White Paper – GEFMA 932
Version 1.0

KRITIS-Dachgesetz und Gesundheitswesen: Facility Management als Garant für Resilienz

Autor: gefma Arbeitskreis Kritische Infrastruktur
Veröffentlicht durch: gefma & FKT
Version: 1.0/2026-04

Inhalt

1 Einleitung

1.1 Vom kostengetriebenen Gebäudebetrieb zum resilienzorientierten Management

Der Betrieb kritischer Infrastrukturen führt zu einem grundlegenden Wandel im Facility Management. Aus einer kostengetriebenen, reaktiven Unterstützungsfunktion wird eine strategische, sicherheitsrelevante und datenbasierte Managementdisziplin.

Kritische Infrastrukturen wie Energieversorgung, Krankenhäuser oder Rechenzentren sind essenziell für die Gesellschaft. Ihre steigende Bedrohungslage erhöht die Anforderungen an Verfügbarkeit, Sicherheit und Resilienz. Damit wird das klassische, primär effizienz- und kostenorientierte Facility Management obsolet. Denn im KRITIS-Kontext stehen nicht mehr Kostenoptimierung und Grundbetrieb im Mittelpunkt, sondern Versorgungssicherheit, Ausfallschutz und Risikominimierung. Facility Management wird Teil des übergeordneten Risikomanagements: Ausfälle gelten als inakzeptabel und müssen präventiv verhindert werden. Ebenso die Digitalisierung beschleunigt diesen Wandel. IoT, Sensorik und Echtzeitdaten ermöglichen vorausschauende Wartung statt starrer Intervalle. Dadurch entwickelt sich Facility Management zu einer datengetriebenen, prädiktiven Entscheidungsinstanz. Letztlich rückt auch das Resilienzmanagement in den Fokus: Redundanzkonzepte, Krisen- und Notfallplanung sowie Business-Continuity-Maßnahmen werden zu Kernaufgaben. Die zunehmende Vernetzung macht zudem die Integration von IT, OT und Cybersecurity unverzichtbar.

All dies sind Gründe. weshalb sich die Rolle des Facility Managements grundlegend verändert. Vom operativen Dienstleister hin zum strategischen Partner, der eng mit IT, Security, Behörden und Management zusammenarbeitet.

Rechenzentren zeigen diesen Paradigmenwechsel bereits heute exemplarisch: Null-Toleranz gegenüber Ausfällen, redundante Systeme und kontinuierliche Überwachung sind Standard.

Insgesamt entwickelt sich Facility Management im KRITIS-Bereich zu einem hoch technologisierten, sicherheitskritischen und strategisch bedeutenden Bestandteil der Unternehmensstabilität – ein Wandel, der durch KI, digitale Zwillinge und höhere Cyber-Resilienz weiter an Dynamik gewinnen wird.

1.2 Motivation und Zielsetzung im Gesundheitsweisen

Die Sicherstellung der Funktionsfähigkeit kritischer Infrastrukturen (KRITIS) wird durch die sich verstärkenden Auswirkungen des Klimawandels, wie extreme Hitze oder Unwetter, die erhöhte Zunahme von Bedrohung durch Cyberangriffe, den allgemein rohere Ton und Umgang in (Welt-) Politik und Gesellschaft sowie andere Krisensituationen zunehmend schwieriger, aber auch wichtiger.

Mit dem KRITIS-Dachgesetz (KRITIS-DachG)[01], das am 29. Januar 2026 den Bundestag und am 6. März 2026 den Bundesrat passiert hat, wurde erstmals ein umfassender Rechtsrahmen zur Stärkung der physischen Sicherheit kritischer Infrastrukturen geschaffen. Das Gesetz setzt die EU-CER-Richtlinie[02] in nationales Recht um und tritt mit zeitlich gestaffelten Pflichten in Kraft. Seit dem 17.03.2026 ist das KRITIS-Dachgesetz verbindlich gültig und bildet damit einen zentralen regulatorischen Rahmen für Betreiber kritischer Anlagen, insbesondere auch für Einrichtungen des Gesundheitswesens. Hierunter fallen gemäß dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe Einrichtungen für die Behandlung von Patientinnen und Patienten, die Versorgung mit Arzneimitteln sowie die Untersuchung von Laborproben.

Hauptsächlich Krankenhäuser stellen dabei einen der zentralen Bausteine für die öffentliche Gesundheit und Sicherheit dar. Ihre Ausfallzeiten oder Funktionsstörungen können schwerwiegende Folgen für Patienten, das Gesundheitswesen und die Gesellschaft insgesamt haben.

Dieses Whitepaper der gefma setzt sich zum Ziel, ein umfassendes Verständnis für die Anforderungen und Herausforderungen der KRITIS-Absicherung in Krankenhäusern zu vermitteln und praxisnahe Handlungsempfehlungen für die Verantwortlichen im Betrieb bereitzustellen. Sie adressiert nicht nur die technischen Aspekte der Krisenbewältigung, sondern auch organisatorische, sicherheitsrelevante und strategische Fragestellungen, die für die Aufrechterhaltung eines stabilen Krankenhausbetriebs unerlässlich sind.

Krankenhäuser müssen als kritische Infrastrukturen in der Lage sein, bei Störungen oder Notfällen schnell zu reagieren und weiterhin eine hochwertige Patientenversorgung sicherzustellen. Dieses Whitepaper bietet daher wertvolle Hinweise zur Planung und Umsetzung von Sicherheitskonzepten, die auch in Krisenzeiten einen ununterbrochenen Betrieb gewährleisten.

Wir hoffen, dass dieses Whitepaper allen Beteiligten als nützliche Orientierungshilfe dient und zur Verbesserung der Sicherheitsvorkehrungen in den Krankenhäusern beiträgt – sowohl für die institutionellen Entscheidungsträger als auch für die Fachkräfte vor Ort, die täglich die Verantwortung für die Infrastruktur und Sicherheit tragen.

[01] Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITISDachG) v. 11.03.2026, BGBl. I 2026, Nr. 66.

[02] Richtlinie (EU) 2022/2557 [...] vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen [...], ABl. L 333 v. 27.12.2022, S. 164–198.

2 KRITIS-Dachgesetz

2.1 Einordnung der Zielsetzung des KRITIS-Dachgesetzes

Das KRITIS-Dachgesetz verfolgt das übergeordnete Ziel, die Resilienz kritischer Infrastrukturen in Deutschland systematisch und sektorübergreifend zu stärken.

Im Zentrum des Gesetzes steht ein präventiver Ansatz, der über reine Gefahrenabwehr hinausgeht. Betreiber kritischer Infrastrukturen werden verpflichtet, Risiken frühzeitig zu identifizieren, geeignete Schutz- und Vorsorgemaßnahmen umzusetzen und deren Wirksamkeit nachzuweisen. Damit wird ein Paradigmenwechsel vollzogen: von reaktiver Störungsbeseitigung hin zu einem integrierten Resilienz- und Risikomanagement.

Für das Gesundheitswesen besitzt diese Zielsetzung eine besondere Bedeutung. Krankenhäuser und weitere medizinische Einrichtungen sind nicht nur klassische KRITIS-Betreiber, sondern gleichzeitig hochkomplexe technische Systeme, deren Betriebsfähigkeit maßgeblich von einer stabilen Gebäude-, Versorgungs- und Infrastruktur abhängt. Das KRITIS-Dachgesetz adressiert damit explizit auch jene organisatorischen und technischen Ebenen, die im Verantwortungsbereich des Facility Managements liegen.

Das KRITIS-Dachgesetz konkretisiert seine Zielsetzung durch die Einführung sektorenübergreifender Mindestanforderungen an die Resilienz kritischer Infrastrukturen. Anders als bisherige Regelwerke, die primär auf einzelne Gefahren oder Sektoren fokussierten, adressiert das Gesetz explizit auch physische und betriebliche Abhängigkeiten, insbesondere auf Ebene von Gebäuden, Anlagen und Versorgungsstrukturen.

So sieht es vor, dass Betreiber kritischer Infrastrukturen jene betrieblichen Komponenten identifizieren müssen, deren Ausfall unmittelbar die Erbringung der kritischen Dienstleistung gefährdet.

Für Einrichtungen des Gesundheitswesens umfasst dies beispielsweise:

- die elektrische Energieversorgung einschließlich Netzanschluss, Netzersatzanlagen und USV-Systeme,
- die Versorgung mit Wasser, Wärme und medizinischen Gasen,
- zentrale gebäudetechnische Systeme wie Lüftungs- und Klimaanlagen in OP- und Intensivbereichen
- Physikalische Sicherheit und Zutrittsmanagement

Die Zielsetzung des Gesetzes wird damit greifbar: Es geht nicht allein um den Schutz vor äußeren Angriffen, sondern um die dauerhafte Funktionsfähigkeit der betrieblichen Infrastruktur. Das Gesetz verankert diese Perspektive ausdrücklich und verlagert die Verantwortung für Resilienzmaßnahmen stärker in den operativen Betrieb – ein Bereich, der maßgeblich durch das Facility Management geprägt ist.

2.2 Erweiterte Pflichten zu Resilienz, Risikomanagement und Nachweisführung

Betreiber müssen systematisch analysieren, welche Gefährdungen die Funktionsfähigkeit ihrer kritischen Dienstleistungen beeinträchtigen können. Dazu zählen unter anderem Ausfälle der Energie- und Medienversorgung, Schäden an Gebäuden und technischen Anlagen, Cyberangriffe auf gebäudetechnische Systeme, Lieferkettenrisiken sowie Extremwetterereignisse. Auf Basis dieser Analysen sind angemessene Resilienzmaßnahmen abzuleiten und umzusetzen.

Ein wesentliches Novum ist die verbindliche Nachweis- und Dokumentationspflicht. Maßnahmen zur Risikovorsorge, Instandhaltung, Redundanz und Notfallbewältigung müssen nachvollziehbar dokumentiert und gegenüber zuständigen Behörden belegbar sein. Damit gewinnt die strukturierte Erfassung von Anlagenzuständen, Wartungs- und Prüfprozessen, Notfall- und Wiederanlaufkonzepten sowie Schulungsmaßnahmen erheblich an Bedeutung.

Für das Facility Management bedeutet dies eine stärkere formale Verantwortung: Technisches, infrastrukturelles und kaufmännisches FM werden zu tragenden Säulen der gesetzlichen Compliance. Resilienz wird nicht mehr als abstraktes Ziel verstanden, sondern als operativ messbare und prüfbare Leistung, die aktiv gesteuert und kontinuierlich verbessert werden muss.

Das KRITIS-Dachgesetzes verpflichtet Betreiber zur Durchführung regelmäßiger Risikoanalysen, die sowohl interne als auch externe Gefährdungen berücksichtigen. Dabei sind nicht nur außergewöhnliche Ereignisse, sondern auch betriebliche Schwachstellen und Abhängigkeiten zu bewerten.

