Matthias Schacht
Aufstiegsbeamter
Feuerwehr Kassel

Fachartikel

Geheimschutzkonzepte

Facharbeit gemäß § 20 Abs. 1 VAP2.2-Feu NRW

Wolfhagen, den 13.12.2025

Aufgabenstellung

Analysieren und vergleichen Sie verschiedene Geheimschutzkonzepte von Feuerwehren in Städten mit mehr als 250.000 Einwohnern. Welcher Personenkreis bzw. welche Funktionsträger müssen regelhaft überprüft werden? Zum Umgang mit welchen Verschlusssachengraden werden die Dienstkräfte damit ermächtigt? Welche Ressourcen nimmt die Prüfung in Anspruch und welche verwaltungstechnische Herausforderung bietet das Vorgehen? Wie wird der materielle Geheimschutz sichergestellt?

Hinweis zur geschlechtergerechten Sprache:
Zur besseren Lesbarkeit wird in dieser Arbeit bei Personen- und Funktionsbezeichnungen überwiegend die männliche Form verwendet. Sie schließt jedoch ausdrücklich alle Geschlechter (männlich, weiblich und divers) ein und ist wertfrei zu verstehen.

Abkürzungsverzeichnis

BABZ ..... Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung
BBK..... Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BCM..... Business Continuity Management
BfV ..... Bundesamt für Verfassungsschutz
BMI .....Bundesministerium des Inneren
BOS ..... Behörden und Organisationen mit Sicherheitsaufgaben
BSI ..... Bundesamt für Sicherheit in der Informationstechnik
DFV.....Deutscher Feuerwehrverband
ELW ..... Einsatzleitwagen
GeKoB ..... Gemeinsames Kompetenzzentrum Bevölkerungsschutz
HRDG ..... Hessisches Rettungsdienstgesetz
HSOG ..... Hessisches Gesetz über die Sicherheit und Ordnung
HSÜVG ..... Hessisches Sicherheitsüberprüfungs- und Verschlusssachengesetz
ISMS ..... Informationssicherheits-Managementsystem
KRITIS ..... Kritische Infrastruktur
KZV.....Konzeption Zivile Verteidigung
LEBEL..... Lebensbedrohliche Einsatzlage
NADIS.....Nachrichtendienstliches Informationssystem
NfD..... Nur für den Dienstgebrauch
OSINT.....Open Source Intellegence
RettDGV HE ..... Durchführungsverordnung zum Hessischen Rettungsdienstgesetz
RRGV .....Rahmenrichtlinie Gesamtverteidigung, Rahmenrichtlinie Gesamtverteidigung
SÜ..... Sicherheitsüberprüfung
SÜG .....Sicherheitsüberprüfungsgesetz
TEL ..... Technische Einsatzleitung
VSA.....Verschlusssachenanordnung
ZAPRL ..... Richtlinie für die Zivile Alarmplanung

Abbildungsverzeichnis

Tabellenverzeichnis

Inhalt

Teil I: Fachartikel

Kurzzusammenfassung

Hybride Bedrohungen, von Cyberangriffen bis Sabotage, rücken den Schutz sensibler Informationen der Feuerwehren insbesondere im Bevölkerungsschutz in den Fokus der Behörden. Feuerwehren sind dabei gefordert sich vor diesen Angriffen von außen zu schützen, aber auch vorbeugende Maßnahmen gegen Innentäter zu treffen. Die Facharbeit analysiert auf Basis semistrukturierter Experteninterviews mit Berufsfeuerwehren aus neun Bundesländern (Abgleich mit Städten >250.000 Einwohner) sowie eines Rechtsvergleichs von Sicherheitsüberprüfungsgesetzen (SÜG) und Verschlusssachenanweisungen (VSA) wie Geheim- und Sabotageschutz organisatorisch, personell und technisch umgesetzt werden kann.

Das Ergebnis ist eindeutig: Rechtsgrundlagen sind vorhanden, die Praxis ist heterogen. In den meisten Feuerwehren ist Geheimschutz noch Nebenaufgabe; Zuständigkeiten, Ressourcen und VS-fähige Prozesse unterscheiden sich erheblich. Sicherheitsüberprüfungen (SÜ) binden Zeit und Personal, Schnittstellen zwischen Behörden und IT-Systemen sind oft nicht VS-tauglich. Positiv fallen Standorte mit institutionalisiertem Geheimschutz, klaren Rollen (Geheimschutzbeauftragte), Einstufungskatalogen und der Einbindung eines Informationssicherheitsmanagementsystem (ISMS) und Business-Continuity-Managementsystem (BCM) auf.

Die Arbeit leitet folgende wirksame Punkte ab: Einerseits eine verbindliche Organisation mit hauptamtlichen Zuständigkeiten und hausinternen Einstufungsregeln; Weiterhin rechtssichere, beschleunigte Personalprozesse einschließlich zulässiger Vorprüfungen zur Aufrechterhaltung der Einsatzfähigkeit. Zudem eine technisch-materielle Befähigung durch VS-fähige IT-Arbeitsplätze und Kommunikationswege. Eine definierte Registratur/Aufbewahrung sowie geübtes BCM nach dem Mehrschichtenprinzip.

Wer wissen will, wie Großstadtfeuerwehren vom Flickenteppich zur belastbaren, interoperablen Sicherheitsarchitektur gelangen und welche konkreten Schritte Führungskräfte morgen anstoßen können, findet in diesem Beitrag eine komprimierte Lageanalyse und praxistaugliche Handlungsempfehlungen für mehr Resilienz in Anbetracht der aktuellen Gefahrenlage.

1 Einleitung

Die sicherheitspolitische Lage in Europa ist seit dem Beginn des russischen Angriffskrieges gegen die Ukraine von tiefgreifenden Umbrüchen geprägt. Der Konflikt markiert nicht nur eine Rückkehr zu konventioneller Kriegsführung, sondern auch eine stetige Ausweitung hybrider Bedrohungen gegen westliche Staaten. Diese umfassen Desinformation, Cyberangriffe, Sabotage und gezielte Einflussnahme auf kritische Infrastrukturen (Deutscher Bundestag, 2025). Deutschland wird als „Rückgrat der kollektiven Verteidigung in Europa“ und damit als vorrangiges Ziel solcher hybriden Angriffe gesehen (Bundesamt für Katastrophenschutz und Katastrophenhilfe [BBK], 01/2024).

Es wird davor gewarnt, dass Russland versucht, die staatliche Handlungsfähigkeit Deutschlands durch kombinierte politische, wirtschaftliche und technische Störmaßnahmen zu schwächen, noch bevor eine militärische Auseinandersetzung die Bündnisstrukturen direkt betreffen (Lange, Nr. 1/2025).

Spionageaktivitäten, Cyberoperationen und Einflussversuche gegen Behörden und sicherheitsrelevante Einrichtungen haben deutlich zugenommen und verdeutlichen die Komplexität der Bedrohungslage. Dabei richtet sich das Interesse ausländischer Nachrichtendienste, insbesondere auf Informationen zur zivilen Verteidigung, zu Kommunikationsinfrastrukturen und zu Entscheidungsprozessen im Bevölkerungsschutz. Der Schutz solcher sensiblen Informationen ist eine zentrale Voraussetzung für die staatliche Resilienz und Gesamtverteidigungsfähigkeit (Bundesministerium des Innern [BMI], 2025).

Feuerwehren sind in diesem Kontext Schlüsselorganisationen der zivilen Verteidigung als Bestandteil eines integrierten Hilfeleistungssystems (Bundesministerium des Innern (BMI), 2016). Sie verfügen über operative Führungsstrukturen, Informationssysteme, Stabsorganisationen und Netzverbindungen, die unmittelbar sicherheitsrelevant sind. Als Teil der kommunalen Verwaltung unterliegen sie den Anforderungen des Sicherheitsüberprüfungsgesetzes (SÜG) und der Verschlusssachenanweisung (VSA) der Länder. Gleichzeitig agieren sie an der Schnittstelle zwischen Verwaltung, Bevölkerung und Kritischen Infrastrukturen, wobei sie auch selbst Teil der Kritischen Infrastruktur sind (Hessische Landesregierung, 2024). Damit tragen sie eine besondere Verantwortung für den Geheim-, IT- und Sabotageschutz innerhalb des Bevölkerungsschutzsystems.

Vor diesem Hintergrund gewinnt die Frage, wie Feuerwehren in Großstädten ihre Geheimschutzkonzepte ausgestalten, besondere Bedeutung. Der Umgang mit Verschlusssachen, die Überprüfung von Personal sowie die Sicherstellung materieller und organisatorischer Schutzmaßnahmen, insbesondere des Sabotageschutzes, sind wesentliche Faktoren für die Aufrechterhaltung der Einsatz- und Führungsfähigkeit in Krisenlagen.

