die Interessensgruppen auf diesen zu lenken.[202]

---

[195] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 263 f.; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, 106, 164; Riecken, M. (2013): Erfolgskritische Faktoren der angewandten Krisenkommunikation, S. 323.

[196] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 106; Riecken, M. (2013): Erfolgskritische Faktoren der angewandten Krisenkommunikation, S. 323.

[197] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 251.

[198] BSI-Standard 200-4 Business Continuity Management, S. 142; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 263 f.; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 107; Riecken, M. (2013): Erfolgskritische Faktoren der angewandten Krisenkommunikation, S. 323; BMI: Leitfaden Krisenkommunikation, S. 21.

[199] BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 11; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 106 f..

[200] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 264; Riecken, M. (2013): Erfolgskritische Faktoren der angewandten Krisenkommunikation, S. 323.

[201] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 251.

[202] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 106.

Das kommunale Amtsblatt im Sinne von § 20 Abs. 3 GemO BW stellt für die Kommunalverwaltung eine Möglichkeit dar, öffentliche Bekanntmachungen durchzuführen.[203] Darüber hinaus dient es der Information der Einwohnerinnen und Einwohner über die allgemein bedeutsamen Angelegenheiten der Gemeinde.[204] Damit ist es, ähnlich wie die kommunale Website, eine zentrales Informationsinstrument der Gemeinde.[205] Das Amtsblatt könnte daher als Kanal genutzt werden, um kontinuierlich, unter eigener Regie, über die aktuelle Entwicklung in Bezug auf das krisenhafte Ereignis zu informieren. Dabei ist jedoch der jeweilige Erscheinungszyklus des Printmediums zu berücksichtigen. Im Falle eines Ransomware–Angriffes ist auch bei diesem Medium sicherzustellen, dass die technischen Herausforderungen gemeistert werden, um den Kanal zu nutzen.

Die Nutzung der Sozialen Medien hat inzwischen einen festen Platz in der einschlägigen DIN-Norm zum Krisenmanagement eingenommen.[206] Die Norm bezeichnet die Kompetenzen, zumindest einzelne Kanäle zu bespielen, als die „grundlegenden Fähigkeiten, die erforderlich sind, um eine Krisensituation zu bewältigen.“[207] Der BSI-Standard 200-4 sieht in den Sozialen Medien einen optionalen Kommunikationskanal, stellt aber klar, dass diesbezüglich zumindest ein Monitoring erfolgen sollte.[208] Neben dem auch an anderer Stelle beschriebenen Monitoring, erfüllen Social-Media die Aufgabe der unmittelbaren und ungefilterten Bürgerinformation durch die Behörde.[209] Neben dem Vorteil, dass ein direkter Dialog auf digitaler Basis stattfinden kann, muss einkalkuliert werden, dass ein Thema mit negativer Konnotation unkontrolliert verbreitet wird und / oder der eigene Kanal mit „Shitstorm“

[203] Verordnung des Innenministeriums zur Durchführung der Gemeindeordnung Baden–Württemberg, § 1 Abs. 1 Nr. 1.
[204] Vgl. Gemeindeordnung Baden–Württemberg, § 20 Abs. 1 i.V.m. § 20 Abs. 3.
[205] Kunze, R.; Bronner, O.; Katz, A. (2023): Gemeindeordnung für Baden-Württemberg Kommentar, RN 3 zu § 20.
[206] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 41.
[207] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 41.
[208] BSI-Standard 200-4 Business Continuity Management, S. 142 f..
[209] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 169; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 262; BMI: Leitfaden Krisenkommunikation, S. 24.

überflutet wird.[210] Eine solche Eskalation kann mit einem nicht unerheblichen Reputationsschaden einhergehen.[211] Um professionell zu agieren und das Potential Sozialer Medien nutzen zu können, ist zu berücksichtigen, dass kompetentes Personal eingesetzt wird und für die Social-Media-Betreuung ausreichend Ressourcen vorhanden sind.[212] Wenn die Behörde nur eingeschränkt die Sozialen Medien bespielen will oder kann, so ist zumindest eine gezielte Lenkung der Nutzer zu einem behördlichen Kanal, z.B. der Website, denkbar.[213]

In der Krise kann zur Kommunikation mit der Bevölkerung neben den vorgenannten Kanälen auch ein „Krisentelefon“ zum Einsatz kommen.[214] Durch die „Hotline“ erhalten die Anrufer aus erster Hand und persönlich von der Behörde Auskünfte und können ihre Anliegen im Rahmen eines Telefongespräches anbringen. Anrufende Medienvertreter können von dem eingesetzten Personal herausgefiltert werden und einen Rückruf durch die zuständige Stelle vereinbaren. Unmittelbar Betroffene wiederum können mit einer Erstinformation versorgt und ggf. an das Krisenbetreuungsteam weitergeleitet werden. Je nach Art und Ausmaß der Krisensituation werden über das Krisentelefon unterschiedliche Bedürfnisse bedient, so dass auch die Anforderungen an den Telefonservice situativ verschieden sind.[215] So muss das Krisentelefon neben rein informativen Zwecken unter Umständen auch der psychologischen Betreuung dienen.[216] Bei der Einrichtung einer gut organisierten zentralen telefonischen Ansprechstelle besteht der Vorteil, dass von außen kommende Anfragen kanalisiert werden und dadurch intern eine Entlastung geschaffen

---

[210] Bachmann, S.; Ternès von Hattburg, A. (2021): Effiziente Krisenkommunikation- transparent und authentisch, S. 24 f.; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 263; Hofmann, T. (2013): Krise 2.0: Erfolgreiches Reputationsmanagement mit Social-Media, S. 345 f..

[211] Bachmann, S.; Ternès von Hattburg, A. (2021): Effiziente Krisenkommunikation- transparent und authentisch, S. 25; Hofmann, T. (2013): Krise 2.0: Erfolgreiches Reputationsmanagement mit Social-Media, S. 346.

[212] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 171; BMI: Leitfaden Krisenkommunikation, S. 23.

[213] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 106.

[214] BMI: Leitfaden Krisenkommunikation, S. 21; BSI-Standard 200-4 Business Continuity Management, S. 142; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 261; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 184.

[215] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 184; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 261.

[216] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 261; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 184 f..

wird.[217] Nach außen hin signalisiert die Behörde, dass sie offen, ansprechbar und aktiv ist.[218] Neben den technischen und organisatorischen Vorkehrungen, die zur Einrichtung eines Krisentelefons erforderlich sind, müssen die im Rahmen der Hotline eingesetzten Kräfte unbedingt für die Tätigkeit im Krisentelefondienstes vorbereitet und geschult sein.[219]

In der Gesamtbetrachtung der vorangegangenen Ausführungen ist festzustellen, dass auch einer kleineren Verwaltung grundsätzlich mehrere eigene Kanäle zur Verfügung stehen, die genutzt werden können, um zielgruppengerecht zu kommunizieren. Auf diese vorhandenen und „bekannten" Instrumente zurückzugreifen bietet sich im Notfall an.[220] Nicht außer Acht gelassen werden darf jedoch, dass die jeweiligen Kanäle auch aus technischer Sicht nutzbar sein müssen, um im Ernstfall adäquat kommunizieren zu können.

Es wurde bereits ausgeführt, dass im Falle des Notfallszenarios „Ransomware–Angriff" die breite Bevölkerung von der zunächst hauptsächlich die Verwaltung betreffenden Krise, faktisch nur eingeschränkt betroffen ist. Verschiedene Personen oder Personengruppen sind jedoch im Falle eines Ransomware–Angriffs, der mit einem Datendiebstahl verbunden ist, stärker betroffen. Diese Personen, sofern diese der Behörde bekannt sind, sollten spezielle Informationen und ggf. Beratungen oder Hilfestellungen, insbesondere bezogen auf den Datendiebstahl, erhalten.[221] Unter dem betroffenen Personenkreis können sich auch z.B. Mitarbeiterinnen und Mitarbeiter, Dienstleisterinnen und Dienstleister oder Newsletter–Abonnentinnen und Abonnenten befinden. Eine gesetzliche Verpflichtung zur unverzüglichen Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffener Person ergibt sich aus Art. 34 Datenschutz-Grundverordnung. Art. 34

---

[217] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 261.
[218] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 261; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 191.
[219] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 185; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 261; BMI: Leitfaden Krisenkommunikation, S. 21.
[220] BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 10; BSI-Standard 200-4 Business Continuity Management, S. 142.
[221] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 15; BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 12 f.; BSI-Standard 200-4 Business Continuity Management, S. 139 f..

i.V.m. Art. 33 Datenschutz–Grundverordnung regelt Einzelheiten zu dem Erfordernis, dem Zeitpunkt, der Art und des Umfangs der Benachrichtigung. Im Anhang zu dieser Arbeit befindet sich ein Mustertext, der als Basis für die Erstellung eines Anschreibens genutzt werden kann. Im konkreten Einzelfall ist er an die jeweiligen Gegebenheiten anzupassen.

Im Falle einer Ransomware–Attacke befindet sich eine Schadsoftware im behördlichen IT-Netzwerk und hat zum Ziel, sich weiter in der Netzwerkinfrastruktur auszubreiten.[222] Zur effizienten und effektiven Abwicklung der gemeindlichen Aufgabenerfüllung besteht heutzutage in verschiedenen Verwaltungsbereichen eine digitale Vernetzung zwischen Kommunalverwaltungen und darüber hinaus zu Land und Bund.[223] Eine Kompromittierung über die lokale Netzwerkinfrastruktur hinaus hätte damit das Potenzial für weitreichende Auswirkungen. Die Komm.ONE, als zentraler IT–Dienstleister für kommunale Körperschaften, ist maßgeblich an der digitalen Verwaltungsvernetzung beteiligt und übernimmt in diesem Kontext verschiedene Aufgaben.[224] Im Notfallszenario „Ransomware–Angriff“ muss die Komm.ONE unverzüglich informiert werden, um den Schaden möglichst zu begrenzen. Sofern das gemeindliche IT–Netzwerk mit weiteren externen Netzwerken verknüpft ist und eine Gefahr der Kompromittierung nicht ausgeschlossen werden kann, muss auch zu diesen Beteiligten, zwecks Schadenminimierung und ggf. aus vertraglichen Vereinbarungen heraus, Kontakt aufgenommen werden. Insbesondere die Komm.ONE, die in die Netzwerkinfrastruktur der Kommunen verwoben ist, stellt einen wichtigen Stakeholder dar. Zum einen aufgrund der potenziellen Kompromittierung der eigenen Infrastruktur und Systeme, zum anderen als Dienstleisterin zahlreicher öffentlicher Verwaltungen im Land.

---

[222] BSI: Die Lage der IT-Sicherheit in Deutschland 2023, S. 16.

[223] Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg, Landtag - Drucksache 16 / 3822, Kleine Anfrage vom 03.04.2018 über die Digitalisierung in Baden-Württemberg, S. 4 f, https://www.landtag-bw.de/files/live/sites/LTBW/files/dokumente/WP16/Drucksachen/3000/16_3822_D.pdf (16.11.2024).

[224] Komm.ONE: Satzung der Komm.ONE AöR (Stand 09.03.2021), S. 1 f. Satzung der Komm.ONE AöR, https://www.komm.one/site/Komm.ONE_Internet/get/documents_E1734798227/Komm.ONE/Komm.ONE_Internet_Objekte/Mitglieder%20VR/Satzung_der_Komm_ONE_AoeR.pdf (16.11.2024); Komm.ONE: Aufgabenspektrum, https://www.komm.one/wer-wir-sind (16.11.2024).

Neben den Meldepflichten gegenüber den von dem Abfluss personenbezogener Daten betroffenen Personen und etwaigen Dienstleistenden können weitere Meldepflichten im Zusammenhang mit einer Krise oder eines Notfalls existieren.[225] Im Kontext des zu behandelnden Notfallszenarios ergibt sich eine weitere Meldepflicht aus Art. 33 der Datenschutz–Grundverordnung gegenüber des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg. Die Norm fordert grundsätzlich eine unverzügliche Meldung, möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde. Die Meldung kann über ein Online–Formular erfolgen.[226]

Eine weitere, aus vertraglichen Regelungen resultierende Meldepflicht könnte sich im Schadensfall auch gegenüber von Versicherungsunternehmen ergeben, mit denen Schadensregulierungsvereinbarungen getroffen wurden. Ungeachtet einer etwaigen Verpflichtung kann eine zeitnahe Kontaktaufnahme mit der Versicherung vorteilhaft sein.[227]

Grundsätzlich sollten sämtliche Meldepflichten bekannt und mit der Notfall- und Krisenkommunikation abgestimmt sein.[228]

3.3.3 Beteiligte im Krisenmanagement

Im Falle einer Krise ist häufig nicht nur eine einzelne Behörde in die Krisenbewältigung involviert. Oftmals sind weitere Organisationen - auf kommunaler, Landes- oder Bundesebene - beteiligt oder zumindest tangiert.[229] Dabei ist sicherzustellen, dass im Rahmen der Krisenbewältigung im engeren Sinn eine gute Abstimmung erfolgt, aber darüber hinaus auch in Bezug auf die Kommunikation mit den internen

[225] Vgl. z.B. BSI–Gesetz, § 8 b Abs. 4 und § 8 c Abs. 3.
[226] Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Formular Datenpanne melden, https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/ (16.11.2024).
[227] BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 13; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 293.
[228] BSI-Standard 200-4 Business Continuity Management, S. 139 f..
[229] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 31; BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 24; BMI: Leitfaden Krisenkommunikation, S. 9 u. S. 17.

und externen Zielgruppen.[230] Erfolgreiche Krisenkommunikation basiert maßgeblich auf einer abgestimmten Kommunikationslinie mit anderen von der Krise betroffenen Organisationen.[231] Wie bereits an anderer Stelle dargelegt, sind dies im Notfallszenario „Ransomware–Angriff“ insbesondere die Strafverfolgungsbehörden (v.a. die Zentrale Ansprechstelle Cybercrime -ZAC-[232]),[233] die Cybersicherheitsagentur Baden–Württemberg,[234] der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden–Württemberg[235] und die Komm.ONE.[236] Je nach Situation können im Einzelfall weitere Institutionen, wie z.B. die Fach- oder Rechtsaufsichtsbehörde[237] oder das BSI beteiligt sein.[238] Die Absprache von Maßnahmen, Sprachregelungen und Publikationen zwischen den beteiligten Stellen und Organisationen ist von großer Bedeutung.[239] Dies setzt jedoch voraus, dass die jeweiligen Ansprechpartnerinnen und Ansprechpartner bekannt sind und auch aus technischer Sicht die Kontaktaufnahme gewährleistet ist.

3.4 Vorbereitung der Krisenkommunikation

An verschiedenen Stellen dieser Arbeit ist bereits erläutert worden, dass erfolgreiche Krisenkommunikation einer gewissen Planung, Vorbereitung und Vorsorge bedarf.[240] Der folgende Abschnitt widmet sich dieser Phase des Krisenmanagements und zeigt wesentliche Aspekte zur Vorbereitung der Krisenkommunikation auf.

---

[230] Vgl. z.B. Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 19 f.; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 41; BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 24; BMI: Leitfaden Krisenkommunikation, S. 18.

[231] BMI: Leitfaden Krisenkommunikation, S. 13.

[232] Ministerium des Inneren, für Digitalisierung und Kommunen Baden–Württemberg: Zentrale Ansprechstellen für Cybercrime. https://lka.polizei-bw.de/zentrale-ansprechstelle-cybercrime/ (16.11.204).

[233] Strafprozessordnung, § 160 u. § 163.

[234] CSBW: Über die CSBW, https://www.cybersicherheit-bw.de/ueber-die-csbw (16.11.2024).

[235] Datenschutz–Grundverordnung, Art. 33 u. Art. 51 i.V.m. Landesdatenschutzgesetz Baden–Württemberg, § 25.

[236] Komm.ONE: Satzung der Komm.ONE AöR (Stand 09.03.2021).

[237] Gemeindeordnung Baden–Württemberg, § 118.

[238] BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 23 f.

[239] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 32; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 41; BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 24; BMI: Leitfaden Krisenkommunikation, S. 19.

[240] Vgl. hierzu auch BMI: Leitfaden Krisenkommunikation, S. 14 u. S. 25; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 91, S. 95 u. S. 103; Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 23; Merten, K. (2013): Krise, Krisenmanagement und Krisenkommunikation, S. 165.

