DIN

Whitepaper

Normung und Standardisierung bei der Ausgestaltung des KRITIS-Dachgesetzes

Vorwort

Sehr geehrte Leserinnen und Leser,

die Ereignisse der letzten Jahre zeigen uns deutlich, dass unsere Kritische Infrastruktur viel mehr in unseren Fokus rücken muss. Das Thema ist aber nicht nur komplex, sondern führt auch zu hohen Investitionen für Unternehmen, Organisationen und staatliche Institutionen.

Das Ahrtal Hochwasser, die Anschläge/Sprengungen der Nord-Stream Pipelines und die Corona Pandemie, um nur einige Beispiele zu nennen, haben uns allen jedoch vor Augen geführt, wie wichtig der Schutz der Kritischen Infrastruktur und damit auch der Schutz der Bevölkerung ist.

Ziel muss die Steigerung der Resilienz der Kritischen Infrastruktur sein, damit diese bei Ereignissen, wie Sabotage, Anschlägen, (Hacker-) Angriffen oder Umweltkatastrophen, weiterhin funktionsfähig bleibt. Im Januar 2023 ist die EU-Richtline über die Resilienz kritischer Einrichtungen (Critical Entities Resilience / CER-Richtlinie) in Kraft getreten und nun blicken wir mit großem Interesse, wie dies ins nationale Gesetz überführt wird und welche Schutzziele das geplante KRITIS-Dachgesetz formuliert.

Im Frühjahr 2023 hat DIN mit Beteiligten aus der Wirtschaft, von Katastrophenschutzbehörden, Verbänden und Bundesämtern in mehreren Workshops das Thema erörtert. Grundlage der Diskussion war das Eckpunktepapier des Bundesministeriums des Innern und für Heimat (BMI) zum KRITIS-Dachgesetz und das gemeinsame Verständnis der Beteiligten bezüglich der Kritischen Infrastruktur. Dabei ist dieses White Paper entstanden, das dem BMI zur Berücksichtigung für das KRITIS-Dachgesetz übermittelt wurde.

Normen und Standards sind hier ein relevantes und wesentliches Mittel, um Schutzziele zu erreichen. DIN bietet eine neutrale Plattform, um alle relevanten Stakeholder unterschiedlicher Sektoren zusammenzubringen, mit ihnen zu diskutieren und die Ergebnisse der Diskussionen in Normen und Standards zu überführen.

Mit der Umsetzung und Anwendung der Normen und Standards wird also ein wichtiger Beitrag zum Schutz der Kritischen Infrastruktur erreicht. Wir sind uns dieser Verantwortung bewusst und werden uns deshalb weiterhin mit allen Stakeholdern dafür einsetzen, unsere Gesellschaft noch resilienter aufzustellen.

Wir wünschen Ihnen eine informative Lektüre.

Dr. Michael Stephan
DIN – Mitglied der Geschäftsleitung
Bereich Normung und Standardisierung

Andreas Schleifer
Geschäftsführer
Koordinierungsstelle Sicherheitswirtschaft (KoSi)

Koordinierungsstelle Sicherheitswirtschaft (KoSi)

Der Bereich Sicherheit umschließt ein sehr breites Spektrum von Fragestellungen und Aspekten, die zugleich eine ebenso hohe Anzahl an Branchen und Technologiefeldern betreffen. Normung und Standardisierung gestalten dabei die Rahmenbedingungen für den Sicherheitsmarkt.

Die Koordinierungsstelle Sicherheitswirtschaft (KoSi) befasst sich mit branchenübergreifenden normungs-, standardisierungs- und forschungsbezogenen Aktivitäten für die Sicherheitsbranche. Sie sorgt für eine enge Zusammenarbeit der DIN-Gremien und steht allen Interessierten der Sicherheitswirtschaft als zentraler Ansprechpartner zur Verfügung.

Ausgewählte Fachexpert*innen aus den interessierten Kreisen bilden ein Beratergremium, das Fragen der Normung und Standardisierung in der Sicherheitswirtschaft diskutiert und inhaltliche Zielstellungen für die Arbeit der Koordinierungsstelle vorgibt.