2 Darstellung der Problemstellung

Der Schutz von Verschlusssachen und sicherheitsrelevanten Informationen gewinnt auch im Bereich der Feuerwehren zunehmend an Bedeutung. Durch die Einbindung kommunaler Feuerwehren in Krisenstäbe, Katastrophenschutzleitungen, Zivile Verteidigung und kritische Infrastrukturen (KRITIS) entstehen vielfältige Berührungspunkte mit geheimhaltungsbedürftigen Informationen von Bund, Ländern und Kommunen. Damit unterliegen auch die Feuerwehrwehren, insbesondere in Großstädten (Einwohnerzahl > 250.000 Einwohnern), den Anforderungen des Geheim- und Sabotageschutzes nach dem SÜG und den VSA der jeweiligen Länder. In der Praxis zeigt sich jedoch, dass die Umsetzung der rechtlichen Vorgaben in Bezug auf den personellen sowie materiellen Geheim- und Sabotageschutz in den Feuerwehren uneinheitlich geregelt ist. Welche Feuerwehr verfügt über ein umfassendes Geheimschutzkonzept? Fehlende Prozesse, unzureichendes Personal und Brisanz der aktuellen Gefahrenlage sind Veranlassung Geheimschutzkonzepte von Feuerwehren zu analysieren. Die Umsetzung der Geheimschutzmaßnahmen stellen für eine Feuerwehr eine erhebliche organisatorische und verwaltungstechnische Herausforderung dar. Vor diesem Hintergrund besteht ein Bedarf, die bestehenden Geheimschutzkonzepte verschiedener Großstadtfeuerwehren systematisch zu analysieren und miteinander zu vergleichen. Die Untersuchung soll aufzeigen, wie die gesetzlichen Vorgaben in der kommunalen Praxis angewendet werden, welche Unterschiede und Gemeinsamkeiten zwischen den untersuchten Feuerwehren bestehen und welche Empfehlungen sich daraus für eine einheitlichere oder effizientere Gestaltung des Geheimschutzes ableiten lassen.

Ziel der Arbeit ist es einen praxisnahen Vergleich zu ermöglichen, die Effektivität bestehender Konzepte zu bewerten und Optimierungspotenziale für den personellen, organisatorischen und materiellen Geheim- und Sabotageschutz in kommunalen Feuerwehren zu identifizieren.

3 Herangehensweise

Zur Beantwortung der Problemstellung wurden zunächst alle deutschen Städte und Stadtstaaten mit mehr als 250.000 Einwohnerinnen und Einwohnern identifiziert (Statistisches Bundesamt, 2025) und mit der Liste der bestehenden Berufsfeuerwehren abgeglichen (Arbeitsgemeinschaft der Berufsfeuerwehren in Deutschland (AGBF), 2025). Auf diese Weise ergab sich eine Auswahl von 29 Berufsfeuerwehren, die sich auf zehn, der sechzehn Bundesländer, verteilten. Um eine ausgewogene und repräsentative Betrachtung sicherzustellen, wurde aus neun der betroffenen Bundesländer jeweils eine Berufsfeuerwehr als Untersuchungseinheit ausgewählt. Die Feuerwehr Berlin stand leider nicht für ein Interview zur Verfügung. Weiterhin wurde als Vergleich einer großen und kleineren Feuerwehr aus Hessen zwei Feuerwehren betrachtet.

Für die Datenerhebung kam die Methode der semistrukturierten Experteninterviews zum Einsatz. Diese Vorgehensweise ermöglichte es, vergleichbare Informationen zu gewinnen und zugleich individuelle Besonderheiten der jeweiligen Organisationen zu berücksichtigen. Eine detaillierte Auflistung der befragten Personen erfolgt in Teil II der Arbeit. Die transkribierten Interviews sowie derer Auswertung können beim Verfasser eingesehen werden.

Ergänzend hierzu wurden die rechtlichen Grundlagen zum Thema Geheimschutz herangezogen und vergleichend analysiert. Dazu zählen insbesondere die Sicherheitsüberprüfungsgesetze sowie die Verschlusssachenanweisungen der jeweiligen Länder. Durch den Vergleich dieser Regelwerke konnten Begriffsbestimmungen, Unterschiede und Abweichungen identifiziert und herausgearbeitet werden. Soweit vorhanden, wurden auch einschlägige Verwaltungsvorschriften und Erlasse der Länder in die Betrachtung einbezogen.

Zur Klärung und Einordnung zentraler Begriffe erfolgte zudem eine Auswertung eines Kommentars zum Sicherheitsüberprüfungsgesetz (SÜG) sowie einschlägiger Fachliteratur aus dem Bereich Sicherheits- und Staatsrecht. Für die Einleitung in das Themenfeld und zur Darstellung der aktuellen sicherheitspolitischen Lage wurden darüber hinaus Publikationen des Bundes herangezogen.

Ziel dieses Arbeitsschrittes war es, die gesetzlichen Grundlagen und den organisatorischen Rahmen zu verstehen, innerhalb dessen kommunale Feuerwehren Geheimschutzmaßnahmen umsetzen müssen.

Die beantragte erweiterte Sicherheitsüberprüfung (SÜ2) des Verfassers war bei Fertigstellung der Facharbeit noch nicht abgeschlossen. Ein Zugriff auf entsprechend klassifizierte Dokumente war daher nicht gestattet.

4 Ergebnisse

Im folgenden Abschnitt werden die Ergebnisse dargestellt, welche sich in den personellen und materiellen Geheimschutz sowie des Sabotageschutzes gliedern lassen (siehe Abbildung 1).

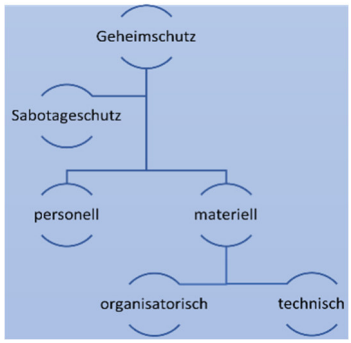

Abbildung 1: Gliederung (eigene Darstellung)

4.1 Rechtliche Grundlagen

In allen Kommunen bilden das jeweilige Landessicherheitsüberprüfungsgesetz und die Landesverschlusssachenanweisung die rechtliche Grundlage. Im weiteren Verlauf verweist der Verfasser auf das Hessische Sicherheitsüberprüfungs- und Verschlusssachengesetz (HSÜVG) und die Verschlusssachenanweisung des Landes Hessen so weit nicht anders erwähnt. Das HSÜVG regelt die Sicherheitsüberprüfung von Personen, die in Bereichen tätig sind, in denen ihnen Zugang zu VS möglich ist oder sicherheitsempfindlichen Tätigkeiten ausgeführt werden (HSÜVG, 2014). Das Gesetz dient dem Schutz von VS sowie von sonstigen sicherheitsempfindlichen Tätigkeiten gegen sicherheitsgefährdende Einflüsse, der sogenannte vorbeugende personelle Sabotageschutz. Das HSÜVG unterscheidet drei Stufen der Sicherheitsüberprüfung:

Tabelle 1: Stufen der SÜ (eigene Darstellung)

SÜ 1	Einfache Sicherheitsüberprüfung	Zugang zu VS-Vertraulich
SÜ 2	Erweiterte Sicherheitsüberprüfung	Zugang zu VS-Geheim
SÜ 3	Erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen	Zugang zu VS-Streng Geheim

Die VSA konkretisiert die materiellen Anforderungen des Geheimschutzes und dient als Verwaltungsvorschrift gemäß des SÜG. Sie legt fest, wie Verschlusssachen eingestuft, gekennzeichnet, behandelt und aufbewahrt werden müssen, um ihre Vertraulichkeit zu wahren. Verschlusssachen sind im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse unabhängig von ihrer Darstellungsform (VSA Hessen, § 2). Die Einstufung erfolgt nach dem möglichen Schadensausmaß, das bei unbefugter Kenntnisnahme für das Land/ den Bund entstehen könnte (VSA Hessen, § 3):

Tabelle 2: VS-Einstufung (eigene Darstellung)

VS-Nur für den Dienstgebrauch (VS-NfD)	Kenntnisnahme für die Interessen nachteilig sein kann
VS-Vertraulich	Kenntnisnahme für die Interessen schädlich sein kann
VS-Geheim	Kenntnisnahme die Sicherheit gefährden oder Interessen schweren Schaden zufügen kann
VS-Streng Geheim	Kenntnisnahme den Bestand oder lebenswichtige Interessen gefährden kann

Die praktische Umsetzung dieser Vorgaben erfordert organisatorische, technische und personelle Maßnahmen, um die Informationssicherheit und die Geheimhaltungspflicht gleichermaßen zu gewährleisten. Unterschiede bestehen in den landesspezifischen Ausführungsverordnungen und Erlassen. Ergänzend werden örtliche Dienstanweisungen oder Geschäftsanweisungen verwendet. In Hessen regelt das Hessische Rettungsdienstgesetz (HRDG) sowie dessen Durchführungsverordnung (RettDGV HE) die Sicherheitsüberprüfung der Bediensteten der Leitstellen. Das Hessische Gesetz über die Sicherheit und Ordnung (HSOG) regelt das Verfahren der Zuverlässigkeitsüberprüfung. Weiterhin regeln die Bundesländer Bayern, Hamburg und Hessen in einer Verordnung zur Bestimmung lebenswichtiger Einrichtungen nach den jeweiligen SÜG, dass unter anderem die Organisationseinheiten des Katastrophen- und Zivilschutzes sowie Organisationseinheiten zur Aufrechterhaltung der inneren Sicherheit – u.a. die Leitstellen (Bayrische Staatsregierung, 2004) - darunter zu zählen sind. Hamburg bestimmt, dass das Unternehmen Dataport, als IT-Dienstleister, als ein sicherheitsempfindlicher öffentlicher Bereich der Informations- und Kommunikationstechnik einzustufen ist (Freie Hansestadt Hamburg, 2020).