Ein konkretes Beispiel aus dem Facility Management ist die Bewertung der Notstromversorgung eines Krankenhauses:

- Das Gesetz verlangt, Risiken eines Stromausfalls zu analysieren.
- Daraus ergibt sich die Pflicht, die Auslegung, Wartung und Betankungslogistik von Netzersatzanlagen zu prüfen.
- Zusätzlich ist zu bewerten, ob personelle Ressourcen, Ersatzteile und externe Dienstleister im Krisenfall verfügbar sind.

Weiterhin wird die Umsetzung angemessener technischer und organisatorischer Resilienzmaßnahmen gefordert. Für das Facility Management bedeutet dies unter anderem:

- redundante Auslegung kritischer Anlagen (z. B. doppelte Kältemaschinen für OP-Bereiche),
- bauliche Schutzmaßnahmen gegen Extremwetterereignisse (z. B. Hochwasserschutz für Technikzentralen),
- organisatorische Maßnahmen wie Vertretungsregelungen für Schlüsselpersonal im technischen Betrieb.

Neu ist insbesondere die verpflichtende Nachweisführung. Betreiber müssen dokumentieren können, dass identifizierte Risiken bewertet, Maßnahmen umgesetzt und auf Wirksamkeit geprüft wurden. In der Praxis betrifft dies beispielsweise:

- nachvollziehbare Wartungs- und Prüfkonzepte für sicherheitsrelevante Anlagen,
- dokumentierte Notfall- und Wiederanlaufpläne für die technische Infrastruktur,
- regelmäßige Übungen und Schulungen des FM-Personals mit entsprechender Protokollierung.
- Regelmäßige Wirksamkeitskontrolle bis hin zu Penetrationstest (wenn erforderlich)

Das KRITIS-Dachgesetz macht damit deutlich, dass Resilienz nicht allein durch Investitionen entsteht, sondern durch strukturierte, überprüfbare Betriebsprozesse.

2.3 Relevanz für Betreiber im Gesundheitswesen

Für Betreiber im Gesundheitswesen hat das KRITIS-Dachgesetz unmittelbare und weitreichende Auswirkungen. Die Aufrechterhaltung der medizinischen Versorgung ist in hohem Maße von der Verfügbarkeit kritischer Gebäude- und Versorgungssysteme abhängig – etwa Strom, Wärme, Wasser, medizinische Gase, IT-Infrastruktur und Sicherheitstechnik. Diese Systeme fallen überwiegend in den Zuständigkeitsbereich des Facility Managements.

Das Gesetz rückt das Facility Management damit aus einer unterstützenden Rolle heraus und positioniert es als strategischen Faktor für die Versorgungs- und Krisensicherheit von Gesundheitseinrichtungen. Betreiber müssen sicherstellen, dass FM-Strukturen, Prozesse und Ressourcen den gesetzlichen Anforderungen an Resilienz und Risikomanagement entsprechen. Dies betrifft insbesondere die Bewertung von Anlagenkritikalitäten, die Planung von Redundanzen, die Absicherung von Wartungs- und Instandhaltungsprozessen sowie die Integration des Facility Management in Notfall- und Krisenstäbe.

Gleichzeitig erhöht sich der organisatorische und wirtschaftliche Druck auf Betreiber. Investitionen in technische Redundanzen, Digitalisierung, Dokumentation und Qualifizierung des Personals werden unvermeidlich. Das KRITIS-Dachgesetz kann jedoch auch als Chance zur Professionalisierung verstanden werden: Ein strategisch ausgerichtetes Facility Management trägt nicht nur zur Erfüllung regulatorischer Anforderungen bei, sondern verbessert langfristig Betriebssicherheit, Transparenz und Wirtschaftlichkeit.

Für Betreiber im Gesundheitswesen wird deutlich, dass die Betriebsfähigkeit von Gesundheitseinrichtungen untrennbar mit dem Zustand der Immobilien- und Anlagentechnik verbunden ist. Das Gesetz verlangt, dass Betreiber ihre Rolle als KRITIS-Verantwortliche aktiv wahrnehmen und diese Verantwortung nicht ausschließlich delegieren.

Ein praktisches Beispiel ist die Einbindung des Facility Managements in das übergeordnete Risikomanagement:

- Das Gesetz sieht vor, dass Maßnahmen zur Resilienz auf Leitungsebene verantwortet werden.
- Gleichzeitig stammen wesentliche Risikoinformationen (z. B. Anlagenzustände, Störanfälligkeiten, Wartungsrückstände) aus dem operativen FM.
- Betreiber müssen daher sicherstellen, dass FM-Daten systematisch erfasst und in strategische Entscheidungen eingebunden werden.

Darüber hinaus wird die Abhängigkeit von externen Dienstleistern explizit relevant. Viele Krankenhäuser betreiben technische Anlagen nicht vollständig in Eigenleistung. Betreiber müssen dennoch die Verantwortung für Resilienz und Nachweisführung tragen. Dies hat konkrete Folgen:

- FM-Verträge müssen Anforderungen an Dokumentation, Reaktionszeiten und Krisenverfügbarkeit enthalten.
- Betreiber müssen prüfen, ob Dienstleister im Krisenfall tatsächlich handlungsfähig sind.

Insgesamt verdeutlicht das KRITIS-Dachgesetzes, dass Betreiber im Gesundheitswesen ihre Facility-Management-Strukturen strategisch weiterentwickeln müssen. Das Gesetz wirkt damit als Katalysator für

eine stärkere Verzahnung von Betrieb, Technik und Governance – mit dem Ziel, die medizinische Versorgung auch unter außergewöhnlichen Bedingungen sicherzustellen.

Für das Gesundheitswesen ist es daher entscheidend, das KRITIS-Dachgesetz nicht isoliert als Compliance-Thema zu betrachten, sondern als integralen Bestandteil einer nachhaltigen Betriebs- und Immobilienstrategie.

2.4 Wer ist Betreiber im Sinne des Gesetzes?

Im Sinne des KRITIS-Dachgesetzes ist Betreiber grundsätzlich nicht der Facility-Manager, sondern diejenige natürliche oder juristische Person, die tatsächliche und rechtliche Verfügungsmacht über eine kritische Anlage besitzt.

Diese Einschätzung deckt sich sowohl mit der etablierten Rechtsauffassung in Deutschland als auch mit der Position maßgeblicher Branchenverbände wie der GEFMA. Nach GEFMA 190[03] werden Facility-Management-Dienstleister primär als Verrichtungs- oder Erfüllungsgehilfen des Auftraggebers eingeordnet. Zwar können Betreiberpflichten intern oder extern delegiert werden, doch führt die Übertragung einzelner Aufgaben nicht dazu, dass der FM-Dienstleister selbst zum Betreiber wird. Vielmehr bleibt die Grundverantwortung – insbesondere Organisations-, Auswahl- und Kontrollpflichten – stets beim Auftraggeber.

Diese Sichtweise wird zusätzlich durch das allgemeine deutsche Betreiberverständnis gestützt: Betreiber ist derjenige, der tatsächlichen und rechtlichen Einfluss auf den sicheren Betrieb einer Anlage ausübt, also über die tatsächliche Verfügungsmacht verfügt. Facility-Manager erfüllen typischerweise keine dispositiven Entscheidungen über Austausch, Modernisierung oder grundlegende Instandsetzung einer Anlage und können daher nicht als Betreiber im Rechtssinne angesehen werden.

Auch die Legaldefinition des Betreiberbegriffs im KRITIS-Dachgesetz bestätigt dieses Verständnis. § 2 Nr. 1 KRITISDachG verweist auf die Begriffsbestimmungen der Richtlinie (EU) 2022/2557, deren Anhang in der dritten Spalte klar benennt, wer als „Betreiber kritischer Anlagen“ zu gelten hat. Dort werden regelmäßig Eigentümer, Betreiberorganisationen eines Unternehmens oder entsprechende juristische Einheiten genannt – jedoch nicht FM-Dienstleister.

Zusammengenommen ergibt sich daraus, dass im Rahmen des KRITIS-Dachgesetzes der Facility-Manager nicht als Betreiber im Rechtssinne anzusehen ist, sondern als unterstützender Dienstleister, der Aufgaben wahrnimmt, deren Verantwortung und Letztverantwortlichkeit beim tatsächlichen Betreiber verbleibt.

[03] GEFMA 190 Betreiberverantwortung 2.0 im Facility Management (inkl. ESG) v. 2023-06, gefma e. V.

3 Handlungsfelder und Umsetzungsempfehlungen für ein gesetzeskonformes und resilientes Facility Management

3.1 Sicherheitsmanagement – Notwendigkeit, Aufbau, Einordnung und Funktion

Sicherheitsmanagement ist im Krankenhaus ein strukturierter, bereichsübergreifender Ansatz zur Planung, Steuerung und kontinuierlichen Weiterentwicklung aller sicherheitsrelevanten Maßnahmen. Ziel ist es, Risiken systematisch zu erkennen, zu bewerten und in abgestimmte technische, organisatorische und personelle Maßnahmen zu überführen. Einzelmaßnahmen werden dabei nicht isoliert betrachtet, sondern zu einem wirksamen Gesamtsystem verbunden, das die Sicherheit von Patienten, Mitarbeitenden, Besuchern und Infrastruktur unterstützt.

Die Notwendigkeit eines solchen Sicherheitsmanagements ergibt sich aus der besonderen Bedeutung eines Krankenhauses für die öffentliche Daseinsvorsorge und aus der hohen Komplexität seiner Abläufe. Störungen in der Stromversorgung, IT-Ausfälle, technische Defekte, Brände, Evakuierungslagen oder andere Sicherheitsvorfälle können die Patientenversorgung unmittelbar beeinträchtigen. Hinzu kommt, dass Risiken im Krankenhaus häufig an Schnittstellen entstehen – etwa zwischen medizinischem Betrieb, Medizintechnik, IT, Gebäudebetrieb und externen Dienstleistern. Sicherheitsmanagement ist deshalb keine rein ergänzende Verwaltungsaufgabe, sondern eine notwendige Führungs- und Steuerungsfunktion, um Betriebsfähigkeit, Resilienz und Patientensicherheit dauerhaft zu stärken.

Der Aufbau eines Sicherheitsmanagements setzt voraus, dass Sicherheit als eigenständige Querschnittsaufgabe verstanden und von der Krankenhausleitung verbindlich unterstützt wird. Grundlage ist zunächst eine systematische Bestandsaufnahme bestehender Risiken, Schutzmaßnahmen, Prozesse und Schnittstellen. Darauf aufbauend können Zuständigkeiten, Berichtswege, Prioritäten und Abstimmungsformate festgelegt werden. Ziel ist es, belastbare Strukturen zu schaffen, in denen sicherheitsrelevante Themen nicht nur im Ereignisfall, sondern dauerhaft und vorausschauend gesteuert werden. Der Aufbau ist damit kein einmaliger Schritt, sondern ein fortlaufender Entwicklungsprozess.