In Kapitel 2 wurde bereits ausgeführt, dass in den Krisenstab eine für den Bereich Kommunikation verantwortliche Personen zu integrieren ist. Die Rollen, Aufgaben, Rechte und Pflichten der einzelnen Stabsmitglieder sollten im Vorfeld festgelegt und festgehalten werden.[241] Mit vorbezeichneter Festlegung eng verbunden ist die Planung personeller Ressourcen auch über den Krisenstab hinaus. Sind die zu erledigenden kommunikativen Aufgaben ermittelt, sollte eine vernünftige Ressourcenplanung unter Berücksichtigung der örtlichen Rahmenbedingungen erfolgen.[242] Die Personalkapazitäten, die im regulären Betrieb im Bereich Öffentlichkeitsarbeit eingesetzt werden, sind im Krisenfall in der Regel nicht ausreichend.[243] Entsprechend müssen Lösungen mit internem oder externem Personal zur Sicherstellung der Krisenkommunikation im Vorhinein ausgelotet und schließlich festgelegt werden.[244] Weiterhin sollten im Zuge der Vorbereitung die internen Abläufe bestimmt und darüber hinaus Checklisten, Formulare, Handlungsleitfäden und Kontaktlisten erstellt und regelmäßig aktualisiert werden.[245]

Neben dem Erfordernis, intern Klarheit über die Strukturen und Abläufe für die Bewältigung des Ernstfalls zu schaffen, sollte auch im Vorhinein eruiert und dokumentiert werden, welche externen Akteure bei der Krisenbewältigung mitwirken und wie (technisch u. organisatorisch) der Austausch im Ernstfall erfolgt.[246] Dazu zählt auch die Klärung von Zuständigkeiten und Verantwortlichkeiten der einzelnen Organisationen.[247] Im vorherigen Kapitel wurden die wichtigsten Beteiligten

[241] BSI-Standard 200-4 Business Continuity Management, S. 99.
[242] Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 23; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 245 f.
[243] Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 23; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 245 f.; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 29.
[244] Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 23 f.; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 246.
[245] BMI: Leitfaden Krisenkommunikation, S. 27; DIN EN ISO 22361:2023–2 Krisenkommunikation, S. 36.
[246] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 95; Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S. 19.
[247] BMI: Leitfaden Krisenkommunikation, S. 18.

bereits genannt. Idealerweise erfolgt der Erstkontakt mit den beteiligten Organisationen bereits vor dem Eintritt des Ernstfalles, in der Präventions- und Vorbereitungsphase des Krisenmanagements.[248]

In Kapitel 3.3.2 wurde die besondere Bedeutung der medialen Berichterstattung verdeutlicht. In der Krise auf ein etabliertes (Medien-) Netzwerk zurückgreifen zu können und die verschiedenen Kontakte verfügbar zu haben, kann nur durch eine vorzeitige Aktivität und Vorarbeit gewährleistet werden.[249] Allerdings ist nicht nur ein gepflegter Medienverteiler und ein gelebtes Netzwerk rechtzeitig herzustellen, sondern idealerweise kann auch auf vorbereitete Dokumente, wie vorgefertigte Pressemitteilungen, Statements, Dossiers etc. zurückgegriffen werden.[250]

Weiterhin ist im Vorhinein für den Ernstfall bereits festgelegt, welche Kommunikationskanäle und welche Medienformate zur Information und ggf. zum Austausch sowohl mit externen Zielgruppen als auch mit internen Interessensgruppen eingesetzt werden.[251] Das Versäumnis, geeignete Kanäle zum Erreichen der gewünschten Zielgruppen zu verwenden, kann ein erhebliches Hindernis für eine effektive Krisenkommunikation darstellen.[252] Für die Beantwortung wiederkehrender Fragen und die Übermittlung wesentliche Botschaften der Behörde eignen sich auf die Situation anpassbare FAQs in geeigneter Sprache, die über adäquate Kanäle, z.B. einer vorbereiteten Website oder dem Intranet, veröffentlicht werden.[253]

Um sicherzustellen, dass die Behörde - im Idealfall nahtlos - in den Krisenkommunikationsmodus „umschalten“ und die Vorarbeit in der Krise umsetzen kann, sollte die Behörde im Vorhinein einen Krisenkommunikationsplan bzw. Krisenkommunikationskonzept erstellen, in dem sämtliche Vorkehrungen und Planungen für das

---

[248] Gahlen, M.; Kranaster, M. (2019): Krisenmanagement, S.19 u. S. 24; BMI: Leitfaden Krisenkommunikation, S. 18.
[249] BMI: Leitfaden Krisenkommunikation, S. 20; Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 255.
[250] BMI: Leitfaden Krisenkommunikation, S. 20; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 36.
[251] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 36; BSI-Standard 200-4 Business Continuity Management, S. 140.
[252] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 40.
[253] BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 11; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 106 f.; BSI-Standard 200-4 Business Continuity Management, S. 142.

Notfallszenario festgehalten werden.[254] Entsprechend der DIN 22361:2023 sollte der Krisenkommunikationsplan Entwürfe erster Stellungnahmen, Leitlinien für Mitarbeiterinnen und Mitarbeiter, die Anrufe entgegen nehmen, Informationsblätter und Pressemappen, Orte für Pressekonferenzen, Liste der zu nutzenden Medienkanäle, Instrumente und Systeme für die Überwachung und Einbindung sozialer Medien, Liste der Beteiligten und ihrer Aufgaben und Funktionen, Kontaktinformationen für Ressourcen, einschließlich der Ansprechpartnerinnen und Ansprechpartner beinhalten.[255] Darüber hinaus sollte der Krisenkommunikationsplan eine strukturierte Konzeption für die Durchführung der Kommunikation vorsehen, Zuständigkeiten und Verantwortlichkeiten eindeutig zuweisen, Verfahren und Maßnahmen für Bekanntmachungen festlegen und die Optionen für die Bereitstellung von Ressourcen identifizieren.[256] Selbst wenn dies nicht bis ins Detail umsetzbar oder realistisch ist, kann auch ein Grobgerüst zu effizienter und effektiver Krisenkommunikation verhelfen.[257] Im Anhang zu dieser Arbeit befinden sich Mustertexte (Aushang, FAQs, Pressemitteilung), die als Basis dienen können. Sie sind im konkreten Einzelfall auf die vorherrschenden Gegebenheiten anzupassen.

Ein zentraler Gesichtspunkt, insbesondere im Falle eines Ransomware–Angriffes, ist die Funktionsfähigkeit der Kommunikationstechnik.[258] Bei der Planung der einzusetzenden Kommunikationskanäle und Medienformate muss die besondere Situation in Bezug auf die IT-Infrastruktur im Ernstfall von Vorneherein mitbedacht und entsprechend vorgesorgt werden.[259] Der BSI-Standard 200–4 bietet die Anleitung, wie zeitkritische Geschäftsprozesse gegen Ausfälle abgesichert werden können.[260] Für die Geschäftsprozesse, die zur Gewährleistung der erforderlichen Kommunikationstechnik (z.B. Alarmierung, Kommunikation im Stab, Nutzung der

[254] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 36; BMI: Leitfaden Krisenkommunikation, 25-23; BSI-Standard 200-4 Business Continuity Management, S. 141 f..
[255] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 36 f.
[256] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 36 f.; vgl. auch BMI: Leitfaden Krisenkommunikation, S. 25 ff..
[257] Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 105 f..
[258] BSI-Standard 200 - 4 Business Continuity Management, S. 140; BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 10.
[259] BSI-Standard 200-4 Business Continuity Management, S. 140; BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 10.
[260] BSI-Standard 200-4 Business Continuity Management, S. 14 u. S. 19.

Kommunikationskanäle und Medienformate zur Erreichung der relevanten Zielgruppen) notwendig sind, sollten daher im Vorhinein Kontinuitätsstrategien i.S.d. BSI Standards entwickelt, entsprechende Vorkehrungen getroffen und die Ergebnisse in einem Notfallhandbuch, ggf. im Krisenkommunikationsplan festgehalten werden.[261] Ob die entwickelten Strategien und getroffenen Maßnahmen dazu führen, dass im Ernstfall die Kommunikation weitestgehend reibungslos erfolgt, sollte regelmäßig im Rahmen von Übungen und Tests überprüft werden.[262]

Übungen sollten nicht nur in Bezug auf die Kommunikationswege stattfinden. Um zu gewährleisten, dass das praktische Zusammenspiel der Akteure im Notfall effektiv und effizient funktioniert, sollte die Organisation ihren Krisenkommunikationsprozess regelmäßig proben und trainieren.[263] Darüber hinaus sollten die in der Krisenkommunikation eingesetzten Personen entsprechen geschult (z.B. Medientraining, Sprechertraining, Umgang mit investigativen Journalisten) werden.[264]

4. Zwischenfazit

Nach dem Einleitungskapitel wurde in den Kapiteln 2 und 3, auf Basis einer systematischen Literaturrecherche, eine Einordnung der Krisenkommunikation in die relevanten Managementsysteme vorgenommen und diese näher betrachtet. Darüber hinaus wurde aufgearbeitet und dargestellt, welche Gesichtspunkte die Literatur im Zusammenhang mit Krisenkommunikation für beachtenswert hält. Daneben wurde in diesem Kontext bereits ein Bezug zum Notfallszenario „Ransomware–Angriff auf eine kleinere Kommunalverwaltung“ hergestellt. Bevor im nächsten Kapitel der empirische Teil der Master–Thesis folgt, wird in diesem Abschnitt ein Zwischenfazit gezogen. Dabei wird die Frage beantwortet, welche wesentlichen Erkenntnisse für das Gelingen einer erfolgreichen Krisenkommunikation anhand der bis zu dieser Stelle erfolgten Abhandlungen gezogen werden können.

---

[261] BSI-Standard 200-4 Business Continuity Management, S. 222 ff.; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 36 f.; BMI: Leitfaden Krisenkommunikation, S. 25 ff..
[262] BSI-Standard 200-4 Business Continuity Management, S. 253.
[263] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 37; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 96 ff.
[264] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 288 ff.; Latsch, J. (2019): Bürgermeister und Krisenkommunikation, S. 97 f.; BMI: Leitfaden Krisenkommunikation, S. 20.

Es hat sich herauskristallisiert, dass Krisenkommunikation innerhalb der Behörde nicht erst in der Krise selbst eine Rolle spielen darf. Erfolgreiche Krisenkommunikation bedarf einer gewissen Vorarbeit und Vorsorge. Die frühzeitige Planung und Vorbereitung auf den Krisenfall betreffen dabei nicht nur die Kommunikation im engeren Sinne, sondern auch organisatorische und technische Aspekte.

Weiterhin wurde festgestellt, dass im Falle eines Ransomware–Angriffes die technischen Einschränkungen eine besondere Rolle in Bezug auf die Krisenkommunikation einnehmen. In diesem Zusammenhang wurde deutlich, dass das (Krisen-) Kommunikationsmanagement nicht losgelöst betrachtet werden kann. Begleitend müssen auch die Anforderungen an die Geschäftsfortführung kritischer Prozesse berücksichtigt und die sich stellenden Aufgaben im Rahmen eines Business Continuity Managements abgearbeitet werden. Insofern konnten die enge Verzahnung und die Überschneidung zwischen dem Krisenmanagement und dem Business Continuity Management konkret aufgezeigt werden.

In der Krisenkommunikation stellen Vertrauen in die Behörde und Glaubwürdigkeit der Behörde die wesentlichen Aspekte dar. Vertrauen und Glaubwürdigkeit muss jedoch im Vorhinein und nicht erst in der Krise aufgebaut werden. Dessen ungeachtet wurde aufzeigt, dass die Beachtung verschiedener Prinzipien maßgeblich zum Erfolg der Krisenkommunikation beitragen, auch wenn im Einzelfall eine Abweichung erforderlich werden kann.

Die Identifikation der relevanten Interessengruppen ist für die Krisenkommunikation wesentlich. Die für das Notfallszenario „Ransomware–Angriff“ für die Verwaltung wichtigen Gruppen, wurden beleuchtet und deren Ansprüche und Anforderungen erläutert. Es lassen sich für den betreffenden Ernstfall spezielle Zielgruppen bzw. Stakeholder ausmachen. Die häufig vernachlässigten, eigenen Beschäftigten sollten ausreichend informiert und im Idealfall aufkommende Verunsicherung genommen werden. Die Medienarbeit kann eine große Herausforderung darstellen und einige Ressourcen binden. Für die Wahrnehmung der Krise und der Krisenbewältigung seitens der Verwaltung in der breiten Bevölkerung ist die Medienberichterstattung von übergeordneter Bedeutung.

Es wurde dargelegt, dass eine Kommunalverwaltung mit der eigenen Website, einem Bürgertelefon, ggf. mit einem Amtsblatt, Social-Media oder dem Intranet, durchaus über eigene, selbst gesteuerte und für die relevanten Zielgruppen bekannte Kommunikationskanäle verfügt, die entsprechend den Krisenkommunikationsgrundsätzen bespielt werden sollten.

Um in der Krise erfolgreich kommunizieren zu können, sind ausreichend personelle Ressourcen und Kompetenzen erforderlich. Dieses Erfordernis besteht nicht erst beim Auftreten des Ernstfalles, sondern bereits in der Vorbereitungsphase. Im Ernstfall selbst sind die Herausforderungen und Aufgaben mit der Regelbesetzung der Pressestellen häufig nicht zu bewältigen. Entsprechende Vorkehrungen müssen daher getroffen werden.

5. Interviews mit Expertinnen und Experten zur Erhebung von Schlüsselfaktoren für eine erfolgreiche Krisenkommunikation

In den vorangegangenen Kapiteln wurde, basierend auf einer systematischen Literaturrecherche, der Stand der Forschung in Bezug auf Krisenkommunikation dargestellt. Die für eine erfolgreiche Krisenkommunikation zu berücksichtigenden Aspekte wurden in diesem Zusammenhang herausgearbeitet. Darüber hinaus fand eine Einordnung der Krisenkommunikation in das Feld des Krisenmanagements statt. Die besonderen Herausforderungen und typischen Eigenheiten, die eine Ransomware–Attacke mit sich bringen kann, wurden aufgezeigt.

Als Zwischenfazit kann festgestellt werden, dass die Anforderungen an eine Kommune in Bezug auf die Krisenkommunikation, im nicht unrealistischen Szenario „Ransomware–Attacke“, vielfältig und hoch sind.[265] Zu klären ist nun, wie einer kleineren Kommune in vorbezeichneter Situation eine erfolgreiche Krisenkommunikation in der Praxis gelingen kann.

[265] Vgl. Zwischenfazit in Kapitel 4.

Um Aufschluss über die besonderen Herausforderungen kleinerer Kommunalverwaltungen zu erlangen und Schlüsselfaktoren zu ermitteln, wurden Leitfadeninterviews mit Expertinnen und Experten geführt. Im Anschluss daran fand eine Auswertung der Interviews anhand einer qualitativen Inhaltsanalyse statt. Die Erwägungsgründe für die ausgewählte methodische Vorgehensweise und die Vorstellung des Forschungsdesigns werden im Folgenden vorgestellt.

5.1 Forschungsmethode

Untersuchungen, die einen speziellen Ausschnitt der sozialen Welt beobachten, um auf Basis dieser Beobachtungen zur Weiterentwicklung oder Überprüfung von Theorien beizutragen, werden als empirische Sozialforschung bezeichnet.[266] Der Forschungsprozess umfasst verschiedene Phasen von der Auswahl des Forschungsproblems bis hin zur Publikation der Ergebnisse.[267] Im Allgemeinen wird bei der empirischen Sozialforschung zwischen quantitativer und qualitativer Sozialforschung differenziert.[268] Dabei stellt der wichtigste Unterschied der beiden Vorgehensweisen die Art und Weise dar, wie man mit empirischen Untersuchungen zu kausalen Erklärungen gelangt.[269] Eng damit verbunden ist der Einsatz der verschiedenen Methoden: Will man von statistischen Zusammenhängen auf Kausalzusammenhänge schließen, erfolgt der Einsatz einer quantitativen Methode. Wird die Erklärung sozialer Sachverhalte über die Suche nach Kausalmechanismen und die Bestimmung ihres Geltungsbereiches angestrebt, wird eine qualitative Methode gewählt.[270]

Zur Beantwortung der Forschungsfrage wurde eine qualitative Untersuchung in Form von Leitfadeninterviews mit Expertinnen und Experten durchgeführt. Der Forschungsstand in Bezug auf Krisenkommunikation im Allgemeinen ist, wie aus den vorangegangenen Kapiteln deutlich wurde, weitreichend und liefert wertvolle

[266] Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, S. 24; Schnell, R.; Hill, P. B.; Esser, E. (2023): Methoden der empirischen Sozialforschung, S. 2.
[267] Schnell, R.; Hill, P. B.; Esser, E. (2023): Methoden der empirischen Sozialforschung, S. 3.
[268] Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, S. 24.
[269] Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, S. 28.
[270] Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, S. 28.

Erkenntnisse. Die vorhandenen Quellen geben darüber hinaus auch praxisorientierten Input, wie eine erfolgreiche Krisenkommunikation im Ernstfall realisiert werden kann. Die Frage, wie eine Kommune mit nur sehr begrenzenten Ressourcen im Bereich Krisen-/ Notfallmanagement und Kommunikation die theoretischen Erkenntnisse und Empfehlungen im Falle eines Ransomware-Angriffes erfolgreich umsetzt, wird bislang nicht beantwortet. Vielmehr stehen kleinere Kommunen vor der Herausforderung, trotz ihrer eingeschränkten Leistungsfähigkeit, sich für das „Worst-Case“ Szenario eigenständig vorzubereiten und im Ernstfall „lehrbuchmäßig“ kommunizieren zu müssen.

Durch die vorliegende Masterarbeit und die Beantwortung der Forschungsfrage soll diese Lücke geschlossen und für die Kommunalverwaltungen praxistaugliche Handlungsempfehlungen generiert werden.

Die Anzahl der erfolgreich durchgeführten Ransomware-Angriffe auf kleinere Kommunen in Baden–Württemberg ist bisher übersichtlich. Die Forschungsfrage bringt daher die Herausforderung mit sich, dass deren Beantwortung auf Basis einer überschaubaren Anzahl an Fällen erfolgen muss. Es wird in Folge dessen eine Mechanismen orientierte Erklärungsstrategie auf Basis einer rekonstruierenden Untersuchung angestrebt. Im Rahmen der Untersuchung werden Einzelfälle weitestgehend durchleuchtet, das heißt die Situation und Prozesse rekonstruiert. Sämtliche Informationen werden zusammengetragen, um die Zusammenhänge verstehen zu können.[271] Aufgrund der limitierten Anzahl an Einzelfällen würden Quantifizierungen nicht zu belastbaren Ergebnissen führen. Eine relationsorientierte Erklärungsstrategie wird infolgedessen nicht verfolgt.