Das zentrale Entscheidungsorgan der KoSi ist der Fachbeirat, der durch eigene, aus der Praxis herangetragene und abstrahierte Bedarfe, strategische Impulse hinsichtlich einer intensiveren Verfolgung bereits bestehender oder neu aufzunehmender Aktivitäten, in die Normung gibt.

Ihr Ansprechpartner

DIN e. V.

Andreas Schleifer (Geschäftsführer KoSi)
Andreas.Schleifer@din.de

Am DIN Platz
Burggrafenstraße 6
10787 Berlin

Inhaltsverzeichnis

1 Einleitung und Ziele

Im Dezember 2022 wurde das Eckpunktepapier des Bundesministeriums des Innern und für Heimat (BMI) zu dem geplanten KRITIS-Dachgesetz veröffentlicht. Dieses Dachgesetz wird national die EU-Richtlinie für Critical Entities Resilience (CER-Richtlinie) umsetzen. Die Koordinierungsstelle Sicherheitswirtschaft (KoSi) hat in diesem Zusammenhang mit Vertreter*innen aus unterschiedlichen Bereichen dieses White Paper erarbeitet. Dieses White Paper beinhaltet Punkte, die das KRITIS-Dachgesetz, aus Sicht der Beteiligten, berücksichtigen sollten. Dabei haben u. a. Bundesministerien, Wirtschaft und Wirtschaftsverbände wie auch Hilfsorganisationen sehr wichtigen Input geliefert.

Folgende Personen waren u.a. bei der Erarbeitung des White Papers beteiligt:

- Herr Dr. Urban Brauer (BHE Bundesverband Sicherheitstechnik)
- Herr Sebastian Brose (VdS Schadensverhütung GmbH)
- Herr Dirk H. Bürhaus (KÖTTER Unternehmensgruppe)
- Herr Alexander Dobert (Datenschutz Dobert)
- Herr Frank Drescher (Malteser Hilfsdienst)
- Herr Bernd Giegerich (Bosch Sicherheitssysteme GmbH)
- Herr Karsten Göwecke (Projektgruppe zur Schaffung eines Landesamts für Katastrophenschutz)
- Herr Dr. Timo Hauschild (BSI - Bundesamt für Sicherheit und Informationstechnik)
- Herr Jürgen Rumeney (Siemens AG)
- Herr Frank Schnürer (Fraunhofer-Institut für Chemische Technologie (ICT))
- Frau Annegrit Seyerlein-Klug (TH Brandenburg)
- Herr Fabian Stegmaier (ZVEI e. V.)
- Herr Martin Zeidler (Technisches Hilfswerk)

Nachfolgend werden einige Ziele des White Papers aufgegriffen, deren Ausgestaltung und Bedeutung in den nachfolgenden Abschnitten ausführlicher erklärt werden.

Für KRITIS-Betreibende ist es wichtig zu wissen welchen Regularien und Anforderungen sie unter dem geplanten KRITIS-Dachgesetz unterliegen werden und mit welchen Normen und Standards sie diese erfüllen können. Voraussetzungen sind jedoch eine klare Abgrenzung und eindeutige Schwellenwerte für die KRITIS-Sektoren, damit sich Organisationen einordnen können. Dabei wäre eine Abstufung in **verschiedene „Gefährdungsstufen“** sinnvoll und notwendig, um eine angemessene Dimensionierung der Maßnahmen erleichtern. Im Abschnitt 2 wird dies näher erläutert.

Um die Resilienz einer Organisation verbindlich zu erhöhen, ist ein ganzheitliches und prozess- und ressourcenbasiertes **Business Continuity Management (BCM)** unverzichtbar. Die Einführung eines BCM ermöglicht es Organisationen, für sich passgenaue Maßnahmen zu identifizieren. Wo hingegen Sektor-bezogene, gleichlautende und organisations-unspezifische Maßnahmen dieses Ziel verfehlen würden.

