OCTOTHORPE

Leitfaden Drohnen
für Betreiber Kritischer Infrastrukturen in Deutschland

Schutz vor Ausspähung, Sabotage und hybriden Bedrohungen durch unbemannte Luftfahrtsysteme (Unmanned Aircraft System - UAS)

Version 3.6 vom 27.07.2026

Praxisorientierte Empfehlungen auf Grundlage nationaler und internationaler gesetzlicher, normativer und technischer Anforderungen

Open Community Release

Lizenzierung & Nutzungsbedingungen

Creative Commons (CC BY-NC 4.0)

Dieser Leitfaden ist unter einer Creative Commons Namensnennung - Nicht-kommerziell - 4.0 International Lizenz lizenziert.

Das bedeutet für Sie:

Teilen, Bearbeiten & Verbreiten:
Sie dürfen das Dokument in jedem Format oder Medium vervielfältigen, remixen, verändern, darauf aufbauen und weiterverbreiten (z. B. als PDF versenden, herunterladen, ausdrucken oder verlinken).

Unter folgenden Bedingungen:

- Namensnennung (BY): Sie müssen angemessene Urheber- und Rechteangaben machen und den Herausgeber Octothorpe GmbH deutlich als Urheber kennzeichnen.
- Nicht-kommerziell (NC): Sie dürfen das Material nicht für kommerzielle Zwecke nutzen, verkaufen oder in kostenpflichtigen Angeboten/Schulungen verwenden.

Den vollständigen Lizenztext finden Sie unter:
https://creativecommons.org/licenses/by-nc/4.0/deed.de

Kommerzielle Nutzung & Erweiterte Rechte:

Möchten Sie Inhalte dieses Leitfadens für kommerzielle Zwecke nutzen oder anpassen? Kommerzielle Lizenzen und schriftliche Nutzungsrechte können direkt über den Herausgeber angefragt werden:

Bahnhofstraße 5
97828 Marktheidenfeld

www.octothorpe.de kontakt@octothorpe.de

Über diesen Leitfaden

Dieser Leitfaden wurde als unabhängige, praxisorientierte Orientierungshilfe für Betreiber Kritischer Infrastrukturen entwickelt.

Er basiert auf öffentlich verfügbaren gesetzlichen, normativen, technischen und behördlichen Quellen sowie auf Erfahrungen aus den Bereichen Informationssicherheit, KRITIS, OT-Sicherheit, Business Continuity Management und Objektschutz.

Der Leitfaden ist ausdrücklich als Open Community Release ausgelegt und kann durch zukünftige Versionen fortgeschrieben werden.

Versionshistorie

Version	Datum	Freigabestatus	Beschreibung
2.9	06/2026	Entwurf	Konsolidierte Arbeitsversion
3.0	07/2026	Review	Grundlegende Neustrukturierung und inhaltliche Erweiterung
3.6	27.07.2026	Open Community Release	Fachlich und redaktionell überarbeitete Release-Version

Dokumentverantwortung

Herausgeber

Octothorpe GmbH
Bahnhofstraße 5
97828 Marktheidenfeld

Fachliche Gesamtverantwortung und Redaktion

Volker Noë

Mitwirkende

Dr. Andreas Biller, Gerrik Noë, Sophia Noë, Dirk Rodigast, Marco Schüritz, Prof. (FH) Dr. Roger Weninger

Dokumentenstatus

Open Community Release

Nächste planmäßige Überprüfung

Spätestens 12 Monate nach Veröffentlichung oder anlassbezogen bei wesentlichen Änderungen der Bedrohungslage, regulatorischen Anforderungen oder relevanten technischen Entwicklungen.

Inhalt

1 Teil I – Grundlagen und Kontext 10
1.1 Executive Summary 10
1.1.1 Zielsetzung des Leitfadens 10
1.1.2 Wesentliche Erkenntnisse 10
1.1.3 Zielgruppen 11
1.1.4 Aufbau des Leitfadens 11
1.1.5 Zentrale Handlungsempfehlungen 11
1.2 Hinweise zur Nutzung des Leitfadens 12
1.2.1 Nutzung des Leitfadens 12
1.2.2 Hinweise zur Aktualisierung 13
1.3 Zielsetzung und Anwendungsbereich 14
1.3.1 Anlass und Motivation 14
1.3.2 Zielsetzung des Leitfadens 14
1.3.3 Anwendungsbereich 15
1.3.4 Zielgruppen innerhalb der Organisation 15
1.3.5 Einordnung in das Sicherheitsmanagement 16
1.3.6 Rechtliche und normative Einordnung 16
1.3.7 Leitprinzipien 17
1.3.8 Abgrenzung 17
1.3.9 Weiterführende Quellen 18
1.3.10 Kernaussagen für Entscheider 22
1.3.11 Handlungsempfehlungen 22
1.4 Bedrohungsmodell und Gefährdungslage 23
1.4.1 Zielsetzung 23
1.4.2 Bezug zu Managementsystemen und Regelwerken 23
1.4.3 Entwicklung der Bedrohungslage 24
1.4.4 Schutzziele 25
1.4.5 Bedrohungsakteure 26
1.4.6 Typische Angriffsszenarien 27
1.4.7 Angriffsmethoden 28
1.4.8 Auswirkungen auf Kritische Infrastrukturen 28
1.4.9 Taxonomie drohnenbezogener Bedrohungen (UAS Threat Taxonomy) 29
1.4.10 Risikomatrix für Betreiber Kritischer Infrastrukturen 34
1.4.11 Bewertung der Bedrohung 36
1.4.12 Kernaussagen für Entscheider 39
1.4.13 Handlungsempfehlungen 39
1.5 Rechtliche und regulatorische Rahmenbedingungen 40
1.5.1 Zielsetzung 40

1.5.2 Bezug zu Managementsystemen und Regelwerken 40
1.5.3 Hierarchie der Anforderungen 41
1.5.4 BSI-Gesetz, NIS-2 und KRITIS-Dachgesetz 41
1.5.5 Luftverkehrsrecht 43
1.5.6 Strafrecht 43
1.5.7 Datenschutzrecht 43
1.5.8 Arbeits- und Gesundheitsschutz 43
1.5.9 Hausrecht und Objektschutz 44
1.5.10 Rechtliche Grenzen aktiver Gegenmaßnahmen 44
1.5.11 Stand der Technik 45
1.5.12 Kernaussagen für Entscheider 46
1.5.13 Handlungsempfehlungen 46

2 Teil II – Governance und Risikomanagement 47
2.1 Governance und Sicherheitsorganisation 47
2.1.1 Zielsetzung 47
2.1.2 Bezug zu Managementsystemen und Regelwerken 47
2.1.3 Governance-Grundsätze 47
2.1.4 Einbindung in bestehende Managementsysteme 48
2.1.5 Rollen und Verantwortlichkeiten 48
2.1.6 Defence in Depth als Schutzprinzip 50
2.1.7 Melde- und Eskalationswege 51
2.1.8 Dokumentation und Berichtswesen 51
2.1.9 Schulung und Sensibilisierung 52
2.1.10 Kontinuierliche Verbesserung 52
2.1.11 Governance-Reifegradmodell 52
2.1.12 Kernaussagen für Entscheider 54
2.1.13 Handlungsempfehlungen 54
2.2 Schutzbedarfsfeststellung und Risikoanalyse 55
2.2.1 Zielsetzung 55
2.2.2 Bezug zu Managementsystemen und Regelwerken 55
2.2.3 Grundsätze der Risikoanalyse 55
2.2.4 Vorgehensmodell 56
2.2.5 Festlegung des Betrachtungsumfangs 56
2.2.6 Schutzbedarfsfeststellung 57
2.2.7 Identifikation schutzbedürftiger Objekte 57
2.2.8 Bedrohungsanalyse 58
2.2.9 Schwachstellenanalyse 58
2.2.10 Risikobewertung 59
2.2.11 Priorisierung von Maßnahmen 59

2.2.12 Dokumentation 59
2.2.13 Regelmäßige Überprüfung 60
2.2.14 Kernaussagen für Entscheider 61
2.2.15 Handlungsempfehlungen 61

3 Teil III – Risikobehandlung und Schutzmaßnahmen 62
3.1 Organisatorische Schutzmaßnahmen 62
3.1.1 Zielsetzung 62
3.1.2 Bezug zu Managementsystemen und Regelwerken 62
3.1.3 Grundprinzipien 62
3.1.4 Sicherheitsrichtlinien 63
3.1.5 Prozesse und Verfahrensanweisungen 63
3.1.6 Sensibilisierung der Beschäftigten 63
3.1.7 Besucher- und Fremdfirmenmanagement 64
3.1.8 Informationsschutz 64
3.1.9 Zusammenarbeit mit externen Stellen 65
3.1.10 Übungen und Tests 65
3.1.11 Erfolgskontrolle 66
3.1.12 Dokumentation 66
3.1.13 Kernaussagen für Entscheider 67
3.1.14 Handlungsempfehlungen 67
3.2 Bauliche und infrastrukturelle Schutzmaßnahmen 68
3.2.1 Zielsetzung 68
3.2.2 Bezug zu Managementsystemen und Regelwerken 68
3.2.3 Planungsgrundsätze 68
3.2.4 Zonenkonzept 69
3.2.5 Perimeterschutz 69
3.2.6 Schutz kritischer Gebäude 69
3.2.7 Schutz von Freianlagen 70
3.2.8 Sichtschutz und Informationsschutz 70
3.2.9 Schutz kritischer Infrastrukturkomponenten 70
3.2.10 Baustellen und temporäre Einrichtungen 71
3.2.11 Wechselwirkung mit technischen Schutzmaßnahmen 71
3.2.12 Grenzen baulicher Schutzmaßnahmen 71
3.2.13 Kernaussagen für Entscheider 72
3.2.14 Handlungsempfehlungen 72
3.3 Technische Schutzmaßnahmen und Drohnendetektion 73
3.3.1 Zielsetzung 73
3.3.2 Bezug zu Managementsystemen und Regelwerken 73
3.3.3 Grundsätze technischer Schutzmaßnahmen 73

3.3.4 Technische Schutzziele 74
3.3.5 Mehrschichtiges Detektionskonzept 74
3.3.6 Videoüberwachung 74
3.3.7 Drohnendetektion 75
3.3.8 Alarmierung und Leitstellenintegration 79
3.3.9 Protokollierung und Beweissicherung 79
3.3.10 Integration in bestehende Sicherheitsarchitekturen 79
3.3.11 Grenzen technischer Schutzmaßnahmen 80
3.3.12 Aktive Drohnenabwehr 80
3.3.13 Wartung und kontinuierliche Verbesserung 81
3.3.14 Kernaussagen für Entscheider 82
3.3.15 Handlungsempfehlungen 82

4 Teil IV – Betrieb und Reaktion 83
4.1 Ereigniserkennung, Incident Response und Beweissicherung 83
4.1.1 Zielsetzung 83
4.1.2 Bezug zu Managementsystemen und Regelwerken 83
4.1.3 Grundsätze der Incident Response 83
4.1.4 Ereigniserkennung 84
4.1.5 Erstbewertung 84
4.1.6 Klassifizierung des Vorfalls 84
4.1.7 Operative Reaktionsmaßnahmen 86
4.1.8 Zusammenarbeit mit Behörden 87
4.1.9 Beweissicherung 87
4.1.10 Kommunikation 87
4.1.11 Operative Incident-Nachbereitung 88
4.1.12 Dokumentation 88
4.1.13 Kernaussagen für Entscheider 89
4.1.14 Handlungsempfehlungen 89
4.2 Krisenmanagement und Business Continuity Management 90
4.2.1 Zielsetzung 90
4.2.2 Bezug zu Managementsystemen und Regelwerken 90
4.2.3 Grundsätze 90
4.2.4 Einordnung in das Business Continuity Management 91
4.2.5 Ereignisse mit Krisenpotenzial 91
4.2.6 Aktivierung des Krisenmanagements 92
4.2.7 Aufgaben des Krisenstabs 92
4.2.8 Lagebild und Lageführung 93
4.2.9 Schutz kritischer Geschäftsprozesse 93
4.2.10 Notfall- und Wiederanlaufmaßnahmen 94

4.2.11 Kommunikation im Krisenfall 94
4.2.12 Zusammenarbeit mit Behörden 94
4.2.13 Übungen, Tests und Nachbesprechungen 95
4.2.14 Kennzahlen und Wirksamkeitskontrolle 95
4.2.15 Kontinuierliche Verbesserung 95
4.2.16 Kernaussagen für Entscheider 96
4.2.17 Handlungsempfehlungen 96

5 Teil V – Überwachung und Verbesserung 97
5.1 Übungen, Audits und kontinuierliche Verbesserung 97
5.1.1 Zielsetzung 97
5.1.2 Bezug zu Managementsystemen und Regelwerken 97
5.1.3 Grundsätze 97
5.1.4 Übungsplanung 98
5.1.5 Übungsarten 98
5.1.6 Auditierung und Wirksamkeitsprüfung 100
5.1.7 Auditfragen beispielhaft 100
5.1.8 Kennzahlen und Leistungsindikatoren 101
5.1.9 Lessons Learned 101
5.1.10 Maßnahmenmanagement 101
5.1.11 Management Reviews 102
5.1.12 Reifegradmodell für Übungen und Verbesserung 102
5.1.13 Kontinuierliche Verbesserung 103
5.1.14 Kernaussagen für Entscheider 103
5.1.15 Handlungsempfehlungen 103
5.2 Nachbereitung drohnenbezogener Ereignisse 104
5.2.1 Zielsetzung 104
5.2.2 Bezug zu Managementsystemen und Regelwerken 104
5.2.3 Wiederfreigabe betroffener Bereiche 104
5.2.4 Bewertung möglicher Informationsabflüsse 105
5.2.5 Bewertung möglicher Vorbereitungshandlungen 105
5.2.6 Rückführung temporärer Maßnahmen 105
5.2.7 Aktualisierung der Risikoanalyse 106
5.2.8 Dokumentation und Abschlussbewertung 106
5.2.9 Kernaussagen für Entscheider 107
5.2.10 Handlungsempfehlungen 107

6 Teil VI – Anhänge und Arbeitshilfen 108
Anhang A – Rechtsquellen- und Compliance-Matrix 108
Anhang B – Rechts- und Compliance-Kataster 109
Anhang C – Drohnen-Compliance-Checkliste 110

Anhang D – Detektionsverfahren..... 111
Anhang E – Handlungsanweisung bei unklarer Bedrohungslage..... 112
Anhang F – Leitfaden zur Beweissicherung..... 113

1 Teil I – Grundlagen und Kontext

1.1 Executive Summary

1.1.1 Zielsetzung des Leitfadens

Unbemannte Luftfahrtsysteme (Unmanned Aircraft Systems – UAS), umgangssprachlich als Drohnen bezeichnet, haben sich in den vergangenen Jahren zu einer breit verfügbaren und leistungsfähigen Technologie entwickelt. Neben zahlreichen legitimen Einsatzmöglichkeiten können Drohnen auch für Ausspähung, Sabotage, Spionage oder die Vorbereitung weiterer Angriffe auf Kritische Infrastrukturen genutzt werden. Die zunehmende technische Leistungsfähigkeit, sinkende Anschaffungskosten sowie die einfache Verfügbarkeit führen dazu, dass drohnenbezogene Bedrohungen Für Betreiber Kritischer Infrastrukturen sowie weitere Einrichtungen mit erhöhtem Schutzbedarf zunehmend an Bedeutung gewinnen.

Ziel dieses Leitfadens ist es, Betreibern Kritischer Infrastrukturen eine strukturierte und praxisorientierte Orientierungshilfe für den Umgang mit drohnenbezogenen Bedrohungen bereitzustellen. Er fasst den aktuellen Stand der gesetzlichen Anforderungen, behördlichen Empfehlungen, anerkannten Normen und technischen Erkenntnisse zusammen und leitet daraus konkrete Handlungsempfehlungen für die Praxis ab.

Der Leitfaden versteht sich als managementorientiertes Referenzdokument. Er ersetzt keine objektspezifische Risikoanalyse und keine rechtliche Einzelfallbewertung, unterstützt jedoch Verantwortliche dabei, drohnenbezogene Risiken systematisch zu identifizieren, zu bewerten und angemessen zu behandeln.

1.1.2 Wesentliche Erkenntnisse

Aus den ausgewerteten gesetzlichen Regelungen, Normen und Fachveröffentlichungen ergeben sich insbesondere folgende Kernaussagen:

- Drohnen stellen für Kritische Infrastrukturen eine eigenständige und wachsende Bedrohung dar.
- Drohnenangriffe sind häufig Bestandteil hybrider Angriffsszenarien und können mit Cyberangriffen, Sabotage, Desinformation oder Insider-Unterstützung kombiniert werden.
- Ein wirksamer Schutz erfordert das Zusammenwirken organisatorischer, baulicher, technischer und personeller Maßnahmen.
- Technische Detektionssysteme unterstützen die frühzeitige Erkennung von Drohnen, ersetzen jedoch keine organisatorischen Prozesse und qualifizierten Entscheidungen.
- Maßnahmen zur aktiven Einwirkung auf Drohnen unterliegen in Deutschland erheblichen rechtlichen Einschränkungen und bedürfen einer sorgfältigen rechtlichen Bewertung.
- Drohnenbezogene Risiken sollten integraler Bestandteil bestehender Managementsysteme für Informationssicherheit, Business Continuity, Notfall- und Krisenmanagement sein.

1.1.3 Zielgruppen

Der Leitfaden richtet sich insbesondere an:

- Geschäftsführungen und Vorstände,
- Chief Information Security Officer (CISO),
- Informationssicherheitsbeauftragte (ISB),
- Sicherheitsverantwortliche,
- Notfall- und Krisenmanager,
- Werkschutz- und Sicherheitsorganisationen,
- Compliance- und Risikomanagement,
- Facility Management,
- Revisoren und Auditoren,
- beratende Unternehmen sowie Planer sicherheitsrelevanter Einrichtungen.

1.1.4 Aufbau des Leitfadens

Der Leitfaden folgt dem Lebenszyklus eines ganzheitlichen Sicherheitsmanagements. Ausgehend von der Bedrohungsanalyse werden Governance-Strukturen, Risikoanalysen sowie organisatorische, bauliche und technische Schutzmaßnahmen behandelt. Anschließend werden die Behandlung drohnenbezogener Vorfälle, das Krisenmanagement sowie Verfahren zur kontinuierlichen Verbesserung beschrieben. Ergänzende Anlagen stellen praxiserprobte Muster, Checklisten und Bewertungshilfen zur Verfügung.

1.1.5 Zentrale Handlungsempfehlungen

Für Betreiber Kritischer Infrastrukturen sowie weitere Einrichtungen mit erhöhtem Schutzbedarf ergeben sich insbesondere folgende Handlungsempfehlungen:

- drohnenbezogene Risiken in bestehende Risiko- und Sicherheitsmanagementprozesse integrieren;
- Verantwortlichkeiten eindeutig festlegen;
- regelmäßige Risikoanalysen durchführen und fortschreiben;
- organisatorische, bauliche und technische Schutzmaßnahmen risikoorientiert kombinieren;
- Verfahren zur Erkennung, Bewertung und Behandlung drohnenbezogener Vorfälle etablieren;
- Übungen durchführen und Erkenntnisse systematisch in den kontinuierlichen Verbesserungsprozess einfließen lassen.

Der Schutz Kritischer Infrastrukturen gegen drohnenbezogene Bedrohungen ist keine einmalige Maßnahme, sondern eine dauerhafte Managementaufgabe. Der Leitfaden unterstützt Organisationen dabei, ihre Sicherheitsmaßnahmen kontinuierlich an neue Bedrohungen sowie an den Stand der Technik anzupassen.

1.2 Hinweise zur Nutzung des Leitfadens

Der vorliegende Leitfaden ist als praxisorientiertes Referenzdokument aufgebaut. Er kann sowohl vollständig als auch kapitelweise genutzt werden. Die einzelnen Kapitel bauen inhaltlich aufeinander auf, sind jedoch so gestaltet, dass sie bei konkreten Fragestellungen auch unabhängig voneinander verwendet werden können.

Je nach Funktion innerhalb einer Organisation unterscheiden sich die relevanten Inhalte. Die nachfolgende Übersicht soll den Einstieg erleichtern.

Zielgruppe	Besonders relevante Teile
Geschäftsführungen und Vorstände	Teil I Grundlagen und Kontext, Teil II Governance und Risikomanagement, Teil IV Betrieb und Reaktion, Teil V Überwachung und Verbesserung
Informationssicherheitsbeauftragte (ISB), CISO und Informationssicherheit	Teil I bis Teil V
Sicherheitsverantwortliche sowie Werkschutz- und Sicherheitsorganisationen	Teil II Governance und Risikomanagement, Teil III Risikobehandlung und Schutzmaßnahmen, Teil IV Betrieb und Reaktion
Notfall- und Krisenmanagement	Teil II Governance und Risikomanagement, Teil IV Betrieb und Reaktion, Teil V Überwachung und Verbesserung
Compliance-, Risiko- und Datenschutzmanagement	Teil I Grundlagen und Kontext, Teil II Governance und Risikomanagement, Teil IV Betrieb und Reaktion
Facility Management	Teil III Risikobehandlung und Schutzmaßnahmen
Revisoren und Auditoren	Teil II bis Teil V
Beratende Unternehmen sowie Planer sicherheitsrelevanter Einrichtungen	Gesamter Leitfaden

1.2.1 Nutzung des Leitfadens

Der Leitfaden eignet sich insbesondere als Grundlage für:

- die Entwicklung oder Weiterentwicklung von Sicherheitskonzepten,
- Risikoanalysen und Schutzbedarfsfeststellungen,
- Managemententscheidungen,
- interne Audits,
- Schulungen und Sensibilisierungsmaßnahmen,
- Notfall- und Krisenübungen,
- Ausschreibungen und Beschaffungsvorhaben,
- die Vorbereitung auf regulatorische Prüfungen und Audits.

Zusammenhang mit bestehenden Managementsystemen und Regelwerken

Der Leitfaden ist bewusst so aufgebaut, dass er bestehende Managementsysteme und regulatorische Anforderungen ergänzt und keine parallelen Strukturen schafft. Er unterstützt insbesondere die Umsetzung von Anforderungen aus dem Informationssicherheitsmanagement, Business Continuity Management, Risiko- und Krisenmanagement sowie branchenspezifischen Sicherheitsanforderungen.

Die beschriebenen Maßnahmen sind daher grundsätzlich in vorhandene organisatorische Prozesse und Managementsysteme zu integrieren.

Managementsystem / Regelwerk	Relevante Kapitel
ISO/IEC 27001 (ISMS)	1.4 bis 5.2
ISO 22301 (BCM)	2.1, 2.2, 4.1, 4.2, 5.1, 5.2
BSI IT-Grundschutz	1.4 bis 5.2
IEC 62443	1.4, 2.2, 3.3, 4.1, 4.2
BSIG / NIS-2	1.5 bis 5.2
Branchenspezifische Sicherheitsstandards (B3S)	1.4 bis 5.2
KRITIS-Dachgesetz (KRITISDachG)	1.5.4 sowie ergänzend 2.1 bis 5.2

Hinweis: Die Anforderungen des KRITIS-Dachgesetzes betreffen nur einen Teil der Zielgruppe dieses Leitfadens. Betreiber kritischer Anlagen sollten daher zusätzlich prüfen, inwieweit drohnenbezogene Bedrohungen im Rahmen von Resilienzbewertungen, Notfallvorsorge, Business Continuity Management und Krisenmanagement zu berücksichtigen sind.

Einordnung in den PDCA-Zyklus

Der Leitfaden orientiert sich an den Grundprinzipien kontinuierlicher Managementsysteme und kann in den Plan-Do-Check-Act-Zyklus (PDCA) bestehender Informationssicherheits-, Resilienz- und Business-Continuity-Managementsysteme eingeordnet werden.

PDCA	Teil	Schwerpunkt
Plan	Teil I + II	Kontext, Governance, Risikoanalyse
Do	Teil III	Umsetzung von Schutzmaßnahmen
Check	Teil IV + V.1	Betrieb, Incident Response, BCM, Audits, Übungen
Act	Teil V.2	Lessons Learned, Nachbereitung, Verbesserungsmaßnahmen

Die Behandlung drohnenbezogener Risiken ist dabei nicht als einmaliges Projekt zu verstehen, sondern als fortlaufender Managementprozess. Erkenntnisse aus Vorfällen, Audits, Übungen, Änderungen der Bedrohungslage oder technischen Entwicklungen sollten regelmäßig in die Weiterentwicklung des Sicherheitskonzeptes einfließen.

1.2.2 Hinweise zur Aktualisierung

Die Bedrohungslage, technische Entwicklungen sowie gesetzliche und normative Anforderungen unterliegen einem kontinuierlichen Wandel. Betreiber Kritischer Infrastrukturen sollten den Leitfaden daher regelmäßig auf Aktualität überprüfen und Erkenntnisse aus Sicherheitsvorfällen, Übungen, Audits sowie neue Veröffentlichungen zuständiger Behörden und Fachorganisationen in ihre Sicherheitskonzepte übernehmen.

1.3 Zielsetzung und Anwendungsbereich

1.3.1 Anlass und Motivation

Die Verfügbarkeit kostengünstiger und leistungsfähiger unbemannter Luftfahrtsysteme (Unmanned Aircraft Systems – UAS), im allgemeinen Sprachgebrauch als Drohnen bezeichnet, hat in den vergangenen Jahren erheblich zugenommen. Parallel hierzu hat sich das Einsatzspektrum dieser Systeme deutlich erweitert. Neben zahlreichen legitimen Anwendungen in Industrie, Vermessung, Logistik, Medien oder Gefahrenabwehr werden Drohnen zunehmend auch für sicherheitsrelevante und kriminelle Zwecke eingesetzt.

Nationale und internationale Sicherheitsbehörden – u. a.
- Bundesamt für Verfassungsschutz (BfV)
- Bayerisches Landesamt für Verfassungsschutz (BayLfV)
- Joint Air Power Competence Centre (JAPCC)
- National Protective Security Authority (NPSA) –

weisen seit mehreren Jahren auf die steigende Bedeutung unbemannter Luftfahrtsysteme als Mittel der Ausspähung, Sabotage und Vorbereitung hybrider Angriffe hin. Aufgrund ihrer hohen Mobilität, geringen Betriebskosten, einfachen Verfügbarkeit sowie der Möglichkeit zum autonomen oder ferngesteuerten Betrieb stellen moderne Drohnen eine ernstzunehmende Bedrohung für Betreiber Kritischer Infrastrukturen und sonstige Einrichtungen mit hohem Schutzbedarf dar.

Die Gefährdung beschränkt sich hierbei nicht auf Angriffe gegen informationstechnische Systeme. Vielmehr können Drohnen sowohl die physische Sicherheit als auch die Informationssicherheit beeinträchtigen und dadurch mittelbar oder unmittelbar die Verfügbarkeit, Integrität und Vertraulichkeit kritischer Geschäftsprozesse gefährden.

1.3.2 Zielsetzung des Leitfadens

Ziel dieses Leitfadens ist die Bereitstellung eines einheitlichen, praxisorientierten und risikobasierten Vorgehensmodells zur Behandlung drohnenbezogener Bedrohungen durch Betreiber Kritischer Infrastrukturen sowie weiteren Organisationen mit vergleichbarem Schutzbedarf.

Der Leitfaden unterstützt Betreiber dabei,
- drohnenbezogene Gefährdungen systematisch zu identifizieren,
- Risiken nachvollziehbar zu bewerten,
- geeignete organisatorische, bauliche und technische Schutzmaßnahmen auszuwählen,
- Sicherheitsvorfälle strukturiert zu bewältigen,
- bestehende Informationssicherheits-, Notfall- und Krisenmanagementprozesse sinnvoll zu ergänzen sowie
- die Resilienz der Organisation gegenüber hybriden Bedrohungen nachhaltig zu stärken.