Für die organisatorische Einordnung bietet sich eine stabsähnliche Verankerung an, die direkt oder indirekt an die Krankenhausleitung beziehungsweise Geschäftsführung angebunden ist. Eine solche Positionierung ermöglicht bereichsübergreifendes Arbeiten, sichert die notwendige Unabhängigkeit und erleichtert es, sicherheitsrelevante Anforderungen frühzeitig in strategische und operative Entscheidungen einzubringen. Sicherheitsmanagement ist damit weder ausschließlich operativ tätig noch einem einzelnen Fachbereich zugeordnet, sondern übernimmt eine verbindende Rolle zwischen Leitungsebene, medizinischen Bereichen, Technik, IT, Verwaltung und externen Partnern.

Vor dem Hintergrund regulatorischer Anforderungen, insbesondere im Kontext des KRITIS-Dachgesetzes, kommt dem Sicherheitsmanagement zudem eine wichtige Schnittstellenfunktion zu. Es kann als zentrales Verbindungsglied zwischen dem Krankenhaus und zuständigen Behörden, Aufsichtsstellen sowie weiteren relevanten Stellen fungieren, etwa im Zusammenhang mit Meldepflichten, Nachweisen, Risikoanalysen, Resilienzmaßnahmen und der Vorbereitung auf Prüfungen. So wird sichergestellt, dass regulatorische Anforderungen nicht isoliert behandelt, sondern in betriebliche Abläufe integriert und konsistent umgesetzt werden.

Die Funktion des Sicherheitsmanagements geht damit deutlich über die Umsetzung einzelner Schutzmaßnahmen hinaus. Zu seinen zentralen Aufgaben gehören die Koordination sicherheitsrelevanter Themen, die Beratung der Leitung und der Fachbereiche, die Entwicklung und Pflege von Richtlinien, Prozessen sowie Notfall- und Krisenstrukturen und die regelmäßige Überprüfung ihrer Wirksamkeit. Dazu zählen auch Übungen für Szenarien wie Stromausfälle, IT-Störungen oder Evakuierungen. Nicht zuletzt trägt das Sicherheitsmanagement durch Schulungen, Kommunikation und Sensibilisierung zur Entwicklung einer gelebten Sicherheitskultur bei, denn Sicherheit hängt im Krankenhaus wesentlich auch vom Verhalten der Mitarbeitenden ab.

3.2 Dokumentation & Reporting

Die Dokumentations- und Reportingpflichten setzen sich aus vier Schritten zusammen. Zunächst erfolgt die Registrierung der kritischen Anlage. Die Registrierung ist nicht bloß ein administrativer Akt, sondern der Ausgangspunkt sämtlicher weiteren Dokumentations-, Analysepflichten. Im Anschluss an die Registrierung folgt die betreiberbezogene Risikoanalyse und Risikobewertung. Der dritte Schritt ist die Erstellung eines Resilienzplans, in dem auf Basis von Schritt 2 die Risikoanalyse und -bewertung und die daraus abgeleitete Resilienzmaßnahmen zunächst strukturiert zusammengeführt werden. Der Resilienzplan ist das zentrale Steuerungs- und Nachweisdokument. Der vierte Schritt ist die Dokumentation der Umsetzung der einzelnen Resilienzmaßnahmen aus Schritt 3 und die entsprechende Aktualisierung des Resilienzplans.

Kritische Anlagen im Sinne des KRITIS-Dachgesetz unterliegen zunächst einer formellen Registrierung. Mit der Registrierung wird ein Krankenhaus rechtlich als Betreiber einer kritischen Anlage erfasst und damit in den Anwendungsbereich der gesetzlichen Risiko- und Resilienzpflichten einbezogen. Im Rahmen der Registrierung sind die wesentlichen Angaben zur kritischen Anlage zu übermitteln. Dazu gehören insbesondere:

- den Namen des Betreibers kritischer Anlagen, einschließlich der Rechtsform und, falls einschlägig, die Handelsregisternummer
- die Anschrift und aktuelle Kontaktdaten des Betreibers kritischer Anlagen, einschließlich der E-Mail-Adresse und der Telefonnummer
- den Sektor und, falls einschlägig, die Branche, zu dem oder zu der die kritische Anlage gehört, sowie die kritische Dienstleistung, für deren Erbringung die Anlage erheblich ist
- eine Kontaktstelle, über die der Betreiber kritischer Anlagen immer erreichbar ist

Bei Anlagen mit hohem Versorgungsgrad zudem

- den Standort der kritischen Anlagen und deren Versorgungsgebiet sowie deren öffentlichen IP-Adressbereiche, falls vorhanden

Mit der Registrierung beginnen Fristen zu laufen, insbesondere für die erstmalige Durchführung der Risikoanalyse und Risikobewertung sowie für die Erstellung eines Resilienzplans. Die Registrierung markiert somit den formalen Startpunkt eines strukturierten Compliance- und Dokumentationsregimes. Bestehende Anlagen, die bereits als kritische Anlagen eingestuft sind, müssen gemäß dem aktuell angestrebten Zeitplan des Gesetzgebers bis zum 17.07.2026 registriert werden. Neuanlagen müssen innerhalb von 3 Monaten nach Einstufung als kritische Anlage registriert werden.

Bei der Risikoanalyse und Risikobewertung ist zwischen zwei Analyseebenen zu unterscheiden: der nationalen Risikoanalyse und Risikobewertung einerseits und der betreiberbezogenen Risikoanalyse und Risikobewertung andererseits. Die nationale Risikoanalyse wird auf staatlicher Ebene erstellt und fortgeschrieben. Sie identifiziert übergreifende Gefährdungslagen, Bedrohungsszenarien und sektorübergreifende Abhängigkeiten. Die Risikoanalyse des Krankenhauses als kritische Anlage baut hierauf auf. Sie ist eigenständig durchzuführen, muss sich jedoch an den Erkenntnissen und Vorgaben der nationalen

Risikoanalyse orientieren. Es besteht somit ein systematisches Wechselspiel: Die nationale Analyse setzt den strategischen Rahmen, die anlagenspezifische Analyse konkretisiert die Risiken für den individuellen Standort. Werden nationale Risikoanalysen aktualisiert, entsteht regelmäßig Anpassungsbedarf bei der betreiberseitigen Bewertung.

Die anlagenspezifische Risikoanalyse ist mindestens alle vier Jahre sowie zusätzlich anlassbezogen durchzuführen, etwa bei wesentlichen baulichen Veränderungen, technischen Systemwechseln oder veränderter Bedrohungslage. Inhaltlich sind folgende Risikokategorien systematisch zu erfassen und zu bewerten:

- naturbedingte Risiken,
- klimatische Risiken,
- vom Menschen verursachte Risiken,
- Risiken aus technischen Ausfällen gebäudetechnischer und versorgungstechnischer Systeme,
- Abhängigkeiten von anderen Betreibern kritischer Anlagen, auch sektorenübergreifend und grenzüberschreitend,
- Abhängigkeiten anderer Sektoren von der eigenen kritischen Dienstleistung.

Für Krankenhäuser bedeutet dies insbesondere die strukturierte Analyse von Wechselwirkungen zwischen Energieversorgung, Notstromsystemen, Gebäudeleittechnik, IT-Infrastruktur, medizinischer Versorgungstechnik und versorgungskritischen Bereichen wie Intensivstation oder OP-Zentren. Die Dokumentation muss die Risikoidentifikation, die Bewertungsmethodik, Eintrittswahrscheinlichkeiten, Schadensausmaß, potenzielle Auswirkungen auf die kritische Dienstleistung sowie angenommene Wiederherstellungszeiten enthalten. Bewertungsmaßstäbe und Annahmen sind transparent darzustellen, um die Prüfbarkeit sicherzustellen.

Auf Grundlage dieser Risikoanalyse sind Resilienzmaßnahmen abzuleiten und in einem Resilienzplan zusammenzuführen. Dieser Plan ist das zentrale Steuerungs- und Nachweisdokument. Ziel der Maßnahmen ist es,

- das Auftreten von Vorfällen zu verhindern,
- einen angemessenen physischen Schutz von Liegenschaften und Anlagen sicherzustellen,
- auf Vorfälle wirksam reagieren und deren Auswirkungen begrenzen zu können,
- die zügige Wiederherstellung der kritischen Dienstleistung zu gewährleisten.

Bei der Auswahl und Ausgestaltung der Maßnahmen ist ausdrücklich eine Zweck-Mittel-Relation herzustellen. Der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls ist gegen das Risiko und dessen potenzielles Schadensausmaß abzuwägen. Maßnahmen müssen verhältnismäßig sein; wirtschaftliche Aspekte und die Leistungsfähigkeit des Betreibers sind zu berücksichtigen. Für die Dokumentation bedeutet dies, dass jede wesentliche Maßnahme einer konkreten Risikozuordnung bedarf und die Entscheidungsgrundlage nachvollziehbar festgehalten wird. Es sollte dokumentiert werden, welche Alternativen geprüft wurden, warum bestimmte technische oder organisatorische Lösungen gewählt wurden und in welchem Verhältnis sie zum identifizierten Risiko stehen.

Der Resilienzplan selbst sollte konsolidiert folgende Elemente enthalten:

- strukturierte Risikomatrix mit Priorisierung,
- Zuordnung konkreter Maßnahmen zu identifizierten Risiken,
- Beschreibung des jeweiligen Schutzziels,
- technische oder organisatorische Ausgestaltung,
- Zuständigkeiten und Schnittstellen,
- Prüf-, Wartungs- und Aktualisierungsintervalle,
- definierte Wiederherstellungszeiten für versorgungskritische Funktionen,
- Nachweisführung durch Prüfprotokolle, Wartungsberichte und Zertifikate.

Die Umsetzung der Maßnahmen ist fortlaufend zu dokumentieren. Dazu gehören insbesondere Wartungs- und Prüfprotokolle, Nachweise über Funktionstests (z. B. Notstrom-Lasttests), Aktualisierungen von Notfall- und Wiederanlaufkonzepten sowie revisionssichere Ablagen aller relevanten Unterlagen. Bestehende Dokumentationen aus anderen öffentlich-rechtlichen Verpflichtungen können integriert werden, sofern sie inhaltlich gleichwertig sind. Doppelstrukturen sind zu vermeiden, die Integrität und Vollständigkeit der Nachweisführung müssen jedoch jederzeit gewährleistet bleiben.

Für Facility-Management-Unternehmen im Krankenhausbereich bedeutet dies, Dokumentation und Reporting nicht isoliert als Verwaltungsaufgabe zu behandeln, sondern als integralen Bestandteil der technischen Betriebsführung. Risikoanalyse, Resilienzplanung, Maßnahmenumsetzung und Nachweisführung sind in einem geschlossenen, regelmäßig überprüften System abzubilden, das sowohl regulatorischen Anforderungen genügt als auch die tatsächliche Versorgungsfähigkeit des Krankenhauses dauerhaft absichert.