Normen und Standards sind ein wichtiges Werkzeug, um präventive Maßnahmen zur Stärkung der Resilienz von Organisationen zu etablieren. Um präventive Maßnahmen sukzessive aufzudecken, ist eine gesamtheitliche Bedrohungs- und Ausfallbetrachtung in Form einer **Business Impact Analyse** wichtig. Diese sollte auch in regelmäßigen Abständen wiederholt werden, um die Maßnahmen nachzuschärfen und dem Bedarf nach anzupassen. Normen und Standards sind hier ein etabliertes Mittel, um einen einheitlichen und konsensbasierten Stand schnell auf den Markt zu bringen. **Das KRITIS-Dachgesetz sollte**

Normen und Standards eindeutig als Mittel zur Erfüllung der Schutzziele nennen.

Dabei muss die Normungslandschaft im Bereich der KRITIS und des Bevölkerungsschutzes sektorübergreifend gut aufeinander abgestimmt sein. Zudem müssen Normungsbedarfe aufgedeckt und geschlossen werden. Hier sei auch der „Wirtschaftsgrundschutz“ genannt, welcher Organisationen im Bereich der Wirtschaftsspionage und in Ansätzen in der physischen Sicherheit in Unternehmen, bereits einen Rahmen gibt. Betroffene brauchen jedoch konkretere Maßnahmen, besonders im Bereich der physischen Sicherheit in Unternehmen. Normen und Standards sind auch hier ein gutes und effektives Hilfsmittel.

Ein weiterer essenzieller Baustein, um präventive Maßnahmen abzuleiten, ist das Störungsmonitoring, welches auch in dem Eckpunkte-Papier des BMI zum KRITIS-Dachgesetz erwähnt wurde. Damit dieses Monitoring auch zum Tragen kommt, ist der Austausch zwischen den KRITIS-Betreibern mit den zuständigen Behörden unverzichtbar (siehe Abschnitt 5).

2 KRITIS klar identifizieren

Betreiber Kritischer Infrastrukturen, welche bereits der bestehenden Regulierung unterliegen oder einer nunmehr "neuen" unterliegen werden, haben verschiedene Facetten ihrer Organisation bzw. ihrer Organisationsteile zu betrachten. Hierfür ist von entscheidender Bedeutung, dass für Betreiber klar herleitbar ist, ob sich die Organisation (Unternehmen, Behörden usw.) unter der Definition der "Kritischen Infrastruktur" subsumieren lässt. So sollte es für Betreiber auch ersichtlich sein, ob benachbarte Organisationen aufgrund ihrer räumlichen Nähe oder andere Organisationen im Rahmen der engen prozessualen Integration in die Wertschöpfungskette des Betreibers ebenfalls unter KRITIS fallen. Es muss daher auch zentrales Anliegen eines KRITIS-Dachgesetzes sein, eine einheitliche Definition des Begriffs "Kritische Infrastruktur" festzulegen, auch in Bezugnahme auf bereits andere, bestehende Regelungen. Nur hierdurch ist es zukünftig möglich, den aktuell bestehenden Herausforderungen aus den teilweise unterschiedlichen und uneinheitlichen Definitionen von KRITIS entgegentreten zu können und ein einheitliches gesamtgesellschaftliches Verständnis zu entwickeln.

Das Problem des einheitlichen Verständnisses zeigt sich beispielsweise konkret im Bereich der Energieversorgungsunternehmen als möglicher Teil der KRITIS. Diese fallen im Großteil der Fälle erst mit Erreichen der Schwellenwerte aus dem BSI-Gesetz und der BSI-KRITIS-Verordnung unter den Begriff "Kritische Infrastruktur". Wenn sie jedoch ein Energieversorgungsnetz – gleich welcher Größe – betreiben, müssen sie im energierechtlichen Kontext bei der Umsetzung des IT-Sicherheitskatalogs (nach DIN EN ISO/IEC 27001 bzw. DIN EN ISO/IEC 27019) und Vorhaltung sogenannter Systeme zur Angriffserkennung (SzA) bereits die Maßnahmen nach § 11 des EnWG (Energiewirtschaftsgesetz) erfüllen.