Der Leitfaden verfolgt dabei ausdrücklich einen risikoorientierten Ansatz. Ziel ist nicht die vollständige Verhinderung jeglicher Drohnenaktivität, sondern die angemessene Reduzierung des Risikos entsprechend dem Schutzbedarf der jeweiligen Einrichtung.

Der Leitfaden verfolgt einen ganzheitlichen Managementansatz. Drohnenbezogene Bedrohungen werden nicht isoliert betrachtet, sondern als Bestandteil des unternehmensweiten Risiko-, Sicherheits-, Notfall- und Krisenmanagements. Ziel ist die Integration in bestehende Managementsysteme und Prozesse, um Doppelstrukturen zu vermeiden und vorhandene Governance-Mechanismen zu nutzen.

1.3.3 Anwendungsbereich

Der Leitfaden richtet sich insbesondere an

- Betreiber Kritischer Infrastrukturen nach dem BSI-Gesetz,
- Einrichtungen, die nach jeweils geltendem Recht unter die NIS-2-Regulierung oder deren nationale Umsetzung fallen,
- Betreiber kritischer Anlagen im Sinne des KRITIS-Dachgesetzes (KRITISDachG),
- Unternehmen mit erhöhtem Schutzbedarf,
- öffentliche Verwaltungen,
- Betreiber sicherheitsrelevanter Industrie- und Energieanlagen,
- Unternehmen mit Forschungs- und Entwicklungsstandorten,
- Einrichtungen mit erhöhtem Geheimhaltungs- oder Sabotageschutz.

Der Leitfaden ist branchenübergreifend anwendbar und kann unabhängig von Größe, Rechtsform oder Organisationsstruktur eingesetzt werden. Art und Umfang der umzusetzenden Maßnahmen richten sich stets nach dem individuellen Schutzbedarf, der konkreten Gefährdungslage sowie den jeweiligen gesetzlichen und regulatorischen Anforderungen.

Hinweis: Der Leitfaden verwendet grundsätzlich den Begriff "Kritische Infrastrukturen" als Oberbegriff. Gesetzliche Begriffe wie "kritische Anlagen" (KRITISDachG) oder "wichtige und besonders wichtige Einrichtungen" (NIS-2) werden verwendet, wenn ausdrücklich auf den jeweiligen Rechtsrahmen Bezug genommen wird.

1.3.4 Zielgruppen innerhalb der Organisation

Die Umsetzung wirksamer Schutzmaßnahmen gegen drohnenbezogene Bedrohungen erfordert eine organisationsübergreifende Zusammenarbeit verschiedener Funktionen.

Der Leitfaden richtet sich insbesondere an

- Geschäftsführung und Unternehmensleitung,
- Chief Information Security Officer (CISO),
- Informationssicherheitsbeauftragte (ISB),
- Business-Continuity-Manager,
- Krisenstabsleitungen,
- Verantwortliche für Werkschutz und Objektsicherheit,
- Leitstellen,
- Facility Management,
- IT-/OT-/ICS-Verantwortliche,
- Sicherheitsdienstleister,
- Datenschutzbeauftragte,
- Compliance-Verantwortliche

1.3.5 Einordnung in das Sicherheitsmanagement

Bedrohungen durch Drohnen sind kein isoliertes Luftfahrtthema.

Sie betreffen gleichzeitig
- die physische Sicherheit,
- die Informationssicherheit,
- die Betriebssicherheit,
- das Business Continuity Management,
- das Notfallmanagement,
- das Krisenmanagement,
- den Wirtschaftsschutz.

Eine wirksame Behandlung drohnenbezogener Risiken setzt daher ein integriertes Sicherheitsmanagement voraus. Die Verantwortung darf weder ausschließlich dem Werkschutz noch ausschließlich der Informationssicherheit übertragen werden. Vielmehr ist eine enge Zusammenarbeit aller betroffenen Fachbereiche erforderlich.

Drohnenbedrohungen sind folglich nicht als eigenständiges Sicherheitsmanagementsystem zu behandeln, sondern in bestehende Managementsysteme (ISMS, BCM, Risiko- und Krisenmanagement) zu integrieren.

1.3.6 Rechtliche und normative Einordnung

Für Deutschland existiert derzeit kein eigenständiges Gesetz, das den organisatorischen Schutz von Betreibern Kritischer Infrastrukturen vor Drohnen umfassend regelt.

Gleichwohl ergeben sich aus verschiedenen Rechtsgebieten und anerkannten Standards Anforderungen, die bei der Planung und Umsetzung geeigneter Schutzmaßnahmen zu berücksichtigen sind. Hierzu zählen insbesondere das BSI-Gesetz, die Vorgaben zur Umsetzung der NIS-2-Richtlinie, luftverkehrsrechtliche Vorschriften, strafrechtliche Bestimmungen, datenschutzrechtliche Anforderungen sowie arbeitsschutzrechtliche Verpflichtungen. Ergänzend bilden etablierte Managementsysteme und technische Regelwerke – insbesondere ISO/IEC 27001, ISO 22301, der BSI IT-Grundschutz, branchenspezifische Sicherheitsstandards (B3S) sowie im Bereich der industriellen Automatisierung IEC 62443 – den maßgeblichen Orientierungsrahmen für die Umsetzung angemessener Sicherheitsmaßnahmen.

Zudem können Anforderungen aus dem allgemeinen Objektschutz, dem Wirtschaftsschutz sowie aus Betreiberpflichten gegenüber Beschäftigten und Dritten mittelbar die Berücksichtigung drohnenbezogener Risiken erforderlich machen.

Der vorliegende Leitfaden ersetzt diese Regelwerke nicht. Er konkretisiert vielmehr deren Anwendung hinsichtlich drohnenbezogener Gefährdungen.

Der Leitfaden basiert auf dem zum Zeitpunkt seiner Erstellung verfügbaren Stand von Gesetzgebung, Normung, behördlichen Veröffentlichungen sowie anerkannten wissenschaftlichen und technischen Fachquellen. Da sich sowohl die Bedrohungslage als auch technische Möglichkeiten der Drohnennutzung und Drohnendetektion kontinuierlich weiterentwickeln, sollte der Leitfaden regelmäßig überprüft und erforderlichenfalls aktualisiert werden.

Es wird empfohlen, insbesondere Änderungen der gesetzlichen Rahmenbedingungen, neue Veröffentlichungen der zuständigen Behörden sowie Erkenntnisse aus Sicherheitsvorfällen und Übungen systematisch in die Fortschreibung des Leitfadens einzubeziehen.

1.3.7 Leitprinzipien

Der Leitfaden basiert auf folgenden Grundprinzipien:

- Risikoorientierung: Art und Umfang der Schutzmaßnahmen richten sich nach Schutzbedarf, Gefährdungslage und möglichen Auswirkungen.
- Defence in Depth (Mehrschichtiger Schutzansatz): Ein wirksamer Schutz gegen drohnenbezogene Bedrohungen kann nur durch mehrere aufeinander abgestimmte organisatorische, personelle, bauliche und technische Schutzebenen erreicht werden. Der Ausfall oder die Umgehung einer einzelnen Maßnahme darf nicht unmittelbar zum Versagen des Gesamtschutzes führen.
- Stand der Technik: Maßnahmen sind regelmäßig auf ihre Wirksamkeit zu überprüfen und unter Berücksichtigung technischer Entwicklungen fortzuschreiben.
- Kontinuierliche Verbesserung: Erkenntnisse aus Vorfällen, Übungen und Änderungen der Bedrohungslage sind systematisch in das Sicherheitsmanagement zurückzuführen.

1.3.8 Abgrenzung

Der Leitfaden behandelt insbesondere

- Ausspähung,
- Sabotage,
- hybride Bedrohungen,
- Vorbereitungshandlungen,
- organisatorische Schutzmaßnahmen,
- technische Schutzmaßnahmen,
- Incident Response,
- Krisenmanagement,
- Übungen,
- Wiederherstellung des Regelbetriebs.

Nicht Gegenstand dieses Leitfadens sind

- militärische Einsatzgrundsätze,
- taktische Verfahren von Polizei und Sicherheitsbehörden,
- operative Counter-UAS-Maßnahmen mit hoheitlichen Eingriffsbefugnissen,
- der Einsatz rechtlich unzulässiger oder genehmigungspflichtiger Abwehrmittel.

1.3.9 Weiterführende Quellen

Verwendete Primärquellen:

- Bundesamt für Verfassungsschutz (BfV): Veröffentlichungen zum Wirtschafts- und Wissenschaftsschutz.
- Bayerisches Landesamt für Verfassungsschutz (BayLfV): Informationsblatt „Schutz vor Ausspähung durch Drohnen“.
- Bundesamt für Sicherheit in der Informationstechnik (BSI): Anforderungen an Betreiber Kritischer Infrastrukturen, BSI IT-Grundschutz und branchenspezifische Sicherheitsstandards.
- Joint Air Power Competence Centre (JAPCC): Drone Drills – How to Prepare for a Drone Incident.
- National Protective Security Authority (NPSA): Counter Uncrewed Aerial Systems (C-UAS) Guidance Suite.
- Bundesverband der Energie- und Wasserwirtschaft (BDEW): Effektive und zukunftssichere Drohnenabwehr für kritische Infrastrukturen – Herausforderungen und gemeinsame Lösungsansätze (Positionspapier, 2025)

Die in diesem Leitfaden herangezogenen Quellen unterscheiden sich hinsichtlich ihrer rechtlichen Verbindlichkeit und ihres normativen Charakters. Gesetzliche und regulatorische Anforderungen bilden den verbindlichen Rahmen. Europäische Rechtsakte wurden entsprechend ihrer jeweiligen Rechtsnatur und ihrem Geltungsanspruch berücksichtigt. Anerkannte Normen konkretisieren den Stand der Technik sowie bewährte Vorgehensweisen. Veröffentlichungen zuständiger Behörden, wissenschaftliche Fachpublikationen und weitere anerkannte Fachquellen dienen der fachlichen Einordnung und Interpretation der Bedrohungslage sowie der Ableitung geeigneter Schutzmaßnahmen. Bei widersprüchlichen Aussagen wurden gesetzliche Anforderungen, europäische Rechtsakte, Veröffentlichungen zuständiger Behörden sowie anerkannte Normen vorrangig berücksichtigt.

1.3.9.1 Veröffentlichungen zum Wirtschafts- und Wissenschaftsschutz

Herausgeber: Bundesamt für Verfassungsschutz (BfV)

Das Bundesamt für Verfassungsschutz (BfV) ist die Inlandsnachrichtendienstbehörde des Bundes. Zu seinen gesetzlichen Aufgaben gehören insbesondere die Spionageabwehr, der Schutz vor extremistischen Bestrebungen sowie der Wirtschafts- und Wissenschaftsschutz. Inhaltliche Schwerpunkte

Die Veröffentlichungen des BfV zum Wirtschafts- und Wissenschaftsschutz beschreiben aktuelle Bedrohungen durch staatliche und nachrichtendienstlich gesteuerte Akteure. Behandelt werden insbesondere Ausspähungsaktivitäten gegen Unternehmen, Forschungseinrichtungen und Kritische Infrastrukturen sowie die hierbei genutzten Methoden und Angriffsmittel.

Die Veröffentlichungen liefern wichtige Erkenntnisse zu Bedrohungsakteuren, Ausspähungsmethoden, hybriden Bedrohungen sowie möglichen Vorbereitungs- und Unterstützungsmaßnahmen für Angriffe gegen Kritische Infrastrukturen.

Weiterführende Informationen: https://www.verfassungsschutz.de

1.3.9.2 Schutz vor Ausspähung durch Drohnen

Herausgeber: Bayerisches Landesamt für Verfassungsschutz (BayLfV)

Das Bayerische Landesamt für Verfassungsschutz (BayLfV) ist die Verfassungsschutzbehörde des Freistaates Bayern. Zu seinen Aufgaben gehören insbesondere die Beobachtung sicherheitsgefährdender Bestrebungen sowie die Beratung von Unternehmen und Behörden zu Fragen des Wirtschaftsschutzes.

Das Informationsblatt „Schutz vor Ausspähung durch Drohnen“ beschreibt typische Aufklärungsszenarien mittels Drohnen, mögliche Angriffsindikatoren sowie organisatorische, personelle und bauliche Schutzmaßnahmen gegen luftgestützte Ausspähung.

Die Veröffentlichung bildet eine wichtige Grundlage für die Bewertung von Ausspähungsrisiken sowie die Entwicklung geeigneter organisatorischer und baulicher Schutzmaßnahmen.

Weiterführende Informationen: https://www.verfassungsschutz.bayern.de

1.3.9.3 Veröffentlichungen zu KRITIS, IT-Grundschutz und Informationssicherheit

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die nationale Cyber-Sicherheitsbehörde Deutschlands und zentrale Stelle für Informationssicherheit sowie Cyber-Resilienz.

Das BSI veröffentlicht Anforderungen an Betreiber Kritischer Infrastrukturen, Standards und Empfehlungen zur Informationssicherheit, den IT-Grundschutz, Standards für Business Continuity Management sowie branchenspezifische Sicherheitsstandards (B3S).
Relevanz für diesen Leitfaden
Die Veröffentlichungen des BSI bilden einen wesentlichen Orientierungsrahmen für Risikoanalysen, Schutzbedarfsfeststellungen, Sicherheitsmaßnahmen, Incident Response, Business Continuity Management sowie die Bewertung des Stands der Technik.

Weiterführende Informationen: https://www.bsi.bund.de

1.3.9.4 Drone Drills – How to Prepare for a Drone Incident

Herausgeber: Joint Air Power Competence Centre (JAPCC)

Das Joint Air Power Competence Centre (JAPCC) ist ein von der NATO unterstütztes Kompetenzzentrum für Luft- und Weltraumoperationen. Es entwickelt Konzepte, Analysen und Handlungsempfehlungen zu aktuellen und zukünftigen Bedrohungen im Luft- und Sicherheitsumfeld.

Die Veröffentlichung „Drone Drills – How to Prepare for a Drone Incident“ beschreibt die Vorbereitung auf Drohnenvorfälle, Alarmierungs- und Eskalationsverfahren, Übungen, Kommunikationsmaßnahmen sowie Verfahren zur Lagebewertung und Ereignisbewältigung.

Die Publikation liefert praxisnahe Ansätze zur Incident Response, Krisenvorsorge, Schulung und Durchführung von Übungen für drohnenbezogene Sicherheitsvorfälle.

Weiterführende Informationen: https://www.japcc.org

1.3.9.5 Counter Uncrewed Aerial Systems (CUAS) Guidance Suite

Herausgeber: National Protective Security Authority (NPSA)

Die National Protective Security Authority (NPSA) ist die britische Fachbehörde für Schutz kritischer Einrichtungen, Sicherheitsberatung und Resilienz. Sie unterstützt Betreiber kritischer und besonders schutzbedürftiger Einrichtungen bei der Entwicklung wirksamer Schutzkonzepte.

Die Counter Uncrewed Aerial Systems (CUAS) Guidance Suite beschreibt Bedrohungsmodelle, Risikoanalysen sowie organisatorische, bauliche und technische Schutzmaßnahmen gegen drohnenbezogene Bedrohungen. Ein besonderer Schwerpunkt liegt auf mehrschichtigen Schutzkonzepten und risikoorientierten Sicherheitsmaßnahmen.

Die Guidance Suite stellt eine der umfassendsten öffentlich verfügbaren internationalen Best-Practice-Sammlungen zum Schutz vor Drohnenbedrohungen dar und liefert wertvolle Impulse für Risikoanalyse, Schutzkonzepte und Sicherheitsorganisation.

Weiterführende Informationen: https://www.npsa.gov.uk

1.3.9.6 Effektive und zukunftssichere Drohnenabwehr für kritische Infrastrukturen – Herausforderungen und gemeinsame Lösungsansätze

Herausgeber: Bundesverband der Energie- und Wasserwirtschaft (BDEW)

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW) vertritt Unternehmen der Energie- und Wasserwirtschaft in Deutschland und engagiert sich für die Sicherheit und Resilienz kritischer Versorgungsinfrastrukturen.

Das Positionspapier beschreibt die aktuelle Bedrohungslage durch Drohnen, Herausforderungen bei autonomen und nicht-kooperativen Systemen sowie Anforderungen an Resilienz, Detektionsfähigkeiten, Lagebilder und standortübergreifende Zusammenarbeit.

Die Veröffentlichung liefert aktuelle Erkenntnisse aus Sicht eines besonders exponierten KRITIS-Sektors und unterstützt die Bewertung zukünftiger Entwicklungen im Bereich drohnenbezogener Bedrohungen und Schutzmaßnahmen.

Weiterführende Informationen: https://www.bdew.de

1.3.10 Kernaussagen für Entscheider

- Drohnen sind als relevante Bedrohungsquelle im unternehmensweiten Risiko- und Sicherheitsmanagement zu berücksichtigen.
- Die Behandlung drohnenbezogener Risiken ist eine interdisziplinäre Aufgabe und erfordert die Zusammenarbeit von Informationssicherheit, Werkschutz, Business Continuity Management, Krisenmanagement und Unternehmensleitung.
- Schutzmaßnahmen sind risikobasiert auszuwählen und in bestehende Managementsysteme zu integrieren.
- Organisatorische Maßnahmen bilden die Grundlage eines wirksamen Schutzkonzeptes und sind regelmäßig durch Übungen und Reviews zu validieren.

1.3.11 Handlungsempfehlungen

Zum Aufbau eines wirksamen Schutzkonzeptes sollten Betreiber Kritischer Infrastrukturen bereits zu Beginn folgende Maßnahmen umsetzen:

- Aufnahme drohnenbezogener Bedrohungen in das unternehmensweite Risiko- und Informationssicherheitsmanagement.
- Benennung eindeutiger Verantwortlichkeiten und Entscheidungswege.
- Integration des Themas in Business Continuity Management, Notfallmanagement und Krisenmanagement.
- Berücksichtigung drohnenbezogener Szenarien in Schutzbedarfsfeststellungen und Risikoanalysen.
- Festlegung eines Programms zur schrittweisen Einführung organisatorischer, baulicher und technischer Schutzmaßnahmen.

1.4 Bedrohungsmodell und Gefährdungslage

1.4.1 Zielsetzung

Ziel dieses Kapitels ist die systematische Beschreibung drohnenbezogener Bedrohungen für Betreiber Kritischer Infrastrukturen und sonstige Einrichtungen mit hohem Schutzbedarf.

Es schafft die Grundlage für die in den nachfolgenden Kapiteln behandelten Risikoanalysen, Schutzbedarfsfeststellungen und Schutzmaßnahmen.

Hierzu werden
- Bedrohungsakteure,
- Angriffsziele,
- Angriffsmethoden,
- Angriffsmittel,
- mögliche Auswirkungen

strukturiert beschrieben.

1.4.2 Bezug zu Managementsystemen und Regelwerken

Dieses Kapitel unterstützt die Analyse interner und externer Einflussfaktoren sowie die Identifikation relevanter Bedrohungen und Risiken.

Relevante Regelwerke:
- ISO/IEC 27001: Kontext der Organisation
- ISO/IEC 27005: Informationssicherheitsrisiken
- ISO 31000: Risikomanagement
- BSI IT-Grundschutz: Gefährdungsübersichten
- IEC 62443: Threat Landscape für OT-Systeme

1.4.3 Entwicklung der Bedrohungslage

Unbemannte Luftfahrtsysteme haben sich innerhalb weniger Jahre von Spezialgeräten zu weltweit verfügbaren Massenprodukten entwickelt. Moderne Systeme verfügen über hochauflösende Kameras, Wärmebildsensoren, präzise Satellitennavigation, autonome Flugfunktionen, Hinderniserkennung sowie hohe Reichweiten und Flugzeiten.

Diese technische Entwicklung eröffnet legitime Anwendungsfelder, erhöht jedoch gleichzeitig das Missbrauchspotenzial. Sicherheitsbehörden beobachten seit mehreren Jahren eine zunehmende Nutzung von Drohnen zur Ausspähung sicherheitsrelevanter Einrichtungen, zur Vorbereitung von Sabotagehandlungen sowie zur Unterstützung hybrider Bedrohungen. Deutsche Verfassungsschutzbehörden weisen ausdrücklich darauf hin, dass Betreiber Kritischer Infrastrukturen aufgrund ihrer gesellschaftlichen Bedeutung bevorzugte Ziele entsprechender Aktivitäten sein können.

Internationale Entwicklungen – insbesondere der Einsatz ziviler Drohnen in aktuellen bewaffneten Konflikten – zeigen zudem, dass handelsübliche Systeme innerhalb kurzer Zeit für militärische oder terroristische Zwecke angepasst werden können. Auch wenn solche Szenarien nicht unmittelbar auf Deutschland übertragbar sind, verdeutlichen sie die Notwendigkeit einer vorausschauenden Sicherheitsplanung.

Ein wesentlicher Entwicklungstrend besteht in der zunehmenden Verfügbarkeit autonomer und nicht-kooperativer Drohnen. Diese benötigen teilweise keine aktive Funkverbindung zum Steuerer und können dadurch die Wirksamkeit klassischer Funkdetektions- und Störverfahren erheblich reduzieren. Für Betreiber Kritischer Infrastrukturen sowie weitere Einrichtungen mit erhöhtem Schutzbedarf steigt dadurch die Bedeutung mehrschichtiger Sensorik sowie organisatorischer und resilienzorientierter Schutzmaßnahmen.

Darüber hinaus zeigen internationale Entwicklungen die zunehmende Nutzung glasfasergeführter Drohnen. Diese verfügen zwar über eine Verbindung zum Bediener, nutzen jedoch keine Funkstrecke. Dadurch können klassische Verfahren der Funkdetektion sowie funkbasierte Störmaßnahmen in ihrer Wirksamkeit eingeschränkt sein. Die Entwicklung verdeutlicht die Notwendigkeit technologieoffener und mehrschichtiger Schutzkonzepte.

1.4.4 Schutzziele

Aus Sicht der Informationssicherheit können Drohnen sämtliche grundlegenden Schutzziele beeinträchtigen.

Schutzziel	Beispielhafte Beeinträchtigung durch Drohnen
Vertraulichkeit	Ausspähung schutzbedürftiger Informationen, Betriebsabläufe, Sicherheitsmaßnahmen, Leitstände oder Forschungs- und Entwicklungsbereiche durch Bild-, Video- oder Sensoraufnahmen
Integrität	Manipulation oder Beeinträchtigung von Anlagen, Prozessen oder Sicherheitsmaßnahmen, beispielsweise durch physische Einwirkung oder vorbereitende Angriffshandlungen
Verfügbarkeit	Betriebsunterbrechungen, Evakuierungen, Sperrungen von Betriebsbereichen oder Störungen kritischer Prozesse und Dienstleistungen
Authentizität	Täuschung über Herkunft, Zweck oder Legitimität einer Drohne, beispielsweise durch den Anschein behördlicher, dienstlicher oder betrieblicher Aktivitäten
Nachvollziehbarkeit	Erschwerte Identifizierung von Verursachern sowie eingeschränkte Aufklärung und Nachverfolgung drohnenbezogener Vorfälle aufgrund anonymer oder autonomer Betriebsweisen

Für OT-Umgebungen gewinnen zusätzlich die Schutzziele Safety (Schutz von Menschen und Umwelt) sowie Betriebs- und Versorgungskontinuität besondere Bedeutung.

Schutzziel	Beispielhafte Beeinträchtigung durch Drohnen
Safety (Schutz von Menschen und Umwelt)	Gefährdung von Beschäftigten, Besuchern oder der Umwelt durch Abstürze, Kollisionen oder Sabotage kritischer Anlagen
Betriebskontinuität / Resilienz	Beeinträchtigung oder Unterbrechung kritischer Geschäftsprozesse, Versorgungsleistungen oder Wiederanlaufverfahren nach sicherheitsrelevanten Vorfällen

Die einzelnen Schutzziele sind nicht isoliert zu betrachten. Die Beeinträchtigung eines Schutzziels kann mittelbar Auswirkungen auf weitere Schutzziele nach sich ziehen. Bei der Bewertung drohnenbezogener Bedrohungen sollten daher stets die Wechselwirkungen zwischen Informationssicherheit, physischer Sicherheit, OT-Sicherheit sowie Business Continuity Management berücksichtigt werden.

1.4.5 Bedrohungsakteure

Die Motivation eines Angreifers bestimmt maßgeblich Art und Intensität der Bedrohung.

Im Rahmen dieses Leitfadens werden folgende Akteursgruppen unterschieden:

1.4.5.1 Staatliche Akteure

Ziel ist die Gewinnung strategischer Informationen, die Vorbereitung hybrider Operationen oder die Beeinflussung Kritischer Infrastrukturen.

1.4.5.2 Nachrichtendienstlich gesteuerte Akteure

Diese handeln häufig verdeckt und konzentrieren sich auf langfristige Informationsgewinnung sowie Vorbereitungshandlungen.

1.4.5.3 Organisierte Kriminalität

Mögliche Ziele sind Erpressung, Diebstahl, Schmuggel oder Unterstützung weiterer Straftaten.

1.4.5.4 Terroristische oder extremistische Gruppierungen

Der Einsatz von Drohnen kann der Vorbereitung oder Durchführung von Sabotageakten sowie der Erzeugung öffentlicher Aufmerksamkeit dienen.

1.4.5.5 Aktivistische Gruppen

Je nach Motivation können Drohnen zur Dokumentation, Störung von Betriebsabläufen oder öffentlichkeitswirksamen Aktionen eingesetzt werden.

1.4.5.6 Einzelpersonen

Auch Einzelpersonen verfügen heute über technische Möglichkeiten, erhebliche Sicherheitsrisiken zu verursachen – sei es vorsätzlich oder fahrlässig.

1.4.5.7 Innentäter / Insider

Auch eigene Beschäftigte, Dienstleister oder sonstige Personen mit berechtigtem Zugang können externe Drohnenakteure unterstützen, beispielsweise durch die Weitergabe von Betriebsinformationen, Lageplänen, Schichtzeiten oder Informationen zu Sicherheitsmaßnahmen.

1.4.6 Typische Angriffsszenarien

Für Betreiber Kritischer Infrastrukturen sowie weitere Einrichtungen mit erhöhtem Schutzbedarf sind insbesondere folgende Szenarien relevant.

1.4.6.1 Ausspähung

- Fotografieren von Sicherheitsmaßnahmen
- Beobachtung von Schichtwechseln
- Erfassung von Kennzeichen
- Dokumentation von Lieferwegen
- Ausspähen von Leitständen
- Erfassen geöffneter Fenster
- Beobachtung von Wartungsarbeiten

Dieses Szenario wird von BfV und BayLfV als besonders wahrscheinlich beschrieben.

1.4.6.2 Vorbereitung physischer Angriffe

Drohnen können genutzt werden, um
- Fluchtwege zu erkunden,
- Schwachstellen zu identifizieren,
- Alarmierungsabläufe zu beobachten,
- Reaktionszeiten des Werkschutzes zu messen.

1.4.6.3 Sabotage

Hierzu zählen beispielsweise
- Beschädigung technischer Einrichtungen,
- Auslösen von Kurzschlüssen,
- Einbringen kleiner Gegenstände,
- Störung sensibler Prozesse.

1.4.6.4 Einschleusen von Gegenständen

Bekannt sind insbesondere
- Datenträger,
- Werkzeuge,
- Mobiltelefone,
- Schlüssel,
- kleinere Gefahrstoffe.

1.4.6.5 Unterstützung hybrider Angriffe

Im Rahmen koordinierter Angriffe können Drohnen eingesetzt werden zur
- Lageaufklärung,
- Echtzeitüberwachung,
- Koordination weiterer Täter,
- Unterstützung paralleler Cyberangriffe.