Als Datenerhebungsmethode werden Leitfadeninterviews mit Expertinnen und Experten durchgeführt. Die Vorgehensweise verspricht, bedingt durch die offene Gesprächsführung, die Möglichkeit des gezielten Nachfragens und der prognostizierten Ausführlichkeit der Antworten, bessere Erkenntnisse über die Zusammenhänge und Kausalitäten zu erlangen. Durch das Vorgehen können substantielle und um-

[271] Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, S. 37.

fassende Informationen, sowie persönliche Meinungen und Haltungen der Befragten erhoben werden. Auf dieser Grundlage werden die in den nächsten Kapiteln dargestellten Erkenntnisse gewonnen und Handlungsempfehlungen abgeleitet. Eine Datenerhebung auf Basis einer standardisierten Befragung wird vor den dargelegten Hintergründen nicht als zielführend erachtet.[272] Die persönlichen Erfahrungen und Einschätzungen der Expertinnen und Experten werden für die Beantwortung der Forschungsfrage als sehr wichtig eingestuft, um die Komplexität und die Zusammenhänge im gesamten zu erfassen und nicht isoliert Fakten zu erheben.[273] Durch die Modalität eines leitfadengestützten Interviews sind die Befragten nicht an vorgegebene Antwortmöglichkeiten und Kategorien gebunden und können freier und vollständig Rede und Antwort stehen. Die Orientierung an einem Leitfaden sorgt für die Abhandlung aller forschungsrelevanten Themen, ohne dass die Reihenfolge eines Fragenkataloges eingehalten werden muss. Darüber hinaus wird eine Vergleichbarkeit der Interviewergebnisse gewährleistet.[274] Leitfadeninterviews unterliegen höheren Anforderungen an eine systematische und theoriegeleitete Vorgehensweise als nichtstandardisierte Interviews ohne Leitfaden.[275]

Nicht von der Hand zu weisen ist die Tatsache, dass die qualitative Sozialforschung in Form von Leitfadeninterviews auch Schwächen mit sich bringt. Die Reaktivität im Kontext eines Interviews kann die Messergebnisse verändern. Inzwischen konnten unterschiedlichste Formen der Antwortverzerrung im Interview, sog. „Response Errors“ nachgewiesen werden.[276] Den Reaktivitätseffekten kann jedoch durch eine sorgfältige Vorbereitung und eine empirische Absicherung entgegengewirkt werden. Nicht zuletzt müssen den methodologischen Prinzipien sozialwissenschaftlicher Forschung Beachtung geschenkt werden, um nutzbare Ergebnisse zu erarbeiten.[277] Insbesondere seien in diesem Zusammenhang die von Mayring abgeleiteten

[272] Vgl. Schnell, R.; Hill, P. B.; Esser, E. (2023): Methoden der empirischen Sozialforschung, S. 356.
[273] Vgl. Mayring, P. (2022): Qualitative Inhaltsanalyse, S. 19.
[274] Schnell, R.; Hill, P. B.; Esser, E. (2023): Methoden der empirischen Sozialforschung, S. 356.
[275] Kaiser, R. (2021): Qualitative Experteninterviews, S. 36; Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, S. 41.
[276] Schnell, R.; Hill, P. B.; Esser, E. (2023): Methoden der empirischen Sozialforschung, S. 324.
[277] Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, S. 29 ff.; Schnell, R.; Hill, P. B.; Esser, E. (2023): Methoden der empirischen Sozialforschung, S. 328.

Gütekriterien qualitativer Sozialforschung[278] genannt. Vor diesem Hintergrund ist den Interviews eine intensive Vorbereitung vorausgegangen. Vor der Erstellung des Leitfadens wurden die potenziellen Fehlerquellen eruiert und diesen soweit möglich im Zuge der Ausarbeitung des Leifadens entgegengewirkt.

Ungeachtet wissenschaftstheoretischer und methodologischer Problemfelder sind auch forschungsethische Aspekte zu berücksichtigen. Menschen, die in einem Forschungsprojekt einbezogen werden, darf daraus kein Schaden entstehen.[279] Im Zusammenhang mit der Befragung von Expertinnen und Experten sind personenbezogene Daten zu schützen, hat eine informierte Zustimmung zur Teilnahme zu erfolgen, muss die Vertraulichkeit gewahrt bleiben und müssen die Grundsätze der Integrität und Objektivität eingehalten werden.[280] Das Prinzip der informierten Einwilligung stellt das wichtigste Prinzip für den Umgang mit Untersuchten dar.[281] Die konkreten Inhalte des Prinzipes ergeben sich insbesondere aus § 2 des Ethik-Kodex der deutschen Gesellschaft für Soziologie.[282] Um vorgenannten Aspekten der Forschungsethik bestmöglich Rechnung zu tragen, werden die Interviewpartnerinnen und Interviewpartner frühzeitig über das Forschungsprojekt aufgeklärt. Mit einer Einwilligungserklärung sowie einer entsprechende Datenschutzerläuterung kommen weitere Instrumente zum Einsatz, um die Untersuchten zu schützen. Die jeweiligen Inhalte werden im Forschungsvorhaben beachtet bzw. umgesetzt.

Die Auswertung der Interviews findet bei dem Forschungsprojekt anhand einer qualitativen Inhaltsanalyse statt. Die Analyse des gewonnenen Datenmaterials erfolgt bei der qualitativen Inhaltsanalyse systematisch und läuft nach expliziten Regeln ab. Dadurch wird gewährleistet, dass Dritte die Analyse verstehen, nachvollziehen und überprüfen können.[283] Darüber hinaus zeichnet sich die Inhaltsanalyse

[278] Mayring, P. (2023): Einführung in die qualitative Sozialforschung, S. 123 ff..
[279] Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, S. 50.
[280] Kaiser, R. (2021): Qualitative Experteninterviews, S. 56 f..
[281] Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, S. 52.
[282] Deutsche Gesellschaft für Soziologie, Ethik-Kodex der Deutschen Gesellschaft für Soziologie (DGS) und des Berufsverbandes Deutscher Soziologinnen und Soziologen (BDS): Ethikkodex, https://soziologie.de/dgs/ethik/ethik-kodex (16.11.2024).
[283] Mayring, P. (2022): Qualitative Inhaltsanalyse, S. 13.

durch ein theoriegeleitetes Vorgehen aus und verfolgt das Ziel, konkrete Rückschlüsse auf bestimmte Aspekte der Kommunikation zu ziehen.[284] In Kapitel 5.4 wird die konkrete Vorgehensweise zu diesem Forschungsprojekt detaillierter erläutert.

5.2 Auswahl und Beschreibung der Expertinnen und Experten

Qualitative Interviews mit Expertinnen und Experten zielen primär darauf ab, zunächst den Fall auf Basis einer systematischen Analyse zu verstehen. Unmittelbar Ergebnisse zu gewinnen, die über den Einzelfall hinaus generalisierbar sind, steht dabei nicht im Mittelpunkt.[285] Der Anforderung, eine repräsentative Stichprobe oder alle vorhandenen Expertinnen und Experten zu befragen, muss daher nicht entsprochen werden. Allerdings ist die Auswahl der Expertinnen und Experten, die sich nach rein inhaltlichen Erwägungen richtet, ein sehr wichtiger Gesichtspunkt des Forschungsdesigns und bedarf daher der Begründung.[286] Im folgenden Abschnitt wird daher dargestellt, anhand welcher Kriterien die Auswahl der Expertinnen und Experten erfolgt und erläutert, wie sich der konkrete Expertinnen- und Expertenkreis herauskristallisiert und schließlich gebildet hat.

Zentrale Fragestellungen im Hinblick auf die Auswahl von Expertinnen und Experten sind zunächst nach Gläser u. Laudel:[287] Wer ist im Besitz der relevanten Informationen? Wer (aus diesem Personenkreis) ist in der Lage, genaue Informationen zu geben? Wer ist auch bereit die Informationen auch zu geben? Darüber hinaus stellt sich auch die Frage der Verfügbarkeit einer potenziellen Informationsquelle.

Auf Basis dieser allgemeinen Fragestellungen wird ein Auswahlkatalog im Kontext der zu beantwortenden Forschungsfrage erstellt, nach dem im Vorhinein zusätzliche Qualitätskriterien festgelegt werden:

---

[284] Mayring, P. (2022): Qualitative Inhaltsanalyse, S. 13.
[285] Kaiser, R. (2021): Qualitative Experteninterviews, S. 84.
[286] Kaiser, R. (2021): Qualitative Experteninterviews, S. 84 f..
[287] Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, S. 117; vgl. auch Kaiser, R. (2021): Qualitative Experteninterviews, S. 85.

Q1: Kenntnisse und Erfahrungen in Bezug auf Krisenkommunikation

Essentielle Anforderung an eine Expertin bzw. einen Experten stellt der Aspekt dar, dass die zu interviewende Person selbst zumindest eingeschränkte Kenntnisse in Bezug auf Krisen- bzw. Notfallkommunikation besitzt und über Erfahrung in dem Bereich verfügt. Eine einmalige maßgebliche Beteiligung im Zuge der Krisenkommunikation in einem konkreten Krisenszenario wird als ausreichend betrachtet.

Q2: Erfahrung mit der Bewältigung einer Ransomware-Attacke

Als weiteres Qualitätsmerkmal wird das Vorliegen von Erfahrung mit der Bewältigung einer Ransomware-Attacke definiert. Potenzielle Expertinnen und Experten müssen dabei insoweit unmittelbar betroffen gewesen sein, als dass sie zumindest in der Bewältigung der krisenhaften Lage mitgewirkt haben.

Q3: Einschätzungsvermögen über die vorhandenen Rahmenbedingungen innerhalb von Kommunalverwaltungen bis ca. 20.000 Einwohnerinnen und Einwohnern

Die zu interviewende Person muss in der Lage sein, die grundlegenden Rahmenbedingungen, die in einer kleineren Kommunalverwaltung in Bezug auf Aufbau- und Ablauforganisation, Ressourcen und Kompetenzen vorliegen, einschätzen zu können.

Es wird zur Beantwortung der Forschungsfrage als weniger zielführend eingeschätzt, Expertinnen und Experten zu befragen, die nur einzelne der oben genannten Qualitätskriterien erfüllen. Die Erhebung könnte zwar so ausgestaltet werden, dass Expertinnen und Experten je nach Erfüllung der Qualitätskriterien individualisierte Fragen gestellt bekommen, so dass im Nachgang durch ein Zusammenfügen der Antworten ein Gesamtbild erhalten wird. Allerdings bestehen Zweifel daran, dass durch diese Vorgehensweise realistische und qualitativ hochwertige Erkenntnisse gewonnen werden können. Infolgedessen sehen die Modalitäten für das Erhebungsverfahren vor, dass alle Expertinnen und Experten die Qualitätskriterien kumulativ erfüllen. Die Anzahl potenzieller Interviewpartnerinnen und Interviewpartner verringert sich dadurch erheblich. Aufgrund der eingeschränkten Anzahl potenzieller

Informantinnen und Informanten kann nicht gewährleistet werden, dass alle Interviewpartnerinnen und Interviewpartner gleichermaßen alle Kriterien erfüllen. Dadurch ergibt sich zwar einerseits ein Qualitätsverlust, anderseits führt dies zu einem eingeschränkt heterogenen Informantinnen- und Informantenkreis.

Aus den vorgenannten Auswahlkriterien resultiert, dass potenzielle Expertinnen und Experten in Kommunalverwaltungen tätig sind bzw. waren oder in Organisationen, die sehr eng mit Kommunalverwaltungen zusammenarbeiten. Darüber hinaus könnten auch weitere Personen als Expertinnen und Experten geeignet sein, die aufgrund ihres individuellen Wissens und Erfahrungen die geforderten Qualitätskriterien erfüllen.

Näher geprüft wurde daher, ob potenzielle Interviewpartnerinnen und Interviewpartner bei der Polizei, der CSBW, der Komm.ONE und bei Kommunalverwaltungen zur Datenerhebung geeignet sind.

Zunächst werden Personen als geeignete Interviewpartnerinnen und Interviewpartner eingestuft, die in kleineren Kommunalverwaltungen tätig sind und im Rahmen einer Ransomware Attacke bei der Notfallbewältigung mitgewirkt haben und darüber hinaus Q 1 erfüllen.

In Erwägung gezogen wurden weiterhin Expertinnen und Experten, die bei der Polizei im Kontext von Cyberangriffen tätig sind. Einzelne Auswahlkriterien (insbesondere Q3) werden jedoch nicht ausreichend erfüllt. Die Polizei, als Strafverfolgungsbehörde, ist primär auf die Erledigung der eigenen Aufgabenstellungen fokussiert. Eine intensive Unterstützung der Kommunen und eine enge Zusammenarbeit im Zuge der Krisen- bzw. Notfallbewältigung ist grundsätzlich nicht vorgesehen.

Die im Jahr 2022 gegründete CSBW hat inzwischen verschiedene Kommunalverwaltungen im Rahmen der Notfallbewältigung im Zusammenhang mit Ransomware-Angriffen aktiv unterstützt. Die Unterstützung ist dabei nicht auf die Bewältigung der technischen Schwierigkeiten beschränkt. Vielmehr kann sich eine Zusammenarbeit auch auf weitere Aspekte des Krisenmanagements, wie zum Beispiel

Krisenkommunikation, erstrecken.[288] Die CSBW besitzt durch das CSG auch den gesetzlichen Auftrag zur Unterstützung der kommunalen Verwaltungen in der Cybersicherheit.[289] Die Mitarbeiterinnen und Mitarbeiter des Vorfallmanagements sind daher grundsätzlich als Informantinnen und Informanten geeignet.

Als Anstalt des öffentlichen Rechts in gemeinsamer Trägerschaft des Landes und der Kommunen in Baden-Württemberg berät und begleitet die Komm.ONE ihre Kundinnen und Kunden auf dem Weg in eine zunehmend technologiebasierte Zukunft. Sie beschafft, entwickelt und betreibt Verfahren der automatisierten Datenverarbeitung für kommunale Körperschaften, deren Zusammenschlüsse und deren Unternehmen im Land Baden-Württemberg im Rahmen ihres gesetzlichen Auftrags. Träger der Komm.ONE sind die Kommunen mit 88 Prozent und das Land Baden-Württemberg mit 12 Prozent.[290] Die Komm.ONE unterstützt die Kommunen dabei, Aufgaben für Bürger und Gesellschaft zu erfüllen. In Folge des vorbezeichneten Sachverhaltes findet flächendeckend eine enge Zusammenarbeit der baden–württembergischen Kommunen mit der Komm.ONE in Bezug auf elektronische Datenverarbeitung statt.[291] Die enge Kooperation und zum Teil auch die Abhängigkeit von den Leistungen der Komm.ONE führt dazu, dass auch im Notfallszenario „Ransomware-Angriff“ die Komm.ONE stark im Rahmen der Bewältigung der krisenhaften Lage involviert ist. Auch in Bezug auf die (Krisen-) Kommunikation dürfte die Komm.ONE im Ernstfall zumindest beteiligt sein. Mitarbeiterinnen und Mitarbeiter der Komm.ONE, die im Notfallszenario „Ransomware-Angriff“ gemeinsam mit den betroffenen Kommunen bei der Lagebewältigung agieren und idealerweise im Zusammenhang mit der Krisenkommunikation tätig sind, erfüllen grundsätzlich die Qualitätskriterien.

---

[288] CSBW: Unterstützung und Beratung: Vorfallmanagement und Krisenreaktion, https://www.cybersicherheit-bw.de/unterstuetzung-und-beratung-vorfallmanagement-und-krisenreaktion (16.11.2024).

[289] Vgl. Gesetz für die Cybersicherheit in Baden–Württemberg, § 3.

[290] Komm.ONE: Aufgabenspektrum.

[291] Vgl. hierzu ausführlich Komm.ONE: Jubiläumsmagazin - 50 Jahre digitale Partnerschaft, https://www.komm.one/site/Komm.ONE_Internet/get/documents_E1797062213/Komm.ONE/Komm.ONE_Internet_Objekte/Sonstiges/FlipBook/index.html (16.11.2024).

Neben den vorgenannten potenziellen Personengruppen, die die Qualitätskriterien erfüllen, könnten grundsätzlich weitere Personen als Expertinnen oder Experten in Frage kommen, wenn sie die Auswahlkriterien erfüllen. Dies könnte aufgrund individueller Kenntnisse und Erfahrungen der Fall sein, z.B. bei speziellen Beratern oder Professoren.

Auf Basis der dargelegten Modalitäten und der Feststellung potenziell geeigneter Expertinnen- und Expertengruppen fand eine Akquise statt. Um aussagekräftige Erkenntnisse zu gewinnen und um Informationen aus möglichst vielen Perspektiven zu erhalten, wurde seitens des Verfassers dieser Arbeit großen Wert daraufgelegt, Daten nicht nur bei betroffenen Kommunen selbst zu erheben, sondern auch bei Personen von externen Organisationen, wie z.B. der CSBW oder der Komm.ONE.

Die Akquisition von Expertinnen und Experten erfolgte zunächst telefonisch. Im Rahmen des Erstgespräches wurden zur Qualitätssicherung die Qualitätskriterien abgefragt. Bei positiver Prüfung und signalisierter Teilnahmebereitschaft seitens des Gesprächspartners, wurde ein Interviewtermin vereinbart.