Für Betreiber Kritischer Infrastruktur wäre es sehr wichtig, die neuen Anforderungen an die Sicherheit aus dem KRITIS-Dachgesetz im Prozess und Management möglichst weitgehend mit erprobten vorhandenen Strukturen zur IT-Sicherheit zu harmonisieren.

Daher sind eine **einheitliche Definition und Anwendung des Begriffs "Kritische Infrastruktur"** erforderlich und maßgeblich für die Erreichung der Ziele eines KRITIS-Dachgesetzes. Aufbauend auf dem einheitlichen Verständnis für Kritische Infrastruktur unterstützen Normen und Standards Betreiber bei der Bewertung und Ermittlung von präventiven Maßnahmen zur Steigerung der Resilienz.

Wie kann eine Definition "Kritische Infrastruktur" aussehen? Getreu dem Leitspruch "Das Wagenrad nicht neu erfinden" wäre denkbar, die bereits etablierten Schwellenwerte aus der **BSI-KRITIS-Verordnung** im Grundsatz zu übernehmen und an einigen Stellen auf ihre Praxistauglichkeit zu **prüfen und ggf. zu konkretisieren.** Dabei sollten auch die Auswirkungen in Betracht gezogen werden,

sollten diese Betreiber ausfallen – z. B. gibt es kleinere Versorgerunternehmen, die unter der jetzigen Definition nicht unter KRITIS fallen, aber bei Ausfall eine erhebliche Auswirkung auf die Bevölkerung der Region hätten. Somit werden einerseits diejenigen Betreiber, die bereits der Regulierung unterfallen, nicht einer neuerlichen Prüfung ihres Status' unterworfen. Andererseits erhalten Betreiber, die sich bislang noch nicht sicher waren, ob sie eine "Kritische Infrastruktur" im Sinne des Gesetzes bzw. der Verordnung darstellen, eine konkrete Prüfmöglichkeit. Letztgenannte Prüfmöglichkeit könnte darüber hinaus auch über eine Art **Eigenerklärung oder Registrierungsvoranfrage** (Entscheidungshilfe anhand von übersandten Betreiberkennzahlen, ob man unter KRITIS fällt) erfolgen.

Bei der Prüfung und ggf. Anpassung der Schwellenwerte und der Erarbeitung der daraus resultierenden gefahrenbezogenen Anforderungen und Maßnahmen, sollte es über das KRITIS-Dachgesetz ermöglicht werden, eine **dem entsprechenden Gefahrenniveau angemessene Abstufung in verschiedene "Gefährdungsstufen" durchzuführen** (z. B. in Form von Verordnungen oder über von Normen und Richtlinien gestützte Dokumente). Dies würde, bei einer entsprechenden angemessenen Ausgestaltung, die Abstufung und angemessene Dimensionierung von Maßnahmen erleichtern und somit aus der unternehmerischen Betrachtung der Anforderungen die Akzeptanz und Umsetzungsfähigkeit nachhaltig positiv beeinflussen, mithin also die Gesamtresilienz des Systems und seiner Komponenten stärken. Über Normen und Standards können derartige Prüfabläufe (z. B. auch für eine Eigenerklärung) festgelegt werden und sie bilden dadurch eine sinnvolle Unterstützung eines entsprechenden Gesetzestextes. Als Beispiel sei auch der CyberRisikoCheck nach DIN SPEC 27076, *IT-Sicherheitsberatung für Klein- und Kleinstunternehmen* genannt. Das Dokument wurde durch das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) gefördert und gibt KMUs eine Hilfestellung zur Bewertung der IT- und Informationssicherheit im Unternehmen. Solche Standardisierungsdokumente wären auch in Hinblick der physischen Sicherheit in Organisationen wünschenswert.