Gerade die Kombination physischer und cyberbezogener Angriffe erhöht das Schadenspotenzial erheblich.

1.4.6.6 Unterstützung Social Engineering

Zunehmend in kombinierten Angriffsszenarien beobachtbar:
- Drohne erzeugt Ablenkung
- Sicherheitspersonal wird gebunden
- Parallel erfolgt Zutritt durch Dritte

1.4.6.7 Koordinierte Mehrfachangriffe

Mehrere gleichzeitig eingesetzte Drohnen können Detektions-, Reaktions- und Sicherheitsprozesse gezielt überlasten. Solche Mehrfachangriffe können sowohl synchron als auch zeitlich versetzt erfolgen und Bestandteil hybrider Angriffsszenarien sein.

1.4.7 Angriffsmethoden

Die Analyse verfügbarer Quellen zeigt, dass sich Drohnenangriffe typischerweise in fünf Phasen gliedern:
- Informationsbeschaffung
- Zielaufklärung
- Vorbereitung
- Durchführung
- Rückzug und Spurenverwischung

Diese Struktur bildet die Grundlage für spätere Detektions- und Interventionsmaßnahmen.

Moderne Angriffsszenarien können zudem automatisierte oder KI-gestützte Planungs- und Navigationsverfahren nutzen. Hierdurch kann die Durchführung komplexer Aufklärungs- oder Angriffsprofile auch ohne permanente Steuerung durch einen Operator ermöglicht werden.

1.4.8 Auswirkungen auf Kritische Infrastrukturen

Bereits einzelne drohnenbezogene Vorfälle können erhebliche Auswirkungen auf Betreiber Kritischer Infrastrukturen sowie andere Einrichtungen mit erhöhtem Schutzbedarf haben.

Mögliche Auswirkungen umfassen insbesondere:
- Beeinträchtigung oder Unterbrechung kritischer Dienstleistungen und Geschäftsprozesse,
- Einschränkungen der Versorgungssicherheit,
- Evakuierungen oder Sperrung betroffener Betriebsbereiche,
- Produktions- und Betriebsausfälle,
- Ausspähung und Verlust schutzbedürftiger Informationen,
- Vorbereitung oder Unterstützung weiterer physischer, cyberbezogener oder hybrider Angriffe,
- Kaskadeneffekte auf verbundene oder nachgelagerte Kritische Infrastrukturen,
- Gefährdungen von Beschäftigten, Dienstleistern, Besuchern oder der Umwelt,
- regulatorische, rechtliche oder vertragliche Konsequenzen,
- erhebliche wirtschaftliche Schäden,
- Reputations- und Vertrauensverluste gegenüber Kunden, Partnern, Behörden und der Öffentlichkeit.

Die Auswirkungen beschränken sich dabei häufig nicht auf das eigentliche Drohnenereignis. Wesentliche betriebliche Folgen können sich auch aus notwendigen Sicherheitsmaßnahmen, Betriebsunterbrechungen, behördlichen Maßnahmen, Untersuchungen sowie der Bewältigung und Nachbereitung des Vorfalls ergeben.

1.4.9 Taxonomie drohnenbezogener Bedrohungen (UAS Threat Taxonomy)

1.4.9.1 Zielsetzung

Für eine konsistente Risikoanalyse ist eine einheitliche Klassifizierung drohnenbezogener Bedrohungen erforderlich. Unterschiedliche Organisationen verwenden bislang uneinheitliche Begriffe wie „Drohnenvorfall“, „Ausspähung“ oder „Sabotage“. Dies erschwert den Erfahrungsaustausch, die Bewertung von Vorfällen sowie die Ableitung geeigneter Schutzmaßnahmen.

Die nachfolgende Taxonomie dient daher als Referenzmodell für diesen Leitfaden. Sie ermöglicht eine standardisierte Beschreibung von Vorfällen und unterstützt die Integration in bestehende Risiko- und Sicherheitsmanagementprozesse.

Hinweis: Die nachfolgenden Klassifizierungen dienen der systematischen Risikobewertung, der Gefährdungsanalyse sowie der Post-Incident-Analyse.
Im Echtzeit-Sicherheitsbetrieb (Live-Incident) ist eine eindeutige Zuordnung der Angriffsmethode aus der Ferne meist nicht sofort zweifelsfrei möglich, da sich unbemannte Luftfahrtsysteme (UAS) optisch und frequenztechnisch unabhängig von ihrer Nutzlast ähneln. Das operative Sicherheitspersonal hat im Verdachtsfall daher primär nach dem Schutzprinzip der maximalen Annahme (Worst-Case-Prinzip) zu handeln, bis eine genaue Identifikation durch Sensorfusion oder Entschärfung erfolgt ist.

1.4.9.2 Zur Anwendung kommende Klassifikationsdimensionen

Die UAS Threat Taxonomy besteht aus drei voneinander unabhängigen Klassifikationsdimensionen:

- (Vermutete) Angriffsabsicht (T-Kategorien)
- (Vermutete) Angriffsmethode (M-Kategorien)
- (Vermutetes) Zielobjekt (O-Kategorien)

Diese Dimensionen können einzeln oder kombiniert verwendet werden.

Die nachfolgenden Indikatoren dienen ausschließlich als Beispiele möglicher Beobachtungen. Sie ersetzen keine technische Bewertung und erlauben regelmäßig keine abschließende Beurteilung der tatsächlichen Absicht einer Drohne.

1.4.9.3 Klassifizierung nach Angriffsabsicht (Threat Objective)

Kategorie	Angriffsabsicht	Beschreibung	Typische Beispiele
T1	Informations-gewinnung	Gewinnung von Informationen über Personen, Anlagen, Prozesse, Sicherheitsmaßnahmen oder Betriebsabläufe	Luftbilder, Videoaufnahmen, Erstellung von Lagebildern, Beobachtung von Prozessen
T2	Vorbereitungs-handlungen	Sammlung von Informationen zur Vorbereitung weiterer Angriffe oder Störungen	Erkundung von Zufahrten, Sicherheitsmaßnahmen, Schichtwechseln, Reaktionszeiten
T3	Betriebsstörung	Beeinträchtigung oder Unterbrechung von Geschäfts- oder Betriebsabläufen ohne unmittelbare Sabotage	Auslösen von Evakuierungen, Unterbrechung von Wartungsarbeiten, Blockierung von Betriebsflächen
T4	Sabotage	Gezielte Schädigung, Manipulation oder Funktionsbeeinträchtigung von Anlagen, Prozessen oder Infrastruktur	Einbringen von Gegenständen, Beschädigung technischer Einrichtungen, Auslösen von Störungen
T5	Unterstützung weiterer Angriffe	Unterstützung oder Koordination physischer, cyberbezogener oder hybrider Angriffe	Unterstützung eines Cyberangriffs, Koordination weiterer Täter, Echtzeit-Lageaufklärung
T6	Psychologische Wirkung	Einschüchterung, Verunsicherung oder Demonstration von Handlungsfähigkeit	Wiederholte Überflüge, demonstrative Präsenz, medienwirksame Aktionen

1.4.9.4 Klassifizierung nach Angriffsmethode (Method)

Kategorie	Angriffsmethode	Beschreibung
M1	Optische Aufklärung	Nutzung von Foto-, Video- oder Zoomkameras zur Informationsgewinnung
M2	Thermografische Aufklärung	Nutzung von Wärmebildsensoren zur Identifikation von Personen, Anlagen oder Prozessen
M3	Vermessung und 3D-Erfassung	Erstellung von Karten, Höhenmodellen oder digitalen Zwillingen mittels Sensorik
M4	Beobachtung betrieblicher Abläufe	Überwachung von Betriebsprozessen, Schichtwechseln, Lieferketten oder Sicherheitsmaßnahmen
M5	Transport oder Absetzen von Nutzlasten	Transport, Ablage, Aufnahme oder Übergabe von Gegenständen, Werkzeugen, Datenträgern oder sonstigen Nutzlasten
M6	Physische Einwirkung	Direkte physische Einwirkung auf Personen, Anlagen, Infrastruktur oder Betriebsmittel
M7	Unterstützung und Koordination weiterer Akteure	Echtzeit-Aufklärung, Kommunikation oder Führung weiterer Täter
M8	Täuschung, Ablenkung oder Bindung von Ressourcen	Erzeugung von Fehlreaktionen oder Ablenkung von Schutz- und Sicherheitsmaßnahmen
M9	Kombinierte Angriffsmethoden	Kombination mehrerer Methoden innerhalb eines Angriffs- oder Aufklärungsszenarios

Praxis-Indikatoren zur Fernerkennung physischer Bedrohungen

Eine mögliche Nutzlast (Payload) oder physische Angriffshandlung kann anhand folgender Sensorindikatoren vermutet werden:

- Optisch / Optronisch (Kamera/PTZ): Sichtbare Hängelasten, ungewöhnliche Anbauteile an der Unterseite, veränderter Schwerpunkt/Fluglage.
- Radar / Sensorik: Ungewöhnlich große Radarsignatur (RCS) im Vergleich zur Standard-Drohnenklasse; auffälliges Absinken/Schwebeflug über sensiblen Anlagenkomponenten (z. B. Transformatoren, Ventile, Dächer).
- Flugverhalten: Zielgerichteter, schneller Anflug im Tiefflug unter Umgehung von Standard-Einflugschneisen.

1.4.9.5 Klassifizierung nach Zielobjekt (Object)

Kategorie	Zielobjekt	Beschreibung	Typische Beispiele
O1	Personen	Beschäftigte, Besucher oder sonstige Personen auf dem Gelände	Mitarbeitende, Dienstleister, Sicherheitskräfte
O2	Gebäude und Einrichtungen	Gebäude oder bauliche Einrichtungen	Verwaltungsgebäude, Leitstellen, Betriebsgebäude
O3	Kritische Prozesse	Prozesse und Abläufe mit besonderer Bedeutung für den Betrieb	Netzsteuerung, Wasserversorgung, Produktionssteuerung
O4	Kritische Infrastruktur-komponenten	Technische Anlagen und Infrastruktur mit hoher Kritikalität	Umspannwerke, Wasserwerke, Telekommunikationsanlagen
O5	Liefer- und Versorgungsketten	Material-, Energie- oder Dienstleistungsflüsse	Anlieferzonen, Lagerflächen, Logistikbereiche
O6	Sicherheits-maßnahmen und Schutzsysteme	Sicherheitsrelevante Einrichtungen, Prozesse oder Organisationseinheiten	Kameras, Zäune, Leitstellen, Zutrittskontrollen, Sicherheitsdienst

Praxis-Indikatoren zur Fernerkennung von Cyber- und Aufklärungsszenarien

Passive Aufklärungs- oder Cyber-Szenarien (z. B. Sniffing, Rogue Access Points oder Jamming) weisen häufig charakteristische Merkmale auf:

- Optische Aufklärung: Längeres Verharren (Loitering/Hovering) vor Sichtachsen (z. B. Fenster, Leitstände oder Sicherheitszäune) bei gleichzeitig unauffälligem RF-Signal.
- Cyber-Angriffe / Rogue Access Points: Auftreten neuer oder ungewöhnlicher WLAN-SSIDs, Bluetooth-Signale oder erhöhter Sendeleistungen, die mittels RF-Sensorik einer Drohne zugeordnet werden können.
- Autonomer bzw. RF-silent Flug: Drohnen ohne Steuer- oder Videosignale (z. B. Wegpunktnavigation oder Glasfasersteuerung) können ausschließlich durch Radar-, optische oder thermografische Sensoren erkannt werden.

1.4.9.6 Nutzen der Taxonomie

Beispiel der praktischen Anwendung der Taxonomie:

Beispiel	Bedeutung
T1-M1-O2	Informationsgewinnung mittels optischer Aufklärung gegen Gebäude
T2-M4-O6	Vorbereitungshandlungen durch Beobachtung von Sicherheitsmaßnahmen
T4-M6-O4	Sabotage durch physische Einwirkung gegen kritische Infrastruktur
T5-M7-O3	Unterstützung eines weiteren Angriffs gegen kritische Prozesse
T6-M8-O1	Psychologische Wirkung durch Ablenkung oder Einschüchterung von Personen

Die Taxonomie unterstützt insbesondere
- Risikoanalysen,
- Incident Response,
- Lageberichte,
- Behördenmeldungen,
- Lessons Learned,
- Vergleichbarkeit zwischen Standorten.

Die UAS Threat Taxonomy dient ausschließlich der Beschreibung und Kategorisierung drohnenbezogener Bedrohungen. Sie beschreibt die vermutete Zielsetzung oder Art einer Bedrohung, ersetzt jedoch keine Bewertung der Schwere eines Vorfalls.

Neben langfristigen Entwicklungen sollten Betreiber Kritischer Infrastrukturen insbesondere kurzfristige Veränderungen der Gefährdungslage (z. B. politische Großereignisse, internationale Krisenlagen oder konkrete Warnhinweise zuständiger Sicherheitsbehörden) bei der Bewertung berücksichtigen.

1.4.10 Risikomatrix für Betreiber Kritischer Infrastrukturen

1.4.10.1 Zielsetzung

Die nachfolgende Matrix dient einer ersten qualitativen Einschätzung drohnenbezogener Risiken. Sie ersetzt keine organisationsspezifische Risikoanalyse, unterstützt jedoch die Priorisierung von Schutzmaßnahmen.

Die Bewertung berücksichtigt:

- derzeit bekannte Bedrohungslage,
- öffentlich dokumentierte Vorfälle,
- Einschätzungen nationaler Sicherheitsbehörden,
- Erfahrungen aus internationalen Sicherheitsanalysen.

1.4.10.2 Qualitative Risikobewertung nach KRITIS-Sektor

KRITIS-Sektor	Ausspähung	Sabotage	Hybridangriff	Gesamtrisiko
Energieversorgung	Hoch	Mittel bis hoch	Hoch	Hoch
Wasser / Abwasser	Mittel	Mittel	Mittel	Mittel
Informationstechnik / Telekommunikation	Hoch	Mittel	Hoch	Hoch
Gesundheit	Mittel	Mittel	Mittel	Mittel
Transport und Verkehr	Hoch	Hoch	Hoch	Hoch
Ernährung	Mittel	Gering bis mittel	Mittel	Mittel
Finanz- und Versicherungswesen	Mittel	Gering	Mittel	Mittel
Staat und Verwaltung	Hoch	Mittel	Hoch	Hoch

Hinweis: Diese Bewertung basiert auf einer qualitativen Experteneinschätzung unter Berücksichtigung von Angriffsabsicht, Exponiertheit kritischer Anlagen, möglichem Schadensausmaß und öffentlich bekannten Vorfällen. Sie dient lediglich der Orientierung. Die tatsächliche Risikoeinstufung ist im Rahmen der individuellen Risikoanalyse der jeweiligen Einrichtung vorzunehmen.

1.4.10.3 Bewertung typischer Angriffsszenarien

Szenario	Eintrittswahrscheinlichkeit	Schadenspotenzial	Priorität
Ausspähung mittels Kamera	Hoch	Mittel	Hoch
Wiederholte Aufklärungsflüge	Mittel	Hoch	Hoch
Beobachtung von Sicherheitsmaßnahmen	Hoch	Mittel	Hoch
Unterstützung eines Cyberangriffs	Niedrig bis mittel	Sehr hoch	Hoch
Sabotage mittels Nutzlast	Niedrig	Sehr hoch	Mittel bis hoch
Einschleusen von Gegenständen	Niedrig	Mittel	Mittel
Ablenkungsmanöver	Mittel	Mittel	Mittel

Drohnen stellen keine isolierte Bedrohung dar, sondern können Bestandteil komplexer physischer, cyberbezogener und hybrider Angriffsszenarien sein.

1.4.10.4 Risikofaktoren

Die Priorisierung drohnenbezogener Risiken sollte insbesondere folgende Faktoren berücksichtigen:

Faktorengruppe	Beispiele
Schutzbedarf und Kritikalität	Kritikalität der Prozesse, Auswirkungen auf kritische Dienstleistungen, Schutzbedarf von Anlagen und Informationen, mögliche Kaskadeneffekte
Standort und Exponiertheit	Sichtbeziehungen aus der Luft, Nähe zu öffentlichen Flächen oder Verkehrswegen, Topographie, Bewuchs, Erreichbarkeit des Geländes
Organisatorische Resilienz	Sicherheitskultur, Sensibilisierung der Beschäftigten, Alarmierungs- und Meldewege, Werkschutz, Besucher- und Fremdfirmenmanagement
Technische Schutzmaßnahmen	Videoüberwachung, Drohnendetektion, Perimeterschutz, Zugangskontrollen, Leitstellenanbindung, Beleuchtung
Betriebliche Resilienz	Redundanzen, Verfügbarkeit von Ersatzanlagen, Personalverfügbarkeit, Notfall- und Wiederanlaufplanung
Äußere Rahmenbedingungen	Aktuelle Bedrohungslage, Erkenntnisse von Sicherheitsbehörden, Flugbeschränkungsgebiete und sonstige luftrechtliche Rahmenbedingungen

1.4.10.5 Empfehlungen für die Priorisierung

Schutzmaßnahmen sollten grundsätzlich nach folgendem Prinzip priorisiert werden:

- Organisatorische Maßnahmen (hoher Nutzen, geringer Aufwand)
- Sensibilisierung und Übungen
- Bauliche Maßnahmen
- Technische Detektionsmaßnahmen
- Weitergehende technische Schutzmaßnahmen

Diese Priorisierung entspricht dem Grundsatz, dass technische Lösungen organisatorische Defizite nicht kompensieren können.

1.4.11 Bewertung der Bedrohung

1.4.11.1 Grundsatz

Die in den vorangegangenen Abschnitten dargestellten Bedrohungen, Angriffsszenarien und Risikoeinschätzungen stellen eine allgemeine Bewertung der Gefährdungslage dar. Sie ersetzen nicht die organisationsspezifische Risikoanalyse gemäß den Anforderungen des Informationssicherheitsmanagements, insbesondere nach ISO 27005, IT-Grundschutz oder IEC 62443.

Die tatsächliche Gefährdung eines Unternehmens ergibt sich erst aus der Kombination von:

- Attraktivität des Angriffsziels,
- vorhandenen Schwachstellen,
- Fähigkeiten und Motivation potenzieller Angreifer,
- bestehenden organisatorischen, baulichen und technischen Schutzmaßnahmen,
- möglichen Auswirkungen auf kritische Geschäftsprozesse.

Aus diesem Grund können identische Drohnenereignisse bei unterschiedlichen Organisationen zu einer erheblich abweichenden Risikobewertung führen.

1.4.11.2 Einflussfaktoren

Bei der Bewertung drohnenbezogener Risiken sollten insbesondere folgende Einflussgrößen berücksichtigt werden:

- Standortbezogene Faktoren
- geografische Lage,
- Topografie,
- Sichtbeziehungen,
- angrenzende öffentliche Flächen,
- Flugbeschränkungsgebiete,
- Nähe zu Verkehrswegen.
- Objektspezifische Faktoren
- Schutzbedarf der Einrichtung,
- Größe und Struktur des Betriebsgeländes,
- Anzahl kritischer Gebäude,
- offene Lager- und Freiflächen,
- Exponiertheit sicherheitskritischer Anlagen.
- Organisatorische Faktoren
- Sicherheitsorganisation,
- Werkschutz,
- Alarmierungsprozesse,
- Meldewege,
- Sicherheitsbewusstsein der Beschäftigten,
- Regelungen für Besucher und Fremdfirmen.
- Technische Faktoren
- Videoüberwachung,
- Perimeterschutz,
- Zutrittskontrollsysteme,
- Beleuchtung,
- Möglichkeiten zur Drohnendetektion,
- Leitstellenanbindung.
- Prozessbezogene Faktoren
- Kritikalität der Geschäftsprozesse,
- vorhandene Redundanzen,
- Wiederanlaufzeiten,
- Abhängigkeiten von Dritten,
- Auswirkungen auf die Versorgungssicherheit.

1.4.11.3 Bewertungsmethodik

Die Bewertung sollte mindestens folgende Fragestellungen beantworten:

- Welche schutzbedürftigen Informationen können durch einen Drohnenflug gewonnen werden?
- Welche kritischen Prozesse könnten beeinträchtigt werden?
- Welche Angriffsszenarien sind für den Standort realistisch?
- Welche bestehenden Schutzmaßnahmen reduzieren das Risiko bereits?
- Welche Restrisiken verbleiben?

Die Ergebnisse bilden die Grundlage für die Priorisierung der in den folgenden Kapiteln beschriebenen organisatorischen, baulichen und technischen Maßnahmen.

1.4.11.4 Dynamische Bedrohungslage

Die Bedrohungslage durch Drohnen unterliegt einer kontinuierlichen Veränderung. Technologische Entwicklungen, neue Angriffsmethoden sowie Änderungen der geopolitischen Lage können die Risikobewertung wesentlich beeinflussen.

Die Bewertung sollte daher:

- mindestens jährlich,
- nach sicherheitsrelevanten Vorfällen,
- nach wesentlichen Änderungen der Infrastruktur,
- sowie bei neuen Erkenntnissen der Sicherheitsbehörden

überprüft und erforderlichenfalls angepasst werden.

Hinweis: Die hier dargestellte Bedrohungsbewertung dient der Sensibilisierung und Priorisierung. Die verbindliche organisationsspezifische Risikobewertung erfolgt im Rahmen der in Kapitel 2.2 beschriebenen Schutzbedarfsfeststellung und Risikoanalyse.

1.4.12 Kernaussagen für Entscheider

Drohnen sind kein Nischenthema mehr, sondern Bestandteil der aktuellen Bedrohungslage.
Die größte praktische Relevanz besitzt derzeit die Ausspähung sicherheitsrelevanter Einrichtungen.
Drohnen sind häufig Bestandteil komplexerer Angriffs- oder Vorbereitungshandlungen und sollten nicht isoliert betrachtet werden.
Eine wirksame Sicherheitsstrategie kombiniert organisatorische, bauliche, technische und personelle Maßnahmen.

1.4.13 Handlungsempfehlungen

Betreiber Kritischer Infrastrukturen sollten:

- Drohnen ausdrücklich in ihr Bedrohungsmodell aufnehmen.
- Relevante Angriffsszenarien für den eigenen Standort identifizieren.
- Kritische Bereiche mit besonderem Ausspähungs- oder Sabotagerisiko erfassen.
- Schutzmaßnahmen risikobasiert priorisieren.
- Die Bedrohungsbewertung mindestens jährlich sowie anlassbezogen überprüfen.

1.5 Rechtliche und regulatorische Rahmenbedingungen

1.5.1 Zielsetzung

Die Einführung organisatorischer und technischer Schutzmaßnahmen gegen drohnenbezogene Bedrohungen erfolgt nicht im rechtsfreien Raum. Betreiber Kritischer Infrastrukturen sowie weiterer Einrichtungen mit hohem Schutzbedarf unterliegen einer Vielzahl gesetzlicher, regulatorischer und normativer Anforderungen, die mittelbar oder unmittelbar auch den Umgang mit unbemannten Luftfahrtsystemen betreffen.

Ziel dieses Kapitels ist es, die wesentlichen rechtlichen und regulatorischen Rahmenbedingungen darzustellen und ihre Bedeutung für den Schutz vor Ausspähung, Sabotage und hybriden Bedrohungen durch Drohnen einzuordnen.

Der Leitfaden ersetzt keine Rechtsberatung. Er erläutert die für das Sicherheitsmanagement wesentlichen Anforderungen und zeigt auf, wie diese im Rahmen eines integrierten Schutzkonzeptes berücksichtigt werden können.

1.5.2 Bezug zu Managementsystemen und Regelwerken

Dieses Kapitel unterstützt die Identifikation und Bewertung rechtlicher, regulatorischer und vertraglicher Anforderungen.

Relevante Regelwerke:

- ISO/IEC 27001: Compliance-Verpflichtungen
- ISO 37301: Compliance Management
- BSI IT-Grundschutz
- NIS-2 / BSIG
- B3S der jeweiligen Branche
- Luftverkehrs- und Datenschutzrecht

Für Betreiber kritischer Anlagen können darüber hinaus Anforderungen aus dem KRITIS-Dachgesetz (KRITISDachG) relevant sein.

1.5.3 Hierarchie der Anforderungen

Die Anforderungen an den Schutz vor drohnenbezogenen Bedrohungen ergeben sich aus unterschiedlichen Ebenen.

Diese lassen sich grundsätzlich wie folgt unterscheiden:

Ebene	Charakter	Beispiele
Europäisches Recht	Verbindlich	NIS-2-Richtlinie, KI-Verordnung (AI Act), Datenschutz-Grundverordnung (DSGVO)
Bundesrecht	Verbindlich	BSIG, LuftVG, LuftVO, StGB, BDSG
Landesrecht	Verbindlich	Polizeirecht, Bauordnungsrecht, Datenschutzrecht der Länder
Technische Regelwerke	Stand der Technik	BSI IT-Grundschutz, B3S, ISO/IEC 27001, IEC 62443
Behördenempfehlungen	Best Practice	Veröffentlichungen von BSI, BfV, BayLfV, ENISA, NPSA

Nicht jede Veröffentlichung begründet eine unmittelbare Rechtspflicht. Empfehlungen anerkannter Fachbehörden können jedoch zur Konkretisierung des Stands der Technik herangezogen werden und gewinnen dadurch praktische Bedeutung.

1.5.4 BSI-Gesetz, NIS-2 und KRITIS-Dachgesetz

1.5.4.1 BSI-Gesetz und NIS-2

Für Betreiber Kritischer Infrastrukturen sowie für Betreiber wichtiger und besonders wichtiger Einrichtungen bildet das BSI-Gesetz in Verbindung mit den Anforderungen aus der nationalen Umsetzung der NIS-2-Richtlinie den zentralen regulatorischen Rahmen.

Das Regelwerk verfolgt einen risikobasierten Ansatz. Es verpflichtet die betroffenen Einrichtungen, angemessene technische, organisatorische und personelle Maßnahmen zu treffen, um die Sicherheit ihrer Netz- und Informationssysteme sowie die Kontinuität wesentlicher Dienstleistungen zu gewährleisten.

Drohnen werden in den einschlägigen gesetzlichen Vorschriften zwar nicht ausdrücklich genannt. Gleichwohl können drohnenbezogene Vorfälle erhebliche Auswirkungen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen sowie auf die Verfügbarkeit kritischer Prozesse und Dienstleistungen haben. Entsprechend sind derartige Bedrohungen im Rahmen des Risikomanagements angemessen zu berücksichtigen.

Leitgedanke: Nicht die Drohne als solche ist Gegenstand der Regulierung, sondern das von ihr ausgehende Risiko für kritische Prozesse, Geschäftsabläufe sowie Netz- und Informationssysteme.

1.5.4.2 KRITIS-Dachgesetz

Mit dem KRITIS-Dachgesetz (KRITISDachG) wurde in Deutschland ein sektorenübergreifender Rechtsrahmen zur Stärkung der physischen Resilienz kritischer Anlagen geschaffen. Das Gesetz ergänzt bestehende Anforderungen der Informationssicherheit, insbesondere des BSI-Gesetzes und der NIS-2-Regulierung, um Anforderungen an die Widerstandsfähigkeit gegenüber physischen, technischen, natürlichen und hybriden Gefährdungen.

Das KRITISDachG richtet sich an Betreiber kritischer Anlagen im Sinne des Gesetzes und verfolgt einen All-Gefahren-Ansatz. Im Mittelpunkt stehen dabei die Identifikation relevanter Risiken, die Stärkung der organisatorischen und technischen Resilienz sowie die Aufrechterhaltung kritischer Dienstleistungen auch unter außergewöhnlichen Belastungen und Störungslagen.