4.2 Personeller Geheimschutz

4.2.1 Personenkreis

Übereinstimmend werden leitende Dienstkräfte (Amtsleitungen, A/B-Führungsdienste, Lagedienste), Mitarbeitende der Leitstellen, teilweise Einsatzplaner, Mitarbeitende der Katastrophenschutz-/ Zivilschutzeinrichtungen (untere Katastrophenschutzbehörde), Mitglieder der Analytischen Task Force (ATF) sowie IT-Administratoren überprüft. Die Überprüfungsstufen variieren je nach Zugriffsebene zwischen Verpflichtung nach VS-NfD, SÜ1, SÜ2 und SÜ3. In Mannheim werden auch Mitglieder des Verwaltungsstabes und Fachberater des Stabes nach VS-NfD verpflichtet. Die Feuerwehr Hamburg überprüft alle Bediensteten gem. § 34 HamSÜGG, wobei es sich um eine vereinfachte Sicherheitsüberprüfung durch die Dienststelle ohne Beteiligung des Verfassungsschutzes handelt. Es werden die Sicherheitserklärung und die Personalakte analysiert sowie die Landeskriminalämter des Wohnortes des zu Überprüfenden kontaktiert. In Hessen werden alle Bediensteten der Leitstelle nach der SÜ2 überprüft (Hessisches Ministerium des Innern und für Sport, 2011). Die Feuerwehren, welche Bedienstete für die zivile Verteidigung z.B. Alarmkarteiführer beschäftigen, überprüfen diese nach der SÜ2. Teilweise wird beim Eintritt in die Freiwillige Feuerwehr die Vorlage eines Führungszeugnisses verlangt (Münster).

4.2.2 Befugnisse

In allen Feuerwehren werden vorrangig Unterlagen der Stufe VS-NfD bearbeitet. Die Einstufung der Dokumente erfolgt stets durch die erstellende Stelle, häufig unter Beteiligung der Geheimschutzbeauftragten. Die Befugnisse der überprüften Personen richtet sich nach der VSA der Länder (siehe Tabelle 1). Für die Klassifizierung der Dokumente ist die erstellende Stelle zuständig (Bundesministerium des Innern, für Bau und Heimat, vom 10. August 2021).

4.3 Materieller Geheimschutz

4.3.1 Organisatorischer Geheimschutz

Bis auf die Feuerwehr München besteht derzeit in keiner der befragten Feuerwehren ein vollständig ausgearbeitetes, eigenständiges Geheimschutzkonzept. Die Funktion des Geheimschutzbeauftragten wird, bis auf München, nur im Nebenamt ausgeführt.

Der Geheimschutzbeauftragte der Feuerwehr Braunschweig ist über die Feuerwehr hinaus für die gesamte Stadtverwaltung zuständig. München verfügt über eine zentrale und institutionell fest verankerte Struktur mit klar geregelten Zuständigkeiten zwischen Direktorium (Geheim- und Sabotageschutzbeauftragte), Branddirektion und Leitstelle (Sachbearbeitung für den Geheimschutz) sowie über ein Informationssicherheitsmanagement. Bei vielen der befragten Dienststellen befindet sich die Einrichtung der Geheimschutzbeauftragten mit festen Stellenanteilen oder als Vollzeitstelle im Aufbau.

Alle Dienststellen verfügen über einen Informationstechniksicherheitsbeauftragten (IT-Sicherheitsbeauftragter).

4.3.1.1 Verfahren der Sicherheitsüberprüfung

Das Verfahren wird in allen Kommunen durch den jeweiligen Geheimschutzbeauftragten eingeleitet. Die Bearbeitungsdauer schwankt zwischen 3 Monaten (Münster) und bis zu 24 Monaten (Frankfurt), abhängig von Bundesland und Verfahrenskomplexität sowie Mitarbeit des zu Überprüfenden. Die zu Überprüfenden haben zunächst einen Fragebogen (Sicherheitserklärung) auszufüllen und eine Einverständniserklärung abzugeben. Die Geheimschutzbeauftragten legen eine Sicherheitsakte an. Die Verwahrung ist in den Dienststellen unterschiedlich geregelt (z.B. Mannheim beim Rechtsamt). Die Überprüfung erfolgt in Zusammenarbeit mit den Landesämtern für Verfassungsschutz, welche ein Votum abgeben. Die letztendliche Entscheidung liegt bei dem Geheimschutzbeauftragten. In Braunschweig leitet der Geheimschutzbeauftragte das Verfahren ein, übergibt es dann aber der Polizeidirektion, welche das Verfahren weiterführt. Die Verpflichtung nach VS-NfD wird durch den Geheimschutzbeauftragten durchgeführt und kann daher unmittelbar erfolgen. In der BayVSA Anlage 7 ist ein Merkblatt über die Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NfD anhänglich (Freistaat Bayern, Innenministerium, 1995).

4.3.2 Technischer Geheimschutz

4.3.2.1 IT-Sicherheitsvorkehrungen

Die Umsetzung des IT-Sicherheitsstandards ist unterschiedlich ausgeprägt. Während München und Hamburg über etablierte ISMS verfügen (ISO 27001/BSI-Grundschutz), existieren in anderen Städten (z. B. Braunschweig, Mannheim) lediglich geplante oder teils isolierte Maßnahmen. Nicht in allen Dienststellen ist die Verarbeitung und Speicherung von VS-NfD oder höherwertig eingestuften Dokumenten in den IT-Systemen möglich, lediglich der verschlüsselte Versand. Die Feuerwehr Mannheim plant eine Ausschreibung für ein Dokumentenmanagementsystem inklusive VS-Dokumentenmanagement.

4.3.2.2 Räumliche Sicherheitsmaßnahmen

Sämtliche Feuerwehren setzen auf Zutrittsbeschränkungen, Zugriffsbeschränkungen, verschlossene Aufbewahrung von Dokumenten und den Einsatz von VS-Registraturen oder Safes, soweit diese klassifizierten Dokumente vorgehalten werden, gemäß der jeweils geltenden VSA. Dies erfolgt entweder in den Dienststellen der Feuerwehren oder an einer Stelle innerhalb der Stadtverwaltung. In München und Frankfurt sind gesonderte Sicherheitsbereiche eingerichtet; andere Städte planen die Umsetzung im Rahmen künftiger Geschäfts-/ Dienstanweisungen.

4.4 Sabotageschutz

Der Sabotageschutz ist in den meisten Fällen mit dem IT- und Zugangsschutz, wie Zugriffsbeschränkungen und Zugangsbeschränkungen verknüpft. Typische Maßnahmen sind Zutrittskontrollen, Kameraüberwachung, Torsteuerung oder das offensichtliche Tragen von Dienstausweisen auf den Feuer- und Rettungswachen. Fremdkräfte erhalten nur begleitet Zutritt. Teilweise existieren Pförtnerdienste. Die

Leitstellen und deren Technikräume sind besonders gesicherte Bereiche und der Zutritt erfolgt mehrheitlich über eine Schleuse. Der vorbeugende personelle Sabotageschutz orientiert sich an der unter Punkt 4.2.1 aufgeführten Maßnahmen durch die Sicherheitsüberprüfungen der Funktionsträger.

Als Notfallmaßnahmen dienen Rückstufungen, Notanlaufsysteme, Notfallpläne oder die Inbetriebnahme eines Ausweichsitzes für Leitstellen und Krisenstäbe. Ein Business-Continuity-Management-System ist in München nach Standard 200-4 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vorhanden.

5 Diskussion

Die Interviews zeigen deutlich, dass der Geheimschutz in deutschen Großstadtfeuerwehren aufgrund des föderalen Systems noch keine einheitliche organisatorische Reife erreicht hat.

Während rechtliche Grundlagen und Zuständigkeiten vorhanden sind, unterscheiden sich Struktur, Ressourcenausstattung und Verfahrensqualität erheblich.

Zentral ist die Beobachtung, dass der Geheimschutz häufig als Nebenaufgabe wahrgenommen wird. Mit entsprechend begrenzten personellen, finanziellen und organisatorischen Kapazitäten erschwert dies die Umsetzung der Vorgaben der Rahmenrichtlinie Gesamtverteidigung (RRGV) (Bundesministerium des Innern und für Heimat & Bundesministerium der Verteidigung [BMVg], vom 5. April 2023) sowie der Konzeption Zivile Verteidigung (KZV) (Bundesministerium des Innern [BMI], 2016). Lediglich München zeigt eine institutionalisierte, ressortübergreifende Einbindung, die dem tatsächlichen Sicherheitsbedarf entspricht.