Sobald für einen Betreiber einer Kritischen Infrastruktur klar ist, ob die Organisation in Gänze oder zu Teilen der Definition der "Kritischen Infrastruktur" unterliegt, besteht für Unternehmen und Organisationen die Verpflichtung, alle notwendigen und angemessenen Maßnahmen zum Schutze dieser zu ergreifen. Genau dafür ist es jedoch unabdingbar, dass der jeweilige Betreiber durch ein KRITIS-Dachgesetz auch im Rahmen eindeutiger Anforderungen und Maßgaben das nötige Handwerkszeug und einen konkreten Anforderungskatalog dazu erhält, um daraus Anforderungen für die Organisation ableiten und Maßnahmen implementieren zu können. Mittel der Wahl im Rahmen des KRITIS-Dachgesetzes kann und sollte die **verbindliche Vorgabe zur Einhaltung von existierenden Normen und Standards** sein, wie eindeutig in der CER-Richtlinie formuliert. Als Beispiel sei hier die Normenreihe DIN EN 17483, *Private Sicherheitsdienstleistungen — Schutz kritischer Infrastrukturen* genannt, welche sich mit dem (größtenteils in Deutschland so "gelebten") Schutz von Kritischer Infrastruktur durch private Sicherheitsdienstleister beschäftigt, oder DIN EN ISO/IEC 27001, *Informationssicherheit, Cybersicherheit und Datenschutz — Informationssicherheitsmanagementsysteme — Anforderungen* und DIN EN ISO/IEC 27002, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmaßnahmen* zum Schutz von IT-Systemen, unter anderem auch die physische Sicherheit dieser. Unabhängig davon müssen die Bedarfe an weiteren Normen und Standards mit Bezug zur Kritischen Infrastruktur identifiziert und ggf. initiiert werden. Dabei bietet die Normung bereits eine gute Struktur, um diese Normungs- und Standardisierungsprojekte zu erarbeiten. Als Beispiel sei das internationale Normungsgremium ISO/TC 292 "Sicherheit und Resilienz" genannt, das bereits einige Normen zum Schutz der Bevölkerung erarbeitet hat.

Kritische Infrastrukturen sind – allein schon aus der Begrifflichkeit – im besonderen Interesse der Allgemeinheit, da diese das Zusammenleben in der Gesellschaft im Alltag und darüber hinaus sichern. Daher ist es auch erforderlich, dass der Staat einen umfassenden Überblick hat, welche

Organisationen Betreiber Kritischer Infrastrukturen sind. Das KRITIS-Dachgesetz muss daher über den Tellerrand einer Grundsatzregulierung hinausschauen und neben einer oberen, zuständigen Behörde auch die unteren **Katastrophenschutzbehörden** in den Fokus nehmen. Diese sind z. B. in einem tatsächlichen Krisenfall diejenigen, welche vor Ort entsprechende Entscheidungen über konkrete Maßnahmen zur Gefahrenbekämpfung treffen müssen. Dafür müssen sie einen Überblick über "ihre" Kritischen Infrastrukturen haben, damit bspw. bei einem Brand in zwei Umspannwerken die örtliche Feuerwehr informiert ist, welches der beiden unter KRITIS fällt. Nur so können Prioritäten gesetzt werden, um größtmöglichen Schaden zu begrenzen. Normen und Standards geben hier das Handwerkzeug bei der Bewertung und dem Risikomanagement, z. B. DIN SPEC 91390, *Integriertes Risikomanagement für den Schutz der Bevölkerung*.

Ein Ziel eines KRITIS-Dachgesetzes muss es daher sein, **ein zentrales und bundeseinheitliches KRITIS-Register** einzuführen, welches im Krisenfall durch die relevanten kommunalen Landes- und Bundesbehörden mit Bezug auf ihre Zuständigkeit auf sicherem Wege und unter Wahrung der besonderen Vertraulichkeit der Daten eingesehen werden kann. In einem nicht-Krisenfall sollten dennoch unsensible Grunddaten einsehbar sein, um so auf den Krisenfall bestmöglich vorbereitet zu sein. Normen und Standards unterstützen bei der Einhaltung und Wahrung sensibler Daten durch Anwendung bestehender IT-Sicherheitsstandards.