Drohnen werden im KRITISDachG nicht ausdrücklich genannt. Gleichwohl können drohnenbezogene Bedrohungen, insbesondere Ausspähung, Sabotage oder hybride Angriffsszenarien, Auswirkungen auf kritische Anlagen und die Erbringung kritischer Dienstleistungen haben. Betreiber kritischer Anlagen sollten solche Bedrohungen daher im Rahmen ihrer Risiko- und Resilienzbewertungen angemessen berücksichtigen.

1.5.4.3 Relevanz für Betreiber Kritischer Infrastrukturen

Der vorliegende Leitfaden richtet sich an einen breiten Kreis von Betreibern Kritischer Infrastrukturen, NIS-2-pflichtigen Einrichtungen sowie weiteren Organisationen mit erhöhtem Schutzbedarf. Nicht alle Adressaten dieses Leitfadens fallen in den Anwendungsbereich des KRITISDachG. Daher werden die Anforderungen des KRITISDachG im Leitfaden nicht als eigenständiger Schwerpunkt behandelt, sondern ergänzend eingeordnet.

Für Betreiber kritischer Anlagen im Sinne des KRITISDachG können die im vorliegenden Leitfaden beschriebenen organisatorischen, baulichen und technischen Maßnahmen insbesondere bei folgenden Themenstellungen unterstützen:

- Risiko- und Resilienzbewertungen kritischer Anlagen,
- Schutz vor physischen und hybriden Bedrohungen,
- Aufrechterhaltung kritischer Dienstleistungen,
- Notfall- und Krisenmanagement,
- Business Continuity Management,
- Wiederherstellung der Betriebsfähigkeit nach Störungen,
- Bewertung möglicher Kaskaden- und Folgeeffekte auf andere Kritische Infrastrukturen.

Betreiber kritischer Anlagen sollten daher zusätzlich prüfen, inwieweit drohnenbezogene Bedrohungen in bestehende Prozesse zur Risikoanalyse, Resilienzbewertung, Notfallvorsorge und Krisenbewältigung einzubeziehen sind. Die in diesem Leitfaden beschriebenen Maßnahmen können hierfür als fachliche Orientierung dienen.

Hinweis: Dieser Leitfaden stellt keine Auslegungshilfe zum KRITISDachG dar und erhebt keinen Anspruch auf Vollständigkeit hinsichtlich der dort geregelten Betreiberpflichten. Betreiber kritischer Anlagen sollten die jeweils geltenden gesetzlichen Anforderungen eigenständig bewerten und berücksichtigen.

1.5.5 Luftverkehrsrecht

Das Luftverkehrsrecht regelt den Betrieb unbemannter Luftfahrtsysteme im deutschen Luftraum. Hierzu zählen insbesondere Anforderungen an den zulässigen Betrieb, Flugbeschränkungen, geografische UAS-Gebiete sowie Pflichten der Fernpiloten.

Für Betreiber Kritischer Infrastrukturen sowie weitere Einrichtungen mit erhöhtem Schutzbedarf ist von besonderer Bedeutung, dass luftverkehrsrechtliche Verbote nicht automatisch einen wirksamen Schutz vor Drohnenflügen gewährleisten. Auch rechtswidrige oder unerlaubte Flüge sind in der Risikoanalyse zu berücksichtigen.

Das Luftverkehrsrecht begründet grundsätzlich keine allgemeinen Eingriffsbefugnisse für Betreiber gegenüber Drohnen. Maßnahmen zur aktiven Drohnenabwehr können hoheitlichen Stellen vorbehalten sein oder einer besonderen rechtlichen Bewertung bedürfen.

Betreiber sollten jedoch prüfen, ob ihre Einrichtungen innerhalb bestehender geografischer UAS-Gebiete liegen oder durch zukünftige luftrechtliche Schutzmaßnahmen berücksichtigt werden könnten.

Mit der Weiterentwicklung sogenannter U-Spaces können künftig zusätzliche Möglichkeiten zur Koordinierung und Überwachung des Drohnenverkehrs entstehen. Betreiber Kritischer Infrastrukturen sollten entsprechende Entwicklungen beobachten und deren mögliche Auswirkungen auf die eigene Sicherheits- und Risikobewertung berücksichtigen.

1.5.6 Strafrecht

Je nach Einzelfall können Drohnenflüge verschiedene Straftatbestände erfüllen, etwa wenn sie der Ausspähung, Sabotage oder Vorbereitung weiterer Straftaten dienen.

Zu berücksichtigen sind insbesondere:

- Ausspähen von Daten,
- Verletzung von Privatgeheimnissen,
- Sachbeschädigung,
- Hausfriedensbruch (je nach Sachverhalt),
- nachrichtendienstliche Agententätigkeit,
- staatsgefährdende Delikte.

Die strafrechtliche Bewertung bleibt stets vom konkreten Einzelfall abhängig und obliegt den zuständigen Strafverfolgungsbehörden.

1.5.7 Datenschutzrecht

Der Einsatz von Drohnen kann personenbezogene Daten erfassen, beispielsweise durch Bild-, Video- oder Tonaufzeichnungen.

Unternehmen sollten daher Verfahren zur Dokumentation entsprechender Vorfälle vorsehen und gleichzeitig sicherstellen, dass eigene Schutzmaßnahmen datenschutzkonform ausgestaltet werden. Dies betrifft insbesondere Videoüberwachung, Protokollierung und die Verarbeitung von Bildmaterial.

1.5.8 Arbeits- und Gesundheitsschutz

Drohnenvorfälle können Auswirkungen auf die Sicherheit von Beschäftigten haben, etwa wenn Evakuierungen erforderlich werden oder Gefährdungen durch herabfallende Gegenstände bestehen.

Sicherheits- und Notfallprozesse sollten daher mit den bestehenden Regelungen des Arbeits- und Gesundheitsschutzes abgestimmt werden.

1.5.9 Hausrecht und Objektschutz

Betreiber verfügen grundsätzlich über das Hausrecht auf ihrem Betriebsgelände. Dieses ermöglicht unter anderem Regelungen für den Zutritt, das Verhalten auf dem Gelände sowie den Einsatz eigener Sicherheitsdienste.

Das Hausrecht begründet jedoch keine generelle Befugnis, gegen Drohnen außerhalb des eigenen Verantwortungsbereichs aktiv vorzugehen. Maßnahmen mit Außenwirkung sind ausschließlich im Rahmen der geltenden Rechtsordnung zulässig.

Darüber hinaus können in besonderen Einzelfällen rechtliche Erwägungen zu Notwehr oder rechtfertigendem Notstand relevant werden. Eine pauschale Befugnis zur aktiven Drohnenabwehr lässt sich hieraus jedoch nicht ableiten.

1.5.10 Rechtliche Grenzen aktiver Gegenmaßnahmen

Die Erkennung drohnenbezogener Bedrohungen ist grundsätzlich von Maßnahmen zur aktiven Einwirkung auf Drohnen zu unterscheiden.

Während Detektionsmaßnahmen im Rahmen der geltenden Rechtsordnung grundsätzlich zulässig sein können, unterliegt die aktive Einwirkung auf Drohnen in Deutschland erheblichen rechtlichen Einschränkungen.

Hierzu zählen insbesondere:

- Störung von Funkverbindungen (Jamming),
- Manipulation von Navigationssignalen (Spoofing),
- Übernahme der Steuerung,
- Abschuss oder sonstige physische Einwirkung,
- Einsatz von Fangdrohnen oder vergleichbaren Systemen.

Derartige Maßnahmen können luftverkehrsrechtliche, telekommunikationsrechtliche, strafrechtliche sowie haftungsrechtliche Fragestellungen berühren und sind teilweise ausschließlich staatlichen Stellen vorbehalten oder bedürfen besonderer gesetzlicher Grundlagen.

Betreiber Kritischer Infrastrukturen sollten daher bereits im Vorfeld gemeinsam mit ihrer Rechtsabteilung sowie den zuständigen Behörden festlegen, welche Maßnahmen im Ereignisfall zulässig sind und welche organisatorischen Alternativen zur Verfügung stehen.

Die Entscheidung über aktive Gegenmaßnahmen sollte organisationsintern durch geeignete organisatorische Regelungen, eindeutige Zuständigkeiten und dokumentierte Entscheidungsprozesse flankiert werden. Insbesondere bei zeitkritischen Ereignissen empfiehlt sich eine vorab abgestimmte Verfahrensanweisung unter Einbindung der zuständigen Fachbereiche (z. B. Werkschutz, Informationssicherheit, Rechtsabteilung, Unternehmensleitung).

1.5.11 Stand der Technik

Der Begriff „Stand der Technik“ ist dynamisch und entwickelt sich kontinuierlich weiter. Für den Schutz vor drohnenbezogenen Bedrohungen existiert derzeit kein eigenständiger deutscher Standard.

Der Stand der Technik ist kein statischer Zustand. Betreiber Kritischer Infrastrukturen sollten daher regelmäßig prüfen, ob neue gesetzliche Anforderungen, anerkannte Normen, behördliche Veröffentlichungen oder technische Entwicklungen eine Anpassung bestehender Schutzmaßnahmen erforderlich machen.

Zur Konkretisierung können insbesondere herangezogen werden:

- BSI IT-Grundschutz,
- branchenspezifische Sicherheitsstandards (B3S),
- ISO/IEC 27001,
- ISO 22301,
- IEC 62443,
- Veröffentlichungen von BSI, BfV und BayLfV,
- Jeweils aktuelle TeleTrust-Handreichung „Stand der Technik in der IT-Sicherheit“
- internationale Best Practices, soweit sie auf die deutsche Rechtslage übertragbar sind.

Die Auswahl geeigneter Maßnahmen hat sich stets am individuellen Risiko sowie an der Verhältnismäßigkeit zu orientieren.

1.5.12 Kernaussagen für Entscheider

Drohnenbedrohungen sind Bestandteil des allgemeinen Risikomanagements und keine isolierte luftverkehrsrechtliche Fragestellung.
Das BSI-Gesetz und die NIS-2-Anforderungen verlangen eine risikobasierte Berücksichtigung physischer und informationstechnischer Bedrohungen.
Nicht jede behördliche Empfehlung ist rechtlich verbindlich; sie kann jedoch den Stand der Technik konkretisieren.
Maßnahmen zur aktiven Drohnenabwehr unterliegen in Deutschland engen rechtlichen Grenzen und sind sorgfältig zu prüfen.

1.5.13 Handlungsempfehlungen

Betreiber Kritischer Infrastrukturen sollten:

- drohnenbezogene Risiken ausdrücklich in ihr Informationssicherheits- und Risikomanagement integrieren;
- die Anforderungen aus BSIG, NIS-2 und einschlägigen Managementsystemen in einem konsistenten Sicherheitskonzept zusammenführen;
- klare interne Zuständigkeiten für die rechtliche Bewertung und Behandlung von Drohnenvorfällen festlegen;
- Alarmierungs- und Meldeprozesse unter Berücksichtigung datenschutz-, arbeits- und luftverkehrsrechtlicher Vorgaben definieren;
- Maßnahmen zur Drohnendetektion und -abwehr vor ihrer Einführung rechtlich prüfen und dokumentieren.

2 Teil II – Governance und Risikomanagement

2.1 Governance und Sicherheitsorganisation

2.1.1 Zielsetzung

Die wirksame Behandlung drohnenbezogener Bedrohungen setzt geeignete organisatorische Rahmenbedingungen voraus. Technische Schutzmaßnahmen allein reichen nicht aus, um Risiken durch Ausspähung, Sabotage oder hybride Angriffe angemessen zu beherrschen.
Drohnenvorfälle betreffen regelmäßig mehrere Fachbereiche gleichzeitig. Neben der Informationssicherheit können insbesondere Werkschutz, Objektsicherheit, Business Continuity Management, Krisenmanagement, OT-Sicherheit, Datenschutz sowie die Unternehmensleitung unmittelbar betroffen sein. Ohne eindeutige Zuständigkeiten, abgestimmte Prozesse und klare Entscheidungswege besteht die Gefahr von Fehlentscheidungen, verzögerten Reaktionen oder unzureichend koordinierten Maßnahmen.
Ziel dieses Kapitels ist die Beschreibung eines Governance-Modells für die Behandlung drohnenbezogener Risiken. Hierzu werden organisatorische Verantwortlichkeiten, Entscheidungswege, Meldeprozesse sowie die Einbindung in bestehende Sicherheits- und Managementsysteme dargestellt.

2.1.2 Bezug zu Managementsystemen und Regelwerken

Dieses Kapitel unterstützt die Festlegung von Rollen, Verantwortlichkeiten, Prozessen und Entscheidungswegen für den Umgang mit drohnenbezogenen Risiken.

Relevante Regelwerke:
- ISO/IEC 27001: Führung und Unterstützung
- ISO 22301: Business-Continuity-Governance
- BSI IT-Grundschutz: Organisation der Informationssicherheit
- NIS-2 / BSIG: Managementverantwortung

2.1.3 Governance-Grundsätze

Die Behandlung drohnenbezogener Risiken sollte sich an denselben Grundsätzen orientieren, die auch für andere sicherheitsrelevante Risiken innerhalb der Organisation gelten.

Hierzu zählen insbesondere:
- Risikoorientierung
- Verantwortlichkeit der Unternehmensleitung
- Integration in bestehende Managementsysteme
- Interdisziplinäre Zusammenarbeit
- Nachvollziehbarkeit von Entscheidungen
- Kontinuierliche Verbesserung
- Dokumentation und Revisionssicherheit
- Verhältnismäßigkeit

Drohnenbedrohungen sollten dabei nicht als isoliertes Spezialthema betrachtet werden. Vielmehr handelt es sich um eine besondere Ausprägung physischer und informationsbezogener Bedrohungen, die in bestehende Sicherheits-, Risiko- und Krisenmanagementprozesse einzubetten ist.
Die organisatorische Verantwortung darf daher weder ausschließlich dem Werkschutz noch ausschließlich der Informationssicherheit übertragen werden. Eine wirksame Governance erfordert die koordinierte Zusammenarbeit aller betroffenen Fachbereiche.
Art und Umfang organisatorischer sowie technischer Schutzmaßnahmen sollten sich stets am Schutzbedarf der jeweiligen Einrichtung, der aktuellen Bedrohungslage sowie dem Grundsatz der Verhältnismäßigkeit orientieren. Nicht jede Einrichtung benötigt denselben Umfang an organisatorischen oder technischen Schutzmaßnahmen.

2.1.4 Einbindung in bestehende Managementsysteme

Drohnenbezogene Risiken sollten nicht über separate Prozesse behandelt werden.
Sie sind in bestehende Managementsysteme zu integrieren, insbesondere:

- Informationssicherheitsmanagement (ISMS)
- Business Continuity Management (BCM)
- Notfall- und Krisenmanagement
- Werkschutz und Objektsicherheit
- OT-Sicherheitsmanagement

Ziel ist die Nutzung bestehender Governance-, Risiko-, Incident- und Verbesserungsprozesse sowie die Vermeidung von Doppelstrukturen.

2.1.5 Rollen und Verantwortlichkeiten

Die wirksame Behandlung drohnenbezogener Risiken setzt eine klare Zuordnung von Aufgaben, Verantwortlichkeiten und Entscheidungsbefugnissen voraus.
Unklare Zuständigkeiten führen häufig dazu, dass Vorfälle verspätet eskaliert, Risiken unzureichend bewertet oder notwendige Maßnahmen nicht umgesetzt werden. Die organisatorische Einbindung sollte daher bereits vor dem ersten Vorfall verbindlich geregelt werden.

2.1.5.1 Unternehmensleitung

Die Unternehmensleitung trägt die Gesamtverantwortung für die Steuerung drohnenbezogener Risiken.

Zu ihren Aufgaben gehören insbesondere:

- Festlegung sicherheitsrelevanter Ziele
- Genehmigung wesentlicher Schutzmaßnahmen
- Bereitstellung finanzieller und personeller Ressourcen
- Entscheidung über die Risikobehandlung
- Entgegennahme regelmäßiger Lageberichte

2.1.5.2 Informationssicherheitsbeauftragter

Der Informationssicherheitsbeauftragte unterstützt die Integration drohnenbezogener Risiken in das Sicherheitsmanagement.

Typische Aufgaben sind:
- Moderation von Risikoanalysen
- Bewertung informationssicherheitsrelevanter Risiken
- Integration in das ISMS
- Unterstützung bei Sicherheitsvorfällen
- Berichterstattung an die Unternehmensleitung

2.1.5.3 Werkschutz und Objektsicherheit

Die Verantwortlichen für Werkschutz und Objektsicherheit übernehmen regelmäßig die operative Erstbewertung von Vorfällen.

Zu ihren Aufgaben zählen insbesondere:
- Beobachtung und Dokumentation
- Lageeinschätzung
- Durchführung definierter Erstmaßnahmen
- Einleitung von Eskalationsprozessen
- Zusammenarbeit mit Behörden und Sicherheitsdienstleistern

2.1.5.4 Business Continuity Management

Das BCM stellt sicher, dass drohnenbezogene Szenarien in Notfall- und Wiederanlaufplanungen berücksichtigt werden.

Hierzu gehören:
- Bewertung möglicher Betriebsunterbrechungen
- Notfallplanung
- Wiederanlaufstrategien
- Übungsplanung
- Wirksamkeitsprüfung

2.1.5.5 Krisenmanagement

Bei schwerwiegenden Vorfällen kann die Aktivierung des Krisenmanagements erforderlich werden.

Mögliche Auslöser sind:
- zielgerichtete Ausspähung kritischer Bereiche,
- Verdacht auf Sabotagevorbereitungen,
- Störungen kritischer Prozesse,
- koordinierte hybride Angriffe,
- wiederholte sicherheitsrelevante Vorfälle.

2.1.5.6 Externe Stellen

Die Behandlung drohnenbezogener Vorfälle erfordert regelmäßig die Zusammenarbeit mit externen Stellen.

Bereits vor Eintritt eines Ereignisses sollte festgelegt werden,
- welche Behörden zuständig sind,
- wann diese einzubinden sind,
- welche Informationen bereitzustellen sind,
- welche Ansprechpartner erreichbar sein müssen.

Je nach Art des Vorfalls kommen insbesondere in Betracht:
- Polizei
- Landeskriminalamt
- Verfassungsschutz
- BSI
- CERT
- Luftfahrtbehörden
- Feuerwehr
- Rettungsdienst
- Betreiber benachbarter Kritischer Infrastrukturen
- Sicherheitsdienstleister

2.1.6 Defence in Depth als Schutzprinzip

Der Schutz vor drohnenbezogenen Bedrohungen basiert auf dem Defence-in-Depth-Prinzip. Dabei werden mehrere organisatorische, personelle, bauliche und technische Schutzebenen miteinander kombiniert. Ziel ist, dass das Versagen oder die Umgehung einer einzelnen Maßnahme nicht unmittelbar zu einer erfolgreichen Ausspähung, Sabotage oder sonstigen Beeinträchtigung führt.

Typische Schutzebenen sind:
- Sicherheitsorganisation und Governance
- Sensibilisierung der Beschäftigten
- Melde- und Eskalationsprozesse
- Objektschutz und bauliche Maßnahmen
- Videoüberwachung und Detektionssysteme
- Incident Response
- BCM und Krisenmanagement

Die Wirksamkeit ergibt sich nicht aus einer einzelnen Maßnahme, sondern aus dem koordinierten Zusammenwirken aller Schutzebenen

2.1.7 Melde- und Eskalationswege

Für drohnenbezogene Vorfälle sollten verbindliche Melde- und Eskalationswege definiert werden.

Hierbei sind insbesondere folgende Fragestellungen zu beantworten:

- Wer darf Vorfälle melden?
- Welche Informationen sind zu erfassen?
- Wer bewertet den Vorfall?
- Wann erfolgt eine Eskalation?
- Welche Funktionen oder Gremien sind einzubinden?
- Welche externen Stellen sind gegebenenfalls zu informieren?
- Welche Kriterien lösen eine externe Meldung oder Alarmierung aus?

Soweit möglich sollten bestehende Incident-Response-, Notfall- und Krisenmanagementprozesse genutzt werden.

Die operative Bewertung und Klassifizierung drohnenbezogener Ereignisse sollte im Rahmen des Incident-Response-Prozesses gemäß Kapitel 4 erfolgen.

2.1.8 Dokumentation und Berichtswesen

Eine nachvollziehbare Dokumentation bildet die Grundlage für Risikoanalysen, Vorfalluntersuchungen und Lessons Learned.

Erfasst werden sollten insbesondere:

- Datum und Uhrzeit
- Ort des Ereignisses
- Beschreibung der Beobachtung
- verfügbare Bild- oder Videodokumentation
- beteiligte Personen und Stellen
- eingeleitete Maßnahmen
- Bewertung des Vorfalls
- Zuordnung gemäß der UAS Threat Taxonomy (Kapitel 1.4)
- Erkenntnisse für zukünftige Verbesserungen

Die Ergebnisse sollten regelmäßig ausgewertet und an die Unternehmensleitung berichtet werden.

2.1.9 Schulung und Sensibilisierung

Technische und organisatorische Maßnahmen sind nur wirksam, wenn Beschäftigte drohnenbezogene Bedrohungen erkennen und angemessen darauf reagieren können.

Schulungs- und Sensibilisierungsmaßnahmen sollten daher insbesondere folgende Themen umfassen:

- Erkennung auffälliger Drohnenaktivitäten
- Meldewege
- Verhalten im Ereignisfall
- Grundsätze der Beweissicherung
- Verhalten gegenüber Medien und Dritten
- Schutz sensibler Informationen
- Unterstützung von Sicherheitsmaßnahmen

Besondere Zielgruppen sind:

- Werkschutz
- Leitstellenpersonal
- Facility Management
- Empfangs- und Besucherservice
- Führungskräfte
- Mitarbeitende in sicherheitskritischen Bereichen

2.1.10 Kontinuierliche Verbesserung

Die Bedrohungslage durch Drohnen entwickelt sich kontinuierlich weiter. Technologische Entwicklungen, neue Angriffsmethoden sowie Veränderungen der geopolitischen Lage können Anpassungen organisatorischer Maßnahmen erforderlich machen.

Die Organisation sollte daher regelmäßig überprüfen:

- die Wirksamkeit bestehender Prozesse,
- die Eignung von Rollen und Verantwortlichkeiten,
- die Funktionalität von Meldewegen,
- Erkenntnisse aus Vorfällen und Übungen,
- neue Erkenntnisse von Sicherheitsbehörden,
- technologische Entwicklungen im Bereich unbemannter Luftfahrtsysteme.

Die Ergebnisse sollten systematisch in das Sicherheitsmanagement zurückgeführt werden.

2.1.11 Governance-Reifegradmodell

Die organisatorische Behandlung drohnenbezogener Risiken entwickelt sich in der Praxis häufig schrittweise. Während einige Organisationen bereits über etablierte Prozesse, klare Verantwortlichkeiten und regelmäßige Übungen verfügen, befindet sich der Umgang mit Drohnenbedrohungen in anderen Unternehmen noch im Aufbau.

Zur Unterstützung einer strukturierten Standortbestimmung empfiehlt dieser Leitfaden die Anwendung eines einfachen Governance-Reifegradmodells. Es ermöglicht eine erste Einschätzung des organisatorischen Entwicklungsstandes und unterstützt die Priorisierung weiterer Verbesserungsmaßnahmen.

Das Modell dient ausdrücklich nicht der Zertifizierung oder Bewertung der Rechtskonformität. Vielmehr stellt es ein praxisorientiertes Instrument zur Selbstbewertung dar und kann im Rahmen interner Audits, Management-Reviews oder Reifegradanalysen eingesetzt werden. Es eignet sich zudem, um Fortschritte im Zeitverlauf zu dokumentieren und die Wirksamkeit umgesetzter organisatorischer Maßnahmen nachvollziehbar zu bewerten.

Die Einordnung sollte anhand der tatsächlich gelebten Prozesse erfolgen. Maßgeblich ist dabei nicht das Vorhandensein einzelner Dokumente, sondern deren nachweisbare Umsetzung und Wirksamkeit im operativen Betrieb.

Beispielhaftes Governance-Reifegradmodell

Reifegrad	**Beschreibung**
G0 – Initial	Drohnenbezogene Risiken werden organisatorisch nicht oder nur anlassbezogen behandelt. Zuständigkeiten und Prozesse sind nicht definiert.
G1 – Sensibilisiert	Erste organisatorische Maßnahmen wurden eingeführt. Einzelne Verantwortlichkeiten und Meldewege sind vorhanden, jedoch noch nicht systematisch dokumentiert oder abgestimmt.
G2 – Etabliert	Rollen, Verantwortlichkeiten und grundlegende Prozesse sind definiert. Drohnenbezogene Risiken werden im Informationssicherheits- und Risikomanagement berücksichtigt.
G3 – Gesteuert	Organisatorische Prozesse sind etabliert und in bestehende Managementsysteme (z. B. ISMS, BCM oder Krisenmanagement) integriert. Melde- und Eskalationswege werden regelmäßig angewendet und überprüft.
G4 – Überprüft	Die Organisation führt regelmäßige Schulungen, Übungen, Management-Reviews und interne Audits durch. Erkenntnisse aus Vorfällen und Übungen werden systematisch ausgewertet und Verbesserungsmaßnahmen eingeleitet.
G5 – Optimiert	Die Governance unterliegt einem kontinuierlichen Verbesserungsprozess. Kennzahlen, Reifegradbewertungen und Erkenntnisse aus aktuellen Bedrohungslagen fließen regelmäßig in die Weiterentwicklung des Sicherheitskonzeptes ein. Die Organisation orientiert sich nachweislich am Stand der Technik und überprüft die Wirksamkeit ihrer Maßnahmen fortlaufend.

Hinweis: Das Reifegradmodell dient als Orientierungs- und Bewertungsinstrument. Die angestrebte Reife hängt von Art, Größe, Schutzbedarf und Risikolage der jeweiligen Organisation ab. Für Betreiber Kritischer Infrastrukturen sowie weitere Einrichtungen mit erhöhtem Schutzbedarf sollte mindestens ein Reifegrad angestrebt werden, der eine systematische Integration drohnenbezogener Risiken in die bestehenden Sicherheits- und Managementprozesse sicherstellt.

2.1.12 Kernaussagen für Entscheider

- Drohnenbedrohungen sind Bestandteil des unternehmensweiten Risiko- und Sicherheitsmanagements.
- Die wirksame Behandlung drohnenbezogener Risiken erfordert eine enge Zusammenarbeit von Informationssicherheit, Werkschutz, BCM, Krisenmanagement und Unternehmensleitung.
- Klare Verantwortlichkeiten, definierte Meldewege und standardisierte Eskalationsprozesse bilden die Grundlage einer wirksamen Governance.
- Drohnenbezogene Vorfälle sollten über bestehende Incident-, Notfall- und Krisenmanagementprozesse gesteuert werden.
- Die Unternehmensleitung trägt die Gesamtverantwortung für die Steuerung drohnenbezogener Risiken.

2.1.13 Handlungsempfehlungen

Betreiber Kritischer Infrastrukturen sollten:

- drohnenbezogene Risiken organisatorisch verankern;
- klare Verantwortlichkeiten festlegen;
- Melde- und Eskalationswege definieren;
- Vorfälle standardisiert dokumentieren;
- Schulungs- und Sensibilisierungsmaßnahmen durchführen;
- Drohnenszenarien in Notfall- und Krisenübungen integrieren;
- die Wirksamkeit der Governance regelmäßig überprüfen.

Die beschriebenen Governance-Strukturen sollten in die bestehenden Organisations-, Führungs- und Managementsysteme integriert werden. Parallelstrukturen sind zu vermeiden.