Es gibt keine einheitlichen Vorgaben welche Dokumente als VS einzustufen sind. Grundsätzlich sind Verschlusssachen geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, welche zum Nachteil oder schädlich für ein Schutzgut sein kann (§ 2 Abs. 1 VSA Hessen). Für die Feuerwehr betrifft dies die Innere Sicherheit (Heintschel-Heinegg, 2022). Die erstellende Stelle ist für die Einstufung zuständig (§ 15 VSA Hessen). Hier ist es hilfreich vorher festzulegen, welche Dokumente in einer Feuerwehr, in welcher Form, einzustufen sind. Zum Beispiel ist ein Einsatzplan für einen Weihnachtsmarkt als VS-NfD einzustufen, da die Information eines Bereitstellungsraumes für Rettungsmittel im Fall eines terroristischen Anschlages als Ort für einen Second Hit verwendet werden könnte. Eine Einstufung ist nicht zulässig, um die Informationen nur vor der Öffentlichkeit zu verbergen. Diese Informationen sind der Öffentlichkeit zu verwehren, wenn sie entweder als Verschlusssache eingestuft sind oder das Bekanntwerden der Information die öffentliche Sicherheit gefährden würde (Bundesministerium der Justiz und für Verbraucherschutz, vom 19. Juni 2023). Die Feuerwehr hat ebenfalls im Rahmen einer regelmäßigen Risikoanalyse zu reflektieren, welche Daten öffentlich zur Verfügung gestellt werden. Durch Open Source Intellegence (OSINT) Tools lassen sich sicherheitsrelevante Informationen, zum Beispiel über Social Media geteilte Informationen zu technischen Anlagen oder Ausrüstungen einer Feuerwehr, missbrauchen, um gezielte Angriffe auf Kritische Infrastrukturen zu verüben (J., 2025). Nach dem Grundsatz „Kenntnis nur wenn nötig“, lässt sich durch organisatorische Maßnahmen auch schon der Personenkreis eingrenzen. So werden in Braunschweig Einsatzunterlagen für Lebensbedrohliche Einsatzlagen (LEBEL), welche nicht VS eingestuft sind, in einem verschlossenen Umschlag im Einsatzfahrzeug vorgehalten und nur bei Bedarf geöffnet. Auch in Hamburg ist der Zugriff auf diverse Einsatzunterlagen auf bestimmte Einsatzfunktionen (Führungsdienste/ Fahrzeugführer) begrenzt.

Die Folgen einer Einstufung eines Dokumentes sind weiter zu betrachten. So hat dies Auswirkungen auf die Bearbeitung (Speicherung, Versendung) gemäß der VSA sowohl auch auf den personellen Geheimschutz.

Für nicht eingestufte Dokumente ist der Beamte zur Verschwiegenheit verpflichtet (Gesetz zur Regelung des Statusrechts der Beamtinnen und Beamten in den Ländern, vom 19. Juni 2023). Darüber hinaus ist eine Verpflichtung nach VS-NfD oder eine SÜ gem. dem SÜG notwendig.

Diese SÜ kann auf Grundlage des Geheimschutzes, entweder aufgrund einer sicherheitsempfindlichen Tätigkeit im Umgang mit Verschlusssachen oder aufgrund einer sicherheitsempfindlichen Tätigkeit, an einer sicherheitsrelevanten Stelle, in einer lebenswichtigen Einrichtung gefordert werden (Hessisches Sicherheitsüberprüfungs- und Verschlussachengesetz (HSÜVG), 2014). Ziel des vorbeugenden personellen Sabotageschutzes ist der Schutz vor Innentätern (Heintschel-Heinegg, 2022). Tätig sein

bedeutet, „wer Zugang, Zutritt oder Zugriff hat“. Dies schließt zum Beispiel Reinigungskräfte, Techniker, Handwerker in Leitstellen ein, soweit sie nicht während der Reinigungstätigkeit beobachtet werden können.

Die Länder Hessen, Hamburg und Bayern haben zur Definition der „Lebenswichtigen Einrichtung“ Verordnungen und Erlasse herausgegeben. Hierzu zählen insbesondere die Leitstellen, Einrichtungen der Informations- und Kommunikationstechnik sowie des Bevölkerungsschutzes. Nicht abschließend geklärt sind jedoch die Anforderungen an die SÜ der auch unterhalb einer Katastrophe oder Spannungs- bzw. Verteidigungsfalles agierenden Stäbe der Feuerwehr (operativ-taktisch) und der Verwaltung (administrativ-organisatorisch). Hier wäre eine bundeseinheitliche Definition angebracht. Insbesondere unter dem Blickwinkel der organisations-, bundes- und länderübergreifenden Zusammenarbeit. Hierzu erfolgen gerade Anpassungen der Rechtsgrundlagen der Zivilen Verteidigung (ZV) mit dem Ziel die Handlungs- und Planungssicherheit für die erforderlichen Maßnahmen der ZV umsetzen zu können (Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung (BABZ), 2024). Weiterhin sind insbesondere die Einsatzkräfte bzw. Leitungskräfte der Katastrophenschutzeinheiten sowie der Medizinischen Task Force (MTF) zu berücksichtigen.

Die SÜ stellt für den Betroffenen einen erheblichen Eingriff in die Grundrechte dar (Heintschel-Heinegg, 2022) und bedarf daher dessen Zustimmung (Bundesministerium der Justiz und für Verbraucherschutz, 1994). Bedienstete, bei denen eine Entscheidung negativ ausgefallen ist oder welche die Einwilligung verweigern, darf die sicherheitsempfindliche Tätigkeit nicht übertragen werden. Die Bediensteten sind daher auf einer anderen Funktion innerhalb der Feuerwehr oder Stadtverwaltung einzusetzen. Dies kann gerade in personell dünn besetzten Bereichen wie Leitstellen zu weiteren Engpässen führen. Ergebnisse aus der SÜ können auch zu Erkenntnissen führen, die eine Einleitung eines Disziplinarverfahrens notwendig machen. Die Bereitschaft zur Sicherheitsüberprüfung muss daher zwingend in die Stellenausschreibung mit aufgenommen werden.

Die Dauer der Sicherheitsüberprüfungen wird als erhebliche Verwaltungsbelastung wahrgenommen. Neben dem Verwaltungsaufwand (Auswertung der Sicherheitserklärungen, dem Führen von Sicherheitsakten) verzögert die Beteiligung der Verfassungsschutzämter der Länder das Verfahren erheblich. Dies führt in Einzelfällen zu Funktionslücken in sicherheitsempfindlichen Bereichen. Eine Möglichkeit einer vorab vereinfachten Sicherheitsüberprüfung gem. § 34 HamSÜGG wäre eine Variante um den Vorgaben des vorbeugenden personellen Sabotageschutzes gerecht zu werden und zudem die Verfassungstreue der jeweiligen Landesverfassung sowie des Grundgesetzes abzufragen. Diese Möglichkeit besteht auch in Hessen. Die Zuverlässigkeitsüberprüfung ist ein vereinfachtes Verfahren durch die Polizeibehörde, wenn Bedienstete in besonders gefährdeten Liegenschaften öffentlicher Stellen beschäftigt werden sollen (Hessisches Gesetz über die Sicherheit und Ordnung [HSOG], vom 21. Juni 2018 (GVBl. S. 291)). Denkbar wäre auch ein analoges Vorgehen wie im „Entwurf des Gesetzes zur Stärkung des personellen Schutzes in der Bundeswehr“ vorgesehen. In diesem wird bei der Einstellung eines Soldaten ein vereinfachtes Überprüfungsverfahren u.a. auf die Verfassungstreue durch eine Abfrage in einem Nachrichtendienstlichen Informationssystem (NADIS) und im Bundeszentralregister sowie einem Screening von öffentlichen Quellen (Social Media) durchgeführt wird (Deutscher Bundestag, 2025).

Die technische und bauliche Umsetzung unterscheidet sich stark zwischen den Feuerwehren. Während München über abgestimmte IT-Sicherheitsmanagementsysteme (ISO 27001) und definierte Prozesse zur Behandlung von VS-Dokumenten verfügt, befinden sich andere Kommunen noch im Aufbau oder in der Planungsphase. Andere setzen IT-Dienstleister wie Dataport ein (Hamburg).

Die Cyberangriffe auf Kommunen (Bundesamt für Sicherheit in der Informationstechnik [BSI], 2024) waren Auslöser, dass die Fachgruppe IT-Security des Deutschen Feuerwehrverbandes in Zusammenarbeit mit dem BSI eine Checkliste zum Weg in die Basisabsicherung (WiBA) erstellt hat. Diese richtet sich an Leitstellen, kommunale stationäre (TEL) und mobile (ELW2) Befehlsstellen sowie kommunale Feuerwehren mit ihrer IT-Infrastruktur in den Gerätehäusern. Sie hilft dabei potenzielle IT-Bedrohungen zu erkennen und Maßnahmen zur Mitigation zu identifizieren (Bundesamt für Sicherheit in der Informationstechnik, 2024).

Weiterhin muss betrachtet werden, dass nicht nur die IT-Systeme vor Angriffen durch Externe und Innentätern geschützt sind, sie muss für die Bearbeitung von VS-eingestuften Dokumenten geeignet sein. Hierfür gibt es die Technischen Leitlinien des BSI (SecOPs). Zudem ist darauf zu achten, dass auch der Kommunikationspartner bei Versand von VS-Dokumenten geeignete Systeme vorhält. Dies führt aktuell zu

Problemen beim Versand von ressortübergreifenden Organisationen oder Behörden, wie das als VS-NfD eingestuften Gemeinsame Lagebild des Bevölkerungsschutzes der GeKoB (Bundesregierung, 2022). Wenn zwar der verschlüsselte Versand gewährleistet ist, bleibt die Frage, ob dieses Dokument in den IT-Systemen des Empfängers weiterverarbeitet werden darf. Für höher eingestufte Dokumente sind weitere Maßnahmen zu planen. So halten einige Dienststellen (München, Frankfurt) spezielle Systeme vor. Um die Richtlinie für das zivile Melde- und Lagewesen (ZAPRL) umsetzen zu können ist eine standardisierte Kommunikation durch den Bund geplant. Ziel ist es, flächendeckende Daten- und Kommunikationsmittel bis VS-NfD, für die zivile Verteidigung einzuführen um Akteure in Bund, Ländern und Kommunen zu vernetzen (Bundesministerium des Innern [BMI], 2016).