3.3 Energieversorgung

Eine sichere und stabile Energieversorgung ist eine zentrale Voraussetzung für den Betrieb von Krankenhäusern und anderen Gesundheitseinrichtungen. Medizinische Geräte, IT-Systeme, Kommunikationsinfrastruktur, Beleuchtung, Kühlung sowie die Versorgung mit medizinischen Gasen sind unmittelbar von einer kontinuierlichen Stromversorgung abhängig. Unterbrechungen der Energieversorgung können innerhalb kürzester Zeit zu erheblichen Risiken für Patienten, Personal und Betriebsabläufe führen.

Im Kontext des KRITIS-Dachgesetzes kommt der Energieversorgung daher eine besondere Bedeutung zu. Betreiber kritischer Gesundheitseinrichtungen sind verpflichtet, geeignete Maßnahmen zur Absicherung der Energieversorgung sowie zur Bewältigung von Versorgungsstörungen zu treffen.

3.3.1 Bedeutung der Energieversorgung für den Krankenhausbetrieb

Krankenhäuser zählen zu den energieintensiven Einrichtungen der kritischen Infrastruktur. Neben dem allgemeinen Strombedarf für Gebäude und Verwaltung bestehen hohe Anforderungen an die Versorgungssicherheit für:

- Intensivmedizinische Geräte und lebenserhaltende Systeme
- Operationssäle und medizinische Diagnostik (z. B. bildgebende Verfahren)
- IT-Infrastruktur und klinische Informationssysteme
- Beleuchtung und Sicherheitsanlagen
- Klima-, Lüftungs- und Kühltechnik
- Sterilisation und Labortechnik
- Versorgung mit medizinischen Gasen

Bereits kurze Stromausfälle können kritische Auswirkungen haben. Daher muss die Energieversorgung redundant ausgelegt und gegen externe Störungen abgesichert sein.

3.3.2 Redundanz und Ausfallsicherheit der Stromversorgung

Betreiber sollten sicherstellen, dass ihre Energieversorgung über ausreichende Redundanzen verfügt. Ziel ist es, auch bei Störungen im öffentlichen Stromnetz die Funktionsfähigkeit wesentlicher Bereiche aufrechtzuerhalten.

Empfohlene Maßnahmen umfassen:

- redundante Netzanschlüsse, sofern regional verfügbar
- unterbrechungsfreie Stromversorgungen (USV) für kritische IT- und Medizintechnik
- klare Trennung zwischen kritischen und nichtkritischen Stromverbrauchern
- priorisierte Notstromversorgung für lebenswichtige Bereiche

Eine strukturierte Lastpriorisierung stellt sicher, dass im Krisenfall besonders kritische medizinische Bereiche weiterhin betrieben werden können.

3.3.3 Notstromversorgung

Ein zentrales Element der Resilienz ist die Notstromversorgung. Krankenhäuser müssen in der Lage sein, bei einem Netzausfall innerhalb kürzester Zeit auf alternative Energiequellen umzuschalten.

Wesentliche Anforderungen sind:

- leistungsfähige Notstromaggregate mit ausreichender Kapazität
- automatische Umschaltsysteme zur schnellen Aktivierung
- ausreichende Kraftstoffvorräte für mehrstündige oder mehrtägige Ausfälle
- Lieferverträge für Nachbetankungen bei längeren Netzausfällen
- regelmäßige Wartung und Funktionsprüfungen der Anlagen

Darüber hinaus sollten Betreiber prüfen, ob zusätzliche mobile Stromerzeuger oder externe Notfallkapazitäten in regionalen Krisensituationen verfügbar sind.

3.3.4 Schutz der Energieinfrastruktur

Neben der reinen Verfügbarkeit von Energie muss auch die physische und technische Infrastruktur geschützt werden. Dazu zählen insbesondere:

- Transformatoren und Hauptstromverteilungen
- Notstromaggregate
- Schaltanlagen und Energieverteiler
- Steuerungs- und Überwachungssysteme

Diese Anlagen und Technikräume sollten gegen physische Schäden, Überflutung, Hitzeeinwirkungen sowie unbefugten Zugriff geschützt sein. Eine räumliche Trennung kritischer Komponenten kann die Resilienz zusätzlich erhöhen.

3.4 Klimatisierung & Lüftungsversorgung

Die Klimatisierung und Lüftungsversorgung stellt eine zentrale technische Grundlage für den sicheren Betrieb von Gesundheitseinrichtungen dar. Sie gewährleistet nicht nur den thermischen Komfort für Patienten und Personal, sondern erfüllt vor allem wesentliche hygienische und medizinische Anforderungen. Insbesondere in sensiblen Bereichen wie Operationssälen, Intensivstationen, Isolierbereichen oder Laboren ist eine kontrollierte Luftführung ein entscheidender Bestandteil des Infektionsschutzes und der Patientensicherheit.

Vor dem Hintergrund zunehmender Extremwetterereignisse, steigender Außentemperaturen sowie möglicher Energieversorgungsstörungen gewinnt die Resilienz von Lüftungs- und Klimasystemen weiter an Bedeutung. Betreiber von Krankenhäusern müssen daher geeignete technische und organisatorische Maßnahmen ergreifen, um die Funktionsfähigkeit dieser Systeme auch unter außergewöhnlichen Bedingungen sicherzustellen.

3.4.1 Bedeutung für medizinische Versorgung und Hygiene

Lüftungs- und Klimaanlagen erfüllen in Gesundheitseinrichtungen mehrere sicherheitsrelevante Funktionen:

- Sicherstellung definierter Raumtemperaturen und Luftfeuchtigkeit
- Gewährleistung hygienischer Luftqualität
- Kontrolle von Luftströmungen zwischen Rein- und Unreinbereichen
- Reduktion von Keim- und Partikelbelastungen
- Schutz immungeschwächter Patienten
- Unterstützung steriler Arbeitsbedingungen in Operationsbereichen

Der Ausfall oder eine erhebliche Einschränkung dieser Systeme kann insbesondere in sensiblen Funktionsbereichen zu unmittelbaren Risiken für Patienten führen.

3.4.2 Technische Ausfallsicherheit

Betreiber müssen sicherstellen, dass kritische Lüftungs- und Klimasysteme mit ausreichender Redundanz ausgestattet sind. Ziel ist es, auch bei technischen Störungen oder Energieunterbrechungen den Betrieb der wichtigsten medizinischen Bereiche aufrechtzuerhalten.

Zu den empfohlenen Maßnahmen zählen:

- redundante Lüftungsanlagen oder modulare Anlagenstrukturen
- priorisierte Anbindung kritischer Lüftungssysteme an die Notstromversorgung
- unterbrechungsfreie Stromversorgung für Steuerungs- und Regeltechnik
- klare Trennung von Lüftungssystemen unterschiedlicher Hygienebereiche

Besonders sensible Bereiche wie Operationssäle oder Isolationsstationen müssen über separate oder besonders abgesicherte Lüftungssysteme verfügen.

3.4.3 Resilienz gegenüber Extremwetter

Extreme klimatische Bedingungen können die Leistungsfähigkeit von Klimatisierungs- und Lüftungsanlagen erheblich beeinflussen. Betreiber müssen daher Maßnahmen ergreifen, um die Anlagen gegen externe Einflüsse abzusichern.

Relevante Aspekte sind unter anderem:

- ausreichende Dimensionierung der Kühlleistung für zunehmende Hitzeperioden
- Schutz von Außenluftansaugungen vor Starkregen, Schnee und Verunreinigungen
- Absicherung von Außenanlagen gegen Sturmereignisse
- Schutz sensibler Anlagenteile vor Überflutung
- Regelmäßige Kontrolle und Reinigung der Entwässerungseinrichtungen

Darüber hinaus sollten technische Anlagen so ausgelegt sein, dass auch bei erhöhten Außentemperaturen eine stabile Raumklimatisierung gewährleistet bleibt.

3.5 Brandschutz

Der Brandschutz stellt einen zentralen Bestandteil der Sicherheitsarchitektur von Gesundheitseinrichtungen dar. Krankenhäuser weisen aufgrund ihrer baulichen Struktur, der technischen Ausstattung sowie der eingeschränkten Mobilität vieler Patienten ein besonderes Gefährdungspotenzial auf. Gleichzeitig kann ein Brandereignis innerhalb kurzer Zeit die Funktionsfähigkeit kritischer medizinischer Bereiche beeinträchtigen oder vollständig zum Erliegen bringen.

Vor diesem Hintergrund sind Betreiber von Gesundheitseinrichtungen verpflichtet, umfassende bauliche, technische und organisatorische Brandschutzmaßnahmen umzusetzen. Ziel ist es, Brände frühzeitig zu erkennen, ihre Ausbreitung zu verhindern und im Ereignisfall eine sichere Evakuierung sowie die Aufrechterhaltung kritischer Versorgungsbereiche zu gewährleisten. Das KRITIS-Dachgesetz unterstreicht dabei die Bedeutung einer resilienten Sicherheitsinfrastruktur auch gegenüber Brandereignissen.

3.5.1 Besondere Brandrisiken in Gesundheitseinrichtungen

Krankenhäuser verfügen über eine Vielzahl potenzieller Brandrisiken, die sich aus ihrem Betrieb ergeben. Dazu zählen insbesondere:

- umfangreiche elektrische Infrastruktur und medizinische Geräte
- technische Anlagen wie Lüftungs-, Energie- und Versorgungssysteme
- Lagerung von medizinischen Gasen und brennbaren Materialien
- Küchenbetriebe, dezentrale Tee- und Kaffeeküchen und Wäschereibetriebe
- komplexe Gebäudestrukturen mit langen Fluren und vielen Funktionsbereichen

Zusätzlich erschwert die eingeschränkte Mobilität vieler Patienten eine schnelle Evakuierung, wodurch besondere Anforderungen an Prävention und organisatorische Abläufe entstehen.

3.5.2 Baulicher Brandschutz

Der bauliche Brandschutz bildet die Grundlage für eine wirksame Brandprävention. Ziel ist es, die Entstehung und Ausbreitung von Bränden zu begrenzen sowie ausreichend Zeit für Evakuierungsmaßnahmen zu schaffen.

Wesentliche Elemente sind:

- brandschutztechnische Trennung von Gebäudebereichen durch Brandabschnitte
- feuerbeständige Wände, Decken und Türen
- rauchdichte Abschlüsse zwischen Funktionsbereichen
- sichere Flucht- und Rettungswege
- ausreichende Brandlastbegrenzung in sensiblen Bereichen

Insbesondere kritische technische Infrastrukturen sollten in eigenen brandschutztechnisch gesicherten Bereichen untergebracht werden.

3.5.3 Technischer Brandschutz

Technische Systeme spielen eine entscheidende Rolle bei der frühzeitigen Branderkennung und Brandbekämpfung. Betreiber sollten sicherstellen, dass geeignete Systeme installiert, regelmäßig gewartet und in ein übergeordnetes Sicherheitskonzept integriert sind.