3 Bedrohungslage und Risiken besser erkennen

Essenziell für die Betreiber Kritischer Infrastrukturen ist die Kenntnis über mögliche Bedrohungslagen und daraus für den jeweiligen Betrieb ggf. resultierende zusätzliche Risiken. Bei der Betrachtung von Risiken erscheint es nicht nur notwendig auf die kritische Dienstleistung zu blicken, sondern vielmehr auf die in der Prozess- und Lenkungskette des Betriebs nachgelagerten Organisationen und Bevölkerungsgruppen zu schauen, die von möglichen Ausfällen der jeweiligen Kritischen Infrastruktur betroffen sein könnten.

Vor diesem Hintergrund muss es im KRITIS-Dachgesetz eine **verbindliche Vorgabe für die regelmäßige Durchführung von Business Impact Analysen** geben. In deren Rahmen wird eine gesamtheitliche und prozessorientierte Betrachtung der Kritikalität der im Betrieb bestehenden Prozesse unter Einbezug der für die Umsetzung der Prozesse benötigten Ressourcen sowie der Zeitachse durchgeführt. Hieraus können präventive Maßnahmen abgeleitet werden, die auf Grundlage von Normen und Standards erarbeitet werden können, z. B. DIN EN ISO 22301, *Sicherheit und Resilienz — Business Continuity Management System — Anforderungen*. Bestehende Normen und Standards sollten die Grundlage für das Business Continuity Management sowie die Durchführung von Business Impact Analysen und Risikobewertungen für Kritische Infrastruktur darstellen. Diese Normen und Standards können auch im Rahmen von Zertifizierungsforderungen eine Grundlage bilden.

Exemplarisch kann der Ausfall eines Stromverteilnetzes in einer Gemeinde genannt werden. Dieser Ausfall hat nicht nur Auswirkungen auf den Betrieb des Energieversorgungsunternehmens und des Netzes selbst, sondern auch auf die jeweiligen Gemeindeteile mit den dort ansässigen Teilen der Kritischen Infrastruktur. Ohne laufendende Stromversorgung können diese nicht produktiv tätig sein, woraus ggf. weitere Gefährdungen im Zuge des Wegfalls der Betriebsfähigkeit und Sicherheit von Anlagen(teilen) entstehen können. So kann bereits der kurze Ausfall einer Kritischen Infrastruktur – je nach Art und Gefährdung sowie der Gestaltung der Umgebungsbedingungen – zu erheblichen und nachhaltigen Schäden führen, die gar nicht oder nur mit großem Aufwand beseitigt werden können. Resilienz hiergegen entsteht durch ein **gelebtes und wirksames Business Continuity Management**, was so vielschichtig und individuell wie die KRITIS-Betreiber ausfällt. Alle Aspekte, angefangen bei der Business Impact Analyse über die Wirksamkeitsprüfung von Schutzmaßnahmen bis hin zur

regelmäßigen Prozessbetrachtung des Gesamtsystems bedürfen einer **regelmäßigen Evaluierung**. Die Erfahrung zeigt, dass die neutrale Bewertung durch eine unabhängige, dritte Stelle hierbei wertvolle Impulse liefert und Betriebsblindheit vermeidet. Gleichzeitig wird damit sichergestellt, dass die prozessual-zielorientierten Vorgaben im konkreten Anwendungsfall wirksam umgesetzt bzw. erreicht werden.

Die Stärkung der Resilienz von KRITIS-Betreibern kann nur gelingen, wenn durch entsprechende Regelungen eine ganzheitliche Betrachtung von Prävention, Detektion und Reaktion verankert ist. Darauf aufbauend kann Normung und Standardisierung KRITIS-Betreiber darin unterstützen, diese einzelnen Aspekte zu betrachten, um ihre Resilienz schlussendlich effizient und nachhaltig zu steigern.