„Nach dem Prinzip der mehrschichtigen Sicherheit müssen personelle, organisatorische, materielle und technische Maßnahmen getroffen werden, die in ihrem Zusammenwirken Risiken eines Angriffs reduzieren (Prävention), Angriffe erkennbar machen (Detektion) und im Falle eines erfolgreichen Angriffs die negativen Folgen begrenzen (Reaktion)“ (Bundesamt für Sicherheit in der Informationstechnik, 2023).

Daher empfiehlt es sich die Synergien aus dem IT-Sicherheitsmanagementsystem in einem Business Continuity Management System (BCM) zu nutzen. Das BCM hat das Ziel, abgestuft nach einer Störung, einem Notfall oder einer Krise, die Ausfälle des Dienstbetriebes gering zu halten und im Schadensfall angemessene Möglichkeiten zur Weiterführung des Dienstbetriebes vorzubereiten. Dies erfolgt durch organisatorische, technische, bauliche und personelle Maßnahmen. Abschließend sollte jede Dienststelle über ein internes Krisenmanagement, im Rahmen einer besonderen Aufbauorganisation, wie eines Stabes verfügen (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2023).

6 Fazit

Geheimschutz ist in deutschen Großstadtfeuerwehren rechtlich hinreichend gerahmt, in Teilen jedoch nicht hinreichend definiert sowie organisatorisch uneinheitlich verankert. Häufig bleibt er Nebenaufgabe mit spürbaren Folgen für Tempo, Qualität und Verlässlichkeit in sicherheitsempfindlichen Bereichen. München belegt, dass eine institutionalisierte, ressortübergreifende Einbindung mit klaren Zuständigkeiten, VS-fähigen Prozessen und ISMS/ BCM-Anbindung machbar ist und Maßstab sein sollte.

Wer den Geheimschutz nachhaltig stärken will, muss an drei entscheidenden Punkten ansetzen. Zunächst die verbindliche Organisation: Hauptamtliche Geheimschutzbeauftragte mit definierten Stellenanteilen, ein abgestimmtes Rollenmodell (inkl. IT-Sicherheits- und Sabotageschutz) sowie ein hausinterner Einstufungskatalog für typische Dokumente der Feuerwehr (z. B. Einsatzpläne, Stabsunterlagen, KRITIS-Bezüge) schaffen Klarheit. Nach dem Prinzip „Kenntnis nur wenn notwendig“ sind Zugriffe zu begrenzen; ausdrücklich auch für scheinbar periphere Rollen (z. B. Reinigungsdienste in Leitstellen).

Des Weiteren rechtssichere und zügige Personalprozesse: Sicherheitsüberprüfungen (VS-NfD/ SÜ1–SÜ3) sind unverzichtbar, zugleich eingriffsintensiv und ressourcenbindend. Daher gehören Einwilligung und Bereitschaft zur SÜ in jeder Stellenausschreibung; negative Voten sind durch geordnete Umsetzung auf nicht sicherheitsempfindliche Funktionen abzufedern. Wo rechtlich vorgesehen, beschleunigen vereinfachte Vorprüfungen (z. B. nach landesrechtlichen Modellen) die Besetzung kritischer Funktionen, ohne das Schutzziel des vorbeugenden personellen Sabotageschutzes zu unterlaufen.

Zuletzt technisch- materielle Befähigung: VS-fähige IT-Arbeitsplätze und Kommunikationswege (mind. VS-NfD), getrennte Sicherheitsbereiche, definierte Registratur- und Aufbewahrungsprozesse sowie ein wirksames Business-Continuity-Management nach dem Mehrschichtenprinzip (organisatorisch, personell, technisch, baulich) sind flächendeckend aufzubauen. Entscheidend ist die Interoperabilität: VS-Dokumente dürfen nicht am Schnittstellenproblem zwischen Behörden scheitern.

Wer Einsatz- und Führungsfähigkeit in Krisenlagen sichern will, muss Geheim- und Sabotageschutz als Führungsaufgabe begreifen. Dies beinhaltet klare Strukturen, standardisierte Verfahren, qualifiziertes Personal und VS-taugliche Technik. So wird aus formaler Pflicht gelebte Resilienz im Sinne der Kritischen Infrastruktur und Zivilen Verteidigung.

Teil II: Methoden-, Literatur- und Quellendokumentation

1 Beschreibung der Methodik

In den folgenden Punkten werden die Begründung der Methodik und die Literatur- und Quellendokumentation aufgezeigt.

Zur Beantwortung der Problemstellung wurde ein kombiniertes methodisches Vorgehen gewählt, das qualitative Datenerhebung mit einer systematischen Analyse der rechtlichen und fachlichen Grundlagen verbindet. Diese Vorgehensweise war erforderlich, da der Geheimschutz im Kontext kommunaler Feuerwehren ein spezifischer Bereich einer speziellen Organisation ist, in dem sowohl fachpraktisches Erfahrungswissen als auch normgebende Regelwerke eine zentrale Rolle spielen.

Die zentrale Erhebungsmethode bildeten qualitative Experteninterviews. Sie eignen sich besonders für Themenfelder, bei denen Wissen stark an Funktionsträger gebunden ist und nicht in veröffentlichter Form vorliegt. Flick (2019) betont, dass qualitative Interviews sinnvoll sind, wenn spezifisches, erfahrungsgebundenes Wissen erhoben werden soll, das in organisationalen Kontexten angesiedelt ist.

Die Interviews wurden semistrukturiert durchgeführt. Dieses Vorgehen folgt der qualitativen Forschungspraxis, bei der ein Leitfaden Orientierung bietet, aber gleichzeitig genügend Offenheit gewährleistet, um relevante Zusatzinformationen zu gewinnen (Flick, 2019).

Die befragten Expertinnen und Experten waren Geheimschutzbeauftragte von Berufsfeuerwehren, kommunalen Behörden sowie sicherheitsrelevanten Landesstellen. Ihre unmittelbare Zuständigkeit macht sie zu „Experten im Sinne der Funktionsgebundenheit“ (Flick, 2019), was für das hochspezialisierte Themenfeld Geheimschutz essenziell ist.

Ergänzend wurde eine dokumentenbasierte qualitative Inhaltsanalyse vorgenommen (Mayring, 2015).

Diese Methode dient der systematischen, regelgeleiteten Auswertung von Dokumenten und ist in der Verwaltungs- und Sicherheitsforschung etabliert. Die Analyse erfolgte dabei den Strukturierungs- und Kategorisierungsprinzipien der Inhaltsanalyse nach Mayring (2015).

Durch die Kombination von Expertenwissen und normativen Dokumenten konnten theoretische Grundlagen und praktische Erfahrungswerte zusammengeführt werden, um organisationsspezifische Fragestellungen zum Thema Geheim- und Sabotageschutz fachlich valide zu bearbeiten.

2 Begründung

2.1 Literaturrecherche

Die Literaturrecherche bildet die methodische Grundlage dieser Facharbeit. Ziel war es, die rechtlichen und organisatorischen Rahmenbedingungen von Geheimschutzkonzepten im öffentlichen Dienst, insbesondere in sicherheitsrelevanten Bereichen, wie der Gefahrenabwehr und dem Bevölkerungsschutz, systematisch zu erfassen. Im Mittelpunkt standen dabei die Vorgaben der Sicherheitsüberprüfungsgesetze (SÜG) sowie die Verschlusssachenanweisungen (VSA) der Länder. Ziel der Recherche war es, ein praxisorientiertes Verständnis zu entwickeln, wie diese Regelungen in Behörden und Organisationen mit Sicherheitsaufgaben (BOS) angewendet werden können.

Die Literaturrecherche erfolgte schrittweise und zielgerichtet. Zunächst wurden Primärquellen (Gesetze, Verordnungen, Verwaltungsvorschriften) identifiziert, anschließend Sekundärquellen (Fachliteratur, Kommentare, Veröffentlichungen von Behörden) analysiert.
Durch diese Kombination sollte gewährleistet werden, dass sowohl der rechtliche Rahmen als auch die praktische Umsetzung des Geheimschutzes angemessen berücksichtigt werden.

Die Recherche dieser Quellen erfolgte über die offiziellen Rechtsportale www.gesetze-im-internet.de oder der Portale der Länder. Zusätzlich wurden einschlägige Verwaltungsvorschriften und Bekanntmachungen über die Websites der Innenministerien und nachgeordneter Behörden der Länder gesichtet.