Kennung	**Organisation**	**Größenklasse (Einwohner)**	**Tätigkeitsfeld / Funktion**
E1IANEB1	Kommune	2 bis 11 Tsd.	Bürgermeister
E2IANEB2	Kommune	2 bis 11 Tsd.	Kommunikation
E3IEDLE1	Kommune	2 bis 11 Tsd.	Kommunikation
E4IDNEG1	Kommune	12 bis 21 Tsd.	Kommunikation
E5IBMIE1	Kommune	12 bis 21 Tsd.	Kommunikation
E6IFG1	Externe Organisation		Kommunikation
E7ICE1	Externe Organisation		Kommunikation

Abbildung 5: Interviewpartnerinnen und Interviewpartner (eigene Darstellung)

5.3 Leitfragen als Grundlage für die Interviews

Im Kapitel 5.1 wurde bereits erläutert, dass Interviews mit Expertinnen und Experten zur Gewinnung von Informationen durchgeführt werden. Weiterhin wurde ausgeführt, dass die Befragungen leitfadengestützt erfolgen. Der Leitfaden besitzt dabei verschiedene Funktionen. Er stellt die Operationalisierung von abstrakten Leitfragen in Interviewfragen dar. Durch das Übersetzen kann die interviewte Person an ihren Alltag anknüpfen. Aus den Antworten können schließlich die Informationen gewonnen werden, die zur Beantwortung der Forschungsfrage dienen.[292] Der Leitfaden gibt dem Interviewer, aber auch dem Interviewten, eine grobe Struktur vor und sorgt dafür, dass die einzelnen Interviews vergleichbar sind. Er sichert damit ein gewisses Qualitätsniveau.[293] Der Interviewleitfaden wurde nach Themenkomplexe gegliedert, die einer für die Expertinnen und Experten nachvollziehbaren Logik folgen. Insbesondere wurde sich dabei an den aus der Literaturrecherche resultierenden Themenkomplexen orientiert. Darüber hinaus wurde weitestgehend der Empfehlung von Kaiser gefolgt, dass sich die Themen vom Allgemeinen dem Speziellen nähern.[294] Damit soll eine langsame Annäherung an zum Teil herausfordernde Fragestellungen erreicht werden und dem Interviewpartner ein „Aufwärmen“ ermöglichen. Darüber hinaus wird durch die behutsame Vorgehensweise das Ziel verfolgt, dass die Informanten möglichst ausführlich und ehrlich antworten. Insgesamt wurden Interviewfragen formuliert, die bewusst weitestgehend offengehalten sind, um den interviewten Personen die Möglichkeit einzuräumen, frei und unvoreingenommen ihre Erfahrungen, Erlebnisse und Eindrücke zu schildern. Im Bedarfsfall besteht durch die Fragenkonstruktion dennoch die Option, spezifisch nachzufragen. Durch diese Konzeption ist ein fortwährender Redefluss gewährleistet und eine potenzielle Unterbrechung des Gesprächs wird vermieden. Im Interviewleitfaden sind bewusst Meinungsfragen eingebettet, da die individuelle Einschätzung und Meinung der Informanten zum Erkenntnisgewinn erforderlich sind.

---

[292] Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, S. 142; Kaiser, R. (2021): Qualitative Experteninterviews, S. 68 f..

[293] Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, S. 143; Kaiser, R. (2021): Qualitative Experteninterviews, S. 64 f..

[294] Kaiser, R. (2021): Qualitative Experteninterviews, S. 65.

Insgesamt wurde großen Wert auf die Klarheit und Verständlichkeit der jeweiligen Fragestellungen gelegt.

5.4 Analyse der Interviews

Die nach den durchgeführten Interviews vorliegenden Aufnahmen wurden schließlich transkribiert. Die Transkription kann anhand unterschiedlicher Regeln erfolgen. Für welche Transkriptionsform sich der Forschende entscheidet, wird anhand von Forschungsmethodik, Erkenntniserwartung und darüber hinaus aus forschungspragmatischen Gründen getroffen.[295] Vor diesem Hintergrund wird im vorliegenden Forschungsprojekt auf ein Transkriptionssystem zurückgegriffen, dessen Augenmerk auf den semantisch-inhaltlichem Aspekt der Transkription liegt. In der Folge werden die Transkriptionsregeln von Dresing und Pehl angewendet.[296] Es wird wörtlich transkribiert. Wortschleifungen werden an das Schriftdeutsch angenähert. Dialekte werden möglichst wortgenau ins Hochdeutsche übersetzt. Umgangssprachliche Partikeln werden transkribiert. Stottern wird geglättet bzw. ausgelassen, abgebrochene Wörter werden ignoriert. Wortdopplungen werden nur erfasst, wenn sie als Stilmittel zur Betonung genutzt werden. Halbsätze, denen die Vollendung fehlt, werden mit dem Abbruchzeichen „/“ gekennzeichnet. Interpunktion wird zugunsten der Lesbarkeit geglättet. Rezeptionssignale, die den Redefluss der anderen Person nicht unterbrechen, werden nicht transkribiert. Pausen ab ca. 3 Sekunden werden durch (…) markiert. Besonders betonte Wörter oder Äußerungen werden durch Versalien (z.B. SEHR großen Hunger) gekennzeichnet. Jeder Sprecherbtrag erhält eigene Absätze. Zwischen den Sprechern gibt es eine freie, leere Zeile. Emotionale nonverbale Äußerungen der befragten Person und des Interviewers, welche die Aussage unterstützen oder verdeutlichen (z.B. lachen oder seufzen), werden beim Einsatz in Klammern notiert. Unverständliche Wörter werden mit „(unv.)“ gekennzeichnet. Die interviewende Person wird durch ein „I“, die befragte Person durch ein „B“ gekennzeichnet.

[295] Dresing, T.; Pehl, T. (2018): Praxisbuch Interview, Transkription & Analyse, S. 19; Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, S. 193.
[296] Dresing, T.; Pehl, T. (2018): Praxisbuch Interview, Transkription & Analyse, S. 21 f..

Im weiteren Verlauf der empirischen Erhebung erfolgte die Auswertung der Daten aus den Interviews. Dabei wurde auf die qualitative Inhaltsanalyse nach Mayring zurückgegriffen. Die Stärke dieses Interpretationsverfahrens liegt darin, dass die Analyse in einzelne Schritte aufgeteilt wird, die im Vorhinein festgelegt werden. Infolgedessen wird sie für Dritte nachvollziehbar und intersubjektiv überprüfbar.[297] Ein wichtiges Element der qualitativen Inhaltsanalyse ist das Definieren von Kategorien. Das Kategoriensystem ist das bedeutendste Instrument der Analyse. Es führt ebenso wie die Zerlegung der Analyse in einzelne Schritte zu einer Nachvollziehbarkeit des Vorgehens für andere. Im Mittelpunkt stehen bei der qualitativen Inhaltsanalyse die Konstruktion und Begründung der Kategorien.[298] Kategorien können über einen deduktiven oder induktiven Ansatz gebildet werden. Deduktiv erfolgt die Kategoriendefinition, wenn aus z.B. Voruntersuchungen oder dem aktuellen Stand der Forschung die Kategorien in einem Operationalisierungsprozess vorab im Hinblick auf das noch auszuwertende Material gebildet werden. Beim induktiven Ansatz werden die Kategorien nicht vorab festgelegt, sondern sie ergeben sich aus der Auswertung des Materials.[299] In dem vorliegenden Forschungsprojekt wird der induktive Ansatz verfolgt, auch wenn sich bereits durch die Literaturrecherche einzelne Kategorisierungen andeuteten. Bei dem explorativen Forschungsvorhaben wurde der Interviewleitfaden bewusst sehr offenen gestaltet, um möglichste vielfältige Rückmeldungen zuzulassen. Der induktive, zunächst ergebnisoffene Ansatz passt besser zu dem explorativen Gesamtkonzept und verspricht die fruchtbarere Herangehensweise zu sein. Die konkreten Kategoriedefinitionen erfolgten sukzessive im Rahmen der Durcharbeitung des Materials. Ebenso wurde das Abstraktionsniveau der Kategorien erst bei der detaillierten Sichtung der Interviewtexte festgelegt. Als Kodiereinheiten gelten klare bedeutungstragende Elemente im Text. Das gesamte Material in Form von sechs transkribierten Interviews mit sieben Expertinnen und Experten, stellt die Auswertungseinheit dar.

[297] Mayring, P. (2022): Qualitative Inhaltsanalyse, S. 60.
[298] Mayring, P. (2022): Qualitative Inhaltsanalyse, S. 50.
[299] Mayring, P. (2022): Qualitative Inhaltsanalyse, S. 84.

6. Ergebnisse der qualitativen Befragung

Die transkribierten Interviews wurden entsprechend der in Kapitel 5.4 dargelegten Vorgehensweise analysiert. Resultierend aus diesem Bearbeitungsprozess haben sich fünf Hauptkategorien mit insgesamt 12 Unterkategorien herauskristallisiert.

Hauptkategorie	Unterkategorie
Aufbauorganisation u. Zusammenarbeit in der Krise	Der Krisenstab als Basis
	Einbindung aller relevanten Akteure
	Klare Aufgaben und Rollenverteilung
Kommunikationsverhalten u. Kommunikationsfähigkeit	Proaktive und transparente Kommunikation
	Bedeutung von Kompetenzen und Know-How
Erreichen der wichtigsten Zielgruppen	Kommunikation mit den Mitarbeitenden
	Nutzung vorhandener Kommunikationskanäle
	Website als zentraler Kommunikationskanal nach außen
Vorbereitung auf die Krise	Funktionstüchtigkeit der Kommunikationstechnik
	Organisatorische Vorbereitung auf die Krise
Disponieren der Ressourcen	Einsatz der eigenen personellen Ressourcen
	Unterstützung durch externe Organisationen

Abbildung 6: Matrix der herausgebildeten Kategorien (eigene Darstellung)

Auf die gewonnenen Erkenntnisse und Ergebnisse wird im Folgenden näher eingegangen.

6.1 Aufbauorganisation und Zusammenarbeit in der Krise

Anhand der geführten Interviews hat sich gezeigt, dass die strukturelle Organisation der zur Krisenbewältigung eingesetzten Personen und deren Zusammenarbeit wesentliche Aspekte darstellen, um möglichst effizient und effektiv in der Krise kommunizieren zu können. Dabei haben sich drei Unterkapitel herausgebildet, die in den Abschnitten 5.1.1 bis 5.1.3 näher dargestellt werden.

6.1.1 Der Krisenstab als Basis

Die Auswertung der Interviewdaten zeigt die hohe Bedeutung der Installation eines Krisenstabes zur Krisenbewältigung auf. Die Einrichtung eines umfassenden Krisenstabs wird als bedeutungsvolle organisatorische Maßnahme betrachtet, dessen Umsetzung zum Teil auch als essenziell bezeichnet wird.[300] Bei Vorfällen bei denen zur Krisenbewältigung kein umfassender Krisenstab installiert wurde, wird dies seitens der Interviewpartnerinnen und Interviewpartner bemängelt.[301] Als Vorteil eines Krisenstabes werden direktere Kommunikation, schnellerer und umfassender Informationsaustausch sowie aufeinander abgestimmtes Arbeiten genannt.[302]

Die interviewte Person mit Kennung E3IEDLE1 antwortete auf die Frage, ob - rückblickend betrachtet - aus ihrer Sicht Sinn ergeben hätte, einen Krisenstab einzurichten:

> „Auf jeden Fall! Also Rückversicherung, schnellere Austauschwege, direktere Kommunikation wäre möglich gewesen. Weil man natürlich dann EINE Sitzung hat, bei der jeder ALLES hört und jeder ALLES vorbringen kann. So war sehr viel bilateral, man hat viel doppelt sprechen müssen.“ (…) „Also Austauschrunden, ein Krisenstab ist für mich essenziell in so einer Situation, im NACHHINEIN!“[303]

Den Äußerungen derjenigen interviewten Personen zufolge, die im Rahmen eines Krisenstabes die Situation bewältigt oder begleitet haben, lässt sich zudem entnehmen, dass die eingerichteten Krisenstäbe nicht den organisatorischen Regelungen der VwV Stabsarbeit entsprochen haben. Vielmehr wurde der Stab individuell besetzt oder auf vorhandene Gremien, wie z.B. die „Amtsleiterrunde“, als Kernbesetzung, zurückgegriffen.[304] Die interviewte Person mit Kennung E7ICE1 äußerte sich folgendermaßen zur Fragestellung wie ein Krisenstab ausgestaltet sein sollte:

---

[300] Transkription C, Z. 142-158; Transkription E, Z. 78-86; Transkription F, Z. 87-95.
[301] Transkription B, Z. 400-405; Transkription E, Z. 80-86.
[302] Transkription B, Z. 400-407; Transkription E, Z. 80-86.
[303] Transkription E, Z. 80-86.
[304] Transkription A, Z. 75-79; Transkription D, Z. 41-56.

> „Krise sticht alles andere. Und um darauf vorbereitet sein, muss jede Institution, jede Behörde, jede Kommune, sich eben auch die Frage stellen: Wie sind denn unsere Strukturen vor Ort und wie kann eine solche Organisation aussehen? Wenn das dann deckungsgleich zur Verwaltungsvorschrift ist, WUNDERBAR! Und die kann man sicherlich auch als Folie danebenlegen und sagen: Haben wir die zentralen Punkte alle erfasst? Aber ich würde da kein Paradigma daraus machen.“[305]

Im Ergebnis kann festgehalten werden, dass eine zur jeweiligen Kommune passender Krisenstab zur Krisenbewältigung einen außerordentlichen Mehrwert beiträgt.

6.1.2 Einbindung aller relevanten Akteure

Auf Basis der Interviewdaten lässt sich darlegen, dass die Einbindung aller relevanten Akteure im Zuge der Krisenbewältigung äußerst wichtig ist.[306] Die Krisenkommunikation wird als integraler Bestandteil des Krisenmanagements und damit als festes Mitglied im Krisenstab gesehen.[307] Die Einbindung der Krisenkommunikation in den Krisenstab wird als außerordentlich wichtig erachtet.[308] Erfolgt diese Einbindung nicht, wirkt sich das als Hindernis und zeitverzögernd für die Kommunikationsarbeit aus.[309] Auch die Einbindung externer Akteure, vor allem der Komm.ONE, der CSBW und der Polizei, besitzt einen hohen Stellenwert, insbesondere um in abgestimmter Weise zu agieren und zu kommunizieren.[310] Die interviewte Person mit Kennung E7ICE1 erklärt dazu beispielhaft:

> „Denn nichts ist ja schlimmer, wenn die Presse jetzt bei Ihnen anruft und bei mir anruft und unterschiedliche Auskünfte bekommt. Und dann sagt: Okay, da haben wir jetzt etwas, wo wir einhaken können.“[311]

---

[305] Transkription C, Z. 153-158.
[306] Transkription B, Z. 84-111; Transkription E, Z. 59-86; Transkription F, Z. 87-95.
[307] Transkription C, Z. 469-486; Transkription D, Z. 62-87; Transkription F, Z. 114-116.
[308] Transkription B, Z. 100-111; Transkription C, Z. 469-486; Transkription D, Z. 84-87; Transkription F, Z. 114-115.
[309] Transkription B, Z. 100-111; Transkription C, Z. 469-486; Transkription D, Z. 81-82.
[310] Transkription A, Z. 116-123; Transkription C, Z. 188-193; Transkription D, Z. 233-235.
[311] Transkription C, Z. 191-193.

Im Ergebnis zeigt sich damit, dass die Einbindung aller relevanten Akteure in den Krisenstab von einem hohen Stellenwert ist. Die externen Stakeholder dürfen dabei nicht vergessen werden.

6.1.3 Klare Aufgaben und Rollenverteilung

Um im Krisenfall strukturiert und schnell agieren zu können, auch in Bezug auf Krisenkommunikation, ist eine klare Rollen- und Aufgabenverteilungen elementar. Herrscht diesbezüglich Unklarheit, wird die Situation unmittelbar nach einem Ransomware-Angriff teilweise als ungeordnet bezeichnet oder die Krisenbewältigung als ineffizient erfahren.[312] Im Rahmen zurückliegender Notfälle, bei denen jeder wusste, worin seine Rolle liegt und welche Aufgaben er zu erfüllen hat, wird die Situation als geordnet beschrieben und auch die Zusammenarbeit als reibungslos wahrgenommen.[313] Die interviewte Person mit Kennung E4IDNEG1, bei der eine klare Rollen- und Aufgabenverteilung vorlag, äußerte sich folgendermaßen:

> „Also nach den anfänglichen ersten 20 bis 30 Minuten war es tatsächlich recht geordnet und es hat auch alles Hand in Hand funktioniert, einmal in den Ämtern und dann aber auch mit den Behörden und Komm.ONE und weitere. Es hat eigentlich alles echt reibungslos funktioniert.“[314]

Im Ernstfall auf eine klare Struktur und eine eindeutige Rollen- und Aufgabenverteilung zurückgreifen zu können, hat sich für eine effektive und effiziente Krisenbewältigung als sehr bedeutsam herausgestellt.

6.2 Kommunikationsverhalten und Kommunikationsfähigkeit

Neben den in Kapitel 5.1 genannten organisatorischen Aspekten, wurde aus den Interviews deutlich, dass das Kommunikationsverhalten in der Krise und die Kommunikationsfähigkeiten, der für die Krisenkommunikation zuständigen Personen, ein bedeutsames Element für eine erfolgreiche Krisenkommunikation darstellen. In diesem Kontext haben sich zwei Unterkapitel herausgebildet.

---

[312] Transkription B, Z. 45-82; Transkription E, Z. 40-57 u. Z. 73-76.
[313] Transkription A, Z. 46-70; Transkription C, Z. 142-148; Transkription D, Z. 29-36.
[314] Transkription D, Z. 29-32.