Die zu treffenden Maßnahmen sind dabei so individuell wie die Betreiber selbst. Maßnahmen können personeller, organisatorischer oder technischer Natur sein und werden regelmäßig kombiniert getroffen. Der technische Fortschritt bewirkt hierbei einen kontinuierlichen Wandel auf Seiten der Überwachungs- und Gefahrenabwehrtechnik ebenso wie geänderte Verfahren und Fähigkeiten möglicher Gefährder. **Die gesetzlichen Vorgaben müssen abstrakt sein.** Eine abstrakte Forderung wäre z. B. der aktuelle Stand der Technik, der durch Normen und Standards abgebildet und kontinuierlich weiterentwickelt wird. Normen und Standards können auch identifizierte Lücken schneller schließen, als es durch eine konkrete Gesetzgebung möglich ist. Abweichungen dürfen nur begründet im Rahmen z. B. eines Business Continuity Managements erfolgen.

Erforderliche Maßnahmen zum Schutz von Kritischer Infrastruktur lassen sich zudem in "präventiv" und "reaktiv" einteilen. Zur Prävention ist die Vorhaltung intern beauftragter Personen, die sich dem Thema "KRITIS" ganzheitlich annehmen und hauptverantwortlich bearbeiten, wesentlich und muss zwingende Vorgabe im KRITIS-Dachgesetz sein. Diese offiziell ernannten KRITIS-Beauftragten innerhalb der Organisationen müssen innerhalb der Organisation weisungsbefugt sein und feste Ansprechpersonen bei den relevanten Behörden haben. Es muss ein **regelmäßiger Erfahrungsaustausch** aller am Prozess beteiligten Akteure gewährleistet werden. Nur durch ein gemeinsames, abgestimmtes Agieren der Akteure Kritischer Infrastrukturen wird es möglich sein, auftretenden Sicherheitsvorfällen vorzeitig zu begegnen und sich im konkreten Falle gegenseitig zu unterstützen. Bei der Zusammenarbeit mit Behörden ist insbesondere auch im KRITIS-Dachgesetz ein Prüfmechanismus zu etablieren, im Rahmen dessen Risikobewertungen auch durch eine externe Stelle zumindest auf Schlüssigkeit geprüft werden sollten.

Zur schnellen Reaktion ist eine schnelle Meldung bei sicherheitsrelevanten Vorfällen (unabhängig, ob IT oder physisch) wesentlich und muss nach einem abgestuften Raster in ein durch die **zentrale Meldestelle auf Bundesebene** geführtes Lagebild einfließen. Dieses Lagebild dient einer laufenden, übergeordneten Lagebewertung und hilft allen involvierten Parteien und Behörden, frühzeitig übergeordnete Gefahren oder auch prozessuale Folgegefahren zu erkennen und diesen zu begegnen – Ziel muss es sein, “vor die Lage zu kommen”. Teilinformationen können auch aufbereitet und weiteren eventuell gefährdeten KRITIS-Betreibern zur Verfügung gestellt werden, um besser Betreiber-spezifische präventive Maßnahmen ableiten zu können.

Um einen zuverlässigen Austausch der Daten zu gewährleisten, kann auf bestehende Normen und Standards zurückgegriffen werden bzw. können spezielle Anforderungen für Kritische Infrastruktur entwickelt werden.

4 Schutzniveau verbindlich erhöhen

Mit der Schaffung einer umfassenden Neuregelung des Rechtsrahmens zum Schutz Kritischer Infrastrukturen muss **die Anwendung, Erstellung und Adaptierung von Normen, Standards und verbindlichen Vorgaben einhergehen**. Dies kann einerseits durch die Implementierung bereits bestehender Normen zur Sicherheit von Anwendungen und

Organisationsstrukturen sein, kann gleichzeitig aber auch die Schaffung eines gesetzlichen Korridors zur Vorhaltung bestimmter Maßnahmen beinhalten. Dabei ist jedoch zu beachten, dass die Regelungen in einem KRITIS-Dachgesetz nicht zu konkret ausfallen. Dies hätte sonst zur Folge, dass alle Betreiber kritischer Infrastrukturen Sektor-bezogen gleichlautende und organisationsunspezifische Maßnahmen einführen müssten und dadurch neue Risiken allein aufgrund der Gleichartigkeit der Maßnahmen über Betreiberstrukturen hinweg entstehen.