2.2 Schutzbedarfsfeststellung und Risikoanalyse

2.2.1 Zielsetzung

Die Auswahl geeigneter organisatorischer, baulicher und technischer Schutzmaßnahmen setzt eine nachvollziehbare Bewertung drohnenbezogener Risiken voraus. Ohne Kenntnis des Schutzbedarfs sowie der individuellen Gefährdungslage besteht die Gefahr einer Unter- oder Überdimensionierung von Sicherheitsmaßnahmen.

Ziel dieses Kapitels ist es, ein praxisorientiertes Verfahren zur Schutzbedarfsfeststellung und Risikoanalyse für drohnenbezogene Bedrohungen bereitzustellen. Die dargestellte Methodik orientiert sich an anerkannten Verfahren des Informationssicherheits- und Risikomanagements und berücksichtigt insbesondere die Anforderungen des BSI-Gesetzes, der NIS-2-Richtlinie, des BSI IT-Grundschutzes, der ISO/IEC 27001, der ISO/IEC 27005 sowie der ISO 31000.

Die Ergebnisse der Schutzbedarfsfeststellung und Risikoanalyse bilden die Grundlage für sämtliche in den folgenden Kapiteln beschriebenen organisatorischen, baulichen und technischen Maßnahmen.

2.2.2 Bezug zu Managementsystemen und Regelwerken

Dieses Kapitel beschreibt die Identifikation, Bewertung und Behandlung drohnenbezogener Risiken als Grundlage für die Auswahl geeigneter Schutzmaßnahmen.

Relevante Regelwerke:
- ISO/IEC 27001: Risikobeurteilung und Risikobehandlung
- ISO/IEC 27005: Informationssicherheits-Risikomanagement
- ISO 31000: Risikomanagement
- BSI IT-Grundschutz: Schutzbedarfsfeststellung
- IEC 62443: Security Risk Assessment

2.2.3 Grundsätze der Risikoanalyse

Die Bewertung drohnenbezogener Risiken erfolgt risikobasiert und organisationsspezifisch. Eine pauschale Bewertung ist aufgrund der unterschiedlichen Schutzbedarfe, Standortbedingungen und Bedrohungslagen nicht möglich.

Die Risikoanalyse sollte insbesondere folgende Grundsätze berücksichtigen:
- Nachvollziehbarkeit,
- Dokumentation,
- Aktualität,
- Wiederholbarkeit,
- Verhältnismäßigkeit,
- Einbindung relevanter Fachbereiche.

Die Risikoanalyse ist regelmäßig sowie anlassbezogen zu überprüfen und fortzuschreiben.

2.2.4 Vorgehensmodell

Für diesen Leitfaden wird folgendes siebenstufiges Vorgehensmodell empfohlen:

- Festlegung des Betrachtungsumfangs
- Schutzbedarfsfeststellung
- Identifikation schutzbedürftiger Objekte
- Analyse möglicher Bedrohungen
- Bewertung vorhandener Schutzmaßnahmen
- Risikobewertung
- Ableitung und Priorisierung von Maßnahmen

Dieses Vorgehen lässt sich unabhängig von bestehenden Managementsystemen anwenden und kann in vorhandene Prozesse integriert werden.

2.2.5 Festlegung des Betrachtungsumfangs

Zu Beginn der Risikoanalyse ist festzulegen, welche Organisationseinheiten, Standorte, Anlagen oder Prozesse betrachtet werden.

Hierzu gehören insbesondere:

- Betriebsgelände,
- Verwaltungsgebäude,
- Produktionsanlagen,
- Leitstellen,
- Rechenzentren,
- Umspannwerke,
- Wasserwerke,
- Lagerflächen,
- Freiluftanlagen,
- Kommunikationsstandorte,
- Baustellen,
- temporäre Einrichtungen.

Die Festlegung des Betrachtungsumfangs ist zu dokumentieren und regelmäßig zu überprüfen.

2.2.6 Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung dient der Ermittlung der Auswirkungen, die durch eine erfolgreiche Ausspähung, Sabotage oder sonstige Beeinträchtigung mittels Drohnen entstehen können.

Die Bewertung sollte mindestens die folgenden Schutzziele berücksichtigen:

Schutzziel	Fragestellung
Vertraulichkeit	Welche Informationen könnten ausgespäht werden?
Integrität	Welche Manipulationen wären möglich?
Verfügbarkeit	Welche Auswirkungen hätte ein Ausfall?
Safety (Schutz von Menschen und Umwelt)	Welche Gefährdungen für Menschen oder Umwelt bestehen?
Betriebskontinuität	Welche Auswirkungen bestehen auf kritische Dienstleistungen und die Versorgungssicherheit?

Die Auswahl der betrachteten Schutzziele orientiert sich an den für die Risikoanalyse besonders relevanten Kriterien. Weitere in Kapitel 0 dargestellte Schutzziele können organisationsspezifisch ergänzt werden.

Die Bewertung erfolgt entsprechend der unternehmensweit eingeführten Schutzbedarfskategorien.

2.2.7 Identifikation schutzbedürftiger Objekte

Auf Grundlage des Schutzbedarfs sind alle relevanten Objekte zu identifizieren.

Hierzu zählen insbesondere:
- kritische Gebäude,
- Leitstände,
- Netzleitstellen,
- Produktionslinien,
- Tankanlagen,
- Umspannwerke,
- Rohrleitungsanlagen,
- Telekommunikationsstandorte,
- Sicherheitszentralen,
- Sicherheitszäune,
- Zugangssysteme,
- Videoüberwachung,
- Freilager.

Besondere Aufmerksamkeit ist Bereichen mit guter Einsehbarkeit aus der Luft zu widmen.

2.2.8 Bedrohungsanalyse

Im nächsten Schritt sind die für den jeweiligen Standort relevanten Angriffsszenarien zu identifizieren.

Hierbei sollte auf die in Kapitel 1.4 eingeführte UAS Threat Taxonomy zurückgegriffen werden.

Zu bewerten sind insbesondere:
- Ausspähung,
- Vorbereitungshandlungen,
- Sabotage,
- Einschleusen von Gegenständen,
- Unterstützung hybrider Angriffe,
- psychologische Beeinflussung,
- wiederholte Überflüge,
- koordinierte Mehrfachangriffe und Drohnenschwärme.

Die Bewertung sollte aktuelle Erkenntnisse der Sicherheitsbehörden sowie organisationsspezifische Erfahrungen berücksichtigen.

2.2.9 Schwachstellenanalyse

Im Rahmen der Schwachstellenanalyse ist zu untersuchen, welche Faktoren einen erfolgreichen Drohnenangriff begünstigen können.

Hierzu zählen insbesondere:
- Organisatorische Schwachstellen
- fehlende Meldewege,
- unklare Verantwortlichkeiten,
- unzureichende Sensibilisierung,
- fehlende Übungen.
- Bauliche Schwachstellen
- offene Dachflächen,
- frei zugängliche Innenhöfe,
- ungeschützte Freilager,
- fehlender Sichtschutz.
- Technische Schwachstellen
- fehlende Detektionssysteme,
- unzureichende Videoüberwachung,
- tote Kamerawinkel,
- fehlende Beleuchtung.

2.2.10 Risikobewertung

Das Risiko ergibt sich aus der Kombination von:
- Eintrittswahrscheinlichkeit,
- Schadensausmaß,
- Wirksamkeit vorhandener Schutzmaßnahmen.

Für diesen Leitfaden wird eine qualitative Bewertung empfohlen.

Eintrittswahrscheinlichkeit	Schadensausmaß	Risiko
gering	gering	niedrig
gering	hoch	mittel
mittel	hoch	hoch
hoch	hoch	sehr hoch

Organisationen können alternativ ihre bestehende unternehmensweite Bewertungsmethodik verwenden.

2.2.11 Priorisierung von Maßnahmen

Aus der Risikobewertung sind geeignete Maßnahmen abzuleiten.

Dabei sollte folgende Reihenfolge berücksichtigt werden:
- organisatorische Maßnahmen,
- personelle Maßnahmen,
- bauliche Maßnahmen,
- technische Maßnahmen,
- ergänzende Detektions- und Reaktionsmaßnahmen.

Die Priorisierung richtet sich nach Risiko, Aufwand und Wirksamkeit.

2.2.12 Dokumentation

Die Ergebnisse der Schutzbedarfsfeststellung und Risikoanalyse sollten mindestens folgende Informationen enthalten:
- Betrachtungsumfang,
- Schutzbedarf,
- identifizierte Bedrohungen,
- UAS-Taxonomie,
- vorhandene Maßnahmen,
- Restrisiken,
- empfohlene Maßnahmen,
- Verantwortlichkeiten,
- Umsetzungsfristen,
- Datum der letzten Überprüfung.

Die Dokumentation sollte in bestehende ISMS-, BCM- oder Risikomanagementprozesse integriert werden.

2.2.13 Regelmäßige Überprüfung

Die Risikoanalyse ist regelmäßig zu überprüfen und insbesondere anzupassen bei:

- Änderungen der Bedrohungslage,
- Neubauten oder Umbauten,
- Änderungen kritischer Prozesse,
- Einführung neuer Technologien,
- sicherheitsrelevanten Vorfällen,
- Erkenntnissen aus Übungen,
- neuen Veröffentlichungen der Sicherheitsbehörden.

2.2.14 Kernaussagen für Entscheider

- Schutzmaßnahmen gegen Drohnen müssen auf einer nachvollziehbaren Risikoanalyse beruhen.
- Die Risikoanalyse ist organisationsspezifisch und regelmäßig fortzuschreiben.
- Organisatorische Maßnahmen besitzen häufig das günstigste Verhältnis von Aufwand und Wirksamkeit.
- Die Ergebnisse der Risikoanalyse bilden die Grundlage für Investitionsentscheidungen und Sicherheitskonzepte.

2.2.15 Handlungsempfehlungen

Betreiber Kritischer Infrastrukturen sollten:

- drohnenbezogene Risiken in die bestehende Risikoanalyse integrieren;
- die in Kapitel 1.4 dargestellte UAS Threat Taxonomy als einheitliches Klassifikationsmodell verwenden;
- Schutzbedarfsfeststellung und Risikoanalyse mindestens jährlich sowie anlassbezogen aktualisieren;
- Ergebnisse im ISMS, BCM und Krisenmanagement dokumentieren;
- Maßnahmen nach Risiko, Wirksamkeit und Verhältnismäßigkeit priorisieren.

3 Teil III – Risikobehandlung und Schutzmaßnahmen

3.1 Organisatorische Schutzmaßnahmen

3.1.1 Zielsetzung

Organisatorische Maßnahmen bilden die Grundlage eines wirksamen Schutzkonzeptes gegen drohnenbezogene Bedrohungen. Sie schaffen die Voraussetzungen für ein koordiniertes Handeln, definieren Verantwortlichkeiten und stellen sicher, dass technische sowie bauliche Maßnahmen wirksam in bestehende Sicherheitsprozesse integriert werden.

Erfahrungen aus Sicherheitsvorfällen zeigen, dass organisatorische Defizite häufig schwerwiegendere Auswirkungen haben als fehlende technische Schutzsysteme. Unklare Zuständigkeiten, fehlende Meldewege oder unzureichend vorbereitete Mitarbeitende können die Wirksamkeit vorhandener Sicherheitsmaßnahmen erheblich beeinträchtigen.

Ziel dieses Kapitels ist es, organisatorische Maßnahmen zu beschreiben, die unabhängig von Größe und Branche einer Organisation umgesetzt werden können und sich in bestehende Managementsysteme integrieren lassen.

3.1.2 Bezug zu Managementsystemen und Regelwerken

Dieses Kapitel beschreibt organisatorische Maßnahmen zur Risikobehandlung und zur Erhöhung der Sicherheitsreife der Organisation.

Relevante Regelwerke:
- ISO/IEC 27001: Sicherheitsmaßnahmen (Controls)
- ISO/IEC 27002: Organisatorische Maßnahmen
- BSI IT-Grundschutz: ORP-Bausteine
- NIS-2 / BSIG: Risikomanagementmaßnahmen

3.1.3 Grundprinzipien

Organisatorische Schutzmaßnahmen sollten sich an folgenden Grundprinzipien orientieren:
- Risikoorientierung,
- Verhältnismäßigkeit,
- Integration in bestehende Managementsysteme,
- eindeutige Verantwortlichkeiten,
- Dokumentation,
- kontinuierliche Verbesserung,
- regelmäßige Überprüfung der Wirksamkeit.

Organisatorische Maßnahmen sind nicht als einmalige Projekte zu verstehen, sondern als Bestandteil eines kontinuierlichen Sicherheitsprozesses.

3.1.4 Sicherheitsrichtlinien

Organisationen sollten drohnenbezogene Risiken in ihre bestehenden Sicherheitsrichtlinien aufnehmen.

Hierzu gehören insbesondere:
- Sicherheitsleitlinie,
- Informationssicherheitsrichtlinie,
- Werkschutzordnung,
- Besucherordnung,
- Krisenmanagementhandbuch,
- Notfallhandbuch,
- Alarmierungsrichtlinien.

Die Richtlinien sollten Verantwortlichkeiten, Meldewege sowie Mindestanforderungen an das Verhalten bei Drohnensichtungen eindeutig beschreiben.

3.1.5 Prozesse und Verfahrensanweisungen

Für den Umgang mit Drohnenvorfällen sollten standardisierte Prozesse definiert werden.

Hierzu zählen insbesondere:
- Meldung von Drohnensichtungen,
- Erstbewertung,
- Alarmierung,
- Eskalation,
- Dokumentation,
- Beweissicherung,
- Kommunikation,
- Nachbereitung.

Soweit vorhanden, sollten bestehende Incident-Response-, BCM- und Krisenmanagementprozesse genutzt und um drohnenbezogene Aspekte ergänzt werden.

3.1.6 Sensibilisierung der Beschäftigten

Alle Beschäftigten sollten für drohnenbezogene Risiken angemessen sensibilisiert werden.

Schulungsinhalte können insbesondere umfassen:
- typische Bedrohungsszenarien,
- Erkennen auffälliger Drohnenaktivitäten,
- interne Meldewege,
- Verhalten im Ereignisfall,
- Schutz vertraulicher Informationen,
- Grundsätze der Beweissicherung.

Art und Umfang der Schulungen sollten sich an der jeweiligen Funktion und dem Gefährdungspotenzial orientieren.

3.1.7 Besucher- und Fremdfirmenmanagement

Besucher sowie externe Dienstleister können unbeabsichtigt oder vorsätzlich sicherheitsrelevante Informationen offenlegen.

Daher sollten insbesondere geregelt werden:
- Zutrittsberechtigungen,
- Begleitpflichten,
- Fotografierverbote,
- Umgang mit privaten Drohnen,
- Nutzung mobiler Endgeräte,
- Meldepflichten bei Auffälligkeiten.

Vertragliche Regelungen mit Dienstleistern sollten geeignete Sicherheitsanforderungen enthalten.
Besondere Aufmerksamkeit sollte Konstellationen gelten, in denen interne Kenntnisse über Betriebsabläufe, Schichtzeiten, Sicherheitsmaßnahmen oder kritische Standorte mit externen Aufklärungsaktivitäten kombiniert werden können.

3.1.8 Informationsschutz

Zur Verringerung des Ausspähungsrisikos sollten organisatorische Maßnahmen zum Schutz vertraulicher Informationen umgesetzt werden.

Hierzu zählen beispielsweise:
- Vermeidung offen sichtbarer Unterlagen,
- Schutz sensibler Bildschirminhalte,
- Sichtschutzmaßnahmen,
- sichere Aufbewahrung vertraulicher Dokumente,
- Clean-Desk-Policy,
- abgestimmte Regelungen für Außenbereiche.

Insbesondere bei Besprechungen im Freien oder Arbeiten im Außenbereich sollte berücksichtigt werden, dass Informationen aus der Luft beobachtet oder aufgezeichnet werden können.

Betreiber Kritischer Infrastrukturen sollten darüber hinaus regelmäßig bewerten, welche Geodaten, Luftbilder, technischen Strukturdaten, Leistungsdaten oder sonstigen Informationen über ihre Standorte, Einrichtungen, Anlagenstrukturen oder Betriebsabläufe in öffentlich zugänglichen Informationssystemen verfügbar sind. Hierzu zählen insbesondere Webauftritte, Open-Data-Portale, Ausschreibungsunterlagen, GIS-Dienste, satellitengestützte Kartendienste sowie Veröffentlichungen in sozialen Medien. Die Kombination solcher Informationen kann die Vorbereitung drohnenbezogener Ausspähungs- oder Angriffshandlungen erheblich erleichtern.

3.1.9 Zusammenarbeit mit externen Stellen

Bereits vor Eintritt eines Vorfalls sollten Ansprechpartner und Kommunikationswege zu externen Stellen festgelegt werden.

Je nach Art des Ereignisses können insbesondere folgende Stellen einzubinden sein:

- Polizei,
- Landeskriminalamt,
- Verfassungsschutz,
- Bundesamt für Sicherheit in der Informationstechnik,
- CERT,
- Luftfahrtbehörden,
- Feuerwehr,
- Rettungsdienst,
- Betreiber benachbarter Kritischer Infrastrukturen.

Regelmäßige Abstimmungen mit zuständigen Behörden können die Wirksamkeit der Vorfallbewältigung erhöhen.

Soweit rechtlich und organisatorisch möglich, sollte auch ein regelmäßiger Austausch über drohnenbezogene Erkenntnisse mit benachbarten Betreibern Kritischer Infrastrukturen, Branchennetzwerken und zuständigen Behörden geprüft werden. Ziel kann die frühzeitige Erkennung standortübergreifender Aufklärungs- oder Angriffsmuster sein.

3.1.10 Übungen und Tests

Die Wirksamkeit organisatorischer Maßnahmen sollte regelmäßig überprüft werden.

Geeignete Formate sind insbesondere:

- Tabletop-Übungen,
- Alarmierungsübungen,
- Kommunikationsübungen,
- Krisenstabsübungen,
- Lessons-Learned-Workshops.

Die Ergebnisse sollten dokumentiert und in den kontinuierlichen Verbesserungsprozess einfließen.

3.1.11 Erfolgskontrolle

Organisationen sollten geeignete Kennzahlen (Key Performance Indicators – KPI) definieren, um die Wirksamkeit organisatorischer Maßnahmen regelmäßig zu bewerten.

Beispiele hierfür sind:
- Anzahl gemeldeter Drohnensichtungen,
- Bearbeitungszeit bis zur Erstbewertung,
- Alarmierungszeiten,
- Anteil geschulter Beschäftigter,
- Anzahl durchgeführter Übungen,
- Umsetzungsgrad beschlossener Verbesserungsmaßnahmen.

Die Kennzahlen sollten regelmäßig im Rahmen von Management-Reviews oder Sicherheitsbesprechungen bewertet werden.

3.1.12 Dokumentation

Organisatorische Maßnahmen sollten nachvollziehbar dokumentiert werden.

Hierzu gehören insbesondere:
- Richtlinien,
- Verfahrensanweisungen,
- Rollenbeschreibungen,
- Alarmierungspläne,
- Schulungsnachweise,
- Übungsprotokolle,
- Maßnahmenlisten,
- Auditfeststellungen,
- Verbesserungsmaßnahmen.

Die Dokumentation sollte revisionssicher erfolgen und in bestehende Managementsysteme integriert werden.

3.1.13 Kernaussagen für Entscheider

- Organisatorische Maßnahmen bilden die Grundlage eines wirksamen Schutzkonzeptes gegen drohnenbezogene Bedrohungen.
- Klare Prozesse, Verantwortlichkeiten und Meldewege erhöhen die Reaktionsfähigkeit und reduzieren das Risiko von Fehlentscheidungen.
- Regelmäßige Schulungen und Übungen tragen wesentlich zur Wirksamkeit organisatorischer Schutzmaßnahmen bei.
- Die Wirksamkeit organisatorischer Maßnahmen sollte anhand geeigneter Kennzahlen überwacht und kontinuierlich verbessert werden.

3.1.14 Handlungsempfehlungen

Betreiber Kritischer Infrastrukturen sollten:

- drohnenbezogene Risiken in bestehende Sicherheitsrichtlinien integrieren;
- standardisierte Prozesse für Meldung, Bewertung und Eskalation von Drohnenvorfällen etablieren;
- Beschäftigte regelmäßig sensibilisieren und schulen;
- Zuständigkeiten und Kommunikationswege mit externen Stellen vorab festlegen;
- die Wirksamkeit organisatorischer Maßnahmen regelmäßig durch Übungen, Audits und Management-Reviews überprüfen.

3.2 Bauliche und infrastrukturelle Schutzmaßnahmen

3.2.1 Zielsetzung

Bauliche und infrastrukturelle Schutzmaßnahmen dienen dazu, die Wahrscheinlichkeit einer erfolgreichen Ausspähung, Sabotage oder sonstigen Beeinträchtigung durch unbemannte Luftfahrtsysteme (UAS) zu reduzieren. Sie ergänzen organisatorische und technische Maßnahmen und bilden einen wesentlichen Bestandteil eines mehrschichtigen Sicherheitskonzeptes im Sinne des Defence-in-Depth-Prinzips.

Im Gegensatz zu organisatorischen Maßnahmen entfalten bauliche Schutzmaßnahmen ihre Wirkung dauerhaft und unabhängig vom Verhalten einzelner Personen. Sie können insbesondere dazu beitragen,

- sensible Bereiche der direkten Einsicht zu entziehen,
- Annäherungsmöglichkeiten einzuschränken,
- Angriffsflächen zu reduzieren,
- Auswirkungen eines Vorfalls zu begrenzen sowie
- die Wirksamkeit technischer Schutzmaßnahmen zu erhöhen.

Bauliche Schutzmaßnahmen ersetzen jedoch weder organisatorische Prozesse noch technische Detektions- und Reaktionsmaßnahmen. Sie sind stets Bestandteil eines integrierten Sicherheitskonzeptes.

3.2.2 Bezug zu Managementsystemen und Regelwerken

Dieses Kapitel unterstützt die physische Absicherung kritischer Anlagen, Gebäude und Betriebsbereiche gegen drohnenbezogene Gefährdungen.

Relevante Regelwerke:

- ISO/IEC 27001: Physische Sicherheitsmaßnahmen
- ISO/IEC 27002: Physical Security Controls
- BSI IT-Grundschutz: INF-Bausteine
- IEC 62443: Schutz kritischer OT-Umgebungen

3.2.3 Planungsgrundsätze

Bauliche Schutzmaßnahmen sollten bereits bei der Planung neuer Standorte oder wesentlicher Umbaumaßnahmen berücksichtigt werden. Bei Bestandsobjekten empfiehlt sich eine risikoorientierte Nachrüstung.

Folgende Grundsätze sind zu beachten:

- Schutzbedarf vor Gestaltung,
- Defence in Depth (mehrschichtiger Schutzansatz),
- Verhältnismäßigkeit,
- Redundanz kritischer Einrichtungen,
- Wartungsfreundlichkeit,
- Integration in bestehende Sicherheitskonzepte.

3.2.4 Zonenkonzept

Zur systematischen Planung empfiehlt sich eine Einteilung des Betriebsgeländes in Sicherheitszonen.

Sicherheitszone	Beispiele	Zielsetzung
Zone 0	Öffentlich zugängliche Bereiche	Früherkennung
Zone 1	Werksgelände	Zugangskontrolle
Zone 2	Betriebsbereiche	Schutz kritischer Prozesse
Zone 3	Hochsicherheitsbereiche	Höchstmöglicher Schutz
Zone 4	Leitstellen, Rechenzentren, Netzleitstellen	Schutz besonders kritischer Funktionen

Je höher die Schutzklasse, desto umfangreicher sollten bauliche Schutzmaßnahmen ausgeprägt sein.

3.2.5 Perimeterschutz

Der äußere Perimeter bildet die erste physische Schutzschicht.

Zu berücksichtigen sind insbesondere:
- Einfriedungen,
- Werkszäune,
- Tore,
- Zufahrtskontrollen,
- Geländestruktur,
- Vegetation,
- Beleuchtung.

Bei der Planung sollte berücksichtigt werden, dass Drohnen den klassischen Perimeterschutz überfliegen können. Ziel ist daher nicht die Verhinderung des Überflugs, sondern die Erschwerung nachgelagerter Angriffshandlungen.

3.2.6 Schutz kritischer Gebäude

Gebäude mit erhöhtem Schutzbedarf sollten hinsichtlich ihrer Einsehbarkeit und Erreichbarkeit bewertet werden.

Zu prüfen sind insbesondere:
- Dachflächen,
- Oberlichter,
- Glasfassaden,
- Fensterfronten,
- Lüftungsöffnungen,
- Dachzugänge,
- Wartungsplattformen.

Soweit technisch und wirtschaftlich vertretbar, sollten besonders sensible Bereiche gegen unmittelbare Einsicht geschützt werden.

3.2.7 Schutz von Freianlagen

Viele kritische Einrichtungen befinden sich außerhalb geschlossener Gebäude.

Hierzu gehören beispielsweise:
- Umspannwerke,
- Wasserbehälter,
- Pumpwerke,
- Freiluftschaltanlagen,
- Antennenanlagen,
- Rohrbrücken,
- Tanklager.

Für diese Einrichtungen sind ergänzende Schutzmaßnahmen erforderlich, beispielsweise Sichtschutz, bauliche Abschirmungen oder eine optimierte Anordnung sicherheitskritischer Komponenten.

3.2.8 Sichtschutz und Informationsschutz

Ein wesentliches Ziel baulicher Maßnahmen besteht darin, die Gewinnung sicherheitsrelevanter Informationen aus der Luft zu erschweren.

Geeignete Maßnahmen können sein:
- Sichtschutzwände,
- Lamellensysteme,
- blickdichte Einhausungen,
- Begrünung,
- Überdachungen,
- Verlagerung sensibler Arbeitsbereiche.

Dabei ist zwischen Schutz vor bodengebundener Einsicht und Schutz vor Luftaufklärung zu unterscheiden.

3.2.9 Schutz kritischer Infrastrukturkomponenten

Besonders schutzbedürftig sind unter anderem:
- Netzleitstellen,
- Rechenzentren,
- Schaltanlagen,
- Sicherheitszentralen,
- Notstromversorgung,
- Kommunikationsanlagen,
- Tank- und Gefahrstofflager,
- Gebäudeleittechnik.

Für diese Einrichtungen sollte geprüft werden, ob zusätzliche bauliche Schutzmaßnahmen erforderlich sind.

3.2.10 Baustellen und temporäre Einrichtungen

Während Bau-, Wartungs- und Revisionsarbeiten entstehen häufig zusätzliche Risiken.

Hierzu zählen beispielsweise:
- geöffnete Dachflächen,
- Gerüste,
- Containeranlagen,
- provisorische Leitungsführungen,
- verringerte Zutrittskontrollen.

Temporäre Maßnahmen sollten daher frühzeitig in die Baustellenplanung integriert werden.

3.2.11 Wechselwirkung mit technischen Schutzmaßnahmen

Bauliche Maßnahmen beeinflussen die Wirksamkeit technischer Systeme.

Bereits in der Planungsphase sollte berücksichtigt werden:
- Positionierung von Kameras,
- Sichtfelder von Sensoren,
- Beleuchtung,
- Stromversorgung,
- Kommunikationsanbindungen,
- Wartungszugänge.

Eine abgestimmte Planung erhöht die Wirksamkeit des Gesamtsystems erheblich.

3.2.12 Grenzen baulicher Schutzmaßnahmen

Bauliche Maßnahmen können das Risiko drohnenbezogener Angriffe reduzieren, bieten jedoch keinen vollständigen Schutz.

Insbesondere können sie
- Überflüge nicht verhindern,
- Drohnen nicht aufhalten,
- keine Angriffserkennung ersetzen,
- organisatorische Defizite nicht kompensieren.

Ein wirksames Schutzkonzept setzt daher stets das Zusammenwirken organisatorischer, baulicher und technischer Maßnahmen voraus.