6.2.1 Proaktive und transparente Kommunikation

Eine negative Presseberichterstattung kann vermieden werden, wenn frühzeitig mit offenen Karten gespielt wird, der Sachverhalt faktenbasiert aufgeklärt und für Verständnis gesorgt wird. Darüber hinaus spiegeln die Interviews wider, dass durch vorbezeichnete Kommunikationsweise Rückfragen vermieden oder zumindest reduziert werden konnten.[315] Weiterhin erfährt diese Vorgehensweise positive Resonanz aus der Bevölkerung.[316] Die Rückmeldungen aus den Interviews zeigen damit, dass sich eine proaktive, offene und transparente Krisenkommunikation auszahlt. Die interviewte Person mit Kennung E5IBMIE1 gibt zusammenfassend und repräsentativ folgenden Einblick:

> (…) „also unsere Krisenkommunikation wurde wirklich GELOBT. Auch extern haben wir viele Rückmeldungen bekommen, dass es gut war, dass wir in der Krise so offen und transparent kommuniziert haben und auch so bürgerfreundlich und offen mit dem ganzen Thema umgegangen sind.“ (…) „Aber man muss wirklich sagen, dass unsere Krisenkommunikation in dem Sinne erfolgreich war, als dass wir wenig Rückfragen gestellt bekommen haben, dass wenige kritische Rückfragen auch kamen, dass kein Shitstorm entstanden ist, dass viel Verständnis, auch für die Situation, dann doch da war, gerade auch in der Bevölkerung und wir da wirklich das Medienecho auch gut lenken konnten.“[317]

6.2.2 Bedeutung von Kompetenzen und Know-How

Die Interviewpartnerinnen und Interviewpartner meldeten zurück, dass die in den betroffenen Kommunalverwaltungen zur Krisenkommunikation eingesetzten Personen im Schadensfall nur über eingeschränkte Kenntnisse und Erfahrungen im Bereich Krisenkommunikation verfügten. Das Vorliegen von entsprechenden Kompetenzen wurde seitens der befragten Personen als vorteilhaft und als wichtig erachtet, um im Ernstfall adäquat agieren zu können.[318] Es wurde im Rahmen der Interviews

---

[315] Transkription A, Z. 101-111; Transkription B, Z. 293-301; Transkription C, Z. 193-203; Transkription D, Z. 242-258; Transkription E, Z. 103-115; Transkription F, Z. 301-313.
[316] Transkription B, Z. 297-298; Transkription D, Z. 255-258; Transkription E, Z. 104-108.
[317] Transkription B, Z. 293-385.
[318] Transkription B, Z. 276-306; Transkription C, Z. 336-351; Transkription D, Z. 222-229; Transkription E, Z. 253-261; Transkription F, Z. 189-195.

auch deutlich, dass die betreffenden Kommunen, insbesondere in diesem Zusammenhang, sehr stark durch die Einbindung der CSBW und der Komm.ONE profitierten und sich das Know-How, die Erfahrungen und auch Vorarbeiten zu Nutze gemacht haben.[319] Fehlende Kompetenzen konnten durch die Unterstützung externer Experten kompensiert werden. Die interviewte Person mit der Kennung E4ID-NEG1 zieht folgendes, für dieses Unterkapitel bezeichnendes Resümee zum Schulungsbedarf der kommunalen Verwaltungsmitarbeiterinnen und Verwaltungsmitarbeiter:

> „Ja, insgesamt klar! Es wäre besser gewesen, wir wären entsprechend geschult gewesen. Es ist aber auch viel über die Cybersicherheitsagentur Baden–Württemberg abgefangen worden und die haben uns natürlich auch gut unterstützt. Sehr gut!“[320]

In Kapitel 6.4.2 wird vertieft auf die Bedeutung einer Unterstützung im Zuge der Krisenkommunikation durch externe Organisationen, wie z.B. durch die Komm.ONE oder durch die CSBW eingegangen.

6.3 Erreichen der wichtigsten Zielgruppen

Neben den in den Kapiteln 6.1 und 6.2 bereits dargestellten Kategorien, hat sich das Erreichen der wichtigsten Zielgruppen als weitere Hauptkategorie hervorgetan. Innerhalb dieser hat sich gezeigt, dass im Notfallszenario zum einen die technischen u. organisatorischen Rahmendbedingungen eine Rolle spielen, aber auch eine adäquate Priorisierung der Zielgruppen im Krisenfall angezeigt ist. In den Unterkapiteln 5.3.1 bis 5.3.3 werden die aus den Interviews erzielten Ergebnisse im Einzelnen beleuchtet und ausgeführt.

[319] Transkription A, Z. 93-96 und Z. 101-111; Transkription B, Z. 276-306; Transkription D, Z. 227-229.
[320] Transkription D, Z. 227-229.

6.3.1 Kommunikation mit den Mitarbeitenden

Die Analyse und Auswertung der aus den Interviews gewonnenen Daten zeigt auf, dass die Kommunikation mit den Mitarbeiterinnen und Mitarbeitern bei einem Ransomware - Angriff von sehr hoher Bedeutung ist.[321]

> (…) „Aber auch die Mitarbeitenden müssen mitgenommen werden. Also gerade dieser Aspekt der internen Kommunikation in so einer Situation ist extrem wichtig, einfach, denn es betrifft sehr viele Mitarbeitenden / einfach, dass sie am Morgen eben den Laptop einfach nicht mehr anmachen können, oder dass sie nicht mehr mit der Schlüsselkarte reinkommen.“[322] (…)

Es wird berichtet, dass die Information der Belegschaft zum Teil vergessen wird oder die Mitarbeitenden weniger stark priorisiert (z.B. im Vergleich zu den Medien) angesprochen werden.[323] Darüber hinaus führten auch teilweise die vorherrschenden Einschränkungen zu einer mangelnden internen Kommunikation.[324] Unzureichende Kommunikation führt im Notfallereignis zu Unsicherheiten bei den Mitarbeitenden und zu Kritik aus deren Reihen.[325] Die Mitarbeiterinnen und Mitarbeiter benötigen eine frühzeitige, proaktive und transparente Kommunikation. Entsprechende Vorkehrungen und Maßnahmen werden als erforderlich erachtet.[326] Im Ergebnis kann damit festgehalten werden, dass die Kommunikation mit den Mitarbeitenden ein sehr wichtiges Erfordernis in der Krise darstellt, die Umsetzung der internen Kommunikation aber zugleich auch mit besonderen Herausforderungen im Notfall verbunden ist.

6.3.2 Nutzung vorhandener Kommunikationskanäle

Aus den Interviews wurde deutlich, dass die im Normalfall zur Verfügung stehenden Kommunikationskanäle für die Nutzung zur Krisenkommunikation bei einem

---

[321] Transkription B, Z. 256-268; Transkription C, Z. 164-178; Transkription F, Z. 301-313.
[322] Transkription F, Z. 308-311.
[323] Transkription B, Z. 237-240; Transkription F, Z. 305-309.
[324] Transkription B, Z. 237-251; Transkription E, Z. 52-57.
[325] Transkription B, Z. 257-261; Transkription E, Z. 55-57
[326] Transkription B, Z. 124-129 u. 256-268; Transkription C, Z. 164-178; Transkription F, Z. 301-313.

Ransomware–Angriff grundsätzlich geeignet sind, um die Bevölkerung angemessen zu informieren.[327] Es wird jedoch auch zurückgespiegelt, dass einzelne Bevölkerungsgruppen, insbesondere diejenigen, die auch im Normalbetrieb nicht erreicht werden, auch nicht im Notfallereignis erreicht würden. Dass dies zu negativen Auswirkungen oder Kritik geführt habe, wurde nicht geäußert.[328]

Weiterhin lässt sich aus den Interviewdaten entnehmen, dass sich die technischen Rahmenbedingungen im Notfallszenario auf die Nutzbarkeit der üblicherweise eingesetzten Kommunikationskanäle negativ auswirken. Zum Teil können wichtige Kanäle überhaupt nicht, erst zeitverzögert oder nur mit gesteigertem Aufwand genutzt werden.[329] Die interviewte Person mit der Kennung E4IDNEG1 meldete auf die Frage, wie wichtig sie die Funktionstüchtigkeit der Kommunikationstechnik in der Krise einschätze, zurück:

> „Sehr wichtig! Es ging bei uns noch einigermaßen, weil wir es schnell zum Laufen bekommen haben. Aber wenn man natürlich sofort auf etwas hätte zurückgreifen können, wäre es natürlich deutlich besser gewesen!“[330]

Insbesondere die interne Kommunikation wird maßgeblich erschwert, wenn die Telefonie und E-Mail-System ausfallen.[331] Auf die Bedeutung einer funktionierenden Funktionstechnik wird in Kapitel 6.4.1 im Rahmen der Ausführungen zur Hauptkategorie „Vorbereitung auf die Krise“ näher eingegangen. Für Kapitel 6.3.2 lässt sich zusammenfasend feststellen, dass - wenn die Funktionstüchtigkeit gegeben ist - die üblicherweise eingesetzten Kommunikationskanäle zur Erreichung der relevanten Zielgruppen genutzt werden können, um den Kommunikationsbedarf zu decken.

---

[327] Transkription A, Z. 101-111; Transkription B, Z. 217-233; Transkription C, Z. 324-327; Transkription D, 138-174 u. 203-214; Transkription E, Z. 98-115.
[328] Transkription A, Z. 244-256, Transkription B, Z. 217-233; Transkription E, Z. 222-237 u. 243-247.
[329] Transkription A, Z. 128-135; Transkription B, Z. 135-191; Transkription C, Z. 224-231; Transkription D, Z. 130-174 u. 195-197; Transkription E, Z. 141-166; Transkription F, Z. 125-134.
[330] Transkription D, Z. 195-197.
[331] Transkription A, Z. 144-147 u.167-170; Transkription B, Z. 242-251, Transkription E, Z. 91-94.

6.3.3 Website als zentraler Kommunikationskanal nach außen

Als weiteres Ergebnis hat sich herausgestellt, dass die kommunale Website einen hohen Stellenwert für die externe Kommunikation besitzt und die Kommunikatoren der Gemeinden die Nutzung der Website im Notfall als sehr wichtig erachten.[332] Die interviewte Person mit der Kennung E4IDNEG1 äußerte sich folgendermaßen:

> „Gott sei Dank hat unsere Homepage funktioniert. Das war ein riesiger Gewinn. Da konnten wir dann immer aktuell darüber informieren, wie es aussieht und tagesaktuell etwas rauslassen.“[333]

Die Websites werden, z.T. gemeinsam mit Social-Media-Kanälen, als zentraler Kommunikationskanal nach außen eingesetzt, um die in 6.2.1 beschriebenen Kommunikationsprinzipien umzusetzen.[334] Die Funktionsfähigkeit der Website und je nach Strategie auch die der Social-Media-Kanäle, ist damit wesentlich für die Realisierung der externen Krisenkommunikation. Um, bezugnehmend zu obigem Zitat, das Funktionieren der zentralen Kanäle nicht allein in Gottes Hände zu geben, ist eine angemessene Vorbereitung erforderlich. Dies zeigen die gewonnen Erkenntnisse in dem sich anschließenden Kapitel.

6.4 Vorbereitung auf die Krise

Die Interviews zeigen: Wer sicherstellen will, dass er in der Krise von Beginn an ohne Zeitverlust strukturiert und effektiv agieren kann, kommt an einer Vorbereitung nicht vorbei.[335] Es stellte sich heraus, dass die Vorbereitung auf den Notfall zum einen in Bezug auf technische Aspekte besonders bedeutsam ist und zum anderen aber auch eine Vorsorge auf organisatorischer Ebene von hohem Stellenwert ist.

---

[332] Transkription B, Z. 207-211; Transkription D, Z. 141-143 u. 151-154; Transkription F, Z. 130-134.
[333] Transkription D, Z. 141-143.
[334] Transkription A, Z. 159-170 u. 182-186; Transkription B, Z. 161-169; Transkription D; Z. 141-143; Transkription E, Z. 102-108 u. 188-195.
[335] Transkription A, Z. 208-242; Transkription B, Z. 52-63; Transkription C, Z. 292-311; Transkription D, Z. 176-197; Transkription E, Z. 141-166; Transkription F, Z. 160-174.

6.4.1 Funktionstüchtigkeit der Kommunikationstechnik

Aus verschiedenen Interviews wurde deutlich, dass seitens der betroffenen Kommunen nur sehr eingeschränkt Vorkehrungen oder Maßnahmen im Vorhinein getroffen wurden, um sicherzustellen, dass die Kommunikationstechnik im Notfall funktionsfähig ist.[336] Allerdings haben die Interviewpartnerinnen und Interviewpartner ebenso auf die Bedeutung der IT-gestützten Kommunikationskanäle, insbesondere der Website und des Mailsystems, aufmerksam gemacht.[337]Aus der Praxis wird berichtet, dass es rückblickend teilweise dem Zufall überlassen wurde, welche Kanäle im Notfall zur Verfügung stehen.[338] Die interviewte Person mit der Kennung E7ICE1 fasst für ein Notfallszenario, in dem ohne Vorbereitung im Zusammenhang mit der Kommunikationstechnik, reagiert werden muss, prägnant zusammen:

> „Wenn Ihnen dann gelingt, ad–hoc etwas zu machen, PRIMA! Aber SICHER ist das ja nicht!“[339]

Auch wenn es einzelnen Gemeinden gelungen ist, ohne Vorbereitung in Bezug auf technische Aspekte, die Situation zu meistern, ist dennoch als zentrales Ergebnis den Interviewdaten zu entnehmen, dass retrospektiv eine angemessene Vorbereitung von hoher Bedeutung ist, um im Ernstfall wichtige Kommunikationsmittel nutzen zu können oder im Ernstfall auf Alternativen zurückgreifen zu können.[340] Andernfalls ist man auf eine glückliche Fügung angewiesen.[341]

6.4.2 Organisatorische Vorbereitung auf die Krise

Auch in Bezug auf organisatorische Aspekte zeigt sich, dass eine angemessene Vorbereitung erhebliche Vorteile mit sich bringt. Klare Regelungen, wie Rollen und Aufgabenfestlegungen, feststehende Abläufe, bereits eingerichtete Chatgruppen,

---

[336] Transkription B, Z. 193-203; Transkription D, Z. 176-184 u. 276-279; Transkription E, 197-201; Transkription F, 136-141.
[337] Vgl. Kapitel 5.3.2. u. 5.3.3.
[338] Transkription B, Z. 193-211; Transkription D, Z. 182-184; Transkription E, Z. 197-201; Transkription F, Z. 136-141.
[339] Transkription C, Z. 304-305.
[340] Transkription B, Z. 17-211; Transkription C, Z. 267-281 u. 292-310; Transkription E, Z. 203-216; Transkription F, Z. 151-158.
[341] Vgl. hierzu Transkription D, Z. 141-143.

ausgedruckte Kontaktlisten, aber auch vorgefertigte Textbausteine und Sprachreglungen führen zu einer effizienten und effektiven Krisenbewältigung, zu einer Entlastung und zu einer ruhigen Atmosphäre in der Krisensituation.[342] Die Expertin mit der Kennung E5IBMIE1 meldete auf die Frage, welchen Aspekt sie im Zuge der Krisenkommunikation für besonders wichtig erachte, unter anderem folgendes zurück:

> (…) „das Thema VORBEREITUNG. Das war etwas, was bei uns nicht vorhanden war. Wir hatten leider keine vorgefertigten Pressemitteilungen in der Schublade. Wir hatten keine FAQs in der Form vorbereitet, wo man sagen könnte, das ist etwas, was wir mit Informationen füttern können. Wir hatten keine Vorüberlegungen getroffen, in welcher Form wir wie in der Krise agieren oder kommunizieren möchten. Sprich, wir mussten ad – hoc uns auf die Situation einstellen. Wir mussten gucken, welche Kommunikationskanäle haben wir jetzt überhaupt zur Verfügung, wie können wir diese nutzen. Aber diese Vorüberlegungen: WAS können wir WANN, WIE nutzen? (…) Die Überlegungen haben wir quasi erst in der Krise getroffen und dahingehend auch viel Zeit verloren.“[343]

Auch weitere interviewte Personen machten insbesondere auf den Zeitverlust aufmerksam, der dadurch entsteht, wenn keinerlei oder eine nur sehr eingeschränkte Notfallplanung im Vorhinein stattgefunden hat:

> „Also lieber hat man einen Notfallplan umsonst geschrieben, der in einer Schublade liegt und sich überlegt, wie genau reagiere ich in der Situation, als dass man dann eben tatsächlich in der Situation selbst ist und erstmal DIE Zeit aufwenden muss, die man da eigentlich schon hätte sich sparen können. Und es ist leider SO: Es kann JEDEN treffen!“[344]

---

[342] Transkription A, Z. 208-242; Transkription B, Z. 400-432; Transkription C, Z. 145-158; Transkription E, Z. 206-216; Transkription F, Z. 153-158 u. 248-257.
[343] Transkription B, 414-423.
[344] Transkription F, Z. 154-158.

6.5 Disponieren der Ressourcen

Im Zuge der Datenanalyse hat sich der Themenkomplex „Disponieren der Ressourcen“ als weitere Kategorie herauskristallisiert. Innerhalb dieser Kategorie konnten zwei wesentliche Ergebnisse gewonnen werden. Zum einen in Bezug auf den Einsatz der eigenen personellen Ressourcen zum anderen aber auch in Bezug auf die Bedeutung externer Ressourcen im Notfall.