Zur Ergänzung der Primärquellen wurden Sekundärquellen ausgewertet, um die rechtlichen Vorgaben in den fachlichen Kontext von Informationssicherheit und Verwaltungsorganisation einzuordnen. Dazu zählten:

- Kommentare und Fachliteratur zum Sicherheitsüberprüfungsgesetz,

- Veröffentlichungen des Bundesamtes für Verfassungsschutz (BfV),
- Fachbeiträge und Arbeitshilfen des Bundesministeriums des Innern und für Heimat (BMI),
- Fachaufsätze aus sicherheits- und verwaltungsbezogenen Zeitschriften (BBK, BABZ),

Die Auswertung erfolgte inhaltlich-thematisch, indem zentrale Aussagen zu gesetzlichen Grundlagen, Zuständigkeiten und organisatorischen Anforderungen kategorisiert wurden.
Alle Quellen wurden im Literaturverzeichnis vollständig nachgewiesen.

2.2 Experteninterviews

Zur Beantwortung der Forschungsfrage wurden zunächst alle deutschen Städte und Stadtstaaten mit mehr als 250.000 Einwohnerinnen und Einwohnern identifiziert (Statistisches Bundesamt, 2025) und mit der Liste der bestehenden Berufsfeuerwehren abgeglichen (Arbeitsgemeinschaft der Berufsfeuerwehren in Deutschland (AGBF), 2025). Auf diese Weise ergab sich eine Auswahl von 29 Berufsfeuerwehren, die sich auf zehn, der sechzehn Bundesländer, verteilten. Um eine ausgewogene und repräsentative Betrachtung sicherzustellen, wurde aus neun der betroffenen Bundesländer jeweils eine Berufsfeuerwehr als Untersuchungseinheit ausgewählt. Die Feuerwehr Berlin stand leider nicht für ein Interview zur Verfügung. Weiterhin wurde als Vergleich einer großen und kleineren Feuerwehr aus Hessen zwei Feuerwehren betrachtet.

Hierdurch sollte eine repräsentative Spannweite unterschiedlicher Organisationsformen und Verwaltungsebenen abgebildet sowie unterschiedliche rechtliche Grundlagen der Länder verglichen werden. Die Befragung orientierte sich an acht Themenbereichen des Interviewleitfadens, welcher als Anlage hinzugefügt wurde. Eine detaillierte Auflistung der befragten Personen erfolgt unter dem Punkt 3.2.2 der Arbeit. Die transkribierten Interviews sowie derer Auswertung können beim Verfasser eingesehen werden. Zur Beantwortung der Forschungsfragen dieser Facharbeit wurde die qualitative Forschungsmethode der semistrukturierten Experteninterviews gewählt. Diese Methode ermöglicht es, das Wissen und die praktischen Erfahrungen von Fachleuten gezielt zu erfassen und systematisch auszuwerten. Gerade im Themenfeld des Geheimschutzes und der Sicherheitsüberprüfung in Behörden und Organisationen mit Sicherheitsaufgaben (BOS) sind viele relevante Informationen nicht ausschließlich in Gesetzen oder Dienstvorschriften dokumentiert, sondern beruhen auf Erfahrungswissen, Handlungsroutinen und Verwaltungspraxis.

Ziel der Interviews war es, die in der Literatur ermittelten rechtlichen und organisatorischen Grundlagen, um praktische Einschätzungen und Erfahrungen aus der Verwaltungspraxis zu ergänzen. Dadurch sollten bestehende Unterschiede zwischen theoretischer Vorgabe und praktischer Umsetzung identifiziert werden, beispielsweise:

- bei der Anwendung von Verschlusssachenanweisungen in kommunalen Verwaltungen,
- bei der Durchführung von Sicherheitsüberprüfungen nach dem SÜG,
- oder bei der Sensibilisierung von Beschäftigten für den Geheimschutz.

Durch den qualitativen Ansatz konnte ein tieferes Verständnis für die tatsächliche Umsetzung, Probleme und Lösungsansätze im Geheimschutzsystem gewonnen werden.

Die Wahl der semistrukturierten Interviews erfolgte bewusst, um einen Mittelweg zwischen freiem Gespräch und standardisiertem Fragebogen zu schaffen. Diese Form der Datenerhebung ist insbesondere geeignet, wenn:

- komplexe Sachverhalte untersucht werden, die von organisatorischen, rechtlichen und personellen Faktoren beeinflusst werden,
- praktische Erfahrungen und Einschätzungen von Expertinnen und Experten erhoben werden sollen,
- und ein gewisser Leitfaden erforderlich ist, um die Vergleichbarkeit der Ergebnisse sicherzustellen, ohne die Offenheit der Gespräche zu verlieren.

Gerade im Themenfeld des Geheimschutzes ist der Ermessensspielraum der handelnden Personen hoch. Durch die semistrukturierte Form konnte flexibel auf die unterschiedlichen Erfahrungen und Zuständigkeiten der Befragten eingegangen werden.

Die Auswahl der Expertinnen und Experten erfolgte nach dem Prinzip der gezielten Auswahl (purposive sampling). Es wurden Personen befragt, die über spezifische Fachkenntnisse oder Verantwortung im Bereich Geheimschutz verfügen. Dazu zählten überwiegend die Geheimschutzbeauftragten der Feuerwehren.

Durch diese gezielte Auswahl konnte gewährleistet werden, dass die Aussagen auf praktischer Erfahrung und Fachkompetenz beruhen und somit eine hohe Relevanz für die Fragestellung der Facharbeit besitzen.

Die Interviews wurden auf Basis eines vorgefertigten Leitfadens durchgeführt, der offene Fragen zu den zentralen Themenbereichen enthielt:

- rechtliche Grundlagen und Zuständigkeiten,
- praktische Umsetzung von Geheimschutzmaßnahmen,
- Herausforderungen im Alltag und Verbesserungspotenziale.

Der Leitfaden diente als Orientierung, lies jedoch Raum für spontane Vertiefungen und persönliche Einschätzungen, welches eine Umfrage für den Verfasser ausgeschlossen hat.
Die Interviews wurden per Telefon, persönlich oder per E-Mail beantwortet. Die Interviews wurden schriftlich protokolliert und anschließend inhaltlich ausgewertet. Dabei wurden die Aussagen nach Themenfeldern sortiert und mit den theoretischen Grundlagen aus der Literaturrecherche verglichen. Dadurch leistet die Methode einen wesentlichen Beitrag zur validen und praxisorientierten Beantwortung der Problemstellung dieser Facharbeit.

3 Literatur- und Quellendokumentation

3.1 Beschreibung der Literatur- und Quellensuche und der Datenbanken

Zunächst wurden in der Suchmaschine Google Scholar die Suchbegriffe wie unter 3.2.1. eingegeben. Da die Suche keine ergiebigen, auf das Thema bezogenen, Erkenntnisse geliefert hatte, wurde sich zunächst auf die rechtlichen Grundlagen des Geheim- und Sabotageschutzes bezogen. Hierzu diente die landesrechtlichen SÜG und VSA. Teilweise gab es in einigen Ländern hierzu ergangene Verwaltungsvorschriften und Erlasse. Aufgrund der nicht abgeschlossenen SÜ des Verfassers konnte auf VS eingestufte Dokumente nicht zugegriffen werden. Weitere Ausführungen zu den SÜG und VSA der Länder brachte der Kommentar zum SÜG und der VSA des Bundes und ergangene Rechtsprechungen, welche in dem Buch Staats- und Verfassungsrecht aufgeführt sind. Zur Darstellung der Aktualität des Themas wurde auf Publikationen der Bundesbehörden BSI, BABZ und BBK zurückgegriffen. Die Publikationen waren auf den Webseiten abrufbar.

Die Kontaktaufnahme zu den Experten erfolgte über telefonische oder schriftliche Anfrage an die Dienststellen, welche Personen sich inhaltlich mit dem Thema Geheimschutz in der Behörde (Verwaltung oder Feuerwehr selbst) beschäftigen.

3.2 Übersicht über die Ergebnisse der Literatur- und Quellendokumentation 3.2.1 (Schlüsselbegriffe, Anzahl der Treffer etc.)

Tabelle 3: Auswertung der Suchbegriffe

Begriff	Suchmaschine	Anzahl der Treffer
Geheimschutzkonzepte	Google Scholar	1
Geheimschutzkonzepte Feuerwehr	Google Scholar	0
Geheimschutz	Google Scholar	866
Sabotageschutz	Google Scholar	232
Geheime Schutzkonzepte	Google Scholar	165

3.2.2 Experteninterviews

Tabelle 4: Experteninterviews

Stadt	Bundesland	Name	Funktion	Datum
Berlin*	Berlin	Frau Wächter	Abteilung Zentraler Service, Recht, Berliner Feuerwehr	20.08.2025
Bremen	Bremen	Herr Rinners	Mitarbeiter Referat Zivile Verteidigung, Senator für Inneres	02.10.2025
Bremen	Bremen	Herr Schulenberg	Informations- & Kommunikationstechnik, Feuerwehr Bremen	14.10.2025
Hamburg	Hamburg	Herr Heyne	Stellv. Geheimschutzbeauftragter, Feuerwehr Hamburg	14.08.2025
München	Bayern	Frau Sigl	Sachbearbeiterin Geheim- und Sabotageschutz, Branddirektion München	29.08.2025
Frankfurt am Main	Hessen	Frau Stelzer	Geheimschutzbeauftragte, Stadt Frankfurt	10.09.2025
Leipzig	Sachsen	Herr Bessel	Geheimschutzbeauftragter, Feuerwehr Leipzig	15.10.2025
Mannheim	Baden-Württemberg	Herr Eitzer	Abteilungsleiter Bevölkerungsschutz & Krisenmanagement, Feuerwehr Mannheim	19.08.2025
Münster	Nordrhein-Westfalen	Herr Hülsken	Geheimschutzbeauftragter, Feuerwehr Münster	29.09.2025
Wiesbaden	Hessen	Herr Bock	Geheimschutzbeauftragter, Stadt Wiesbaden	17.10.2025
Braunschweig	Niedersachsen	Herr Hörmann	Geheimschutzbeauftragter, Feuerwehr und Stadt Braunschweig	21.09.2025
Kiel	Schleswig-Holstein	Herr Brandau	Geheimschutzbeauftragter Feuerwehr Kiel	18.10.2025

*Die Feuerwehr Berlin stand leider nicht für ein Experteninterview zur Verfügung. Als Begründung wurde angebracht, dass sich ein Geheimschutzkonzept gerade im Aufbau befindet und hierzu keine Äußerungen getroffen werden sollen.