Dazu gehören unter anderem:

- automatische Brandmeldeanlagen mit direkter Alarmweiterleitung
- Rauch- und Wärmeabzugsanlagen
- automatische Löschanlagen in besonders gefährdeten Bereichen
- tragbare Feuerlöscheinrichtungen
- brandschutztechnische Abschaltungen für Lüftungs- und Versorgungsanlagen

Eine schnelle Alarmierung und klare technische Reaktionsmechanismen können die Ausbreitung eines Brandes erheblich begrenzen.

3.5.4 Organisatorischer Brandschutz

Neben baulichen und technischen Maßnahmen ist ein funktionierender organisatorischer Brandschutz entscheidend für die Sicherheit im Brandfall.

Wichtige Maßnahmen sind:

- Erstellung und regelmäßige Aktualisierung von Brandschutzordnungen
- klare Zuständigkeiten für Brandschutzbeauftragte und Sicherheitsverantwortliche
- regelmäßige Schulungen und Unterweisungen des Personals
- Durchführung von Evakuierungs- und Räumungsübungen
- enge Zusammenarbeit mit lokalen Feuerwehren und Rettungsdiensten

Besonders relevant ist die Vorbereitung auf Teilräumungen, da eine vollständige Evakuierung eines Krankenhauses häufig nur eingeschränkt möglich ist. In manchen Bundesländern besteht gemäß Landesbauordnung bzw. Prüfverordnung zusätzlich die regelmäßige Pflicht zur Wirkprinzip-Prüfung, die in die Wirksamkeitskontrollen integriert werden sollte.

3.6 Schutz gegen Unbefugte

Der Schutz gegen unbefugtes Eindringen ist ein zentraler Bestandteil eines gesetzeskonformen und resilienten Facility Managements in Krankenhäusern als Kritische Infrastrukturen. Ziel ist es, Menschen, Gebäude, technische Anlagen und betriebskritische Ressourcen wirksam vor unberechtigtem Zugriff zu schützen und zugleich einen sicheren, störungsfreien Krankenhausbetrieb zu ermöglichen. Physische Sicherheit wirkt dabei nicht isoliert, sondern als tragende Säule der organisatorischen Stabilität und Betriebssicherheit.

Krankenhäuser sind durch ihre offene Struktur und die Vielzahl unterschiedlicher Nutzergruppen besonders herausgefordert. Mitarbeitende, Patienten, Besucher, Lieferanten und Dienstleister bewegen sich parallel innerhalb derselben Liegenschaft, jedoch mit sehr unterschiedlichen Zugangsbedarfen. Der Schutz gegen Unbefugte erfordert daher klare, nachvollziehbare Regelungen, die Sicherheit gewährleisten, ohne die notwendige Offenheit und Funktionsfähigkeit des Krankenhauses einzuschränken. Ziel ist Kontrolle mit Augenmaß – nicht Abschottung um jeden Preis.

Ein wesentlicher Ansatzpunkt ist die systematische Gliederung der Krankenhausliegenschaft nach Schutzbedarfen. Bereiche mit unterschiedlicher Sensibilität müssen eindeutig definiert und organisatorisch wie technisch voneinander abgegrenzt sein. Öffentlich zugängliche Zonen, interne Arbeitsbereiche und besonders schutzbedürftige Funktionsbereiche wie Notaufnahmen, Intensivstationen, Technikzentralen oder IT-Räume erfordern jeweils abgestufte Schutzmaßnahmen. Diese Struktur bildet die Grundlage für ein rechtssicheres und wirksames Schutzkonzept gegen unbefugten Zutritt.

Darauf aufbauend kommt der Steuerung von Zugängen und Zutrittsrechten eine zentrale Bedeutung zu. Berechtigungen müssen rollenbasiert, bedarfsgerecht und zeitlich begrenzt vergeben werden. Klare Prozesse für Vergabe, Anpassung und Entzug von Zugangsrechten sind unerlässlich, um unbefugte Zugriffe zuverlässig zu verhindern. Besonders sensibel sind Übergänge, etwa bei Personalwechseln oder beim Einsatz externer Dienstleister, da hier Sicherheitslücken häufig entstehen, wenn Prozesse nicht eindeutig geregelt sind.

Technische Sicherungsmaßnahmen wie Zutrittskontrollsysteme, Schließanlagen, Videoüberwachung oder Einbruchmeldetechnik sind wichtige Instrumente, entfalten ihre Wirkung jedoch nur im Zusammenspiel mit klaren organisatorischen Regelungen. Verbindliche Besucher- und Lieferantenprozesse, eindeutige Zuständigkeiten sowie definierte Vorgehensweisen bei Auffälligkeiten sind entscheidend für die Wirksamkeit. Facility Management übernimmt hier eine koordinierende Rolle und sorgt dafür, dass technische Lösungen sinnvoll in den Betriebsalltag integriert sind.

Eine besondere Bedeutung hat die Klärung von Verantwortung und Entscheidungswegen. Schutz gegen Unbefugte ist keine rein operative Aufgabe, sondern eine Führungs- und Organisationsfrage. Unklare Zuständigkeiten führen häufig zu dauerhaft bestehenden Berechtigungen oder unzureichend überprüften Schutzmaßnahmen. Ein resilientes Facility Management stellt daher Transparenz her, legt Verantwortlichkeiten eindeutig fest und sorgt für regelmäßige Überprüfungen der getroffenen Maßnahmen.

Nicht zuletzt ist der Mensch ein zentraler Bestandteil der Schutzwirkung. Mitarbeitende sind tägliche Nutzer der Sicherheitsinfrastruktur und prägen deren Wirksamkeit maßgeblich. Sensibilisierung, Schulungen und klare Verhaltensregeln – etwa im Umgang mit Ausweisen, Türen oder sicherheitsrelevanten Auffälligkeiten – unterstützen dabei, unbefugtes Eindringen frühzeitig zu erkennen und zu verhindern. Sicherheitsmaßnahmen müssen so gestaltet sein, dass sie im klinischen Alltag akzeptiert und mitgetragen werden.

Zusammengefasst ist der Schutz gegen Unbefugte ein kontinuierlicher Bestandteil eines professionellen Facility Managements. Klare Strukturen, abgestufte Schutzmaßnahmen, eindeutige Verantwortlichkeiten und organisatorische Akzeptanz bilden die Grundlage für Gesetzeskonformität und Resilienz. Richtig umgesetzt stärkt der Schutz gegen Unbefugte nicht nur die physische Sicherheit, sondern auch die Verlässlichkeit und Stabilität des Krankenhausbetriebs als Kritische Infrastruktur.

3.7 Cyber-Security

Cybersicherheit im Gesundheitswesen ist eng verbunden mit den umfassenden Datenschutzanforderungen im Gesundheitswesen und ist essenziell, um hochsensible Patientendaten, medizinische Geräte und kritische Infrastrukturen (KRITIS) vor unberechtigtem Zugang zu schützen. Der Jahresbericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) 2025 hat zuletzt wieder gezeigt, dass der Gesundheitsbereich zu denjenigen KRITIS-Sektoren mit den meisten gemeldeten Störungen gehört. Das Gesundheitswesen ist ein Hauptziel für Cyberkriminelle, da vertrauliche Gesundheitsdateneinen hohen Wert für Cyberkriminelle haben. Angriffe können den Betrieb lahmlegen und schlussendlich auch Patientenleben gefährden. Dies macht es erforderlich sowohl die Bereiche der Information Technology (IT) als auch die Operational Technology (OT) durch angemessene Maßnahmen zu schützen. Hierzu zählen unter anderem z. B. Zwei-Faktor-Authentifizierung, Netzsegmentierung, strenge Einhaltung von Normen (z. B. §75c SGB V, NIS-2) und regelmäßige Personalschulungen.Krankenhäuser müssen in Deutschland hohe Standards wie das IT-Sicherheitsgesetz (IT-SiG 2.0)[04], B3S (Branchenspezifischer Sicherheitsstandard) und Art. 1 Nr.7 des DigiG[05] erfüllen. Die Absicherung vernetzter Medizingeräte (Internet of Medical Things – IoMT), die zum Bereich OT gehören, ist ein weiterer kritischer Bereich, um Manipulationen zu verhindern.

Der Schutz vor Cyberangriffen über die IT-Infrastrukturen muss in den IT-Systemen des Krankenhausbetreibers integriert werden, ggfls. durch externe Cyber-Security-Fachfirmen, die die IT-Infrastruktur (IT/OT) vor Angriffen schützen.

Die Risikobewertung und Durchführung der Bestandsaufnahme sollten anhand eines strukturierten Kataloges in Bezug auf die technischen und organisatorischen Maßnahmen erfolgen und folgende Punkte mindestens berücksichtigen;

- Technische Maßnahmen:
  - Netzwerksegmentierung (Trennung IT / OT)
  - Absicherung von Fernwartungszugängen (z. B. VPN, 2-Faktor-Authentifizierung)
  - Patch- und Schwachstellenmanagement für IT/OT-Systeme
  - Härtung von Systemen und Deaktivierung unnötiger Dienste
  - Monitoring, Protokollierung und Anomalieerkennung
  - Absicherung von Schnittstellen und Kommunikationsverbindungen

- Organisatorische Maßnahmen
  - vollständige Inventarisierung aller vernetzten Anlagen
  - durchführen von Business-Impact-Analysen (BIA) sowie die Identifizierung von notwendigen Wiederanlauf- und Wiederherstellungszeiten
  - erstellen von Notfallplänen
  - klare Regelungen für Zugriffs- und Berechtigungsmanagement

[04] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme v. 18. Mai 2021, BGBl. I 2021, Nr. 25, (Artikelgesetz).

[05] Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) v. 22. März 2024, BGBl. I 2024, Nr. 101, (Artikelgesetz).

- Integration von Cyber-Risiken in die bestehende Risikoanalyse
- regelmäßige Schulungen und Sensibilisierung des Personals
- Einbindung von Dienstleistern in Sicherheitsanforderungen
- klare Notfall- und Krisenmanagementstrukturen

Neben dem IT/OT Bereich, gibt es jedoch weitere kritische Bereiche, die gemäß den gesetzlichen Vorgaben ebenfalls Beachtung finden müssen.

Für alle betriebs- und sicherheitsrelevanten Mess-, Steuer- und Regeleinrichtungen gilt gemäß der TRBS 1115[06] bzw. TRBS 1115-1[07], dass Aufzüge, Druckanlagen, MSR-Systeme in OP, kritische Lüftungsanlagen, elektrische Sicherheitseinrichtungen, Notstromversorgungssysteme, etc. in der Risikoanalyse der Gesundheitseinrichtung zu berücksichtigen sind. Betreiber müssen Risiken kennen, Maßnahmen umsetzen und Konformität nachweisen.

Da Krankenhäuser zu den „öffentlichen Gebäuden" gehören, muss der Betreiber die Sorgfaltspflichten entsprechend einhalten. Auch hier konkretisiert die TRBS 1115 die Pflichten aus der Betriebssicherheitsverordnung (BetrSichV)[08] hinsichtlich sicherheitsrelevanter Mess-, Steuer- und Regeleinrichtungen (sMSR). Für öffentliche Immobilien gelten die gleichen Betreiberpflichten wie für private, jedoch mit höherem Augenmerk auf Publikumsverkehr, kritische Infrastruktur und Haftungsrisiken.