6.5.1 Einsatz der eigenen personellen Ressourcen

Aus den Interviews wird deutlich, dass die personelle Ausstattung kleinerer Kommunalverwaltungen sich im speziellen Notfallszenario nicht als unlösbares Problem erweist. Durch großen Einsatz und besonderes Engagement der Mitarbeiterinnen und Mitarbeiter und zum Teil durch Bündelung der Kräfte kann die Situation gemeistert werden.[345] Die für die Krisenkommunikation eingesetzten Personen werden allerdings im Zuge der Notfallbewältigung teilweise sehr stark beansprucht.[346]

> „Dadurch, dass wir im Bereich Presse- und Öffentlichkeitsarbeit eher weniger personelle Ressourcen hatten, konnte das nur dadurch bewältigt werden, dass die entsprechenden Personen die Mehrarbeit geleistet hatten. Hätten wir mehr personeller Ressourcen gehabt, hätte man beispielsweise auch Schichtsysteme einrichten können, um auch Personen zu entlasten.“[347]

Um die Belastungssituation zu entschärfen, wurde in verschiedenen Kommunen der Bereich Krisenkommunikation mit personellen Ressourcen aus anderen Verwaltungsbereichen verstärkt.[348]

6.5.2 Unterstützung durch externe Organisationen

Als weiteres Ergebnis hat sich gezeigt, dass externe Experten einen sehr wertvollen Beitrag im Zuge der Krisenkommunikation leisten können. Die Kommunen profitieren dabei auf unterschiedliche Weise. Das zur Verfügung stellen von vorgefertigten Textbausteinen, FAQs, Pressemitteilungen etc. spart den Kommunen Zeit

---

[345] Transkription A, Z. 344-369; Transkription B, Z. 437-496, Transkription C, Z. 381-404; Transkription D, Z. 289-309; Transkription E; Z. 295-311; Transkription F, Z. 264-273.
[346] Transkription B, Z. 437-496; Transkription E; Z. 300-308; Transkription F, Z. 267-270.
[347] Transkription B, Z. 488-491.
[348] Transkription C, Z. 387-397; Transkription D, Z. 293-98; Transkription E, Z. 298-311.

und personelle Ressourcen. Darüber hinaus kann fehlendes Expertenwissen und Know–How durch erfahrene, externe Profis kompensiert werden. Nicht zuletzt kann durch einen außenstehenden Dritten auch eine objektive Einschätzung zu Einzelfragestellungen eingeholt werden.[349] Insgesamt besitzt die Unterstützung von externen Organisationen einen sehr hohen Stellenwert für die Kommunen. Die interviewte Person mit der Kennung E7ICE1 antworte beispielsweise folgendermaßen auf die Frage, welcher Aspekt bei kleineren Kommunalverwaltungen im Zuge der Krisenkommunikation besonders wichtig sei:

> „Dass die Kommunalverwaltungen die Unterstützung, die sie kriegen können, auch nutzen. Ich glaube, das ist das A und O. (…) Am Ende ist es wichtig, wenn sie in die Situation kommen, dass sie sich die Hilfe reinholen, die sie kriegen können. Und nicht denken, ich muss das aus eigener Kraft schaffen.“[350]

7. Diskussion und Synthese der Ergebnisse

Nachdem in Kapitel 6 die Ergebnisse aus der empirischen Untersuchung dargestellt und erläutert wurden, findet nun eine Synthese zwischen diesen gewonnenen Erkenntnissen und der in den Kapiteln 2 und 3 aufgearbeiteten Theorie statt. Dabei werden insbesondere Überschneidungen, aber auch Widersprüchlichkeiten sowie Abweichungen herausgearbeitet und interpretiert.

An dieser Stelle wird die Forschungsfrage mit ihren Unterfragen, als zentrale und richtungsweisender Aufgabenstellung der Master–Thesis, noch einmal wiederholt, um daran orientiert die Zusammenführung der Ergebnisse auszuarbeiten:

„Welche Schlüsselfaktoren führen zu einer erfolgreichen Krisenkommunikation im Falle eines Ransomware–Angriffes?“

[349] Transkription A, Z. 274-78 u. 340-342; Transkription B, 276-304 u.408-414; Transkription C, Z. 409-420 u. 425-429 u. 449-451; Transkription D, Z. 222-235; Transkription F, Z. 289-296.
[350] Transkription C, Z. 449-453.

- Worin liegen die wesentlichen Herausforderungen für kleinere Kommunalverwaltungen im Zuge der Krisenkommunikation im Zusammenhang mit einem Ransomware - Angriff?
- Welche Rolle spielen dabei die vorherrschenden Rahmenbedingungen?
- Welche Ansatzpunkte ergeben sich daraus für kleinere Kommunalverwaltungen für das Gelingen der Krisenkommunikation?

Grundsätzlich kann festgestellt werden, dass erfolgreiche Krisenkommunikation im Zusammenhang mit einem Ransomware–Angriff nicht nur von einem einzelnen Faktor abhängt. Sowohl die empirische Untersuchung als auch die Literatur zeigen eindrücklich auf, dass mehrere Aspekte auf verschiedenen Ebenen von besonderer Relevanz sind. Übergeordnet lässt sich empirisch und auch auf Basis der Literatur festhalten, dass technische und organisatorische Gesichtspunkte eine wesentliche Rolle einnehmen. Darüber hinaus sind auch ein professionelles Kommunikationsverhalten und eine angemessene Vorbereitung auf den Notfall von Belang.

In organisatorischer Hinsicht geht die Literatur zur Bewältigung der Lage von der Einrichtung eines Krisenstabes aus. Dieses Ergebnis hat sich im Rahmen der empirischen Untersuchung bestätigt. Die Installation eines Stabes wird auch in der Praxis als immens wichtige und wertvolle Maßnahme betrachtet, um im Notfallszenario wirksam und effektiv handeln zu können. Insbesondere wenn kein umfassender Krisenstab zur Notfallbewältigung eingerichtet wurde, kritisierten dies die betreffenden Interviewpartnerinnen und Interviewpartner. Insofern sind die Erkenntnisse aus der Literatur und der empirischen Untersuchung deckungsgleich.

In Bezug auf die konkrete Besetzung des Krisenstabes ist der Literatur keine einheitliche Meinung zu entnehmen. Klarheit herrscht allerdings insoweit, als dass alle relevanten Stellen in den Krisenstab eingebunden werden sollten. Der Bereich

Kommunikation sollte entsprechend der untersuchten Literatur unbedingt, unabhängig vom konkreten Krisenszenario, im Krisenstab vertreten sein.[351] Dahingehend ergibt sich auch unter Berücksichtigung der Ergebnisse der Interviews ein einheitliches Bild. Aus der Analyse der Interviewdaten lässt ich eindeutig aufzeigen, dass alle relevanten Akteure gemeinsam im Stab vertreten sein sollten. Dazu wird auch seitens der Interviewpartnerinnen und Interviewpartner die für Krisenkommunikation zuständige Stelle gezählt. Durch die Interviews lässt sich für das konkrete Notfallszenario weiterhin darlegen, dass auch Vertreterinnen und Vertreter der Komm.ONE, der CSBW und der Polizei wichtige Akteure darstellen, die als Mitglieder des Krisenstabes aufgenommen werden sollten. Auf diese Weise kann ein zielführender Austausch, eine umfassende Beratung und eine abgestimmte Kommunikation erfolgen. Insofern untermauern die Interviewergebnisse die theoretische Basis. Im Hinblick auf die organisatorische Ausgestaltung des Krisenstabes zeigen die empirischen Ergebnisse auf, dass - je nach örtlichen Gegebenheiten - unterschiedliche Strukturen zielführend und praxistauglich sein können. Dieses empirische Ergebnis deckt sich mit der Auffassung von Heimann und Hofinger. Diese stellen in diesem Zusammenhang fest, dass die - besonders innerhalb einer Institution - grundsätzlich gleichen inneren Stabsstrukturen, der Erleichterung der Kommunikation dienen und zur vereinfachten Prozessabläufen führen.[352] In der Gesamtsynthese steht damit im Ergebnis fest, dass die Bildung und der Einsatz eines Krisenstabes einen sehr hohen Stellenwert besitzen. Darüber hinaus ist von wesentlicher Bedeutung, dass alle relevanten Akteure einbezogen werden. Die konkrete organisatorische Ausgestaltung des Stabes muss zur jeweiligen Institution passen, ungeachtet existierender Normen, Standards und Vorschriften.

Die Literatur sieht für das Notfallszenario grundsätzlich vor und empfiehlt, dass der betreffenden Organisation ein möglichst vollständiger Krisenmanagementplan und

[351] DIN EN ISO 22361:2023–2 Krisenmanagement, S. 25; BSI-Standard 200-4 Business Continuity Management, S. 101; BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), S. 9.

[352] Heimann, R.; Hofinger, G. (2022): Stabsarbeit - Konzept und Formen der Umsetzung, S. 6.

ein Notfallhandbuch vorliegt, in dem alle Dokumente abgelegt sind, die eine angemessene Reaktion auf die Krise unterstützen.[353] Die Interviews haben gezeigt, dass in den untersuchten Einzelfällen ein umfassendes Krisenmanagement, das auch ein Krisenmanagementplan und Notfallhandbuch integriert, nicht vorhanden war. Aus den Interviews konnten sich Rückschlüsse dahingehend ziehen lassen, dass eine Klarheit in Bezug auf Rollen, Aufgaben und Funktionen ein wesentlicher Faktor darstellen, um im Notfall besonnen, effektiv und schnell reagieren zu können. Die Ergebnisse der empirischen Untersuchung unterstreichen damit die Empfehlungen der Literatur, dass ein vorhandenes Krisenmanagement zur Bewältigung der Lage und zur erfolgreichen Krisenkommunikation sehr wichtig ist. Insbesondere in Kommunen, in denen kein Krisenmanagement betrieben wurde, werden die negativen Auswirkungen wie Zeitverlust, Unsicherheit und ungeordnete Verhältnisse deutlich. Im Ergebnis zeigt sich, dass sich ein Krisenmanagement bereits auf einem grundlegenden Niveau sehr positiv auf die Krisenbewältigung auswirkt.[354] Inwieweit von einem umfassenden Notfall- und Krisenmanagement abgewichen werden kann, um dennoch sicherstellen zu können, im Schadensfall erfolgreich kommunizieren zu können, bleibt allerdings in dieser Arbeit offen.

Die Literaturrecherche hat im Ergebnis ergeben, dass sich eine offene, proaktive und transparente Kommunikation in der Regel positiv auswirkt.[355] Die Interviewdaten bringen übereinstimmende Ergebnisse hervor.[356] Teilweise wurde im Rahmen der Interviews auch berichtet, dass den Gemeinden für die proaktive und transparente Informationslinie Lob entgegengebracht wurde. Damit bestätigt sich das Ergebnis aus der Literaturrecherche. Die interviewten Personen, ebenso wie die Literatur, spiegeln wider, dass eine offene Kommunikationsstrategie einen sehr hohen Stellenwert besitzt und einen wichtigen Beitrag zu einer erfolgreichen Krisenkommunikation leistet.

---

[353] BSI-Standard 200-4 Business Continuity Management, S. 25 u. S. 85; DIN EN ISO 22361:2023–2 Krisenmanagement, S. 21 ff..
[354] Transkription A, Z. 46-70; Transkription C, Z. 142-148; Transkription D, Z. 29-36.
[355] Vgl. Kapitel 3.3.2.
[356] Vgl. Kapitel 6.2.1.

Um den Anforderungen an eine professionelle Kommunikation im Notfallszenario gerecht zu werden, müssen entsprechende Kompetenzen und ein angemessenes Know–How bei den kommunizierenden Personen vorhanden sein. Davon geht zumindest die Literatur aus. Auch den Interviewdaten lässt sich entnehmen, dass das zur Krisenkommunikation eingesetzte Personal über fachliche Grundlagen verfügen sollte. In diesem Zusammenhang wird jedoch auch die Unterstützung durch externe Organisationen, wie z.B. durch die CSBW oder durch die Komm.ONE angemerkt. Fehlende Kenntnisse und Erfahrungen können durch die Einbindung von externen Experten kompensiert werden. Durch die empirische Untersuchung wird damit eine Option dargelegt, um die Situation - trotz fehlender Kompetenzen - zu meistern. In der Interpretation der Ergebnisse lässt sich entwickeln, dass erfolgreiche Krisenkommunikation stark von den Kommunikationsfähigkeiten und dem damit verbundenen Kommunikationsverhalten des Kommunikators abhängen. Die Einbindung von erfahrenen Krisenkommunikationsprofis, die gerade bei kleineren Kommunalverwaltungen naturgemäß nicht zur Stammbesetzung zählen, ist dabei eine große und wichtige Unterstützung.

Im Hinblick auf die zum Erreichen der relevanten Zielgruppen eingesetzten Kanäle gibt die Literatur grundsätzlich vor, insbesondere auf die üblicherweise eingesetzten und etablierten Kanäle zurückzugreifen und diese ggf. zu ergänzen. Die empirischen Ergebnisse bestätigen diese Empfehlung. Die Interviews zeigen, dass die kommunalen Kommunikationswege geeignet sind, Inhalte ausreichend zu streuen und Botschaften zu übermitteln. Die theoretischen Erkenntnisse stimmen damit mit den empirischen überein. Aus den Interviews wird deutlich, dass die technischen Einschränkungen, was sich bereits auf Basis der untersuchten Literatur herauskristallisiert hat, eine besondere Herausforderung darstellen. Die zentralen Kommunikationskanäle müssen im Krisenfall funktionstüchtig sein, um kommunizieren zu können. Im besonderen Maß sticht dabei die kommunale Website als außerordentlich wichtiger, zentraler Informationskanal der Behörde hervor. Dies zeigen sowohl die Ergebnisse der Literaturrecherche als auch die Interviewdaten. Im Hin-

blick auf die Bedeutung der Website wird sich daher der Auffassung Höbels angeschlossen, der diese als „wertvollstes Kommunikationsmittel schlechthin“[357] bezeichnet.[358] In der Konsequenz bedeutet dies, dass die Website im Notfall funktionstüchtig sein sollte und diese dann mit Inhalten bespielt wird. In Bezug auf die interne Kommunikation hat die empirische Untersuchung im besonderen Maß aufgezeigt, dass das Ausfallen von etablierten Kanälen, wie E–Mail und Telefonie, schnell zu Schwierigkeiten führt, wenn keine Alternativen genutzt werden können. Im Gesamtergebnis decken sich Empirie und Literatur dahingehend, dass die Mitarbeiterinnen und Mitarbeiter unbedingt frühzeitig mit Informationen und Handlungsanweisungen zu versorgen sind. Es hat sich im Rahmen der Interviews (leider) auch bestätigt, dass diese Zielgruppe in der Praxis nicht ausreichend berücksichtigt wird und dies mit negativen Folgen einhergeht. In der Gesamtbetrachtung hat sich damit dieser Aspekt als weiterer zentraler Ansatzpunkt herausgestellt, den es im Rahmen der Krisenkommunikation zu beachten gilt.

Um für die Krise bestmöglich gerüstet zu sein, geht die Literatur von einer umfassenden Vorbereitung auf das Notfallszenario aus. Die Vorsorge und Vorbereitung betreffen mehrere Ebenen, wie z.B. technische oder organisatorische Aspekte. Im Kern verdeutlichen dies auch die Interviews. Wer nicht dem Zufall überlassen will, ob die Krisenkommunikation im Ernstfall erfolgreich verläuft, muss sich zwingend auf den Notfall vorbereiten. Nicht umfassend geklärt werden konnte die Frage, in welchem konkreten Maß eine Vorbereitung und eine Vorsorge erforderlich ist. In organisatorischer Hinsicht hat sich bereits an anderer Stelle festhalten lassen, dass im Vorfeld organisatorische Aspekte geplant und dokumentiert werden sollten, um im Ernstfall Klarheit über Strukturen und Abläufe zu gewährleisten. In Bezug auf die Funktionstüchtigkeit der zentralen Kommunikationsmittel unterstreichen die empirischen Ergebnisse die der Literatur: Ein Mindestmaß an Vorbereitung ist erforderlich, um ohne unverhältnismäßigen Zeitverlust reaktionsfähig zu sein. Die untenstehende Grafik aus dem BSI–Standard 200–4 zeigt anschaulich die Auswirkungen in zeitlicher Dimension.

---

[357] Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, S. 251.
[358] Vgl. Kapitel 3.3.2 u. 6.3.3.

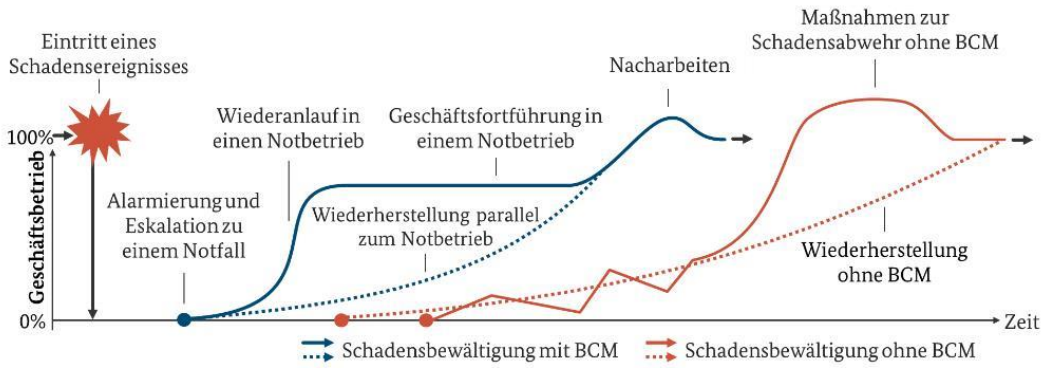

Abbildung 7: Schadensbewältigungsverlauf nach BSI-Standard 200–4[359]

Vor dem Hintergrund, dass die empirischen Ergebnisse die hohe Bedeutung funktionierender Kommunikationsmittel bestätigen, resultiert die Schlussfolgerung, dass sich potentielle Opfer, zumindest eingeschränkt auch in technischer Hinsicht vorbereiten und angemessene Kontinuitätsstrategien entwickeln müssen. Als Kontinuitätsstrategie können dabei auch analoge Lösungen in Frage und zur Anwendung kommen. Zum Beispiel könnten die Mitarbeiterinnen und Mitarbeiter, bei einem Ausfall des E–Mail-Systems und der Telefonanlage, auch regelmäßig und verlässlich über Aushänge oder über mündliche Ansprachen der Vorgesetzten informiert werden.[360] Obenstehende Grafik aus der Literatur ist nicht nur in Bezug auf technische Aspekte relevant. Auch in Bezug auf die Krisenkommunikation im engeren Sinn ist sie aussagekräftig und deckt sich mit den empirischen Ergebnissen. Sowohl die Literatur zur Krisenkommunikation als auch die Interviewdaten verdeutlichen, dass ein Kommunikationsplan, vorbereitete FAQs, Pressemitteilungen, Sprachregelungen und Checklisten im Notfall sehr viel Zeit sparen, für Entlastung in der Krise sorgen und Unsicherheiten entgegenwirken. Zusammenfassend betrachtet, ist eine dem Notfallszenario angemessene Vorbereitung ein wesentlicher Erfolgsfaktor für die Krisenkommunikation. Insbesondere an dieser Stelle der Mas-

[359] BSI–Standard 200–4 Business Continuity Management, S. 26.
[360] Vgl. Kapitel 6.3.2; Transkription D, Z. 211-214.

ter-Thesis wird die enge Verzahnung zwischen dem Business Continuity Management und dem Krisenmanagement deutlich.[361] Die Fragestellung, in welchem Umfang eine Vorplanung und Vorbereitung im Einzelnen erforderlich ist, wird durch die vorliegende Forschungsarbeit nicht beantwortet.