Weiterhin wurden zur Erläuterung der rechtlichen Grundlagen des Geheimschutzes und der Abgrenzung Experteninterviews mit den aufgeführten Personen aus dem Hessischen Innenministerium geführt. Zur Erläuterung der Zusammenarbeit des Feuerwehrverbandes mit dem BSI wurde ein Experteninterview mit Herrn Fick geführt.

Organisation	Name	Funktion	Datum
Deutscher Feuerwehrverband	Herr Fick	Beauftragter für Cybersicherheit	08.09.2025
Hessisches Ministerium des Innern	Frau Schwarz	Stell. Referatsleiterin, Referat Recht, Zivile Verteidigung, Verteidigunsgwesen	25.09.2025
Hessisches Ministerium des Innern	Frau Stewart	Zentralabteilung Organisation und Koordination – Geheimschutz	25.09.2025

3.3 Kriterien der Literatur- und Quellenauswahl

Bei der Auswahl der Literatur wurde auf Aktualität, Verlässlichkeit und Praxisbezug geachtet. Alle verwendeten Quellen wurden nach den Grundsätzen wissenschaftlicher Arbeitsweise geprüft und dokumentiert. Dabei wurde insbesondere auf folgende Kriterien geachtet:

- Gesetzliche und institutionelle Verlässlichkeit (offizielle Herausgeber, z. B. BMI, BfV, Landesministerien),
- Aktualität der Fassungen (Stand 2020–2025),
- Nachvollziehbarkeit und Zitierfähigkeit nach den Zitierregeln des IdF NRW.

Die Auswahl der zu befragenden Feuerwehren erfolgte unter Beachtung folgender Kriterien:

- Größe der Stadt und Struktur der Feuerwehr,
- Vorhandensein oder Bekanntheit eines formalisierten Geheimschutzkonzeptes,
- Bereitschaft zur Mitwirkung durch Auskunft oder Interview.

Weiterhin wurde aus jedem, gemäß der Aufgabenstellung in Frage kommenden Feuerwehr, mind. eine Feuerwehr je Bundesland (bis auf Berlin) befragt, da sich die Themen des Geheim- und Sabotageschutzes auf die jeweiligen unterschiedlichen gesetzlichen Grundlagen der SÜG und VSA beziehen. So konnte ein bundesweiter Vergleich geschaffen werden.

Um weitere Hintergründe zum Thema Geheim- und Sabotageschutz sowie IT-Sicherheit zu erhalten, wurde auf Experten des HMdI und des DFV zurückgegriffen.

3.4 Zusammenfassende Beschreibung der ausgewählten Literatur und Quellen

Für die Bearbeitung des Fachartikels ergaben die Suchergebnisse keine validierten Ergebnisse. So hat der Verfasser auf gesetzlichen Grundlagen des Geheim- und Sabotageschutzes zurückgegriffen. Untermauert wurden diese Erkenntnisse durch das Handbuch Sicherheits- und Staatsschutzrecht und einem Kommentar zum Sicherheitsüberprüfungsgesetz des Bundes.

Diese Literaturen waren notwendig, um die rechtlichen Grundlagen und Begriffsbestimmungen zu verstehen. Wie in der Aufgabenstellung vorgegeben galt es, Geheimschutzkonzepte von Feuerwehren in Städten über 250.000 Einwohnern zu vergleichen. Dies war nur durch die geführten semistrukturierten Interviews möglich. Wobei anzumerken ist, dass die erweiterte Sicherheitsüberprüfung des Interviewers noch nicht abgeschlossen ist und somit nicht auf klassifizierte Dokumente und Informationen zugegriffen werden konnte.

4 Literaturverzeichnis

Arbeitsgemeinschaft der Berufsfeuerwehren in Deutschland (AGBF). (14. Oktober 2025). *www.agbf.de*. Von https://www.agbf.de/berufsfeuerwehren abgerufen

Bayrische Staatsregierung. (2004). *Verordnung zur Bestimmung lebenswichtiger Einrichtungen des Freistaates Bayern [BaySÜBV].* GVBl. S. 406, BayRS 12-3-1-I: Bayrische Staatsregierung. Von https://www.gesetze-bayern.de/Content/Document/BaySUEBV abgerufen

Behm, E. (1/2024). Wie mache ich meine Kommune resilienter gegenüber Cyberangriffen? *Bevölkerungsschutz - Resilienz* , 14-15.

Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung (BABZ). (2024). *Die Konzeption Zivile Verteidigung - Lerneinheit zum Selbstlernen.* Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfen [BBK] & Bundesamt für Sicherheit in der Informationstechnik [BSI]. (2024). *Kommunale IT-Krisen: Handlungsfähigkeit sichern.* Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe & Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Katastrophenschutz und Katastrophenhilfe [BBK]. (01/2024). *Bevölkerungsschutz: Resilienz.* Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe .

Bundesamt für Katastrophenschutz und Katastrophenhilfe. (2011). *Schutz Kritischer Infrastrukturen - Risiko und Krisenmanagement.* Berlin: Bundesministerium des Innern.

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2020). *Informationssicherheit mit System - Der IT-Grundschutz des BSI.* Schneckenlohe: Appel und Klinger Druck & Medien GmbH .

Bundesamt für Sicherheit in der Informationstechnik [BSI]. (2023). *Business Continuity Management, BSI-Standard 200-4.* Köln: Reguvis Fachmedien GmbH. Von 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 abgerufen

Bundesamt für Sicherheit in der Informationstechnik [BSI]. (2024). *DIE LAGE DER IT-SICHERHEIT .* Bonn: BSI. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *BSI-Grundschutz-Kompendium, CON.11.1 Geheimschutz nur für den Dienstgebrauch .* Bonn: BSI. Von https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationssicherheit/IT-Grundschutz/it-grundschutz_node.html abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (19. 09 2023). *www.bsi.bund.de.* Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2023/Umsetzungshinweis_zum_Baustein_CON_11_1_Geheimschutz_VS_NUR_FUER_DEN_DIENSTGEBRAUCH.html abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (15. 02 2024). *www.bsi.de.* Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/WiBA-Feuerwehr.html abgerufen

Bundesministerium der Justiz und für Verbraucherschutz. (1994). *Gesetz über die Voraussetzungen und das Verfahren zur Sicherheitsüberprüfung des Bundes [SÜG].* vom 20. April 1994 (BGBl. I S. 867), zuletzt geändert durch Artikel 8 des Gesetzes vom 4. April 2023 (BGBl. I Nr. 91): Bundesamt für Justiz. Von https://www.gesetze-im-internet.de/s_g/ abgerufen

Bundesministerium der Justiz und für Verbraucherschutz. (vom 19. Juni 2023). *Gesetz zur Regelung des Statusrechts der Beamtinnen und Beamten in den Ländern.* BGBl. I Nr. 160: Bundesamt für Justiz. Von https://www.gesetze-im-internet.de/beamtstg/ abgerufen

Bundesministerium der Justiz und für Verbraucherschutz. (vom 19. Juni 2023). *Informationsfreiheitsgesetz [IFG].* BGBl. I Nr. 160: Bundesamt für Justiz. Von https://www.gesetze-im-internet.de/ifg/ abgerufen

Bundesministerium des Inneren und für Heimat (BMI). (2024). Rahmenrichtlinie Gesamtverteidigung. *GMBl*, Nr. 38, S. 790.

Bundesministerium des Innern [BMI]. (2016). *Konzeption Zivile Verteidigung [KZV].* Berlin: BMI. Von https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/konzeption-zivile-verteidigung.pdf abgerufen

Bundesministerium des Innern [BMI]. (2025). *Verfassungsschutzbericht 2024.* Berlin: Bundesministerium des Innern.

Bundesministerium des Innern. (2011). *Schutz Kritischer Infrastrukturen - Risiko- und Krisenmanagement.* Berlin: Bundesministerium des Innern.