Öffentliche Gebäude, damit speziell bei Krankenhäusern auch 24/7, müssen gewährleisten, dass alle sicherheitsrelevanten MSR-Einrichtungen jederzeit funktionsfähig sind. Die Bedrohungen welche in die Gefährdungsbeurteilung einzubeziehen sind, z. B.:

- Gebäudeleittechnik (GLT, MSR)
- Risiken für sMSR-Einrichtungen analysieren
- „Supply Chain Angriff" über Wartungsfirmen (Fernwartungszugriff)
- Heizungs-, Lüftungs- und Klimaanlagen
- Aufzugssteuerungen
- Steuerungen für brandschutztechnische Einrichtungen (Brandmeldeanlage, Löschanlagen, etc.)
- Zentralversorgung spezieller technischer als auch medizinische Gase
- Notfallsysteme wie Notstromversorgung, USV-Anlagen
- Überwachungssysteme, Alarmanlagen und Videosysteme
- Zugangskontrollsysteme
  - Zugänge zu Technik- und Lagerräumen nur für berechtigtes Personal
  - Beseitigungen von „Standard-Schließungen" der Hersteller (Rital, Siemens, etc.)

[06] TRBS 1115 Sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen v. März 2021, GMBl | 2021, S. 484 [Nr. 22].

[07] TRBS 1115-1 Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen v. November 2022, GMBl | 2023, S. 522 [Nr. 25].

[08] Verordnung über Sicherheit und Gesundheitsschutz bei der Verwendung von Arbeitsmitteln (Betriebssicherheitsverordnung – BetrSichV) v. 03.02.2015, BGBl. I 2015, S. 49.

  - Vergabekonzept für Zutrittsschlüssel
  - wirksame Schutzmaßnahmen gegen unbefugtes betreten oder Manipulationsmöglichkeiten definieren und priorisieren

- Arbeitsmittel müssen technisch sicher und geprüft sein
- Notbefehlseinrichtungen müssen automatisiert und sofort wirksam sein

Alle Maßnahmen müssen regelmäßig geprüft und schriftlich dokumentiert werden, darunter sind u.a.:

- Gefährdungsbeurteilungen
- Prüfungen nach §§ 14, 16 BetrSichV
- Nachweis gleichwertiger Sicherheitsniveaus bei alternativen Lösungen
- Konzept der personifizierten Zugangsberechtigungen (2-Faktor) für IT-Systeme der technischen Infrastruktur
- Protokollieren von Änderungen in den Systemen

Zusammenfassend führt ein erfolgreicher Angriff auf ein öffentliches Gebäude nicht nur zu erheblichem finanziellem Schaden, sondern kann auch ganz erhebliche Konsequenzen für Leib und Leben haben. Im Weiteren ist ein Angriff derartiger Natur dazu geeignet, das Vertrauen der Bürger in den Staat und seine Institutionen zu erschüttern.

Für öffentliche Immobilien, speziell die Gesundheitseinrichtungen, gelten nach TRBS 1115/1115-1 insbesondere folgende Sorgfaltspflichten:

- Funktionssicherheit aller sMSR-Einrichtungen gewährleisten
- Cybersicherheit verbindlich in die Sicherheitsorganisation integrieren
- Vollständige und nachvollziehbare Dokumentation
- Regelmäßige Prüfungen und sicherheitsgerechte Instandhaltung
- Fachgerechte Einweisung aller Beteiligten inkl. Nachunternehmer
- Haftungs- und Betreiberverantwortung aktiv wahrnehmen
- Umsetzung arbeits- und anlagensicherheitsrechtlicher Mindeststandards
- Regelmäßige Kontrolle der Maßnahmen
- Aufrechterhaltung der Redundanzsysteme wie Notstromversorgung
- Business Continuity Management (BCM) ist zu empfehlen für Not- und Krisenfälle auszuarbeiten
- Regelmäßige Penetrationstests

Diese Pflichten gelten für alle Betreiber, aber Gesundheitseinrichtungen haben aufgrund der Nutzergruppen und Sichtbarkeit ein höheres Prüf- und Sicherheitsniveau einzuhalten.

3.8 Witterungsschutz (Natur)

Extremwetterereignisse nehmen in Europa nachweislich an Häufigkeit und Intensität zu. Betreiber sind daher gefordert, Witterungsrisiken systematisch zu analysieren, geeignete Schutzmaßnahmen umzusetzen und organisatorische Vorsorge zu treffen. Das KRITIS-Dachgesetz unterstreicht hierbei die Verpflichtung zu risikobasierten Schutzkonzepten und resilienten Betriebsstrukturen.

3.8.1 Relevante Natur- und Witterungsrisiken

Für Gesundheitseinrichtungen in Deutschland sind insbesondere folgende Naturereignisse relevant:

- Starkregen und Überflutungen
- Flusshochwasser
- Sturm und Orkan
- Hitzewellen
- extreme Kälte und Schneelasten
- Dürreperioden mit Auswirkungen auf Wasserverfügbarkeit
- Gewitterereignisse mit Blitzschlag und Stromausfällen

Die konkrete Gefährdungslage ist stark standortabhängig. Betreiber sollten daher regionale Gefährdungsanalysen durchführen und vorhandene Risikoanalysen (z. B. kommunale Gefahrenkarten, Hochwasserrisikomanagementpläne) einbeziehen.

3.8.2 Bauliche und technische Schutzmaßnahmen

Ein zentraler Bestandteil der Vorsorge ist die bauliche Resilienz der Einrichtungen. Kritische Gebäudeteile sowie technische Infrastruktur müssen gegen witterungsbedingte Schäden geschützt sein.

Empfohlene Maßnahmen umfassen unter anderem:

3.8.2.1 Schutz vor Starkregen und Hochwasser

- Sicherung von Kellerbereichen und Technikräumen durch Rückstauklappen und druckwasserdichte Zugänge
- hochwassersichere Positionierung kritischer Anlagen (z. B. Notstromaggregate, Stromverteilungen, IT-Räume)
- mobile oder feste Hochwasserschutzsysteme
- Entwässerungssysteme mit ausreichender Kapazität
- und regelmäßiger Kontrolle (Bsp Dachabläufe DIN 1986-3:2024-05[09])

[09] DIN 1986-3 Entwässerungsanlagen für Gebäude und Grundstücke – Teil 3: Regeln für Betrieb und Wartung (Ausgabe) 2024-05, DIN Media, Berlin.

3.8.2.2 Sturm- und Orkanschutz

- regelmäßige Überprüfung von Dachkonstruktionen und Fassadenelementen
- Sicherung von Außenanlagen, technischen Aufbauten und Solaranlagen
- Sturmsichere Verankerung von Antennen, Lüftungsanlagen und technischen Aufbauten

3.8.2.3 Schutz vor Hitze

- leistungsfähige Kühl- und Klimasysteme für medizinische Bereiche, Serverräume und Arzneimittellager
- Verschattungssysteme und geeignete Gebäudedämmung
- Notfallkonzepte für Kühlung bei Stromausfällen

3.8.2.4 Schutz vor Schnee- und Eislast

- statische Auslegung von Dachkonstruktionen auf erhöhte Schneelasten
- geregelte Prozesse zur Schneeräumung von Dächern und kritischen Verkehrsflächen

3.8.3 Organisatorische Vorsorge und Krisenmanagement

Neben technischen Maßnahmen ist eine klare organisatorische Vorbereitung entscheidend.

Dazu gehören:

- Integration von Extremwetterlagen in bestehende Notfall- und Krisenpläne
- definierte Alarmierungs- und Entscheidungsstrukturen
- Schulungen und Übungen für Personal
- klare Zuständigkeiten für Gebäudemanagement und Krisenreaktion
- Kooperation mit lokalen Behörden, Katastrophenschutz und Energieversorgern

Auch Frühwarnsysteme und Wetterwarnungen sollten in die Entscheidungsprozesse eingebunden werden.

3.8.4 Kontinuitätsplanung und Betriebsaufrechterhaltung

Bei schweren Naturereignissen kann es erforderlich sein, den Krankenhausbetrieb teilweise anzupassen oder temporär einzuschränken. Betreiber sollten daher Notfall- und Kontinuitätspläne vorhalten, die insbesondere folgende Aspekte berücksichtigen:

- Priorisierung kritischer medizinischer Leistungen
- Evakuierungs- und Verlegungskonzepte
- Versorgungssicherheit für Patienten und Personal
- Sicherstellung logistischer Lieferketten (Medikamente, Lebensmittel, Medizinprodukte)

Diese Planungen sollten regelmäßig überprüft und an neue Gefährdungslagen angepasst werden.

3.9 Hygiene

Das Hygienebewusstsein der Mitarbeiter in Medizinischen- und Pflegeberufen ist essenziell und wird ab dem ersten Tag sensibilisiert, praktiziert und nachgehalten.

In den FM-Dienstleistungsbereichen Food-Services und Reinigung ist hygienerelevantes Verhalten fester Bestandteil von Ein- und Unterweisungen, entsprechende Kontrollmechanismen und die Dokumentation der Prüfungen sind i.d.R. in Prozessbeschreibungen und Verfahrensanweisungen fest verankert.

Im Bereich der technischen Dienstleistungen werden normativ hygienerelevante Aktivitäten gefordert, jedoch sind diese keine Bestandteile der grundsätzlichen Qualifikationen in den entsprechenden Berufsbildern – vielmehr muss hier im Rahmen von Weiterbildungen ein Verständnis für mikrobiologische Zusammenhänge und Abhängigkeiten erlangt werden.

Bei Betrachtung von Luft und Wasser als die primären Lebensmittel für den Menschen, erschließt sich dadurch unmittelbar, dass auch diese Anlagen der Gebäudetechnik mit in die Betrachtungen zur kritischen Infrastruktur einzubeziehen sind.

Seitens des Gesetzgebers werden dabei in Bundesverordnungen (TrinkwV[10], 42. BImSchV[11]), flankiert von allgemein anerkannten Regeln der Technik, umfänglich die erforderlichen Maßnahmen zum hygienischen Umgang mit Trinkwasseranlagen, Klima- / Lüftungssystemen und adiabaten Rück-kühlwerken definiert.

Ein wichtiger Bereich, der meist vernachlässigt wird, ist die Entsorgung. Das Entsorgungsmanagement beginnt mit Altpapier und endet mit Wäscheentsorgung. Neben Infektiösem Müll gehört die Abwasserentsorgung zu den komplexeren Themen, bei denen das öffentliche / kommunale Netz meist stark eingebunden ist.

Durch den Betreiber sind die Regelwerke anlagenbezogen in den einzelnen Liegenschaften zu adaptieren und umzusetzen, dabei kann nur durch ein weitreichendes Verständnis der physikalischen und technischen Zusammenhänge in TGA-Systemen potenziell gesundheitsgefährdende Auswirkungen erkannt werden, um hieraus durch Risikoabschätzungen und Gefährdungs-beurteilungen präventive Kontrollmaßnahmen zur Sicherstellung eines hygienisch unbedenklichen Betriebes abzuleiten.