Auf Grundlage der Literaturanalyse konnte bereits ermittelt werden, dass der Umfang der zur Verfügung stehenden personellen Ressourcen ein Aspekt darstellt, dem im Zuge der Krisenkommunikation Beachtung geschenkt werden muss. Der Literatur ist im Ergebnis zu entnehmen, dass die im Regelbetrieb eingesetzten personellen Kapazitäten häufig nicht ausreichend sind und dementsprechend Handlungsbedarf besteht. Die empirische Untersuchung hat ergeben, dass die in einer kleineren Kommunalverwaltung zur Verfügung stehenden knappen personellen Ressourcen nicht dazu führen, dass die Krisenkommunikation misslingt. Es hat sich jedoch weiterhin herausgestellt, dass die im Zuge der Krisenkommunikation eingesetzten Personen zum Teil außerordentlich stark belastet werden und das Funktionieren der Kommunikation „auf dem Rücken der eingesetzten Mitarbeiterinnen und Mitarbeitern“ ausgetragen wird.[362] Teilweise wird die Situation in der Praxis entschärft, in dem Arbeitskräfte aus anderen Verwaltungsbereichen temporär in der Krisenkommunikation eingesetzt werden. Je nach Einzelfall decken sich damit die Ergebnisse der empirischen Untersuchung mit den Erkenntnissen aus der Literatur. Dass grundsätzlich immer ein Handlungsbedarf bestünde, hat sich durch die Auswertung der Interviews nicht belegen lassen. Im Zuge der Interpretation der Ergebnisse lässt sich folgende Erkenntnis ableiten: Es ist sinnvoll und wichtig im Vorhinein eine Ressourcenplanung unter Berücksichtigung der örtlichen Rahmenbedingungen vorzunehmen und dabei auch Worst-Case Szenarien (Urlaub, Krankheit, Vakanzen) zu berücksichtigen. Darauf basierenden ergibt sich dann ggf. für das konkrete Notfallszenario das Erfordernis organisatorische Maßnahmen zu ergreifen bzw. diese für den Ernstfall vorzusehen. In Bezug auf gravierendere Krisenereignisse (z.B. Großbrände, Überflutungen) sei ergänzend an dieser Stelle darauf hingewiesen,

[361] Vgl. hierzu BSI–Standard 200-4 Business Continuity Management, S. 26 u. Transkription B, Z. 414-423.
[362] Transkription F, Z. 275-277.

dass einzelne der interviewten Personen explizit angemerkt haben, dass die personellen Ressourcen in solch einem Szenario vermutlich nicht ausgereicht hätten.[363]

Ein Aspekt, der im theoretischen Teil dieser Forschungsarbeit weitestgehend unbeleuchtet geblieben ist, sich jedoch durch die empirische Untersuchung als außerordentlich bedeutsam herauskristallisiert hat, ist die Unterstützung der betroffenen Kommunen durch externe Organisationen. Im Rahmen der Befragung wurden die positiven Effekte durch eine externe Unterstützung, insbesondere der CSBW, aber auch der Komm.ONE von verschiedenen Interviewpartnerinnen und Interviewpartnern proaktiv angesprochen.[364] Die externen Experten bringen auf Anfrage ihre Expertise sowie Erfahrungen ein, unterstützen im Vorfallmanagement und liefern vorgefertigte Mustertexte. Dadurch können vorhandene Defizite, z.B. in Bezug auf eine adäquate Vorbereitung oder ausreichende Krisenkommunikationskompetenzen, kompensiert werden. Darüber hinaus lässt sich bei der betroffenen Verwaltung eine Entlastung herbeiführen und Zeit eingespart werden. Aus der Synthese der beiden Ergebnisse der Literatur und der empirischen Untersuchung resultierend, drängt sich die Schlussfolgerung auf, bei dem Punkt „Externe Unterstützung“ von einem äußerst wertvollen und wirksamen „Joker“ zu sprechen, der im Notfallszenario seitens der betroffenen Kommune gezogen werden kann. Diese Quintessenz trifft vor der dargestellten Daten- und Ergebnislage im Kern ohne Zweifel zu: Kleinere Kommunalverwaltung sollten sich im Schadensfall unbedingt unterstützen lassen, denn dieser Faktor trägt maßgeblich zum Erfolg der Krisenkommunikation bei. Die CSBW, als Landesbehörde und die Komm.ONE, als Anstalt des öffentlichen Rechts in gemeinsamer Trägerschaft des Landes und der Kommunen dürfen jedoch nicht (nur) als „Joker“ in der Hinterhand für den einmaligen Einsatz im Notfall verstanden werden.[365] Die empirischen Ergebnisse haben gezeigt, dass die betroffenen Kommunen nur sehr eingeschränkt auf einen Ransomware–Angriff vorbereitet gewesen sind und dies negative Auswirkungen unmittelbar nach dem Impact mit sich gebracht hat. Der Rückgriff auf externe Expertise ist vor diesem Hintergrund sicher

[363] Vgl. Transkription B, Z. 493-496.
[364] Transkription A, Z. 56-62 u. 86-96; Transkription B, Z. 276-306; Transkription D, Z. 227-229.
[365] Vgl. hierzu auch Transkription C, Z. 449-463.

auch bereits in der Präventions- und Vorbereitungsphase sinnvoll. Dies kann in dieser Arbeit jedoch nicht explizit belegt werden, sondern ergibt sich aus der Interpretation der Ergebnisse.

Durch die vorliegende Arbeit haben sich damit verschiedene Gesichtspunkte aufzeigen lassen, die im Hinblick auf die Forschungsfrage als Schlüsselfaktoren bezeichnet werden können. Der Fokus lag dabei darauf, die wesentlichen Aspekte herauszuarbeiten und darzulegen. Dabei wurde nicht erörtert, welche Schritte und Maßnahmen im Einzelnen erfolgen müssen, um in der Krise erfolgreich zu kommunizieren. Dass z.B. eine grundlegende Vorbereitung auf das Notfallszenario erforderlich ist und dies ein wesentlicher Erfolgsfaktor darstellt, wurde aus dieser Arbeit erkennbar und lässt sich eindeutig belegen. Die Frage nach dem zwingend erforderlichen Umfang einer Vorbereitung in technischer und organisatorischer Hinsicht, wurde jedoch nicht beantwortet. Diese Fragestellung könnte ein Ausgangspunkt für eine sich anschließende Untersuchung sein. Darüber hinaus trifft das vorliegende Forschungsprojekt keine Aussage darüber, welche Relevanz ein als Schlüsselfaktor herausgearbeiteter Aspekt im Vergleich zu den anderen wesentlichen Faktoren besitzt. Eine Gewichtung zueinander liefert die vorliegende Arbeit nicht. Auch an dieser Stelle bietet sich ein Ansatzpunkt für eine weitere und tiefere Beschäftigung mit der Materie.

8. Erkenntnisse und Ableitung von Handlungsempfehlungen

Nachdem in Kapitel 7 die Synthese und Diskussion der gewonnen Ergebnisse erfolgt ist, werden nun daraus Erkenntnisse und Handlungsempfehlungen für die kommunale Praxis abgeleitet. Diese werden entsprechend der Phasen des Krisenmanagements zugeordnet und strukturiert.

Präventions- und Vorbereitungsphase (vor der Krise)

- Vorbereitungen in organisatorischer Hinsicht führen zu Klarheit und geordneten Verhältnissen im Ernstfall. Aufgaben, Rollen, Funktionen und Abläufe sollten im Vorhinein festgelegt werden. Die Kernbesetzung des Krisenstabes und die für das Notfallszenario einzubinden Akteure sollten vorab

bestimmt werden. Die Struktur des Stabes passt idealerweise zu der eigenen Organisation. Im Notfallszenario gehört die Krisenkommunikation, die CSBW, die Komm.ONE und die Polizei unbedingt dem Krisenstab an. Diesbezüglich sollte bereits im Vorhinein Klarheit geschaffen und entsprechende Vorkehrungen getroffen werden. Weiterhin sollten im Vorfeld die vorhanden personellen Ressourcen in Bezug auf Kompetenzen und Kapazitäten in den Blick genommen und deren Auskömmlichkeit für den Notfall hinterfragt und Maßnahmen abgeleitet werden.

- Vorbereitungen in technischer Hinsicht sichern die Funktionsfähigkeit der wichtigsten Kommunikationsmittel in der Krise und sparen im Notfall Zeit. Im Vorfeld sollten für die wichtigsten Kommunikationsprozesse Kontinuitätsstrategien entwickelt werden, so dass im Krisenfall schnell die relevanten Zielgruppen kommunikativ erreicht werden können. Dies setzt voraus, dass vor der Krise schon geklärt ist, welcher Kommunikationskanal wie bespielt werden soll, bzw. welche Zielgruppe, wie erreicht werden kann. Die kommunale Website hat sich als sehr wertvoller Kommunikationskanal herausgestellt. Deren Funktionsfähigkeit in der Krise sollte im Vorhinein sichergestellt werden.

- Vorgefertigte Mustertexte zum Krisenszenario (wie z.B. FAQs, Pressemitteilungen, Aushänge), Check- und Kontaktlisten sowie Planungsdokumente sparen im Krisenfall Zeit und bringen Entlastung mit sich. In einem für das Notfallszenario angemessenen Umfang und zur Größe der Kommunalverwaltung passend, sollten entsprechende Dokumente im Notfall vorhanden sein.

<u>Bewältigungsphase (während der Krise)</u>

- Tritt das Notfallszenario ein, sollte unbedingt ein Krisenstab mit allen relevanten Akteuren einberufen werden. Krisenkommunikation ist integraler Bestandteil des Krisenmanagements. Die Einbindung aller wichtigen Per-

sonen und Organisationen führt zu einem effizienten, effektiven und harmonischen Handeln in der Krise und einer abgestimmten, konsistenten Kommunikation.

- Wenn noch nicht im Vorfeld geschehen, sollte spätestens jetzt eine Ressourcenplanung stattfinden und auf dessen Basis organisatorische Maßnahmen veranlasst werden. Durch kluges Disponieren der personellen Ressourcen kann eine Entlastung der eingesetzten Personen erreicht werden.

- Die Einbindung externer Krisenkommunikationsexperten bringt auf verschiedenen Ebenen einen wertvollen Mehrwert und wird daher empfohlen. Möglicherweise existierende Defizite können kompensiert und zusätzliche Ressourcen genutzt werden. Die positive Wirkung der Unterstützung durch die CSBW und durch die Komm.ONE wurde im Rahmen der empirischen Untersuchung durch die interviewten Personen stark betont.

- Es sollte eine proaktive, offene und transparente Kommunikationslinie verfolgt werden, die mit den relevanten Akteuren abgestimmt ist. Diese zahlt sich aus und kann zu positiver Resonanz führen.

- Die interne Kommunikation ist bedeutsam und darf nicht vernachlässigt werden. Die Mitarbeiterinnen und Mitarbeiter zu erreichen ist im Falle eines Ransomware–Angriffs ggf. mit erheblichen Schwierigkeiten verbunden. Dennoch sollte im Notfall ein Kanal existieren, über den die Belegschaft verlässlich und kontinuierlich erreicht wird. Im Zweifel sollten zumindest analoge Kommunikationsmittel, wie z.B. Aushänge, genutzt werden.

- Im Zuge der externen Kommunikation sollte auf die im Regelbetrieb eingesetzten Kommunikationskanäle zurückgegriffen werden. Insbesondere die kommunale Website ist ein sehr wichtiger Kanal, der bespielt werden sollte.

<u>Nachbereitungsphase (nach der Krise)</u>

- Für die Nachbereitungsphase wird eine Reflexion und Evaluierung der erfolgten Krisenbewältigung empfohlen.

Folgende Abbildung fasst die vorgenannten Handlungsempfehlungen zusammen:

Vorbereitungs- und Präventionsphase	**organisatorische Vorbereitung**	o Einrichtung eines Krisenstabes für den Notfall vorsehen und planen o Struktur des Krisenstabes mit Rücksicht auf die bereits bestehende Behördenorganisation festlegen o Alle relevanten Akteure berücksichtigen, insbesondere die Krisenkommunikation, CSBW, Komm.ONE und Polizei o Rollen, Aufgaben und Abläufe festlegen o Ressourcenplanung vornehmen
	Vorbereitung der Kommunikationsmittel	o Planen, welcher Kanal, wie genutzt werden soll bzw. welche Zielgruppe, wie erreicht werden kann o Entwicklung von Kontinuitätsstrategien für die wichtigsten Kommunikationsprozesse (z.B. der Website)
	Dokumente vorbereiten	o Erstellen von Planungsdokumenten, Mustertexten, Check- und Kontaktlisten
Bewältigungsphase	**Organisatorische Maßnahmen**	o Krisenstab mit allen relevanten Akteuren einberufen o Ressourcenplanung umsetzen und Personal sinnvoll disponieren o Externe Organisationen (z.B. CSBW, Komm.ONE) zur Unterstützung anfordern
	Kommunikative Maßnahmen	o Proaktive, offene und transparente Kommunikationslinie verfolgen, die mit den relevanten Akteuren abgestimmt ist o Interne Kommunikation nicht vernachlässigen o Üblicherweise eingesetzte Kommunikationskanäle nutzen o Kommunale Website bespielen
Für die Nachbereitungsphase wird eine Evaluierung der Planungen und Maßnahmen empfohlen		

Abbildung 8: Handlungsempfehlungen (eigene Darstellung)

9. Fazit

Die vorliegende Master–Thesis hat zum Ziel, auf Basis der Forschungsfrage „Welche Schlüsselfaktoren führen zu einer erfolgreichen Krisenkommunikation im Falle eines Ransomware–Angriffes?“ mit ihren Unterfragen, Erkenntnisse zu gewinnen, Ansatzpunkte herauszuarbeiten und Handlungsempfehlungen für die Managementebene kleinerer Kommunalverwaltungen abzuleiten.

Im Ergebnis zeigt sich, dass für eine erfolgreiche Krisenkommunikation verschiedene Aspekte auf unterschiedlichen Ebenen von besonderer Relevanz sind. Im Notfall in einer zur jeweiligen Kommune passenden Stabsform zu arbeiten, ist dabei ein entscheidender Faktor. In diesem Zusammenhang ist von Bedeutung, dass alle wichtigen Akteure gemeinsam „am Stabstisch sitzen“. Dazu gehört, als integraler Bestandteil des Krisenmanagements, die Krisenkommunikation. Im Falle eines Ransomware–Angriffes zählen zu diesem Kreis aber auch externe Stakeholder, wie die CSBW, die Komm.ONE und die Polizei. Herrscht in der Krise Klarheit in Bezug auf die jeweiligen Rollen, Funktionen und Aufgaben, führt das zu einer effektiven und effizienten Krisenbewältigung. Auf dieser Basis kann dann besonnen agiert und fruchtbar zusammengearbeitet werden. Ist diese, für den Erfolg der Krisenkommunikation wichtige organisatorische Grundlage geschaffen, sollte eine proaktive, offene und transpatente Kommunikationslinie verfolgt werden, die mit der CSBW, der Komm.ONE und der Polizei abgestimmt ist. Diese Vorgehensweise zahlt sich aus. Die interne Kommunikation mit den Mitarbeiterinnen und Mitarbeitern ist von einem sehr hohen Stellenwert. Sie darf daher nicht vernachlässigt werden, ansonsten drohen negative Auswirkungen. In der Krise sollte mit den üblicherweise eingesetzten Kommunikationskanälen kommuniziert werden. Insbesondere die kommunale Website fungiert im Notfallszenario als ein sehr wertvoller und zentraler Kanal für viele Zielgruppen. Damit in der Krise die Kommunikation wirksam und reibungslos erfolgen kann, ist zwingend eine Vorbereitung auf das Schadensereignis erforderlich. Ein verantwortungsvoller Umgang mit der realistischen Gefahr eines Ransomware–Angriffes lässt keinen anderen Rückschluss zu. Um den Erfolg nicht dem Zufall zu überlassen, sind technische und organisatorische Vorbereitungen notwendig. Dies stellt sicher, dass die im Notfall erforderlichen Kommunikationsmittel verfügbar oder Alternativen vorhanden sind und die für die Krise vorgesehenen Strukturen und Abläufe ohne Zeitverlust greifen können. Zur erforderlichen Vorarbeit zählt auch die Überprüfung der vorhandenen personellen Ressourcen in Bezug auf Kapazitäten und Kompetenzen. Im Notfall über kompetentes und zahlenmäßig ausreichendes Personal zu verfügen ist sehr wichtig. Die Einbindung externer Organisationen, wie die CSBW und die Komm.ONE, ist im Notfall

eine enorme Unterstützung und bringt einen erheblichen Mehrwert. Diese Hilfestellung sollte daher unbedingt beansprucht werden.