Bundesministerium des Innern und für Heimat & Bundesministerium der Verteidigung [BMVg]. (vom 5. April 2023). *ahmenrichtlinie Gesamtverteidigung [RRGV].* GMBl, Nr. 12–13, S. 324–351: BMVg. Von https://www.gmbi.bund.de/ abgerufen

Bundesministerium des Innern und Für Heimat. (14. 10 2025). *www.bmi.bund.de.* Von https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/RRGV.html abgerufen

Bundesministerium des Innern, für Bau und Heimat. (vom 10. August 2021). *Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA).* GMBl. S. 1123: Bundesministerium des Innern, für Bau und Heimat. Von https://www.gesetze-im-internet.de/vsa_2021/ abgerufen

Bundesregierung. (24. 06 2022). *www.bundesregierung.de*. Von https://www.bundesregierung.de/breg-de/bundesregierung/bbk-gmlz-2054798 abgerufen

Bundesrepublik Deutschland. (in der Fassung der Bekanntmachung vom 25. März 2021 (BGBl. I S. 575), zuletzt geändert durch Artikel 3 des Gesetzes vom 8. Oktober 2023 (BGBl. I Nr. 269).). *Zivilschutz- und Katastrophenhilfegesetz [ZSKG]*. Von https://www.gesetze-im-internet.de/zskg/ abgerufen

Deutscher Bundestag. (21. 01 2025). *Drucksache 20/14595*. Berlin: Bundesanzeiger. Von https://dserver.bundestag.de/btd/20/145/2014595.pdf abgerufen

Deutscher Bundestag. (29. 09 2025). *www.dserver.bundestag.de.* Von https://dserver.bundestag.de/btd/21/018/2101846.pdf abgerufen

Deutscher Feuerwehrverband. (14. 10 2025). *www.feuerwehrverband.de*. Von https://www.feuerwehrverband.de/informationssicherheit-bei-feuerwehren-und-in-leitstellen-schuetzen/ abgerufen

Die Bundesregierung. (2024). *Umsetzungsplanung der Deutschen Strategie zur Stärkung der Resilienz gegenüber Katastrophen.* Berlin: Bundesministerium des Innern und für Heimat.

Flick. (2019). *Qualitative Sozialforschung: Eine Einführung.* Rowohlt.

Freie Hansestadt Hamburg. (2020). *Verordnung zur Bestimmung sicherheitsempfindlicher Bereiche nach dem Hamburgischen Sicherheitsüberprüfungs- und Geheimschutzgesetz [HmbSÜBestVO].* HmbGVBl. 2020, 534: Freie Hansestadt Hamburg. Von https://www.landesrecht-hamburg.de/bsha/document/jlr-S%C3%9CGSBerBestVHA2020pELS abgerufen

Freistaat Bayern, Innenministerium. (1995). *Verschlussachenanweisung für die Behörden des Freistaates Bayern [VSA Bayern].* Von https://www.verfassungsschutz.bayern.de/mam/sonstige_aufgaben/content/vsa.pdf?utm_source=chatgpt.com abgerufen

Freistaat Bayern, Innenministerium. (1995). *Verschlusssachenanweisung für die Behörden des Freistaats Bayern [VSA Bayern].* München: Freistaat Bayern. Von https://www.verfassungsschutz.bayern.de/mam/sonstige_aufgaben/content/vsa.pdf?utm_source=chatgpt.com abgerufen

Heintschel-Heinegg, D. /. (2022). *Handbuch Sicherheits- und Staatsschutzrecht.* München: C.H.Beck GmbH & Co. KG.

Hessische Landesregierung. (2007). *Verordnung zur Bestimmung lebenswichtiger Einrichtungen nach dem Hessischen Sicherheitsüberprüfungsgesetz .* GVBl. I S. 623: Hessiche Landesregierung.

Hessische Landesregierung. (21. 03 2024). *www.hessen.de.* Von https://hessen.de/sites/hessen.hessen.de/files/2021-11/kritis-uebersicht_sektoren-branchen-kdl-prozesse_he.pdf abgerufen

Hessisches Ministerium des Innern und für Sport. (2011). *Verordnung zur Durchführung des Hessischen Rettungsdienstgesetzes [HessRDGDV].* (GVBl. I S. 2). Von https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-RettDGDVHE2011pP1 abgerufen

Hessisches Rettungsdienstgesetz . (16. 12 2010). GVBl. I 2010, 646. Von https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-RettDGHE2010V3P5 abgerufen

Hessisches Sicherheitsüberprüfungs- und Verschlussachengesetz (HSÜVG). (19. 12 2014). GVBl. S. 338. Von https://www.rv.hessenrecht.hessen.de/perma?d=jlr-S%C3%9CGHE2015V3IVZ abgerufen

IDF. (21. März 2023). Anforderungen an die Facharbeit Teil I der Verordnung über die Ausbildung und Prüfung für die Laufbahn des zweiten Einstiegsamtes der Laufbahngruppe 2 des feuerwehrtechnischen Dienstes im Land Nordrhein- Westfalen. Münster, NRW, Deutschland: Selbstverlag.

J., F. R. (03 2025). Digitale Offenheit – reale Risiken: Zur Ambivalenz von Open Source Intelligence: Sabotagepotenziale und die Konsequenzen. *Bevölkerungsschutz*, S. 26-31.

Land Hessen. (vom 21. Juni 2018 (GVBl. S. 291)). *Hessisches Gesetz über die Sicherheit und Ordnung [HSOG].* Wiesbaden: Land Hessen. Von https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-SOGHEV29IVZ abgerufen

Lange, P. (Nr. 1/2025). Noch nicht Krieg, aber auch nicht Frieden - Drei Impulse für die nationale Wehrhaftigkeit und Resilienz. *Arbeitspapier Sicherheitspolitik*, 1.

Mayring. (2015). *Qualitative Inhaltsanalyse: Grundlagen und Techniken (12. Aufl.).* Beltz.

Ministerium des Inneren des Landes Nordrhein- Westfalen. (22. November 2022). *Verordnung zur Änderung des Ausbildungs- und Laufbahnrechts im feuerwehrtechnischen Dienst.* Von www.recht.nrw.de: https://recht.nrw.de/lmi/owa/br_vbl_detail_text?anw_nr=6&vd_id=19554&ver=8&val=19554&sg=0&menu=0&vd_back=N abgerufen

Ministerium des Innern, für Sicherheit und Heimatschutz. (22. 02 2010). Verschlusssachenanweisung für das Land Hessen. Wiesbaden: StAnz. 2010, 934. Von https://www.rv.hessenrecht.hessen.de/bshe/document/VVHE-VVHE000006869 abgerufen

Ruthig, S. &. (2019). *Sicherheitsrecht des Bundes.* München: C.H.Beck.

Senator für Inneres der Freien Hansestadt Bremen. (2016). *Verschlusssachenanordnung des Landes Bremen [VSA Bremen].* Bremen: Senator für Inneres. Von https://www.inneres.bremen.de/ abgerufen

Statistisches Bundesamt. (23. 09 2025). *www.destatis.de.* Von https://www.destatis.de/DE/Themen/Laender-Regionen/Regionales/Gemeindeverzeichnis/Administrativ/05-staedte.html abgerufen

Verordnung zur Bestimmung sicherheitsempfindlicher öffentlicher Bereiche für Sicherheitsüberprüfungen ohne Mitwirkung des Landesamtes für Verfassungsschutz nach dem Hamburgischen Sicherheitsüberprüfungsgesetz. (2004). *Hamburgisches Gesetz- und Verordnugsblatt, Teil I, Nr. 10*, 63-64.

Wahlen, R. D. (2015). *Geheimschutzrecht - Voraussetzungen und Folgen der Einstufung von Informationen als Verschlussachen.* Berlin: Deutscher Bundestag, Wissenschaftliche Dienste.

A. Anhänge

Interviewleitfaden

Organisatorischer Geheimschutz

→ Besteht ein Geheimschutzkonzept? Welche Funktionen sind eingerichtet (z. B. Geheimschutzbeauftragte, VS-Stellenverantwortliche, IT-Sicherheitsbeauftragte)?

Rechtliche Grundlagen

→ Welche gesetzlichen bzw. verwaltungsinternen Grundlagen gelten im jeweiligen Bundesland (z. B. SÜG, VSA, Erlasse, Durchführungsverordnungen)?

Personeller Geheimschutz

→ Welche Personenkreise werden, überprüft oder zur Geheimhaltung verpflichtet (z. B. Stabsleiter, Lagedienstführer, Einsatzbearbeiter)?

→ Gibt es untergeordnete Maßnahmen (Belehrungen, Führungszeugnisse etc.)?

Verfahren der Sicherheits-/Zuverlässigkeitsüberprüfung

→ Wie läuft die Überprüfung ab, wer ist zuständig und wie lange dauert sie?

Befugnisse und Verschlusssachengrade

→ Welche Personen dürfen mit welchen VS-Graden umgehen („VS – Nur für den Dienstgebrauch“, „VS - Vertraulich“, „Geheim“ etc.)?

IT-Sicherheitsvorkehrungen

→ Welche Maßnahmen bestehen (Netzwerktrennung, Zugriffsbeschränkungen etc.)?

→ Wer klassifiziert die Dokumente?

Materieller Geheimschutz

→ Wie erfolgt die sichere Aufbewahrung, Ablage und physische Sicherung von Dokumenten und Datenträgern?

Sabotageschutz

→ Welche physischen, organisatorischen oder technischen Maßnahmen sind vorgesehen, um Sabotage oder Manipulation zu verhindern?