[10] Verordnung über die Qualität von Wasser für den menschlichen Gebrauch (Trinkwasserverordnung – TrinkwV) v. 20.06.2023, BGBl. I 2023, Nr. 159, S. 2.

[11] Zweiundvierzigste Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Verordnung über Verdunstungskühlanlagen, Kühltürme und Nassabscheider – 42. BImSchV) v. 12.07.2017, BGBl. I 2017, S. 2379 | 2018, S. 202.

3.9.1 Raumlufthygiene

Die seit 1998 regelmäßig weiterentwickelte Richtlinie VDI 6022 (aktuell Blatt 1 – 8)[12] formuliert ganzheitlich Erfordernisse, um Beeinträchtigungen der Gesundheit durch raumlufttechnische Anlagen auszuschließen.

In konkreten Anforderungen an Bauherrn, Planer, Gerätehersteller, Anlagen-Errichter, Instandhalter und Betreiber werden detailliert Ziele und Maßnahmen definiert, deren Einhaltung sicherstellt, dass die in RLT-Anlagen aufbereitete Atemluft gesundheitlich unbedenklich ist.

Da nach der Errichtung einer Anlage die grundsätzlichen Parameter zu Materialauswahl und Konstruktion festgelegt sind, sind insbesondere die Kontroll- und Prüfanforderungen in der Betriebsphase zu fokussieren und im Sinne der geforderten KRITIS-Resilienz umzusetzen.

3.9.2 Trinkwasserhygiene

Wasser für den menschlichen Gebrauch ist ein sensibles Lebensmittel – von Natur aus nie keimfrei, ist es die Aufgabe von Wasserversorgern sicherzustellen, dass nicht durch Keimwachstum oder andere Verunreinigungen eine Beeinträchtigung der Gesundheit erfolgen kann.

Seitens der öffentlichen Wasserversorger endet dabei die Zuständigkeit an der Übergabestelle ins Gebäude: Der Gebäudeeigentümer / Betreiber übernimmt ab der Einspeisung die Rolle des Trinkwasserversorgers und damit die Verantwortung für die Sicherstellung der Trinkwasserqualität bis zur Verwendungsstelle.

Die Anforderungen der Trinkwasser-Verordnung werden in DIN-Normen, DVGW / ZVSHK Arbeits- und Merkblättern hinsichtlich Materialauswahl, konstruktiven Anforderungen konkretisiert und in der Richtlinie VDI 6023[13] insbesondere hinsichtlich der hygienischen Anforderungen fokussiert.

Da bei Trinkwasseranlagen (wie in der Raumlufttechnik) nach der Errichtung die grundsätzlichen Parameter gesetzt sind, ist auch hier durch Kontroll- und Prüfmaßnahmen während der Betriebsphase der hygienische Betrieb sicherzustellen.

Dabei ist zu berücksichtigen, dass Wasser z. T. sensibler ist als andere Lebensmittel:

nicht bestimmungsgemäß genutzte Wasserversorgungs- und verteilanlagen oder Nutzungsänderungen ohne Anpassung der Wasserverteilanlage erhöhen das Risiko von Keimwachstum deutlich.

[12] VDI 6022 Blatt 1 Raumlufttechnik, Raumluftqualität – Hygieneanforderungen an raumlufttechnische Anlagen und Geräte (Ausgabe) 2018-01, DIN Media, Berlin, sowie weitere Blätter.

[13] VDI 6023 Blatt 1 Hygiene in Trinkwasser-Installationen – Anforderungen an Planung, Ausführung, Betrieb und Instandhaltung (Ausgabe) v. 2023-09, DIN Media, Berlin, sowie weitere Blätter.

Die genannten Regelwerke beinhalten daher konkrete Anweisungen zur Überwachung von mikrobiologischen und chemischen Grenzwerten, Handlungsanforderungen bei Änderungen der Nutzung und Maßnahmen zur Sicherstellung eines hygienisch unbedenklichen Betriebes.

Die Abwasserentsorgung wird zukünftig eine größere Rolle einnehmen, da vermehrt der Betreib von eigenen Kläranlagen verpflichtend wird.

3.9.3 Adiabate Rückkühlwerke

Durch Wasserverdunstung Kühleffekte zu realisieren, ist ein energetisch und betriebswirtschaftlich hochattraktives Verfahren, um die Aufwendungen für mechanische Kühlung zu reduzieren.

Im Umlaufwasser oder nicht durchspülten Wasser-Anschlussleitungen können sich jedoch dabei

systembedingt ideale Bedingungen für Keimwachstum einstellen, die dann aerosolgetragen potenzielle Krankheitserreger in die Umwelt emittieren. Insbesondere Legionellen werden hierbei als besonders kritische Bakterien eingestuft.

Ausgelöst durch Vorfälle in Ulm und Warstein wurden daher in den technischen Regelwerken VDI 2047[14] und 42. BImSchV Maßnahmen zur Minimierung der Gesundheitsrisiken erfasst:

Adiabate Kühlsysteme, die Luft in die Umwelt abgeben, sind im behördlichen Überwachungssystem KAVKA (Kataster für Verdunstungskühl-Anlagen) zu registrieren, und nach den Anforderungen zu betreiben – Qualifikationen, Eigenkontrollen, Laboruntersuchungen von Wasserproben und Sachverständigen-Prüfpflichten sind in den Vorschriften geregelt.

[14] VDI 2047 Blatt 1 Rückkühlwerke – Begriffe zu Verdunstungs- und Trockenkühlanlagen und Durchlaufkühlsystemen (Ausgabe) v. 2021-01, DIN Media, Berlin, sowie weitere Blätter.

3.10 Zutrittsmanagement

Gerade in KRITIS-Umgebungen entscheidet ein durchdachtes Zutrittsmanagement darüber, ob Facility-Management-Strukturen rechtssicher, belastbar und zugleich handlungsfähig bleiben. Es gewährleistet eine ausgewogene Abstimmung zwischen Sicherheitsanforderungen, Betriebsfähigkeit und organisatorischer Flexibilität. Dabei beschränkt sich Zutrittsmanagement nicht auf das Öffnen oder Verschließen von Türen, sondern umfasst die gezielte Steuerung von Personenströmen, Zuständigkeiten und Verantwortlichkeiten innerhalb komplexer Liegenschaften – mit unmittelbarem Einfluss auf die Stabilität des Gesamtbetriebs.

Grundlage eines wirksamen Zutrittsmanagements ist eine klare räumliche Ordnung. Alle Bereiche einer Liegenschaft müssen nach ihrem jeweiligen Schutzbedarf systematisch erfasst und eindeutig voneinander abgegrenzt werden. Öffentlich zugängliche Flächen, betriebsinterne Zonen und besonders schützenswerte Bereiche erfordern jeweils unterschiedliche Zugriffsniveaus. Diese Differenzierung ist nicht nur eine bauliche oder technische Aufgabe, sondern vor allem eine organisatorische Entscheidung, die Transparenz schafft und Fehlinterpretationen im Alltag vermeidet.

Darauf aufbauend rückt die gezielte Vergabe und Pflege von Zutrittsrechten in den Fokus. Berechtigungen dürfen sich nicht an Personen, sondern müssen sich an Funktionen und Aufgaben orientieren. Sie sind zeitlich zu begrenzen, regelmäßig zu überprüfen und konsequent anzupassen, sobald sich Tätigkeiten oder Zuständigkeiten ändern. Für das Facility Management bedeutet dies, klare und verbindliche Abläufe zu etablieren, die verhindern, dass Zugänge „mitwandern“ oder aus Bequemlichkeit bestehen bleiben. Gerade temporäre Berechtigungen für externe Dienstleister erfordern besondere Aufmerksamkeit und Kontrolle.

Ein weiterer zentraler Aspekt ist das Zusammenspiel von Technik und Organisation. Zutrittskontrollsysteme, Schließkonzepte oder Identifikationsmedien sind nur dann wirksam, wenn sie in klare Prozesse eingebettet sind. Facility Management stellt sicher, dass technische Lösungen rechtssicher betrieben werden, im Arbeitsalltag praktikabel bleiben und von den Nutzern akzeptiert werden. Dazu zählen unter anderem nachvollziehbare Regelungen zur Protokollierung, ein sensibler Umgang mit personenbezogenen Daten sowie definierte Vorgehensweisen bei Störungen oder Systemausfällen.

Ebenso entscheidend ist die eindeutige Festlegung von Verantwortlichkeiten. Ein belastbares Zutrittsmanagement braucht klare Entscheidungswege: Wer beantragt, wer genehmigt, wer überprüft und wer greift im Bedarfsfall ein? Fehlt diese Klarheit, entstehen über Jahre gewachsene Berechtigungsstrukturen, die kaum noch zu überblicken sind und erhebliche Risiken bergen. Facility Management nimmt hier eine vermittelnde Rolle ein und sorgt für abgestimmte Abläufe zwischen Leitung, Sicherheit, IT und den operativen Bereichen.

Neben Technik und Prozessen bleibt der Mensch der entscheidende Erfolgsfaktor. Mitarbeitende prägen den Umgang mit Zutrittsregelungen im Alltag maßgeblich. Regelmäßige Sensibilisierung, verständliche Regeln und praxisnahe Schulungen helfen, den Sinn von Zutrittsbeschränkungen zu vermitteln und sicherheitsbewusstes Verhalten zu fördern. Akzeptanz entsteht dort, wo Regelungen als sinnvoll und unterstützend wahrgenommen werden – nicht dort, wo sie als zusätzliche Hürde erscheinen.

Zutrittsmanagement muss zudem so gestaltet sein, dass es auch in außergewöhnlichen Betriebssituationen verlässlich funktioniert. Ereignisse mit erhöhtem Koordinationsbedarf erfordern flexible, aber kontrollierte Anpassungen von Zugangsrechten. Systeme und Prozesse müssen schnelle Entscheidungen ermöglichen, ohne die Übersicht oder Kontrolle zu verlieren. Regelmäßige Überprüfungen und praktische Tests tragen dazu bei, diese Fähigkeit dauerhaft sicherzustellen.

Insgesamt ist Zutrittsmanagement ein fortlaufender Organisations- und Steuerungsprozess. Richtig umgesetzt verbindet es Rechtssicherheit, Betriebssicherheit und Resilienz zu einem stabilen Gesamtsystem. Es wirkt im Hintergrund, fällt im Idealfall nicht auf – und wird gerade deshalb zu einem entscheidenden Faktor für Verlässlichkeit und Handlungssicherheit in KRITIS-Umgebungen.

3.11 FM-Personal (+ deren Qualifikationen)

In KRITIS-Umgebungen ist das Facility-Management-Personal weit mehr als eine unterstützende operative Kraft: Es bildet das Rückgrat der technischen und organisatorischen Betriebsstabilität. Die Qualifikation, Zuverlässigkeit und Struktur dieses Personals entscheiden unmittelbar darüber, ob Anlagen sicher, regelkonform und resilient betrieben werden können. Damit rückt das FM-Personal in eine sicherheitsrelevante Rolle, die hohe Anforderungen an Fachwissen, Prozessverständnis und persönliche Eignung stellt.