In der Gesamtbetrachtung haben sich damit mehrere Faktoren herausarbeiten lassen, die für das Gelingen der Krisenkommunikation kleinerer Kommunalverwaltungen eine übergeordnete Rolle spielen. Welcher dabei der wichtigste Gesichtspunkt und welcher in dem dargelegten Gesamtkomplex der unbedeutendste Aspekt ist, zeigt die vorliegende Arbeit nicht auf. Es konnte darüber hinaus nicht detailliert aufgezeigt werden, in welchem konkretem Maß eine Vorbereitung erfolgen muss, so dass die Krisenkommunikation im Schadensfall gelingt. Diese Fragestellungen können Ausgangspunkte für sich anschließende und auf dieser Master-Thesis aufbauende Forschungsarbeiten sein.

Literaturverzeichnis

Bachmann, S.; Ternès von Hattburg, A. (2021): Effiziente Krisenkommunikation- transparent und authentisch. Wie Kommunikation in extremen Situationen heute aussehen muss, um Organisationen zukunftsfähig zu machen, 2. Aufl., Springer Gabler.

Bedé, A. (2022): Grundsätze und Leitlinien zum Führen von (Unternehmens-) Krisenstäben, in: Hofinger G.; Heimann R. (Hrsg.), Handbuch Stabsarbeit. Führungs- und Krisenstäbe in Einsatzorganisationen, Behörden und Unternehmen, 2. Aufl., Springer, S. 131–137.

Dresing, T.; Pehl, T. (2018): Praxisbuch Interview, Transkription & Analyse. Anleitung und Regelsysteme für qualitativ Forschende, 8. Aufl., (Eigenverlag).

Einwiller, S.; Sackmann, S.; Zerfaß, A. (Hrsg.) (2021): Handbuch Mitarbeiterkommunikation. Interne Kommunikation in Unternehmen, Springer Gabler.

Freudenberg, D.; Kuhlmey, M. (Hrsg.) (2021), Krisenmanagement, Notfallplanung, Zivilschutz. Festschrift anlässlich 60 Jahre Zivil- und Bevölkerungsschutz in Deutschland, Berliner Wissenschafts- Verlag.

Gahlen, M. (2022): Aufgaben und Strukturen von Verwaltungsstäben, in: Hofinger G.; Heimann R. (Hrsg.), Handbuch Stabsarbeit. Führungs- und Krisenstäbe in Einsatzorganisationen, Behörden und Unternehmen, 2. Aufl., Springer, S. 69–74.

Gahlen, M.; Kranaster, M. (2019): Krisenmanagement. Planung und Organisation von Krisenstäben, 3. Aufl., Kohlhammer; Deutscher Gemeindeverlag.

Gißler, D. (2019): Erfolg der Stabsarbeit, Verlag für Polizeiwissenschaft.

Gißler, D. (2019): Führung und Stabsarbeit trainieren, Kohlhammer.

Gläser, J.; Laudel, G. (2010): Experteninterviews und qualitative Inhaltsanalyse, 4. Aufl., VS.

Heide, M. (2021): Interne Krisenkommunikation: eine Möglichkeit für Kommunikatoren, strategische Werte nachzuweisen, in: Einwiller S.; Sackmann S.; Zerfaß

A. (Hrsg.), Handbuch Mitarbeiterkommunikation. Interne Kommunikation in Unternehmen, Springer Gabler, S. 565–582.

Heimann, R. (2022): Historie von Stäben, in: Hofinger G.; Heimann R. (Hrsg.), Handbuch Stabsarbeit. Führungs- und Krisenstäbe in Einsatzorganisationen, Behörden und Unternehmen, 2. Aufl., Springer, S. 11–20.

Heimann, R.; Gahlen, M. (2022): Räume für Verwaltungsstäbe, in: Hofinger G.; Heimann R. (Hrsg.), Handbuch Stabsarbeit. Führungs- und Krisenstäbe in Einsatzorganisationen, Behörden und Unternehmen, 2. Aufl., Springer, S. 247–253.

Heimann, R.; Hofinger, G. (2022): Stabsarbeit - Konzept und Formen der Umsetzung, in: Hofinger G.; Heimann R. (Hrsg.), Handbuch Stabsarbeit. Führungs- und Krisenstäbe in Einsatzorganisationen, Behörden und Unternehmen, 2. Aufl., Springer, S. 3–10.

Höbel, P. (2022): Ohne Krisenkommunikation geht es schief, in: Trauboth J. H. (Hrsg.), Krisenmanagement in Unternehmen und öffentlichen Einrichtungen. Professionelle Prävention und Reaktion bei sicherheitsrelevanten Bedrohungen von innen und außen, 2. Aufl. , Boorberg, S. 234–342.

Hoffjann, O. (2013): Kommunikative Grenzen des Krisenmanagements, in: Thießen A. (Hrsg.), Handbuch Krisenmanagement, Springer VS, S. 413–432.

Hofinger, G. u. a. (2021): Stabsarbeit aus Sicht der Human Factors - Psychologie, in: Freudenberg D.; Kuhlmey M. (Hrsg.), Krisenmanagement, Notfallplanung, Zivilschutz. Festschrift anlässlich 60 Jahre Zivil- und Bevölkerungsschutz in Deutschland, Berliner Wissenschafts- Verlag, S. 187–208.

Hofinger, G. (2022): Kommunikationsmittel in Verwaltungs- und Unternehmensstäben, in: Hofinger G.; Heimann R. (Hrsg.), Handbuch Stabsarbeit. Führungs- und Krisenstäbe in Einsatzorganisationen, Behörden und Unternehmen, 2. Aufl., Springer, S. 289–297.

Hofinger, G. (2022): Sprachliche Kommunikation im Stab - Grundsätze des Sprechens und Schreibens, in: Hofinger G.; Heimann R. (Hrsg.), Handbuch Stabsarbeit. Führungs- und Krisenstäbe in Einsatzorganisationen, Behörden und Unternehmen, 2. Aufl., Springer, S. 343–348.

Hofinger, G.; Heimann, R. (Hrsg.) (2022): Handbuch Stabsarbeit. Führungs- und Krisenstäbe in Einsatzorganisationen, Behörden und Unternehmen, 2. Aufl., Springer.

Hofmann, T. (2013): Krise 2.0: Erfolgreiches Reputationsmanagement mit Social Media, in: Thießen A. (Hrsg.), Handbuch Krisenmanagement, Springer VS, S. 343–357.

Kaiser, R. (2021): Qualitative Experteninterviews. Konzeptionelle Grundlagen und praktische Durchführung, 2. Aufl., Springer VS.

Kulow, A.-C. (2022): Informations- und Cybersicherheit, in: Trauboth J. H. (Hrsg.), Krisenmanagement in Unternehmen und öffentlichen Einrichtungen. Professionelle Prävention und Reaktion bei sicherheitsrelevanten Bedrohungen von innen und außen, 2. Aufl., Boorberg, S. 343–377.

Kunze, R.; Bronner, O.; Katz, A. (2023): Gemeindeordnung für Baden - Württemberg Kommentar, Loseblattsammlung (Stand: 11/2024) 4. Aufl., Kohlhammer.

Künzer, L.; Hofinger, G.; Mähler, M. (2022): Psychologische Einflussfaktoren auf Stabsarbeit, in: Hofinger G.; Heimann R. (Hrsg.), Handbuch Stabsarbeit. Führungs- und Krisenstäbe in Einsatzorganisationen, Behörden und Unternehmen, 2. Aufl., Springer, S. 193–199.

Latsch, J. (2019): Bürgermeister und Krisenkommunikation, Kommunal- und Schul- Verlag.

Mayring, P. (2022): Qualitative Inhaltsanalyse. Grundlagen und Techniken, 13. Aufl., Beltz.

Mayring, P. (2023): Einführung in die qualitative Sozialforschung, 7. Aufl., Beltz.

Merten, K. (2013): Krise, Krisenmanagement und Krisenkommunikation, in: Thießen A. (Hrsg.), Handbuch Krisenmanagement, Springer VS, S. 153–173.

Riecken, M. (2013): Erfolgskritische Faktoren der angewandten Krisenkommunikation, in: Thießen A. (Hrsg.), Handbuch Krisenmanagement, Springer VS, S. 317–330.

Roselieb, F. (Hrsg.) (2022): Business Continuity Management in der Praxis. Mit Krisen professionell umgehen- erfolgreiche Konzepte und Fallbeispiele, Erich Schmidt Verlag.

Roselieb, F. (2022): Grundlagen des Business Continuity Managements, in: Roselieb F. (Hrsg.), Business Continuity Management in der Praxis. Mit Krisen professionell umgehen- erfolgreiche Konzepte und Fallbeispiele, Erich Schmidt Verlag, S. 9–91.

Schmitt-Geiger, A. (2013): Litigation-PR: Strategische Rechtskommunikation bei Unternehmenskrisen, in: Thießen A. (Hrsg.), Handbuch Krisenmanagement, Springer VS, S. 291–315.

Schnell, R.; Hill, P. B.; Esser, E. (2023): Methoden der empirischen Sozialforschung, 12. Aufl., De Gruyter.

Spielvogel, C. (2018): Stabsorganisation, in: Spielvogel C.; Reissig-Hochweller R. (Hrsg.), Taschenbuch Stabsarbeit, 2. Aufl. , Boorberg, S. 80–186.

Spielvogel, C.; Reissig-Hochweller, R. (Hrsg.) (2018): Taschenbuch Stabsarbeit, 2. Aufl., Boorberg.

Thießen, A. (Hrsg.) (2013): Handbuch Krisenmanagement, Springer VS.

Töpfer, A. (2013): Die Managementperspektive im Krisenmanagement - Welche Rolle spielt das Management bei der Bewältigung von Krisensituationen, in: Thießen A. (Hrsg.), Handbuch Krisenmanagement, Springer VS, S. 237–268.

Trauboth, J. H. (2022): Grundlagen für professionelles Krisenmanagement in einer sich verändernden Welt, in: Trauboth J. H. (Hrsg.), Krisenmanagement in Unternehmen und öffentlichen Einrichtungen. Professionelle Prävention und Reaktion bei sicherheitsrelevanten Bedrohungen von innen und außen, 2. Aufl., Boorberg, S. 19–64.

Trauboth, J. H. (Hrsg.) (2022): Krisenmanagement in Unternehmen und öffentlichen Einrichtungen. Professionelle Prävention und Reaktion bei sicherheitsrelevanten Bedrohungen von innen und außen, 2. Aufl., Boorberg.

Weitere Quellen:

B2B-Cyber–Security: Stadtverwaltung Burladingen durch Ransomware lahmgelegt, https://b2b-cyber-security.de/stadtverwaltung-burladingen-durch-ransomware-lahmgelegt/ (16.11.2024), zitiert als: B2b–Cyber–Security: Stadtverwaltung Burladingen durch Ransomware lahmgelegt.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: Krise, https://www.bbk.bund.de/SharedDocs/Glossareintraege/DE/K/krise.html (16.11.2024), zitiert als: BBK: Krise.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: Krisenkommunikation, https://www.bbk.bund.de/SharedDocs/Glossareintraege/DE/K/krisenkommunikation.html (16.11.2024), zitiert als: BBK: Krisenkommunikation.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: Krisenmanagement, https://www.bbk.bund.de/DE/Themen/Krisenmanagement/krisenmanagement_node.html (16.11.2024), zitiert als: BBK: Krisenmanagement.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: Krisenmanagement ist ein Zyklus, https://www.bbk.bund.de/DE/Themen/Krisenmanagement/KMZirkel/KMZirkel_node.html (16.11.2024), zitiert als: BBK: Krisenmanagement ist ein Zyklus.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: Risikokommunikation. Ein Handbuch für die Praxis, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/Risikomanagement/handbuch-risikokommunikation.pdf?__blob=publicationFile&v=5 (16.11.2024), zitiert als: BBK: Risikokommunikation.

Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-4 Business Continuity Management, Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Stan-

dards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html (16.11.2024), zitiert als: BSI–Standard 200–4 Business Continuity Management.

Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2023, Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html (16.11.2024), zitiert als: BSI: Die Lage der IT-Sicherheit in Deutschland 2023.

Bundesamt für Sicherheit in der Informationstechnik: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.html (16.11.2024), zitiert als: BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall (Version 1.2.), Bundesamt für Sicherheit in der Informationstechnik.

Bundesministerium des Innern und für Heimat: Schutz Kritischer Infrastrukturen - Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden, 2. Aufl., 2011, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis-leitfaden.html (16.11.2024), zitiert als: BMI: Schutz Kritischer Infrastrukturen - Risiko- und Krisenmanagement.

Bundesministerium des Innern und für Heimat: Leitfaden Krisenkommunikation, 5. Aufl., 2014, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/leitfaden-krisenkommunikation.html (16.11.2024), zitiert als: BMI: Leitfaden Krisenkommunikation.

Cybersicherheitsagentur Baden–Württemberg: Cybersicherheitsagentur Baden-Württemberg, Über die CSBW, https://www.cybersicherheit-bw.de/ueber-die-csbw (16.11.2024), zitiert als: CSBW: Über die CSBW.

Cybersicherheitsagentur Baden–Württemberg: Jahresbericht 2023, Cybersicherheitsagentur Baden–Württemberg, https://www.cybersicherheit-bw.de/jahresbericht-2023 (16.11.2024), zitiert als: CSBW: Jahresbericht 2023.

Cybersicherheitsagentur Baden–Württemberg: Unterstützung und Beratung: Vorfallmanagement und Krisenreaktion, https://www.cybersicherheit-bw.de/unterstuetzung-und-beratung-vorfallmanagement-und-krisenreaktion (16.11.2024), zitiert als: CSBW: Unterstützung und Beratung: Vorfallmanagement und Krisenreaktion.

Cybersicherheitsagentur Baden–Württemberg: Leitfaden zur Cybersicherheit, 2023, https://www.cybersicherheit-bw.de/fuer-cybersicherheit-sensibilisieren (16.11.2024), zitiert als: CSBW: Leitfaden Cybersicherheit.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden–Württemberg: Formular Datenpanne melden, https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/ (16.11.2024), zitiert als: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden–Württemberg: Formular Datenpanne melden.

Deutsche Gesellschaft für Soziologie, Ethik-Kodex der Deutschen Gesellschaft für Soziologie (DGS) und des Berufsverbandes Deutscher Soziologinnen und Soziologen (BDS): Ethikkodex, https://soziologie.de/dgs/ethik/ethik-kodex (16.11.2024), zitiert als: Deutsche Gesellschaft für Soziologie, Ethik-Kodex der Deutschen Gesellschaft für Soziologie (DGS) und des Berufsverbandes Deutscher Soziologinnen und Soziologen (BDS): Ethikkodex.

Duden, Cornelsen Verlag GmbH: Krise, https://www.duden.de/rechtschreibung/Krise (16.11.2024), zitiert als: Duden: Krise.

Komm.ONE: Jubiläumsmagazin - 50 Jahre digitale Partnerschaft, https://www.komm.one/site/Komm.ONE_Internet/get/documents_E1797062213/Komm.ONE/Komm.ONE_Internet_Objekte/Sonstiges/FlipBook/index.html (16.11.2024), zitiert als: Komm.ONE: Jubiläumsmagazin - 50 Jahre digitale Partnerschaft.

Komm.ONE: Satzung der Komm.ONE AöR, https://www.komm.one/site/Komm.ONE_Internet/get/documents_E1734798227/Komm.ONE/Komm.ONE_Internet_Objekte/Mitglieder%20VR/Satzung_der_Komm_ONE_AoeR.pdf (16.11.2024), zitiert als: Komm.ONE: Satzung der Komm.ONE AöR.

Komm.ONE: Aufgabenspektrum, https://www.komm.one/wer-wir-sind (16.11.2024), zitiert als: Komm.ONE: Aufgabenspektrum

Ministerium des Inneren, für Digitalisierung und Kommunen Baden–Württemberg: Zentrale Ansprechstellen für Cybercrime, https://lka.polizei-bw.de/zentrale-ansprechstelle-cybercrime/ (16.11.204), zitiert als: Ministerium des Inneren, für Digitalisierung und Kommunen Baden–Württemberg: Zentrale Ansprechstellen für Cybercrime

Ministerium für Inneres, Digitalisierung und Migration Baden–Württemberg: Landtag-Drucksache 16 / 3822, Kleine Anfrage vom 03.04.2018 über die Digitalisierung in Baden-Württemberg. https://www.landtag-bw.de/files/live/sites/LTBW/files/dokumente/WP16/Drucksachen/3000/16_3822_D.pdf (16.11.2024), zitiert als: Ministerium für Inneres, Digitalisierung und Migration Baden–Württemberg: Landtag-Drucksache 16 / 3822, Kleine Anfrage vom 03.04.2018 über die Digitalisierung in Baden–Württemberg.

Stadtverwaltung Schriesheim: Cyberangriff bei der Stadt Schriesheim - Datenverlust leider bestätigt, https://www.schriesheim.de/de/Aktuelles/Stadtnachrichten/Nachricht?view=publish&item=article&id=1141 (16.11.2024), zitiert als: Stadtverwaltung Schriesheim: Cyberangriff bei der Stadt Schriesheim - Datenverlust leider bestätigt.

Ehrenerklärung

Ich versichere, dass ich diese Hausarbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe. Mir ist bekannt, dass die schriftliche Arbeit im Verdachtsfall auf Plagiate überprüft werden kann.

……

Datum, Unterschrift

Anlagen