3.2.13 Kernaussagen für Entscheider

- Bauliche Schutzmaßnahmen sind ein dauerhaft wirksamer Bestandteil eines mehrschichtigen Sicherheitskonzeptes.
- Der Schwerpunkt sollte auf der Reduzierung von Ausspähungs- und Sabotagemöglichkeiten liegen.
- Bereits bei Neuplanungen sollten Anforderungen des Schutzes gegen Drohnen berücksichtigt werden.
- Die Wirksamkeit baulicher Maßnahmen hängt wesentlich von ihrer Integration in organisatorische und technische Sicherheitsprozesse ab.

3.2.14 Handlungsempfehlungen

Betreiber Kritischer Infrastrukturen sollten:

- drohnenbezogene Anforderungen frühzeitig in Bau- und Infrastrukturprojekte integrieren;
- Betriebsgelände anhand eines Zonenkonzeptes strukturieren;
- kritische Gebäude und Freianlagen hinsichtlich ihrer Einsehbarkeit aus der Luft bewerten;
- bauliche Maßnahmen mit technischen Detektions- und Überwachungssystemen abstimmen;
- bauliche Schutzmaßnahmen regelmäßig auf ihre Wirksamkeit überprüfen und bei Umbauten oder Nutzungsänderungen anpassen.

3.3 Technische Schutzmaßnahmen und Drohnendetektion

3.3.1 Zielsetzung

Technische Schutzmaßnahmen dienen der frühzeitigen Erkennung, Bewertung und Dokumentation drohnenbezogener Bedrohungen sowie der Unterstützung geeigneter organisatorischer und operativer Reaktionsmaßnahmen. Sie ergänzen bauliche und organisatorische Schutzmaßnahmen und erhöhen die Fähigkeit einer Organisation, Drohnenvorfälle rechtzeitig zu erkennen und angemessen zu behandeln.

Technische Systeme können jedoch organisatorische Defizite nicht kompensieren und ersetzen weder qualifiziertes Personal noch definierte Melde- und Entscheidungsprozesse. Ihre Auswahl und Ausgestaltung hat sich daher stets an den Ergebnissen der Schutzbedarfsfeststellung und Risikoanalyse zu orientieren.

Technische Schutzmaßnahmen sind Bestandteil eines ganzheitlichen Schutzkonzeptes. Ihre Wirksamkeit entfaltet sich erst im Zusammenwirken mit organisatorischen Schutzmaßnahmen, Incident Response, Business Continuity Management und Krisenmanagement.

Die Einführung technischer Systeme sollte grundsätzlich erst nach Festlegung organisatorischer Verantwortlichkeiten, Meldeprozesse und Reaktionsverfahren erfolgen.

3.3.2 Bezug zu Managementsystemen und Regelwerken

Dieses Kapitel beschreibt technische Maßnahmen zur Erkennung, Bewertung und Dokumentation drohnenbezogener Ereignisse.

Relevante Regelwerke:

- ISO/IEC 27001: Technische Sicherheitsmaßnahmen
- ISO/IEC 27002: Technological Controls
- IEC 62443: System- und Netzwerksicherheit
- BSI IT-Grundschutz: DET-, OPS- und SYS-Bausteine

3.3.3 Grundsätze technischer Schutzmaßnahmen

Bei der Planung und Einführung technischer Schutzmaßnahmen sollten insbesondere folgende Grundsätze berücksichtigt werden:

- Risikoorientierung,
- Mehrschichtigkeit (Defence in Depth),
- Verhältnismäßigkeit,
- Interoperabilität,
- Skalierbarkeit,
- Ausfallsicherheit,
- Datenschutz und Datensparsamkeit,
- Wartbarkeit,
- Integration in bestehende Sicherheitsprozesse.

Technische Schutzmaßnahmen sind regelmäßig hinsichtlich ihrer Wirksamkeit zu überprüfen und an den Stand der Technik anzupassen.

3.3.4 Technische Schutzziele

Technische Maßnahmen verfolgen insbesondere folgende Ziele:

- frühzeitige Erkennung von Drohnenaktivitäten,
- Identifikation und Bewertung möglicher Bedrohungen,
- Unterstützung der Lagebeurteilung,
- Dokumentation sicherheitsrelevanter Ereignisse,
- Alarmierung verantwortlicher Stellen,
- Unterstützung der Beweissicherung,
- Verbesserung der Reaktionsfähigkeit.

3.3.5 Mehrschichtiges Detektionskonzept

Einzelne Sensorsysteme weisen regelmäßig technische Einschränkungen auf. Daher empfiehlt sich für schutzbedürftige Einrichtungen ein mehrschichtiges Detektionskonzept nach dem Defence-in-Depth-Prinzip.

Dieses kann insbesondere folgende Sensorprinzipien kombinieren:

- optische Sensorik,
- thermische Sensorik,
- Radarsensorik,
- akustische Sensorik,
- Funkfrequenzanalyse (RF),
- weitere geeignete Sensortechnologien.

Neben klassischen aktiven Sensorsystemen gewinnen passive Detektionsverfahren zunehmend an Bedeutung. Insbesondere für Betreiber Kritischer Infrastrukturen werden derzeit Konzepte untersucht, bei denen bereits vorhandene Funksignale als sogenannte „Beleuchter“ für Passivradarsysteme genutzt werden. Hierdurch kann eine energieeffiziente und emissionsfreie Drohnendetektion unterstützt werden, ohne selbst zusätzliche Radarsignale auszusenden. Experimentelle Untersuchungen mit LTE450 als Signalquelle zeigen, dass dieser Ansatz grundsätzlich für die frühzeitige Erkennung autonom fliegender Drohnen geeignet sein kann.

Die Kombination mehrerer Sensortypen erhöht die Erkennungswahrscheinlichkeit und reduziert Fehlalarme.

3.3.6 Videoüberwachung

Vorhandene Videoüberwachungssysteme können einen wichtigen Beitrag zur Erkennung und Dokumentation drohnenbezogener Vorfälle leisten.

Dabei sollte insbesondere geprüft werden:

- ausreichende Blickfelder,
- Abdeckung kritischer Bereiche,
- Bildqualität,
- Nachtsichtfähigkeit,
- Speicherung der Aufzeichnungen,
- datenschutzkonforme Konfiguration.

Eine ausschließliche Nutzung klassischer Videoüberwachung zur Drohnendetektion ist jedoch regelmäßig nicht ausreichend.

3.3.7 Drohnendetektion

Spezialisierte Detektionssysteme ermöglichen die Erkennung von Drohnen bereits vor einem unmittelbaren Eindringen in den Schutzbereich.

Je nach technischer Ausführung können sie Informationen bereitstellen über:
- Annäherungsrichtung,
- Flughöhe,
- Fluggeschwindigkeit,
- Flugbahn,
- Aufenthaltsdauer,
- Anzahl erkannter Objekte.

Je nach Technologie unterscheiden sich Reichweite, Erkennungswahrscheinlichkeit, Fehlalarmanfälligkeit, Wetterabhängigkeit sowie die Fähigkeit zur Erkennung autonomer oder ferngesteuerter Drohnen. Keine einzelne Sensortechnologie bietet unter allen Einsatzbedingungen optimale Ergebnisse. Für schutzbedürftige Einrichtungen empfiehlt sich daher regelmäßig die Kombination mehrerer Verfahren.

Die Auswahl geeigneter Systeme richtet sich nach Schutzbedarf, Geländestruktur und den betrieblichen Anforderungen.

3.3.7.1 Optische Detektionssysteme

Optische Systeme nutzen Kamerasysteme und Bildanalyseverfahren zur Erkennung und Klassifizierung von Flugobjekten.

Vorteile:
- hohe Detailerkennung,
- visuelle Verifikation,
- Unterstützung der Beweissicherung,
- Integration in bestehende Videoüberwachung.

Einschränkungen bestehen insbesondere bei:
- Dunkelheit,
- Nebel,
- Niederschlag,
- Verdeckungen durch Gebäude oder Vegetation.

Optische Systeme eignen sich insbesondere zur Identifikation bereits erkannter Objekte und zur Unterstützung der Lagebeurteilung.

3.3.7.2 Thermografische Detektionssysteme

Thermografische Systeme erkennen Wärmeabstrahlungen von Flugobjekten und können insbesondere bei schlechten Lichtverhältnissen eingesetzt werden.

Vorteile:
- Nachtfähigkeit,
- Unterstützung bei eingeschränkter Sicht,
- Ergänzung optischer Systeme.

Einschränkungen können auftreten durch:
- große Entfernungen,
- hohe Umgebungstemperaturen,
- ungünstige Witterungsbedingungen.

Thermografische Systeme werden häufig in Kombination mit optischen Kameras eingesetzt.

3.3.7.3 Funkfrequenzbasierte Detektion (RF)

RF-Systeme analysieren Funkverbindungen zwischen Drohnen und ihren Steuergeräten.
Hierdurch können unter bestimmten Voraussetzungen Informationen gewonnen werden über:
- erkannte Drohnentypen,
- Steuerungsverbindungen,
- Fernsteuerungsaktivitäten,
- mögliche Standorte von Fernpiloten.

Vorteile:
- frühzeitige Erkennung,
- teilweise Identifikation von Drohnentypen,
- Erkennung des Steuerungssignals.

Einschränkungen:
- autonome Drohnen ohne Funkverbindung können möglicherweise nicht erkannt werden,
- verschlüsselte oder unbekannte Protokolle können die Erkennung erschweren.

3.3.7.4 Akustische Detektionssysteme

Akustische Systeme identifizieren Drohnen anhand charakteristischer Rotor- und Antriebsgeräusche.

Vorteile:
- passive Betriebsweise,
- keine Funkaussendungen,
- zusätzliche Sensorquelle für Sensorfusion.

Einschränkungen:
- Hintergrundgeräusche,
- Wind,
- Industrieanlagen,
- begrenzte Reichweite.

Akustische Sensoren eignen sich insbesondere als ergänzende Technologie innerhalb eines mehrschichtigen Detektionskonzeptes.

3.3.7.5 Aktive Radarsysteme

Aktive Radarsysteme senden elektromagnetische Signale aus und analysieren deren Reflexionen zur Erkennung von Flugobjekten.

Vorteile:
- Erkennung autonomer Drohnen,
- hohe Reichweiten,
- weitgehende Unabhängigkeit von Lichtverhältnissen,
- Überwachung größerer Flächen.

Einschränkungen können sich ergeben durch:
- Abschattungen,
- komplexe Umgebungen,
- Reflexionen,
- technische und regulatorische Rahmenbedingungen.

Aktive Radarsysteme zählen heute zu den etablierten Technologien der Drohnendetektion.

3.3.7.6 Passive Radarsysteme

Passive Radarsysteme nutzen vorhandene elektromagnetische Aussendungen, beispielsweise Rundfunk-, Fernseh- oder Mobilfunksignale, als Signalquelle. Eigene Radarimpulse werden nicht ausgesendet.

Vorteile:
- keine aktive Aussendung,
- geringe elektromagnetische Signatur,
- Nutzung vorhandener Infrastruktur,
- Detektion auch autonomer Drohnen möglich.

Einschränkungen:
- Abhängigkeit von verfügbaren Signalquellen,
- komplexere Signalverarbeitung,
- technologieabhängige Leistungsfähigkeit.

Für Betreiber Kritischer Infrastrukturen wird derzeit unter anderem die Nutzung bestehender Mobilfunkinfrastrukturen, einschließlich LTE450-basierter Ansätze, untersucht. Solche Systeme können künftig eine sinnvolle Ergänzung bestehender Sensorarchitekturen darstellen, befinden sich jedoch teilweise noch in der Weiterentwicklung.

Derartige Ansätze stellen eine mögliche technologische Entwicklung dar. Die Auswahl geeigneter Detektionsverfahren sollte stets technologieoffen, risikoorientiert und anhand der konkreten Anforderungen der jeweiligen Einrichtung erfolgen.

3.3.7.7 Sensorfusion

Da jede Detektionstechnologie spezifische Stärken und Schwächen aufweist, empfiehlt sich für Einrichtungen mit erhöhtem Schutzbedarf die Kombination mehrerer Sensortechnologien.

Typische Kombinationen sind:
- Radar + Optik,
- Radar + Thermografie,
- RF + Optik,
- Radar + RF + Optik,
- Passivradar + Videoüberwachung.

Die Zusammenführung verschiedener Sensorinformationen kann die Erkennungswahrscheinlichkeit erhöhen, Fehlalarme reduzieren und die Qualität der Lagebeurteilung verbessern.

3.3.8 Alarmierung und Leitstellenintegration

Erkannte Drohnenereignisse sollten in bestehende Leitstellen- und Sicherheitsprozesse integriert werden.

Hierzu gehören insbesondere:
- automatische Alarmierung,
- Visualisierung der Lage,
- Zuordnung zu Sicherheitszonen,
- Unterstützung der Entscheidungsfindung,
- Dokumentation des Ereignisses.

Eine enge Integration reduziert Reaktionszeiten und verbessert die Lageübersicht.

3.3.9 Protokollierung und Beweissicherung

Technische Systeme sollten sicherheitsrelevante Ereignisse nachvollziehbar dokumentieren.

Hierzu zählen insbesondere:
- Zeitpunkt,
- Sensorquelle,
- erkannte Flugbewegungen,
- Bildmaterial,
- Alarmierungen,
- eingeleitete Maßnahmen,
- Abschlussbewertung.

Die Speicherung und Verarbeitung personenbezogener Daten hat unter Beachtung der datenschutzrechtlichen Anforderungen zu erfolgen.

3.3.10 Integration in bestehende Sicherheitsarchitekturen

Technische Schutzmaßnahmen sollten möglichst in bestehende Systeme integriert werden.

Hierzu zählen beispielsweise:
- Leitstellen,
- Gefahrenmanagementsysteme,
- Video-Management-Systeme,
- Zutrittskontrollsysteme,
- Perimeterschutz,
- SIEM-Systeme,
- Incident-Response-Plattformen.

Eine integrierte Sicherheitsarchitektur verbessert die Lagebewertung und vermeidet Medienbrüche.

3.3.11 Grenzen technischer Schutzmaßnahmen

Technische Systeme unterliegen betrieblichen und physikalischen Grenzen.

Diese können unter anderem resultieren aus:
- Witterungseinflüssen,
- Geländeabschattungen,
- Vegetation,
- baulichen Hindernissen,
- elektromagnetischen Störungen,
- Fehlalarmen,
- technischen Ausfällen.

Die Ergebnisse technischer Systeme sollten daher grundsätzlich durch qualifiziertes Personal bewertet werden.

3.3.12 Aktive Drohnenabwehr

Technische Maßnahmen zur aktiven Einwirkung auf Drohnen – beispielsweise durch Stör-, Übernahme- oder Abwehrsysteme – unterliegen in Deutschland besonderen rechtlichen Anforderungen.

Ihre Einführung und Nutzung sind vorab umfassend rechtlich zu prüfen. Insbesondere sind luftverkehrsrechtliche, telekommunikationsrechtliche, strafrechtliche sowie sicherheitsrechtliche Vorgaben zu beachten. Der Einsatz entsprechender Systeme kann hoheitlichen Stellen vorbehalten sein oder einer besonderen Genehmigung bedürfen.

Dieser Leitfaden behandelt daher ausschließlich die organisatorischen Voraussetzungen und die Einordnung solcher Systeme in ein Gesamtsicherheitskonzept. Eine Empfehlung zum Einsatz bestimmter aktiver Abwehrtechnologien wird ausdrücklich nicht ausgesprochen.

Entscheidungen über den Einsatz aktiver Gegenmaßnahmen sind nachvollziehbar zu dokumentieren. Dies umfasst insbesondere Anlass, Entscheidungsgrundlage, beteiligte Stellen, durchgeführte Maßnahmen sowie deren Ergebnis.

Nach derzeitiger Rechtslage wird die aktive Drohnenabwehr grundsätzlich als hoheitliche Aufgabe betrachtet. Betreiber Kritischer Infrastrukturen sollten daher den Schwerpunkt auf Risikoanalyse, Detektion, Alarmierung, organisatorische Vorsorge und Resilienz legen.

3.3.13 Wartung und kontinuierliche Verbesserung

Technische Schutzmaßnahmen sollten regelmäßig überprüft werden.

Hierzu gehören insbesondere:

- Funktionsprüfungen,
- Wartungsintervalle,
- Software-Updates,
- Kalibrierungen,
- Tests der Alarmierung,
- Dokumentation technischer Änderungen,
- Bewertung neuer Technologien.

Die Ergebnisse sind in den kontinuierlichen Verbesserungsprozess des Sicherheitsmanagements einzubeziehen.

3.3.14 Kernaussagen für Entscheider

- Technische Schutzmaßnahmen ergänzen organisatorische und bauliche Maßnahmen, ersetzen diese jedoch nicht.
- Ein mehrschichtiges Detektionskonzept erhöht die Erkennungswahrscheinlichkeit und reduziert Fehlalarme.
- Die Auswahl technischer Systeme muss sich am Schutzbedarf und der Risikoanalyse orientieren.
- Aktive Drohnenabwehr unterliegt in Deutschland besonderen rechtlichen Anforderungen und sollte nur nach sorgfältiger rechtlicher Bewertung in Betracht gezogen werden.

3.3.15 Handlungsempfehlungen

Betreiber Kritischer Infrastrukturen sollten:

- technische Schutzmaßnahmen auf Grundlage der Schutzbedarfsfeststellung und Risikoanalyse auswählen;
- nach Möglichkeit mehrere komplementäre Sensortechnologien kombinieren;
- Detektionssysteme in bestehende Leitstellen- und Sicherheitsprozesse integrieren;
- Alarmierungs- und Dokumentationsprozesse regelmäßig testen;
- technische Systeme kontinuierlich warten und an den Stand der Technik anpassen.

Die Wirksamkeit technischer Detektionssysteme ist im jeweiligen Einsatzumfeld regelmäßig zu überprüfen und anhand praktischer Tests sowie betrieblicher Erfahrungen zu validieren.

4 Teil IV – Betrieb und Reaktion

4.1 Ereigniserkennung, Incident Response und Beweissicherung

4.1.1 Zielsetzung

Trotz geeigneter organisatorischer, baulicher und technischer Schutzmaßnahmen lassen sich Drohnenvorfälle nicht vollständig verhindern. Ziel einer wirksamen Incident Response ist es daher, drohnenbezogene Ereignisse frühzeitig zu erkennen, sachgerecht zu bewerten, geeignete Reaktionsmaßnahmen einzuleiten und Erkenntnisse für die kontinuierliche Verbesserung des Sicherheitsmanagements zu gewinnen.

Die in diesem Kapitel beschriebenen Maßnahmen ergänzen bestehende Prozesse des Informationssicherheits-, Notfall- und Krisenmanagements. Es wird empfohlen, keine eigenständigen Parallelprozesse für Drohnenvorfälle zu etablieren, sondern diese in bestehende Incident-Response-Strukturen zu integrieren.

4.1.2 Bezug zu Managementsystemen und Regelwerken

Dieses Kapitel unterstützt die strukturierte Behandlung drohnenbezogener Sicherheitsvorfälle von der Erkennung bis zur Nachbereitung.

Relevante Regelwerke:

- ISO/IEC 27001: Betrieb und Behandlung von Informationssicherheitsvorfällen
- ISO/IEC 27035: Incident Management
- BSI IT-Grundschutz: Behandlung von Sicherheitsvorfällen
- NIS-2 / BSIG: Meldung und Behandlung von Vorfällen

4.1.3 Grundsätze der Incident Response

Die Behandlung drohnenbezogener Vorfälle sollte sich an folgenden Grundsätzen orientieren:

- Schutz von Menschen hat stets Vorrang.
- Entscheidungen erfolgen risikobasiert.
- Rollen und Verantwortlichkeiten sind eindeutig festgelegt.
- Ereignisse werden vollständig dokumentiert.
- Maßnahmen erfolgen unter Beachtung der geltenden Rechtslage.
- Erkenntnisse fließen in den kontinuierlichen Verbesserungsprozess ein.

4.1.4 Ereigniserkennung

Drohnenvorfälle können durch unterschiedliche Quellen erkannt werden.

Mögliche Informationsquellen sind insbesondere:
- technische Detektionssysteme,
- Videoüberwachung,
- Werkschutz,
- Beschäftigte,
- Besucher,
- externe Sicherheitsdienstleister,
- Polizei oder Sicherheitsbehörden,
- benachbarte Unternehmen.

Alle Meldungen sollten unabhängig von ihrer Quelle einer strukturierten Erstbewertung unterzogen werden.

4.1.5 Erstbewertung

Nach Eingang einer Meldung ist zunächst festzustellen, ob tatsächlich ein sicherheitsrelevanter Vorfall vorliegt.

Dabei sollten insbesondere folgende Fragestellungen berücksichtigt werden:
- Handelt es sich tatsächlich um eine Drohne?
- Befindet sich die Drohne innerhalb oder außerhalb des relevanten Schutzbereichs?
- Besteht eine erkennbare Gefährdung?
- Welche Bereiche sind betroffen?
- Liegen Hinweise auf weitere Beteiligte vor?
- Ist eine sofortige Eskalation erforderlich?

Die Erstbewertung sollte anhand standardisierter Kriterien erfolgen.

4.1.6 Klassifizierung des Vorfalls

Zur einheitlichen Behandlung empfiehlt sich die Zuordnung zu einer standardisierten Ereigniskategorie.

Hierbei sollte auf die in Kapitel 1.4 eingeführte UAS Threat Taxonomy Bezug genommen werden.

Die Klassifizierung sollte mindestens umfassen:
- Ereignisart,
- Bedrohungskategorie,
- betroffene Schutzobjekte,
- vermutete Zielsetzung,
- Bewertung des Risikos,
- aktuelle Bewertung der Vorfallschwere (UAS-Incident-Klassifikation).

4.1.6.1 UAS-Incident-Klassifikation

Zur einheitlichen Bewertung und Behandlung drohnenbezogener Sicherheitsvorfälle empfiehlt dieser Leitfaden eine standardisierte Incident-Klassifikation. Sie dient der schnellen Einordnung des Ereignisses, unterstützt die Auswahl geeigneter Reaktionsmaßnahmen und erleichtert die organisationsübergreifende Kommunikation sowie die spätere Auswertung von Vorfällen.

Die Klassifikation orientiert sich an der tatsächlichen oder potenziellen Auswirkung des Vorfalls auf die Organisation und ergänzt die in Kapitel 1.4 beschriebene UAS Threat Taxonomy und dient der operativen Bewertung der Schwere eines Vorfalls.

Stufe	Bezeichnung	Beschreibung	Typische Maßnahmen
UAS-I0	Kein Sicherheitsvorfall	Verdachtsmeldung oder Fehlalarm. Keine sicherheitsrelevante Drohnenaktivität nachweisbar.	Dokumentation, Abschluss der Meldung
UAS-I1	Geringfügiger Vorfall	Einzelne Drohnensichtung ohne erkennbare Gefährdung oder Bezug zu kritischen Einrichtungen.	Beobachtung, Dokumentation, ggf. Information des Werkschutzes
UAS-I2	Sicherheitsrelevanter Vorfall	Drohne überfliegt oder nähert sich sicherheitsrelevanten Bereichen; Ausspähung oder Vorbereitungshandlungen können nicht ausgeschlossen werden.	Alarmierung, Lagebewertung, Beweissicherung, Information verantwortlicher Stellen
UAS-I3	Schwerwiegender Sicherheitsvorfall	Konkrete Hinweise auf gezielte Ausspähung, Sabotagevorbereitung oder erhebliche Beeinträchtigung kritischer Prozesse.	Erweiterte Alarmierung, Einbindung der Unternehmensleitung, Information zuständiger Behörden, Vorbereitung Krisenstab
UAS-I4	Kritischer Sicherheitsvorfall	Drohnenbedingte Beeinträchtigung kritischer Prozesse, erhebliche Gefährdung von Menschen oder Infrastruktur oder koordinierter Angriff.	Krisenstab aktivieren, umfassende Behördenkommunikation, Einleitung von Notfall- und BCM-Maßnahmen
UAS-I5	Außergewöhnliche Gefahrenlage	Mehrere koordinierte Drohnen, hybride Angriffe oder erhebliche Auswirkungen auf die Versorgungssicherheit bzw. nationale Sicherheitsinteressen.	Vollständige Krisenorganisation, enge Zusammenarbeit mit Sicherheitsbehörden, fortlaufende Lagebewertung und strategische Kommunikation

Die dargestellten Maßnahmen stellen Beispielreaktionen dar. Maßgeblich bleiben die organisationsspezifischen Melde-, Eskalations- und Krisenmanagementprozesse.

Die Einstufung sollte insbesondere berücksichtigen:

- Objektbezogene Kriterien
  - betroffener Sicherheitsbereich,
  - Schutzbedarf des Zielobjekts,
  - Auswirkungen auf Betrieb und Versorgung,
  - Gefährdung von Personen.
- Vorfallsbezogene Kriterien
  - Anzahl der beteiligten Drohnen,
  - Flug- und Bewegungsverhalten,
  - erkennbare Angriffsabsicht,
  - Erkenntnisse aus technischen Detektionssystemen,
  - aktuelle Erkenntnisse der Sicherheitsbehörden.

Für jeden Vorfall sollten mindestens folgende Informationen dokumentiert werden:

- Incident-Kennung,
- Incident-Stufe (UAS-I0 bis UAS-I5),
- zugeordnete Kategorie der UAS Threat Taxonomy (T1 bis T6)
- Datum und Uhrzeit,
- betroffener Standort,
- betroffene Schutzobjekte,
- eingeleitete Maßnahmen,
- Behördenkontakte,
- Abschlussbewertung,
- Lessons Learned.

Hinweis: Jeder drohnenbezogene Vorfall sollte sowohl einer Kategorie der UAS Threat Taxonomy (z. B. T1 Informationsgewinnung oder T4 Sabotage) als auch einer Incident-Stufe (UAS-I0 bis UAS-I5) zugeordnet werden. Dabei beschreibt die Taxonomie die Art der Bedrohung, die Incident-Stufe dagegen die Schwere des Ereignisses.

4.1.7 Operative Reaktionsmaßnahmen

Die einzuleitenden Maßnahmen richten sich nach Art und Schwere des Vorfalls.

Hierzu können insbesondere gehören:

- Lagefeststellung
  - Lagebeobachtung,
  - Dokumentation des Ereignisses.
- Operative Maßnahmen
  - Alarmierung des Werkschutzes,
  - Information zuständiger Führungskräfte,
  - Absicherung gefährdeter Bereiche,
  - Schutz von Beschäftigten und Besuchern.
- Eskalation
  - Information externer Stellen,
  - Einberufung des Krisenstabs.

Maßnahmen zur aktiven Einwirkung auf Drohnen dürfen ausschließlich im Rahmen der geltenden Rechtsordnung erfolgen.

4.1.8 Zusammenarbeit mit Behörden

Je nach Art des Ereignisses kann eine frühzeitige Einbindung zuständiger Behörden erforderlich sein.

Hierzu zählen insbesondere:
- Polizei,
- Landeskriminalamt,
- Verfassungsschutz,
- Bundesamt für Sicherheit in der Informationstechnik,
- zuständige Luftfahrtbehörden,
- Feuerwehr,
- Rettungsdienst.

Die Alarmierungswege sollten bereits im Vorfeld festgelegt und regelmäßig überprüft werden.

4.1.9 Beweissicherung

Eine sorgfältige Dokumentation kann sowohl für interne Untersuchungen als auch für straf- oder zivilrechtliche Verfahren von erheblicher Bedeutung sein.

Soweit rechtlich zulässig, sollten insbesondere gesichert werden:
- Zeitpunkt und Dauer des Vorfalls,
- Ort,
- Flugrichtung,
- Flughöhe,
- Anzahl der Drohnen,
- Bild- und Videomaterial,
- Sensordaten,
- Zeugenaussagen,
- getroffene Maßnahmen,
- Kommunikation mit Behörden.