Grundlegend ist die eindeutige Definition von Rollen, Aufgaben und Befugnissen. KRITIS-Liegenschaften erfordern klar abgegrenzte Verantwortlichkeiten innerhalb des FM-Teams, um Fehlsteuerungen und Sicherheitslücken zu vermeiden. Technische Mitarbeitende, Objektleitungen, Service-Desk-Personal oder Bereitschaftsdienste müssen genau wissen, welche Aufgaben in welchen Situationen auszuführen sind und welche Entscheidungen ausschließlich dem Betreiber vorbehalten bleiben. Unklare Zuständigkeiten führen in kritischen Infrastrukturen schnell zu Verzögerungen, Fehlmeldungen oder unbemerkten Störungen, die die Funktionsfähigkeit ganzer Betriebsbereiche gefährden können.

Ein zentrales Element ist die fachliche Qualifikation des FM-Personals. Mitarbeitende müssen Kenntnisse zu sicherheitskritischen Gewerken, einschlägigen Normen, Betreiberpflichten und gesetzlichen Vorgaben besitzen. Dazu zählen beispielsweise Kenntnisse zu Arbeitsschutz, Brandschutz, Elektrosicherheit, Anlagenbetrieb oder Dokumentationspflichten. Qualifikationen dürfen jedoch nicht als einmalige Voraussetzung verstanden werden. Gerade in dynamischen Betreiberumgebungen sind regelmäßige Weiterbildungen, technische Unterweisungen und jährliche Sicherheitsbelehrungen erforderlich, um neues Wissen, geänderte Regularien oder neue Anlagenkonzepte zu berücksichtigen. Das KRITIS-Umfeld verstärkt diesen Anspruch zusätzlich, da hier hohe Anforderungen an systematische Prozesssicherheit und Informationssicherheit bestehen.

Gleichzeitig spielt die persönliche Zuverlässigkeit des FM-Personals eine wesentliche Rolle. Mitarbeitende haben Zugang zu sensiblen Bereichen, vertraulichen Informationen oder kritischen Schaltstellen der technischen Infrastruktur. Daher sind strukturierte Zuverlässigkeitsprüfungen, abgestufte Sicherheitsfreigaben und ein vertrauenswürdiges Personalmanagement essenziell. Die Einhaltung von Sicherheitsvorgaben, die richtige Reaktion auf Unregelmäßigkeiten sowie ein hohes Maß an Verantwortungsbewusstsein sind unverzichtbare Eigenschaften, die durch Schulung, Sensibilisierung und regelmäßige Kommunikation gefördert werden müssen.

Auch organisatorisch müssen FM-Teams so aufgebaut sein, dass sie die Anforderungen einer KRITIS-Liegenschaft dauerhaft erfüllen können. Dazu gehören belastbare Schicht- und Rufbereitschaftsmodelle, definierte Vertretungsregelungen sowie ausreichend personelle Redundanz, um auch bei Ausfällen und/oder Störfällen reaktionsfähig zu bleiben. Eine sichere Kritikalitätsinfrastruktur darf nicht von Einzelpersonen abhängig sein. Teams müssen daher so strukturiert sein, dass Wissen geteilt wird, Übergaben standardisiert erfolgen und relevante Informationen jederzeit nachvollziehbar verfügbar sind.

Schließlich ist das FM-Personal ein wichtiger Multiplikator für Sicherheit und Bewusstsein in der gesamten Organisation. Durch täglichen Kontakt mit Nutzern, Technik und Prozessen nehmen Mitarbeitende im FM eine Schlüsselrolle ein, wenn es darum geht, Sicherheitsregeln vorzuleben, auf Abweichungen hinzuweisen und im Bedarfsfall angemessen zu reagieren. Eine kontinuierliche Sensibilisierung für Risiken und sicherheitsrelevantes Verhalten trägt entscheidend zur Stabilität der kritischen Infrastruktur bei.

Insgesamt zeigt sich: Die Qualifikation und Struktur des FM-Personals sind ein zentraler Baustein für einen rechtssicheren und resilienten Betrieb. Nur wenn Rollen klar definiert, Fachkenntnisse kontinuierlich aktualisiert, Zuverlässigkeit überprüft und Prozesse fest etabliert sind, kann das Facility Management seine Verantwortung als operative Säule des Betreibers effektiv wahrnehmen und die Anforderungen des KRITIS-Dachgesetzes nachhaltig erfüllen.

4 Fazit

Das KRITIS-Dachgesetz markiert einen grundlegenden Wendepunkt für das Facility Management und stellt Gesundheitseinrichtungen – insbesondere Krankenhäuser – vor weitreichende organisatorische, technische und dokumentarische Anforderungen. Die Anforderungen gehen weit über klassische Betreiberpflichten hinaus und verankern das Facility Management als zentralen Bestandteil der Sicherheits-, Risiko- und Resilienzstrategie von Krankenhäusern. Angesichts zunehmender klimatischer Extremereignisse, wachsender Cyberbedrohungen und der hohen Abhängigkeit medizinischer Leistungen von komplexen technischen Versorgungsstrukturen wird Resilienz zum strategischen Kernziel.

Das Gesetz verschiebt den Fokus von einer reaktiven Gefahrenabwehr hin zu einem präventiven, systematischen Risikomanagement und damit von einer überwiegend operativen, kostengetriebenen Funktion hin zu einer strategischen Verantwortung für die Sicherstellung der Betriebsfähigkeit kritischer Infrastrukturen. Krankenhäuser müssen kritische Anlagen identifizieren, Risiken strukturiert bewerten, geeignete Schutz- und Redundanzmaßnahmen umsetzen und deren Wirksamkeit dauerhaft nachweisen. Es wird vom unterstützenden Dienst zum tragenden Bestandteil gesetzlicher Compliance, Betriebsstabilität und Versorgungssicherheit.

Die vielfältigen Handlungsfelder – von Energieversorgung, Klima- und Lüftungstechnik über Brandschutz, Hygiene und Zutrittsmanagement bis hin zur Cybersicherheit – verdeutlichen, dass Resilienz nur durch ein integriertes Zusammenspiel technischer, organisatorischer und personeller Maßnahmen erreicht werden kann. Dokumentation, Transparenz, regelmäßige Prüfungen und die Qualifikation des FM-Personals werden zu elementaren Bausteinen eines belastbaren Betriebs.

Insgesamt bietet das KRITIS Dachgesetz nicht nur regulatorische Herausforderungen, sondern auch eine Chance zur Professionalisierung und Modernisierung der Betreiberstrukturen. Krankenhäuser, die Resilienz als strategischen Erfolgsfaktor verstehen, sichern nicht nur ihre Compliance, sondern stärken nachhaltig die Betriebssicherheit, Versorgungskontinuität und das Vertrauen von Patienten, Mitarbeitenden und Gesellschaft.

Hinweis: Zum Redaktionsschluss liegt weder die im Gesetz geforderten Resilienzpläne vor, noch steht die Gegistrierungsplattform zur Verfügung, da sich die konkretisierende Identifizierungsverordnung gem. § 4 Abs. 3 und § 5 Abs. 1 KRITISDachG derzeit noch in Erarbeitung und Abstimmung befindet.

5 Literaturverzeichnis

[01] Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITISDachG) v. 11.03.2026, BGBl. I 2026, Nr. 66.

[02] Richtlinie (EU) 2022/2557 [...] vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen [...], ABl. L 333 v. 27.12.2022, S. 164–198.

[03] GEFMA 190 Betreiberverantwortung 2.0 im Facility Management (inkl. ESG) v. 2023-06, gefma e. V.

[04] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme v. 18. Mai 2021, BGBl. I 2021, Nr. 25, (Artikelgesetz).

[05] Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) v. 22. März 2024, BGBl. I 2024, Nr. 101, (Artikelgesetz).

[06] TRBS 1115 Sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen v. März 2021, GMBl | 2021, S. 484 [Nr. 22].

[07] TRBS 1115-1 Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen v. November 2022, GMBl | 2023, S. 522 [Nr. 25].

[08] Verordnung über Sicherheit und Gesundheitsschutz bei der Verwendung von Arbeitsmitteln (Betriebssicherheitsverordnung – BetrSichV) v. 03.02.2015, BGBl. I 2015, S. 49.

[09] DIN 1986-3 Entwässerungsanlagen für Gebäude und Grundstücke – Teil 3: Regeln für Betrieb und Wartung (Ausgabe) 2024-05, DIN Media, Berlin.

[10] Verordnung über die Qualität von Wasser für den menschlichen Gebrauch (Trinkwasserverordnung – TrinkwV) v. 20.06.2023, BGBl. I 2023, Nr. 159, S. 2.

[11] Zweiundvierzigste Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Verordnung über Verdunstungskühlanlagen, Kühltürme und Nassabscheider – 42. BImSchV) v. 12.07.2017, BGBl. I 2017, S. 2379 | 2018, S. 202.

[12] VDI 6022 Blatt 1 Raumlufttechnik, Raumluftqualität – Hygieneanforderungen an raumlufttechnische Anlagen und Geräte (Ausgabe) 2018-01, DIN Media, Berlin, sowie weitere Blätter.

[13] VDI 6023 Blatt 1 Hygiene in Trinkwasser-Installationen – Anforderungen an Planung, Ausführung, Betrieb und Instandhaltung (Ausgabe) v. 2023-09, DIN Media, Berlin, sowie weitere Blätter.

[14] VDI 2047 Blatt 1 Rückkühlwerke – Begriffe zu Verdunstungs- und Trockenkühlanlagen und Durchlaufkühlsystemen (Ausgabe) v. 2021-01, DIN Media, Berlin, sowie weitere Blätter.

Die Erarbeitung des White Papers erfolgte durch die Autoren

Ulrich Glauche, Stefan Klemckow, Bernd Lausch, Gerhard Link, Mandana Banedj-Schafii,
Jürgen Schneider, Sebastian Sichter, Horst Träger

Erstellt am: 31.03.2026

Ansprechpartner:
Sebastian Sichter (gefma)
sebastian.sichter@strabag-pfs.com

Ansprechpartner:
Gerhard Link (FKT)
g.link@gerhardlink.com

Herausgeber:
gefma
Deutscher Verband für Facility Management e. V.
Basteistraße 88
53173 Bonn
Tel. +49 228 850276-0
info@gefma.de
www.gefma.de

Herausgeber:
Geschäftsstelle der
Fachvereinigung Krankenhaustechnik e. V.
Habbesweg 12
59425 Unna
Tel. +49 800 0060 822
fkt@fkt.de
www.fkt.de

Verantwortliches Gremium:
gefma Arbeitskreis Kritische Infrastruktur

Grafik/Layout:
ad-creation

White Paper GEFMA 932
Version 1.0