Die Integrität der Beweismittel sollte jederzeit gewährleistet sein.

Auf die in **Anhang F – Leitfaden zur Beweissicherung** enthaltene Checkliste wird ergänzend verwiesen

4.1.10 Kommunikation

Während eines Drohnenvorfalls sollte die Kommunikation klar geregelt sein.

Hierzu gehören insbesondere:
- interne Lageinformationen,
- Kommunikation mit Führungskräften,
- Behördenkommunikation,
- Kommunikation mit Dienstleistern,
- Medienanfragen,
- Information betroffener Dritter.

Auskünfte gegenüber Medien sollten ausschließlich durch autorisierte Personen erfolgen.

4.1.11 Operative Incident-Nachbereitung

Nach Abschluss der unmittelbaren Vorfallbearbeitung sollte eine erste operative Nachbereitung erfolgen.

Hierzu gehören insbesondere die Vervollständigung der Dokumentation, die Sicherung relevanter Erkenntnisse sowie die Bewertung der Wirksamkeit eingeleiteter Maßnahmen.

Weitergehende Lessons-Learned-Prozesse werden in Kapitel 5 beschrieben. Die strukturierte fachliche Nachbereitung des Ereignisses erfolgt gemäß Kapitel 5.2.

4.1.12 Dokumentation

Für jeden sicherheitsrelevanten Drohnenvorfall sollte eine nachvollziehbare Dokumentation erstellt werden.

Diese sollte mindestens enthalten:

- Aktenzeichen,
- Datum und Uhrzeit,
- Ereignisbeschreibung,
- Klassifizierung,
- beteiligte Organisationseinheiten,
- eingeleitete Maßnahmen,
- Behördenkontakte,
- Beweismittel,
- Abschlussbewertung,
- Verbesserungsvorschläge.

Die Dokumentation sollte revisionssicher erfolgen und in bestehende Incident-Management-Systeme integriert werden.

4.1.13 Kernaussagen für Entscheider

- Eine strukturierte Incident Response reduziert die Auswirkungen drohnenbezogener Vorfälle.
- Standardisierte Prozesse und Eskalationsstufen erleichtern schnelle und nachvollziehbare Entscheidungen.
- Beweissicherung und Dokumentation sind wesentliche Voraussetzungen für die spätere Aufarbeitung und mögliche Strafverfolgung.
- Erkenntnisse aus Vorfällen sollten systematisch in das Sicherheitsmanagement zurückgeführt werden.

4.1.14 Handlungsempfehlungen

Betreiber Kritischer Infrastrukturen sollten:

- drohnenbezogene Vorfälle in bestehende Incident-Response-Prozesse integrieren;
- standardisierte Verfahren zur Erstbewertung und Klassifizierung einführen;
- Alarmierungs- und Kommunikationswege regelmäßig überprüfen und üben;
- Verfahren zur rechtskonformen Beweissicherung etablieren;
- jeden Vorfall systematisch nachbereiten und die Ergebnisse in Risikoanalyse, Schulungen und Sicherheitskonzepte einfließen lassen.

4.2 Krisenmanagement und Business Continuity Management

4.2.1 Zielsetzung

Trotz angemessener organisatorischer, baulicher und technischer Schutzmaßnahmen können Drohnenvorfälle Auswirkungen auf kritische Prozesse, Betriebsabläufe und die Versorgungssicherheit haben. Insbesondere koordinierte Ausspähungs-, Sabotage- oder hybride Angriffsszenarien können eine über den normalen Incident-Response-Prozess hinausgehende Bewältigung erfordern.

Selbst bei wirksamen Detektions- und Schutzmaßnahmen kann ein drohnenbezogener Vorfall nicht in jedem Fall verhindert werden. Daher besitzen Business Continuity Management, Wiederanlaufplanung und organisatorische Resilienz eine vergleichbare Bedeutung wie präventive Sicherheitsmaßnahmen.

Ziel dieses Kapitels ist die Beschreibung der Einbindung drohnenbezogener Ereignisse in das Krisenmanagement und Business Continuity Management (BCM). Hierdurch soll sichergestellt werden, dass auch schwerwiegende Vorfälle strukturiert bewältigt, betriebliche Auswirkungen begrenzt und kritische Dienstleistungen aufrechterhalten werden können.

Das Kapitel ergänzt die in Kapitel 2 beschriebenen Governance-Strukturen, die Risikoanalyse nach Kapitel 2.2 sowie die Incident-Response-Prozesse gemäß Kapitel 4.

4.2.2 Bezug zu Managementsystemen und Regelwerken

Dieses Kapitel beschreibt Maßnahmen zur Bewältigung schwerwiegender Drohnenvorfälle und zur Aufrechterhaltung kritischer Geschäftsprozesse.

Relevante Regelwerke:

- ISO 22301: Business Continuity Management
- ISO 22320: Krisenmanagement
- BSI Standard 200-4
- NIS-2 / BSIG: Resilienz kritischer Dienste

4.2.3 Grundsätze

Die Behandlung drohnenbezogener Krisenszenarien sollte sich an folgenden Grundsätzen orientieren:

- Schutz von Menschen hat Vorrang.
- Kritische Dienstleistungen sind möglichst aufrechtzuerhalten.
- Entscheidungen erfolgen lage- und risikoorientiert.
- Die Krisenorganisation nutzt bestehende Strukturen.
- Zuständigkeiten und Befugnisse sind eindeutig geregelt.
- Kommunikation erfolgt abgestimmt und nachvollziehbar.
- Erkenntnisse fließen in die kontinuierliche Verbesserung ein.

Drohnenbedrohungen sollten dabei nicht isoliert betrachtet werden. Sie können Bestandteil komplexer Sicherheitslagen sein und gleichzeitig physische, organisatorische, informationstechnische und betriebliche Auswirkungen verursachen.

4.2.4 Einordnung in das Business Continuity Management

Aus Sicht des BCM stellen Drohnenvorfälle potenzielle Störungen dar, die Auswirkungen auf die Verfügbarkeit kritischer Prozesse und Dienstleistungen haben können.
Mögliche Folgen sind insbesondere:

- Betriebsunterbrechungen,
- Evakuierungen,
- Zugangsbeschränkungen,
- Ausfall technischer Einrichtungen,
- Unterbrechung von Lieferketten,
- Beeinträchtigung kritischer Dienstleistungen,
- Reputationsschäden.

Drohnenbezogene Szenarien sollten daher Bestandteil bestehender BCM-Prozesse sein und bereits bei Business Impact Analysen sowie Notfallplanungen berücksichtigt werden.

4.2.5 Ereignisse mit Krisenpotenzial

Nicht jede Drohnensichtung stellt einen Krisenfall dar. Bestimmte Ereignisse können jedoch eine Aktivierung der Krisenorganisation erforderlich machen.

Hierzu zählen insbesondere:

- wiederholte zielgerichtete Überflüge kritischer Bereiche,
- Hinweise auf Ausspähung oder Sabotagevorbereitungen,
- koordinierte Angriffe mit mehreren Drohnen,
- Drohnen als Bestandteil hybrider Angriffe,
- Beeinträchtigung kritischer Prozesse,
- Gefährdung von Beschäftigten oder Dritten,
- Auswirkungen auf die Versorgungssicherheit,
- erhebliche öffentliche Aufmerksamkeit oder Medieninteresse.

Die Entscheidung über die Aktivierung der Krisenorganisation sollte anhand definierter Kriterien erfolgen.

4.2.6 Aktivierung des Krisenmanagements

Die Aktivierung der Krisenorganisation sollte auf Grundlage festgelegter Eskalations- und Entscheidungsprozesse erfolgen.

Typische Auslöser können sein:

Ereignis	Mögliche Bewertung
Wiederholte Ausspähung kritischer Bereiche	Krisenrelevant
Verdacht auf koordinierte Angriffsvorbereitung	Krisenrelevant
Sabotageverdacht	Krisenrelevant
Ausfall kritischer Prozesse	Krisenrelevant
Mehrere gleichzeitig eingesetzte Drohnen	Krisenrelevant
Gefährdung von Personen	Krisenrelevant
Erhebliche Auswirkungen auf die Versorgung	Krisenfall

4.2.7 Aufgaben des Krisenstabs

Nach der Aktivierung übernimmt der Krisenstab die strategische Steuerung der Ereignisbewältigung.

Zu seinen Aufgaben gehören insbesondere:

- Lagefeststellung und Lagebewertung,
- Priorisierung von Maßnahmen,
- Schutz kritischer Prozesse,
- Ressourcensteuerung,
- Behördenkommunikation,
- interne Kommunikation,
- externe Kommunikation,
- Entscheidung über BCM-Maßnahmen,
- Vorbereitung von Wiederanlaufmaßnahmen.

Der Krisenstab sollte eng mit Informationssicherheit, Werkschutz, BCM, OT-Sicherheit und Unternehmensleitung zusammenarbeiten.

4.2.8 Lagebild und Lageführung

Für eine wirksame Krisenbewältigung ist ein aktuelles und nachvollziehbares Lagebild erforderlich.

Dieses sollte insbesondere enthalten:
- Zeitpunkt und Ort des Ereignisses,
- Anzahl beteiligter Drohnen,
- aktuelle Bedrohungsbewertung,
- betroffene Schutzobjekte,
- Auswirkungen auf den Betrieb,
- eingeleitete Maßnahmen,
- Behördenkontakte,
- offene Risiken,
- erwartete Entwicklungen.

Die Lagebeurteilung sollte fortlaufend aktualisiert und dokumentiert werden.

Betreiber Kritischer Infrastrukturen sollten darüber hinaus prüfen, inwieweit drohnenbezogene Erkenntnisse mit benachbarten Standorten, verbundenen Unternehmen oder zuständigen Behörden ausgetauscht werden können. Ziel kann der Aufbau eines gemeinsamen Lagebilds zur frühzeitigen Erkennung koordinierter Aktivitäten sein.

4.2.9 Schutz kritischer Geschäftsprozesse

Das zentrale Ziel des Business Continuity Managements besteht in der Aufrechterhaltung kritischer Geschäftsprozesse.

Hierzu können insbesondere folgende Maßnahmen erforderlich sein:
- Verlagerung von Tätigkeiten,
- Nutzung alternativer Standorte,
- Aktivierung von Redundanzen,
- Priorisierung kritischer Ressourcen,
- Einschränkung nicht kritischer Aktivitäten,
- Einsatz zusätzlicher Sicherheitsmaßnahmen,
- Anpassung von Betriebsabläufen.

Diese Maßnahmen sollten bereits im Vorfeld geplant und dokumentiert werden.

4.2.10 Notfall- und Wiederanlaufmaßnahmen

Für Szenarien mit erheblichen Auswirkungen auf den Geschäftsbetrieb sollten Notfall- und Wiederanlaufverfahren vorhanden sein.

Hierzu zählen beispielsweise:
- Ausweichverfahren,
- Ersatzarbeitsplätze,
- alternative Kommunikationswege,
- technische Redundanzen,
- Wiederanlaufpläne,
- Ressourcen- und Personalplanung.

Der Wiederanlauf kritischer Prozesse sollte risikoorientiert priorisiert werden.

4.2.11 Kommunikation im Krisenfall

Drohnenvorfälle können ein erhebliches öffentliches Interesse hervorrufen. Deshalb ist eine strukturierte Kommunikationsstrategie erforderlich.

Zu berücksichtigen sind insbesondere:
- Kommunikation mit Beschäftigten,
- Kommunikation mit Auftraggebern,
- Information von Partnern und Dienstleistern,
- Kommunikation mit Behörden,
- Medienanfragen,
- Kommunikation mit Betreibern benachbarter Kritischer Infrastrukturen.

Auskünfte gegenüber Medien und Öffentlichkeit sollten ausschließlich durch autorisierte Personen erfolgen.

4.2.12 Zusammenarbeit mit Behörden

Bei schwerwiegenden Vorfällen kann eine enge Zusammenarbeit mit zuständigen Behörden erforderlich sein.

Mögliche Ansprechpartner sind insbesondere:
- Polizei,
- Landeskriminalamt,
- Verfassungsschutz,
- Bundesamt für Sicherheit in der Informationstechnik,
- Luftfahrtbehörden,
- Feuerwehr,
- Katastrophenschutzbehörden,
- Betreiber benachbarter Kritischer Infrastrukturen,
- Entsprechende Landesbehörden.

Soweit vorhanden sollten auch sektorspezifische Melde- und Koordinierungsstrukturen berücksichtigt werden, beispielsweise CERTs, branchenspezifische Informationsverbünde oder KRITIS-Koordinierungsgremien.

Zuständigkeiten und Meldewege sollten bereits vor Eintritt eines Ereignisses festgelegt sein.

4.2.13 Übungen, Tests und Nachbesprechungen

Die Krisenorganisation sollte regelmäßig hinsichtlich ihrer Reaktionsfähigkeit überprüft werden.

Geeignete Übungsformate sind insbesondere:
- Tabletop-Übungen,
- Stabsrahmenübungen,
- Alarmierungsübungen,
- Kommunikationsübungen,
- BCM-Übungen,
- standortübergreifende Übungen.

Übungsergebnisse sollten dokumentiert und in Verbesserungsmaßnahmen überführt werden.

4.2.14 Kennzahlen und Wirksamkeitskontrolle

Zur Bewertung der Krisenvorsorge können geeignete Kennzahlen verwendet werden.

Beispiele:
- Zeit bis zur Krisenstabsaktivierung,
- Zeit bis zur Lagefeststellung,
- Dauer der Wiederherstellung kritischer Prozesse,
- Anzahl durchgeführter Übungen,
- Umsetzungsgrad von Verbesserungsmaßnahmen,
- Ergebnisse interner Audits.

Die Kennzahlen sollten regelmäßig im Rahmen von Management Reviews bewertet werden.

4.2.15 Kontinuierliche Verbesserung

Nach jedem relevanten Vorfall sowie nach Übungen sollte eine strukturierte Nachbereitung erfolgen.

Hierzu gehören insbesondere:
- Ursachenanalyse,
- Bewertung der Krisenorganisation,
- Bewertung der BCM-Maßnahmen,
- Lessons Learned,
- Aktualisierung der Risikoanalyse,
- Anpassung von Notfall- und Krisenplänen,
- Aktualisierung von Schulungs- und Übungsprogrammen.

Die Ergebnisse sind systematisch in das Sicherheitsmanagement zurückzuführen.

Erkenntnisse aus Vorfällen, Übungen, Audits sowie wesentlichen Änderungen der Bedrohungslage sollten systematisch ausgewertet und in bestehende Sicherheits-, Notfall- und Business-Continuity-Managementprozesse übernommen werden.

4.2.16 Kernaussagen für Entscheider

- Drohnenvorfälle können erhebliche Auswirkungen auf kritische Prozesse und Dienstleistungen haben.
- Nicht jede Drohnensichtung ist ein Krisenfall; definierte Eskalationskriterien sind erforderlich.
- Krisenmanagement und BCM sollten bestehende Strukturen nutzen und um drohnenbezogene Szenarien ergänzt werden.
- Die Aufrechterhaltung kritischer Prozesse besitzt im Krisenfall hohe Priorität.
- Regelmäßige Übungen und Reviews sind wesentliche Voraussetzungen für eine wirksame Krisenvorsorge.

4.2.17 Handlungsempfehlungen

Betreiber Kritischer Infrastrukturen sollten:

- drohnenbezogene Szenarien in BCM und Krisenmanagement integrieren;
- Aktivierungskriterien für den Krisenstab definieren;
- Notfall- und Wiederanlaufverfahren überprüfen;
- Kommunikations- und Behördenkontakte vorab festlegen;
- regelmäßige Krisen- und BCM-Übungen durchführen;
- Lessons Learned systematisch auswerten und umsetzen.

5 Teil V – Überwachung und Verbesserung

5.1 Übungen, Audits und kontinuierliche Verbesserung

5.1.1 Zielsetzung

Die Wirksamkeit organisatorischer, baulicher und technischer Schutzmaßnahmen kann nicht allein anhand ihrer Planung oder Dokumentation beurteilt werden. Erst durch Übungen, Audits, Tests sowie die systematische Auswertung von Vorfällen lässt sich feststellen, ob die implementierten Maßnahmen tatsächlich geeignet sind, drohnenbezogene Risiken angemessen zu beherrschen.
Ziel dieses Kapitels ist die Beschreibung eines strukturierten Vorgehens zur Überprüfung, Bewertung und kontinuierlichen Verbesserung des Schutzkonzeptes gegen drohnenbezogene Bedrohungen. Die dargestellten Maßnahmen unterstützen Organisationen dabei, die Wirksamkeit ihrer Sicherheitsvorkehrungen regelmäßig zu überprüfen und an veränderte Bedrohungen, regulatorische Anforderungen und technologische Entwicklungen anzupassen.

5.1.2 Bezug zu Managementsystemen und Regelwerken

Dieses Kapitel unterstützt die regelmäßige Überprüfung der Wirksamkeit implementierter Maßnahmen sowie die kontinuierliche Weiterentwicklung der Sicherheitsorganisation.

Relevante Regelwerke:
- ISO/IEC 27001: Leistungsbewertung
- ISO/IEC 27001: Internes Audit
- ISO/IEC 27001: Managementbewertung
- ISO 22301: Übungen und Tests
- BSI IT-Grundschutz: Audit und Revision

5.1.3 Grundsätze

Übungen, Audits und Verbesserungsmaßnahmen sollten auf folgenden Grundsätzen basieren:
- Risikoorientierung,
- Regelmäßigkeit,
- Nachvollziehbarkeit,
- Dokumentation,
- Management-Unterstützung,
- Interdisziplinäre Beteiligung,
- Kontinuierliche Verbesserung,
- Überprüfung der tatsächlichen Wirksamkeit.

Nicht die Existenz von Dokumenten oder Prozessen ist entscheidend, sondern deren praktische Anwendbarkeit und Wirksamkeit im Ereignisfall.

5.1.4 Übungsplanung

Übungen dienen der Überprüfung organisatorischer und operativer Fähigkeiten unter möglichst realistischen Bedingungen.

Eine strukturierte Übungsplanung sollte mindestens festlegen:
- Übungsziele,
- Übungsszenario,
- beteiligte Organisationseinheiten,
- Bewertungskriterien,
- Verantwortlichkeiten,
- Dokumentationsanforderungen,
- Nachbereitungsprozess.

Die Auswahl der Szenarien sollte sich an den Ergebnissen der Risikoanalyse orientieren.

5.1.5 Übungsarten

5.1.5.1 Sensibilisierungsübungen

Sensibilisierungsübungen dienen der Vermittlung grundlegender Kenntnisse über drohnenbezogene Bedrohungen.

Typische Inhalte sind:
- Erkennung von Drohnensichtungen,
- Meldewege,
- Verhalten im Ereignisfall,
- Schutz sensibler Informationen.

5.1.5.2 Tabletop-Übungen

Tabletop-Übungen ermöglichen die strukturierte Diskussion realistischer Szenarien.

Geeignete Übungsannahmen sind beispielsweise:
- wiederholte Aufklärungsflüge,
- Ausspähung kritischer Anlagen,
- Drohne über sicherheitskritischen Bereichen,
- hybride Angriffsszenarien,
- koordinierte Sicherheitsvorfälle.

Sie eignen sich insbesondere für Führungskräfte, Krisenstäbe und Sicherheitsverantwortliche.

5.1.5.3 Alarmierungsübungen

Alarmierungsübungen überprüfen die Funktionsfähigkeit festgelegter Melde- und Eskalationsprozesse.

Hierbei kann insbesondere geprüft werden:
- Erreichbarkeit,
- Reaktionszeiten,
- Vollständigkeit von Alarmierungsketten,

- Rollenverständnis der Beteiligten.

5.1.5.4 Krisenstabsübungen

Krisenstabsübungen dienen der Überprüfung strategischer Entscheidungsprozesse.

Im Mittelpunkt stehen insbesondere:
- Lagebewertung,
- Priorisierung von Maßnahmen,
- Kommunikation,
- BCM-Entscheidungen,
- Behördenkoordination.

5.1.5.5 Technische Übungen und Funktionstests

Technische Übungen überprüfen die Einsatzfähigkeit vorhandener Schutzsysteme.

Hierzu zählen beispielsweise:
- Tests von Detektionssystemen,
- Alarmierungstests,
- Leitstellenintegration,
- Videoüberwachung,
- Kommunikationssysteme,
- Dokumentationsverfahren.

5.1.5.6 Vollübungen

Vollübungen bilden möglichst realistische Einsatzbedingungen ab.

Sie können umfassen:
- Werkschutz,
- Leitstelle,
- BCM,
- Krisenstab,
- externe Dienstleister,
- zuständige Behörden.

Aufgrund ihres hohen Aufwands sollten sie risikoorientiert durchgeführt werden.

5.1.6 Auditierung und Wirksamkeitsprüfung

Neben Übungen sollten drohnenbezogene Sicherheitsmaßnahmen regelmäßig auditiert werden.

Auditgegenstände können insbesondere sein:

- Governance-Strukturen,
- Rollen und Verantwortlichkeiten,
- Melde- und Eskalationsprozesse,
- Risikoanalysen,
- Dokumentationen,
- Schulungsprogramme,
- technische Systeme,
- BCM- und Krisenmanagementprozesse.

Audits können intern oder extern durchgeführt werden.

5.1.7 Auditfragen beispielhaft

Zur Vorbereitung interner Audits können folgende Fragestellungen herangezogen werden:

- Governance
  - Sind drohnenbezogene Risiken dokumentiert?
  - Sind Rollen und Verantwortlichkeiten festgelegt?
  - Existieren dokumentierte Meldewege?
- Organisation
  - Wurden Schulungen durchgeführt?
  - Sind BCM-Szenarien vorhanden?
  - Wurden Krisenstabsübungen durchgeführt?
- Wirksamkeit
  - Werden Vorfälle systematisch dokumentiert?
  - Werden Lessons Learned umgesetzt?
  - Werden externe Behördenkontakte aktuell gehalten?

5.1.8 Kennzahlen und Leistungsindikatoren

Zur Bewertung der Wirksamkeit empfiehlt sich die Definition geeigneter Kennzahlen (Key Performance Indicators – KPI).

Beispiele:

Kennzahl	Zielsetzung
Anteil geschulter Beschäftigter	Sensibilisierung
Anzahl durchgeführter Übungen	Reifegradmessung
Zeit bis zur Erstbewertung	Reaktionsfähigkeit
Zeit bis zur Alarmierung	Prozessqualität
Anzahl wiederkehrender Feststellungen	Verbesserungsbedarf
Umsetzungsgrad von Maßnahmen	Wirksamkeit
Anzahl dokumentierter Lessons Learned	Lernfähigkeit

Kennzahlen sollten regelmäßig im Rahmen von Management Reviews bewertet werden.

5.1.9 Lessons Learned

Erkenntnisse aus Vorfällen, Übungen und Audits stellen eine wesentliche Grundlage für die Weiterentwicklung des Sicherheitskonzeptes dar.

Bewertet werden sollten insbesondere:
- Was hat gut funktioniert?
- Wo bestanden Schwächen?
- Welche Prozesse waren nicht ausreichend wirksam?
- Welche organisatorischen Defizite wurden sichtbar?
- Welche technischen Verbesserungen sind erforderlich?
- Welche Schulungsmaßnahmen sind anzupassen?

Die Ergebnisse sollten dokumentiert und nachverfolgt werden.

5.1.10 Maßnahmenmanagement

Festgestellte Verbesserungsmaßnahmen sollten systematisch erfasst und verfolgt werden.

Für jede Maßnahme sollten mindestens dokumentiert werden:
- Beschreibung,
- Priorität,
- Verantwortliche Stelle,
- Umsetzungsfrist,
- Status,
- Wirksamkeitsnachweis.

Eine regelmäßige Berichterstattung an die Unternehmensleitung wird empfohlen.

5.1.11 Management Reviews

Die Ergebnisse aus Übungen, Audits, Vorfällen und Verbesserungsmaßnahmen sollten regelmäßig durch die Unternehmensleitung bewertet werden.

Hierbei sollten insbesondere betrachtet werden:

- aktuelle Bedrohungslage,
- Wirksamkeit vorhandener Maßnahmen,
- Umsetzungsstand von Verbesserungen,
- Ergebnisse von Audits,
- Erkenntnisse aus Vorfällen,
- Ressourcenbedarf.

Management Reviews unterstützen die strategische Steuerung der Sicherheitsorganisation.

5.1.12 Reifegradmodell für Übungen und Verbesserung

Organisationen können ihre Fähigkeiten anhand eines Reifegradmodells bewerten.

Reifegrad	Beschreibung
U0	Keine Übungen oder Audits
U1	Einzelne Sensibilisierungsmaßnahmen
U2	Dokumentierte Übungen und Audits
U3	Regelmäßige Durchführung und Auswertung
U4	Integration in Managementsysteme
U5	Kontinuierliche Optimierung anhand von Kennzahlen und Trends

Das Reifegradmodell dient als Orientierungs- und Bewertungsinstrument. Der anzustrebende Reifegrad richtet sich nach Schutzbedarf, Risikolage, Größe und Komplexität der jeweiligen Organisation. Für Betreiber Kritischer Infrastrukturen sowie weitere Einrichtungen mit erhöhtem Schutzbedarf sollte mindestens ein Reifegrad angestrebt werden, der eine systematische Planung, Durchführung, Auswertung und kontinuierliche Verbesserung von Übungen und Audits gewährleistet.

5.1.13 Kontinuierliche Verbesserung

Organisationen sollten daher regelmäßig insbesondere überprüfen:

- Bedrohungsmodell,
- Risikoanalyse,
- Sicherheitsorganisation,
- Schutzmaßnahmen,
- BCM-Konzepte,
- Krisenmanagement,
- Schulungsprogramme,
- technische Systeme.

Die gewonnenen Erkenntnisse sind systematisch in das Sicherheitsmanagement zurückzuführen.

5.1.14 Kernaussagen für Entscheider

- Die Wirksamkeit von Schutzmaßnahmen muss regelmäßig überprüft werden.
- Übungen und Audits sind zentrale Bestandteile eines risikoorientierten Sicherheitsmanagements.
- Lessons Learned stellen eine wesentliche Grundlage für Verbesserungen dar.
- Kennzahlen unterstützen die Bewertung der Sicherheitsreife.
- Kontinuierliche Verbesserung erhöht nachhaltig die Resilienz gegenüber drohnenbezogenen Bedrohungen.

5.1.15 Handlungsempfehlungen

Betreiber Kritischer Infrastrukturen sollten:

- ein regelmäßiges Übungsprogramm etablieren;
- drohnenbezogene Szenarien in BCM- und Krisenübungen integrieren;
- interne Audits durchführen;
- Verbesserungsmaßnahmen systematisch nachverfolgen;
- Kennzahlen zur Wirksamkeitsmessung definieren;
- Ergebnisse regelmäßig im Management Review bewerten;
- das Schutzkonzept kontinuierlich weiterentwickeln.

5.2 Nachbereitung drohnenbezogener Ereignisse

5.2.1 Zielsetzung

Dieses Kapitel schließt an die in Kapitel 4.2 beschriebenen Wiederanlauf- und BCM-Maßnahmen an und behandelt die sichere Rückkehr in den Regelbetrieb nach Abschluss der unmittelbaren Ereignisbewältigung.

Denn mit der Bewältigung eines Drohnenvorfalls endet die Sicherheitsaufgabe nicht. Insbesondere bei Ausspähungs-, Sabotage- oder hybriden Angriffsszenarien ist nach Abschluss der unmittelbaren Ereignisbewältigung zu prüfen, ob weitere Risiken bestehen, Informationen kompromittiert wurden oder zusätzliche Schutzmaßnahmen erforderlich sind.

Ziel dieses Kapitels ist die strukturierte Nachbereitung drohnenbezogener Ereignisse sowie die kontrollierte Rückkehr in den Regelbetrieb. Die gewonnenen Erkenntnisse sollen genutzt werden, um die Resilienz der Organisation nachhaltig zu verbessern.

Während Kapitel 4.2 die Bewältigung einer Krisenlage und die Aufrechterhaltung kritischer Prozesse behandelt, beschreibt dieses Kapitel die strukturierte fachliche Nachbereitung nach Abschluss der operativen Ereignisbewältigung.

5.2.2 Bezug zu Managementsystemen und Regelwerken

Dieses Kapitel unterstützt die systematische Auswertung von Ereignissen, die Ableitung von Verbesserungsmaßnahmen und deren Rückführung in das Managementsystem.

Relevante Regelwerke:

- ISO/IEC 27001: Verbesserung
- ISO/IEC 27035: Lessons Learned
- ISO 22301: Continual Improvement
- BSI IT-Grundschutz: Verbesserungsprozess

5.2.3 Wiederfreigabe betroffener Bereiche

Vor der Wiederaufnahme des Regelbetriebs sollten betroffene Bereiche einer abschließenden Bewertung unterzogen werden.

Dabei ist insbesondere zu prüfen:

- Bestehen weiterhin drohnenbezogene Risiken?
- Wurden kritische Einrichtungen beeinträchtigt?
- Sind zusätzliche Sicherheitsmaßnahmen erforderlich?
- Können Sperrungen oder Zugangsbeschränkungen aufgehoben werden?
- Ist eine Wiederaufnahme des Normalbetriebs vertretbar?

Die Freigabe sollte durch die jeweils zuständigen Verantwortlichen erfolgen und nachvollziehbar dokumentiert werden.

5.2.4 Bewertung möglicher Informationsabflüsse

Bei Ausspähungsszenarien sollte bewertet werden, welche Informationen möglicherweise gewonnen wurden.

Zu berücksichtigen sind insbesondere:
- Bild- und Videoaufnahmen kritischer Einrichtungen,
- Sicherheitsmaßnahmen und Schutzvorkehrungen,
- Betriebsabläufe,
- Schicht- und Einsatzzeiten,
- Liefer- und Verkehrsströme,
- technische Anlagen und Infrastrukturen,
- sicherheitsrelevante Dokumente oder Anzeigen.

Erforderlichenfalls sind zusätzliche Schutzmaßnahmen oder Anpassungen der Sicherheitskonzepte einzuleiten.

5.2.5 Bewertung möglicher Vorbereitungshandlungen

Drohnenflüge können Teil einer längerfristigen Angriffsvorbereitung sein.

Nach sicherheitsrelevanten Vorfällen sollte daher geprüft werden:
- Liegen Hinweise auf systematische Aufklärung vor?
- Gab es wiederholte Überflüge?
- Wurden bestimmte Objekte gezielt beobachtet?
- Bestehen Hinweise auf koordinierte Aktivitäten?
- Sind weitere Angriffsversuche zu erwarten?

Die Ergebnisse sollten in die aktuelle Bedrohungsbewertung und Risikoanalyse einfließen.

5.2.6 Rückführung temporärer Maßnahmen

Während eines Vorfalls werden häufig zusätzliche organisatorische oder technische Schutzmaßnahmen umgesetzt.

Hierzu können gehören:
- zusätzliche Wach- und Kontrollgänge,
- temporäre Sperrbereiche,
- erhöhte Alarmbereitschaft,
- Sondermaßnahmen des Werkschutzes,
- zusätzliche Dokumentationspflichten,
- verstärkte Überwachung kritischer Bereiche.

Vor der Rücknahme dieser Maßnahmen sollte geprüft werden, ob einzelne Elemente dauerhaft übernommen werden sollten.

5.2.7 Aktualisierung der Risikoanalyse

Erkenntnisse aus drohnenbezogenen Vorfällen stellen eine wertvolle Informationsquelle für das Risikomanagement dar.

Nach sicherheitsrelevanten Ereignissen sollte insbesondere geprüft werden:

- Sind bestehende Risikobewertungen noch angemessen?
- Haben sich neue Angriffsmethoden gezeigt?
- Wurden bislang unbekannte Schwachstellen festgestellt?
- Sind zusätzliche Schutzmaßnahmen erforderlich?
- Muss die UAS Threat Taxonomy ergänzt werden?

Die Ergebnisse sollten in die Schutzbedarfsfeststellung und Risikoanalyse gemäß Kapitel 2.2 einfließen.

5.2.8 Dokumentation und Abschlussbewertung

Für jeden sicherheitsrelevanten Vorfall sollte eine abschließende Bewertung erfolgen.

Hierbei sollten mindestens dokumentiert werden:

- Art des Vorfalls,
- betroffene Bereiche,
- Klassifizierung des Ereignisses,
- getroffene Maßnahmen,
- beteiligte Stellen,
- Behördenkontakte,
- Bewertung möglicher Auswirkungen,
- Restrisiken,
- empfohlene Verbesserungsmaßnahmen.

Eine vollständige Dokumentation unterstützt spätere Audits, Risikoanalysen und Managementbewertungen.

Die Abschlussbewertung sollte nachvollziehbar dokumentieren, welche Erkenntnisse gewonnen wurden, welche Maßnahmen beschlossen wurden, wer für deren Umsetzung verantwortlich ist und bis wann die Umsetzung erfolgen soll.

5.2.9 Kernaussagen für Entscheider

- Die Nachbereitung eines Drohnenvorfalls ist Bestandteil eines wirksamen Sicherheitsmanagements.
- Ausspähungsereignisse sollten stets hinsichtlich möglicher Informationsabflüsse bewertet werden.
- Drohnenvorfälle können Hinweise auf weitergehende Angriffsvorbereitungen liefern.
- Erkenntnisse aus Vorfällen sind systematisch in Risikoanalyse und Sicherheitskonzept zurückzuführen.
- Die kontrollierte Rückkehr zum Regelbetrieb erfordert eine dokumentierte Bewertung verbleibender Risiken.

5.2.10 Handlungsempfehlungen

Betreiber Kritischer Infrastrukturen sollten:

- nach jedem sicherheitsrelevanten Drohnenvorfall eine strukturierte Nachbereitung durchführen;
- mögliche Informationsabflüsse bewerten;
- Hinweise auf weitere Angriffsvorbereitungen analysieren;
- temporäre Schutzmaßnahmen risikoorientiert zurückführen;
- Risikoanalysen und Schutzkonzepte regelmäßig aktualisieren;
- Ergebnisse nachvollziehbar dokumentieren, Maßnahmen nachverfolgen und die Unternehmensleitung über wesentliche Erkenntnisse und den Umsetzungsstand informieren.

6 Teil VI – Anhänge und Arbeitshilfen

Anhang A – Rechtsquellen- und Compliance-Matrix

Quelle	Kategorie	Relevanz für Drohnenrisiken	Primäre Zuordnung im Leitfaden
BSIG	Gesetz	Risikomanagement, Sicherheit kritischer Dienstleistungen, Nachweispflichten	1.5, 2.1, 2.2, 4.1, 4.2
NIS-2 / nationale Umsetzung	Regulierung	Governance, Risikomanagement, BCM, Incident Handling	1.5, 2.1, 2.2, 4.1, 4.2
KRITIS-Dachgesetz (KRITISDachG)	Gesetz	Resilienz kritischer Anlagen, physische Sicherheit, BCM, Krisenmanagement	1.5.4, 4.2
LuftVG	Gesetz	Luftverkehrsrechtliche Rahmenbedingungen	1.5
LuftVO	Verordnung	Betriebsregeln und Flugbeschränkungen	1.5
DSGVO	Verordnung	Verarbeitung von Bild-, Video- und Sensordaten	1.5, 3.3, 4.1
BDSG	Gesetz	Datenschutz im nationalen Kontext	1.5, 3.3, 4.1
Strafgesetzbuch (StGB)	Gesetz	Straftatbestände, Sabotage, Ausspähung, Beweissicherung	1.5, 4.1
Arbeitsschutzgesetz (ArbSchG)	Gesetz	Schutz von Beschäftigten, Notfallmaßnahmen	1.5, 2.2, 4.2
Hausrecht	Rechtsprinzip	Objektschutz und Verhaltensregeln	1.5, 3.2
ISO/IEC 27001	Norm	Informationssicherheitsmanagement	2.1, 2.2, 4.1, 5.1
ISO/IEC 27002	Norm	Organisatorische und technische Sicherheitsmaßnahmen	3.1, 3.3
ISO/IEC 27005	Norm	Risikoanalyse und Risikobewertung	1.4, 2.2
ISO/IEC 27035	Norm	Incident Response und Vorfallbehandlung	4.1
ISO 22301	Norm	BCM, Krisenmanagement, Wiederanlauf	2.1, 4.2, 5.1, 5.2
ISO 22320	Norm	Krisenmanagement und Ereignisbewältigung	4.1, 4.2
ISO 31000	Norm	Allgemeines Risikomanagement	1.4, 2.2
ISO 37301	Norm	Compliance Management	1.5
IEC 62443	Norm	OT- und ICS-Sicherheit	1.4, 2.1, 2.2, 3.3, 4.1
BSI IT-Grundschutz	Methodik	Schutzbedarfsfeststellung, Risikoanalyse, Maßnahmenauswahl	2.1, 2.2, 3.1, 3.2, 3.3
Branchenspezifische Sicherheitsstandards (B3S)	Branchenstandard	KRITIS-spezifische Konkretisierung	1.5 bis 5.2
TeleTrust „Stand der Technik“	Fachquelle	Einordnung des Stands der Technik	1.5.11
BfV Wirtschafts- und Wissenschaftsschutz	Behördenquelle	Bedrohungslage, Ausspähung, hybride Bedrohungen	1.3.9, 1.4
BayLfV „Schutz vor Ausspähung durch Drohnen“	Behördenquelle	Bedrohungsmodell und Schutzmaßnahmen	1.4, 3.2
BSI-Veröffentlichungen	Behördenquelle	KRITIS, IT-Grundschutz, Resilienz	1.4 bis 5.2
NPSA CUAS Guidance Suite	Best Practice	Mehrschichtige Schutzkonzepte und Counter-UAS-Ansätze	1.4, 3.1, 3.2, 3.3
JAPCC Drone Drills	Best Practice	Vorbereitung auf Drohnenvorfälle, Übungen	4.1, 5.1
BDEW-Positionspapier „Effektive und zukunftssichere Drohnenabwehr“ (2025)	Branchenposition	Drohnenabwehr, Resilienz, Lagebilder, Versorgungssicherheit	1.4, 3.1, 3.3, 4.2

Einordnung der Quellen:

Kategorie	Charakter
Gesetze und Verordnungen	Verbindliche Anforderungen
Europäische Regulierung	Verbindliche Anforderungen nach nationaler Umsetzung
Normen	Anerkannte Methoden und Stand der Technik
BSI IT-Grundschutz	Anerkannte Umsetzungsmethodik
B3S	Branchenspezifische Konkretisierung
Behördenveröffentlichungen	Fachliche Orientierung und Bedrohungsbewertung
Internationale Best Practices	Ergänzende fachliche Orientierung
Branchenpapiere	Praxisnahe Einschätzung und branchenspezifische Empfehlungen

Anhang B – Rechts- und Compliance-Kataster

ID	Quelle	Anforderung	Kapitel	Verantwortlich	Nachweis	Status
RC-01	BSIG / NIS-2	Drohnenrisiken im Risikomanagement berücksichtigen	1.4, 2.2	ISB / CISO	Risikoregister	☐
RC-02	BSIG / NIS-2	Angemessene organisatorische Sicherheitsmaßnahmen umsetzen	2.1, 3.1	ISB	Sicherheitskonzept	☐
RC-03	BSIG / NIS-2	Angemessene technische Sicherheitsmaßnahmen umsetzen	3.3	IT-/OT-Sicherheit	Maßnahmenkatalog	☐
RC-04	BSIG / NIS-2	Sicherheitsvorfälle behandeln und dokumentieren	4.1	Incident Manager	Incident-Prozess	☐
RC-05	BSIG / NIS-2	Kontinuität kritischer Dienstleistungen sicherstellen	4.2	BCM	BCM-Konzept	☐
RC-06	BSIG / NIS-2	Unternehmensleitung einbinden und informieren	2.1	Geschäftsführung	Management Review	☐
RC-07	BSIG / NIS-2	Regelmäßige Wirksamkeitskontrollen durchführen	5.1	ISB	Auditberichte	☐
RC-08	BSIG / NIS-2	Kontinuierliche Verbesserung sicherstellen	5.1, 5.2	ISB	Maßnahmenmanagement	☐
RC-09	KRITISDachG	Drohnenrisiken bei Resilienzbewertungen kritischer Anlagen berücksichtigen	1.5.4, 4.2	BCM / Krisenmanagement	Resilienzbewertung	☐
RC-10	KRITISDachG	Drohnenszenarien in BCM- und Wiederanlaufprozessen berücksichtigen	4.2	BCM	BCM-Handbuch	☐
RC-11	LuftVG / LuftVO	Drohnenereignisse luftrechtlich bewerten	1.5	Werkschutz	Verfahrensanweisung	☐
RC-12	LuftVG / LuftVO	Flugbeschränkungen und UAS-Gebiete berücksichtigen	1.5, 2.2	Werkschutz	Risikoanalyse	☐
RC-13	LuftVG / LuftVO	Entwicklungen zu U-Spaces beobachten	1.5	Sicherheitsmanagement	Bewertungsnachweis	☐
RC-14	StGB	Verdacht auf Straftaten angemessen behandeln	1.5, 4.1	Werkschutz	Vorfallsakte	☐
RC-15	StGB	Beweissicherung unterstützen	4.1	Werkschutz	Beweissicherungsprotokoll	☐
RC-16	DSGVO	Verarbeitung von Bild- und Videodaten dokumentieren	1.5, 3.3, 4.1	Datenschutzbeauftragter	VVT	☐
RC-17	DSGVO	Speicher- und Löschfristen festlegen	3.3, 4.1	Datenschutzbeauftragter	Löschkonzept	☐
RC-18	DSGVO / BDSG	Zugriffsrechte für Aufzeichnungen regeln	3.3, 4.1	Datenschutzbeauftragter	Berechtigungskonzept	☐
RC-19	ArbSchG	Gefährdungen für Beschäftigte berücksichtigen	1.5, 2.2, 4.2	Arbeitsschutz	Gefährdungsbeurteilung	☐
RC-20	ArbSchG	Notfall- und Evakuierungsmaßnahmen abstimmen	4.1, 4.2	HSE / BCM	Notfallhandbuch	☐
RC-21	Hausrecht	Regeln für Verhalten auf dem Betriebsgelände festlegen	1.5, 3.1	Werkschutz	Werkschutzordnung	☐
RC-22	Hausrecht	Vorgehen bei Drohnensichtungen definieren	2.1, 3.1, 4.1	Werkschutz	Arbeitsanweisung	☐
RC-23	ISO/IEC 27001	Drohnenrisiken in das ISMS integrieren	2.1, 2.2	ISB	ISMS-Dokumentation	☐
RC-24	ISO/IEC 27001	Rollen und Verantwortlichkeiten definieren	2.1	Geschäftsführung	Rollenmodell	☐
RC-25	ISO/IEC 27001	Management Reviews durchführen	2.1, 5.1	Geschäftsführung	Review-Protokolle	☐
RC-26	ISO/IEC 27001	Interne Audits durchführen	5.1	Revision / ISB	Auditprogramm	☐
RC-27	ISO/IEC 27005	Drohnenbezogene Risikoanalyse etablieren	2.2	Risikomanagement	Risikoanalyse	☐
RC-28	ISO 31000	Risiken systematisch bewerten und behandeln	2.2	Risikomanagement	Risikoregister	☐
RC-29	ISO 22301	Drohnenszenarien in BIA berücksichtigen	2.1, 2.2, 4.2	BCM	BIA	☐
RC-30	ISO 22301	Wiederanlaufplanung berücksichtigen	4.2	BCM	BCM-Handbuch	☐
RC-31	ISO 22301	Krisenmanagement einbinden	4.2	Krisenstab	Krisenhandbuch	☐
RC-32	ISO 22301	Regelmäßige Übungen durchführen	4.2, 5.1	BCM	Übungsprotokolle	☐
RC-33	ISO/IEC 27035	Incident-Response-Prozess etablieren	4.1	Incident Manager	Prozessbeschreibung	☐
RC-34	ISO/IEC 27035	Incident-Klassifikation anwenden	4.1	Incident Manager	Incident-Dokumentation	☐
RC-35	ISO/IEC 27035	Lessons Learned durchführen	4.1, 5.1	Incident Manager	Abschlussbericht	☐
RC-36	IEC 62443	OT-bezogene Drohnenbedrohungen bewerten	1.4, 2.2	OT-Sicherheit	OT-Risikoanalyse	☐
RC-37	IEC 62443	Schutz industrieller Anlagen berücksichtigen	3.2	OT-Sicherheit	Sicherheitskonzept	☐
RC-38	IEC 62443	OT-Incident-Handling berücksichtigen	4.1	OT-Sicherheit	Incident-Prozess	☐
RC-39	ISO 37301	Regulatorische Anforderungen systematisch identifizieren und überwachen	1.5	Compliance	Compliance-Kataster	☐
RC-40	BSI IT-Grundschutz	Schutzbedarfsfeststellung durchführen	2.2	ISB	Schutzbedarfsanalyse	☐
RC-41	BSI IT-Grundschutz	Sicherheitsorganisation etablieren	2.1	Geschäftsführung	Sicherheitskonzept	☐
RC-42	BSI IT-Grundschutz	Dokumentation und Nachvollziehbarkeit sicherstellen	2.1, 4.1	ISB	Dokumentationsverfahren	☐
RC-43	BSI IT-Grundschutz	Kontinuierliche Verbesserung umsetzen	5.1, 5.2	ISB	KVP-Nachweis	☐
RC-44	B3S	Branchenspezifische Anforderungen berücksichtigen	1.5, 2.2	Compliance	B3S-Nachweis	☐
RC-45	BDEW Positionspapier 2025	Autonome und nicht-kooperative Drohnen bewerten	1.4, 2.2	Risikomanagement	Gefährdungsanalyse	☐
RC-46	BDEW Positionspapier 2025	Versorgungssicherheit berücksichtigen	1.4, 2.2, 4.2	BCM	BIA	☐
RC-47	BDEW Positionspapier 2025	Gemeinsame Lagebilder fördern	3.1, 4.1	Sicherheitsmanagement	Kooperationskonzept	☐
RC-48	BDEW Positionspapier 2025	Geodaten- und Transparenzrisiken bewerten	3.1	Informationssicherheit	Informationsschutzkonzept	☐
RC-49	BDEW Positionspapier 2025	Resilienz- und Wiederanlaufplanung stärken	4.2, 5.2	BCM	Wiederanlaufplanung	☐
RC-50	BfV / BayLfV	Ausspähungsrisiken berücksichtigen	1.4, 2.2	Informationssicherheit	Bedrohungsanalyse	☐
RC-51	BfV / BayLfV	Insider-Unterstützung in Bedrohungsmodellen berücksichtigen	1.4, 3.1	Informationssicherheit	Bedrohungsmodell	☐
RC-52	NPSA CUAS Guidance	Mehrschichtige Schutzkonzepte anwenden	2.1, 3.1, 3.2, 3.3	Sicherheitsmanagement	Schutzkonzept	☐
RC-53	JAPCC Drone Drills	Drohnenszenarien regelmäßig üben	5.1	BCM / Krisenmanagement	Übungsprogramm	☐

Anhang C – Drohnen-Compliance-Checkliste

Nr.	Prüffrage	Ja	Nein	Teilweise
C-01	Sind drohnenbezogene Risiken im Bedrohungsmodell berücksichtigt?	☐	☐	☐
C-02	Wurde eine Schutzbedarfsfeststellung durchgeführt?	☐	☐	☐
C-03	Existiert eine dokumentierte Risikoanalyse?	☐	☐	☐
C-04	Wird die UAS Threat Taxonomy verwendet?	☐	☐	☐
C-05	Sind Rollen und Verantwortlichkeiten definiert?	☐	☐	☐
C-06	Existieren dokumentierte Meldewege?	☐	☐	☐
C-07	Sind Behördenkontakte und Meldewege festgelegt?	☐	☐	☐
C-08	Sind organisatorische Schutzmaßnahmen und Verfahrensanweisungen dokumentiert?	☐	☐	☐
C-09	Sind bauliche Schutzmaßnahmen bewertet worden?	☐	☐	☐
C-10	Wurde der Bedarf technischer Detektionsmaßnahmen risikobasiert bewertet?	☐	☐	☐
C-11	Existiert ein Incident-Response-Verfahren?	☐	☐	☐
C-12	Wird die UAS-Incident-Klassifikation verwendet?	☐	☐	☐
C-13	Ist die Beweissicherung geregelt?	☐	☐	☐
C-14	Sind BCM-Szenarien berücksichtigt?	☐	☐	☐
C-15	Sind drohnenbezogene Szenarien im Krisenmanagement berücksichtigt?	☐	☐	☐
C-16	Werden Übungen durchgeführt?	☐	☐	☐
C-17	Werden drohnenbezogene Maßnahmen regelmäßig überprüft oder auditiert?	☐	☐	☐
C-18	Werden Lessons Learned dokumentiert?	☐	☐	☐
C-19	Werden sensible Informationen, Geodaten und öffentlich verfügbare Standortinformationen regelmäßig bewertet?	☐	☐	☐
C-20	Werden autonome und nicht-kooperative Drohnen in Szenarien betrachtet?	☐	☐	☐

Management-Kurzbewertung

Bewertungsbereich	Status					
	Initial	Sensibilisiert	Etabliert	Gesteuert	Überprüft	Optimiert
Governance und Organisation	☐	☐	☐	☐	☐	☐
Risikomanagement	☐	☐	☐	☐	☐	☐
Organisatorische Schutzmaßnahmen	☐	☐	☐	☐	☐	☐
Bauliche Schutzmaßnahmen	☐	☐	☐	☐	☐	☐
Technische Schutzmaßnahmen	☐	☐	☐	☐	☐	☐
Incident Response	☐	☐	☐	☐	☐	☐
BCM / Krisenmanagement	☐	☐	☐	☐	☐	☐
Übungen und Audits	☐	☐	☐	☐	☐	☐
Kontinuierliche Verbesserung	☐	☐	☐	☐	☐	☐

Anhang D – Detektionsverfahren

Vergleich typischer Detektionsverfahren

Technologie	Erkennt autonome Drohnen	Reichweite	Wetter-abhängigkeit	Identifikation	Bemerkungen
Optik	Teilweise	Niedrig bis mittel	Hoch	Hoch	Gut zur Verifikation
Thermografie	Teilweise	Niedrig bis mittel	Mittel	Mittel	Nachtfähig
RF-Detektion	Nein / eingeschränkt	Mittel bis hoch	Gering	Hoch	Abhängig von Funkverbindung
Akustik	Teilweise	Niedrig	Mittel bis hoch	Niedrig	Ergänzende Sensorik
Aktives Radar	Ja	Hoch	Gering	Mittel	Etablierte Technologie
Passivradar	Ja	Mittel bis hoch	Gering	Mittel	Nutzt vorhandene Signalquellen
Sensorfusion	Ja	Hoch	Gering	Hoch	Höchste Gesamtqualität

Keine einzelne Sensortechnologie bietet unter allen Einsatzbedingungen optimale Ergebnisse.

Die Auswahl geeigneter Verfahren sollte daher:
- risikoorientiert
- schutzbedarfsorientiert
- technologieoffen
- herstellerneutral

erfolgen.

LTE450-basierte Passivradarsysteme stellen einen möglichen technologischen Ansatz zur Erkennung autonomer und nicht-kooperativer Drohnen dar.
Die Technologie nutzt vorhandene Mobilfunksignale als passive Signalquelle und erfordert keine aktiven Radarimpulse.
Der praktische Einsatz sollte anhand konkreter Anforderungen, örtlicher Rahmenbedingungen sowie verfügbarer Leistungsnachweise bewertet werden.

Anhang E – Handlungsanweisung bei unklarer Bedrohungslage

Handlungsanweisung bei unklarer Bedrohungslage (vgl. Kapitel 1.4.9 UAS Threat Taxonomy):

1. **Initial-Status setzen:**
   Jede unidentifizierte Drohne im Nahbereich des Perimeters wird zunächst als potenzielle Sicherheitsbedrohung eingestuft. Bis zur weiteren Lageaufklärung ist sowohl von einem möglichen Aufklärungs- und Cyber-Szenario (T1/T2) als auch von einer potenziellen physischen Bedrohung (T4/T5) auszugehen.

2. **Sensorfusion aktivieren:**
   Schwenk von PTZ- und Thermalkameras auf das Objekt zur Identifikation von Nutzlasten, Flugverhalten und möglichen Angriffsindikatoren. Abgleich mit Radar-, RF- und sonstigen Sensorsystemen auf Auffälligkeiten oder Frequenzanomalien.

3. **Schutzmaßnahmen aufrufen:**
   - Einleitung visueller Schutzmaßnahmen (z. B. Schließen von Jalousien, Sichtschutzmaßnahmen, Unterbrechung exponierter Tätigkeiten) zur Reduzierung möglicher Aufklärungs- und Ausspähungsrisiken.
   - Schutz von Personen sowie Sicherung offener oder besonders exponierter Betriebs- und Instandhaltungsbereiche bei Verdacht auf eine physische Bedrohung.
   - Erhöhte Aufmerksamkeit des Werkschutzes und Durchführung einer Lagebewertung gemäß Incident-Response-Prozess.

4. **Beweissicherung:**
   Automatische Speicherung aller verfügbaren Sensor-, Video-, Radar- und Logdaten zur späteren technischen, organisatorischen und gegebenenfalls juristischen Bewertung des Vorfalls.

5. **Eskalation:**
   Die weitere Behandlung und Klassifizierung erfolgt gemäß Kapitel 4.1.6 Klassifizierung des Vorfalls und der dort beschriebenen UAS-Incident-Klassifikation (UAS-I0 bis UAS-I5).

Anhang F – Leitfaden zur Beweissicherung

Kurz-Leitfaden zur rechtssicheren Beweissicherung bei UAS-Vorfällen

Ziel: Sicherung digitaler und physischer Spuren für ermittelnde Behörden (Polizei, LKA, Staatsanwaltschaft).

1. **Digitale Detektionsdaten sichern:**
   - Exportieren Sie die Logfiles der Detektionssensorik (RF-Scans, Radardaten, Systemmeldungen) mit Zeitstempel.
   - Sichern Sie Aufzeichnungen optischer Kameras (PTZ/Thermo) ungeschnitten als Rohdatei (inkl. Metadaten).

2. **Foto- und Videodokumentation vor Ort:**
   - Machen Sie Fotos vom Flugobjekt aus mehreren Winkeln (sofern sichtbar).
   - Dokumentieren Sie vermutete Pilotenstandorte (Fahrzeuge, Kennzeichen, Personenmerkmale) aus sicherer Distanz.

3. **Umgang mit abgestürzten / gelandeten Drohnen:**
   - Sicherheit geht vor: Flugobjekt nicht berühren (Gefahr durch Spreng-/Gefahrstoffe oder Akkubrand).
   - Fundort sofort weiträumig absperren (mindestens 20 Meter Radius).
   - Keine Modifikationen am Objekt vornehmen (Spurensicherung der Polizei abwarten – Fingerabdrücke / DNA).
   - Bei Brandgefahr: CO2-Löscher bereithalten, kein Wasser bei Lithium-Polymer-Akkus nutzen.