Zur verbindlichen Erhöhung eines Schutzniveaus wird es unabdingbar sein, Betreiber über das KRITIS-Dachgesetz dazu zu verpflichten, ein **ganzheitliches und vor allem prozess- und ressourcenbasiertes Business Continuity Management (BCM)**, beispielsweise nach DIN EN ISO 22301, *Sicherheit und Resilienz — Business Continuity Management System,* zu implementieren. Dieses ergänzt insbesondere das zuvor erwähnte verbindliche Risikomanagement mit dem Ziel, einen ganzheitlichen und präventiven Ansatz zu verfolgen.

Aktuell liegt der allgemeine Fokus bei der Schaffung von "Sicherheit" in Kritischen Infrastrukturen meistens in der Einzelbetrachtung von “Prozess-Silos” wie z. B. IT-Systemen (z. B. nach DIN EN ISO/IEC 27001). Diese Aspekte werden in Zukunft sicherlich noch mehr Platz einnehmen, dürfen jedoch nicht verdrängen, dass ganzheitliche Prävention nur in einer **holistischen Betrachtung von Sicherheitsfragen** inklusive der heute häufig vernachlässigten physischen Sicherheit der Kritischen Infrastruktur zu erreichen ist. Auch wenn der teilweise in Deutschland noch unbekannte **"Wirtschaftsgrundschutz"** den Fokus zunächst auf den Schutz vor Wirtschafts- und Wissenschaftsspionage gelegt hatte, bietet dieser bereits erste Ansätze und Grundlagen zur physischen Sicherheit in Unternehmen. Diese sind jedoch in die grundsätzliche KRITIS-Regulierung bisher noch nicht aufgenommen worden. Dies wird ebenfalls eine Hauptaufgabe eines zukünftigen KRITIS-Dachgesetzes sein müssen. Die Untermauerung des "Wirtschaftsgrundschutz" und damit auch der physische Schutz von Unternehmen durch entsprechende Normen und Standards ist ein wichtiges Handlungsfeld. Hier gibt es bereits Bestrebungen, ein entsprechendes Standardisierungsprojekt zu initiieren, um die Lücke zu schließen.

5 Störungen des Gesamtsystems erkennen und beheben

Neben der Vermeidung von Störungen durch Erreichen eines angemessenen Schutzniveaus zeigen ein gut funktionierendes Risikomanagement und ein damit verbundenes bestehendes prozess- und ressourcenbasiertes Business Continuity Management dann ihre Wirkung, wenn es zu einer konkreten Störung des Gesamtsystems kommt, welche behoben werden muss. Genau hieran muss das KRITIS-Dachgesetz auch anknüpfen.

Um Störungen rechtzeitig – möglichst präventiv – und effizient zu erkennen, ist in der Regel ein **Monitoring** mit entsprechenden Alarmierungen erforderlich, die in einem Lagezentrum und ggf. einen Security Operation Center zusammengeführt und bewertet werden müssen. Wichtig ist in diesem Zusammenhang auch die **Ermächtigung von handelnden ausgebildeten Personen**, bei einem Vorfall schnell aktiv werden zu können, bzw. es muss sehr schnell Entscheidungsfähigkeit herbeiführbar sein (bspw. DIN EN ISO 22361, *Sicherheit und Resilienz — Krisenmanagement — Leitlinien*, DIN ISO 22320, *Sicherheit und Resilienz — Gefahrenabwehr — Leitfaden für die Organisation der Gefahrenabwehr bei Schadensereignissen*).

Das **Zusammenwirken** des betrieblichen Krisenmanagements und dem der Genehmigungs-, Aufsichts- und der Gefahrenabwehrbehörden muss sichergestellt sein. Gleichzeitig zeigt die Praxis, dass sich Unternehmen und Organisationen auch einen **engen Austausch mit den Behörden**, die für Kritische Infrastrukturen bereits jetzt zuständig sind, im Rahmen des Risiko- und Krisenmanagements wünschen, um Zuständigkeiten und Verantwortlichkeiten abzustimmen. Dieser Austausch muss aus diesseitiger Sicht zur Pflicht der relevanten Behörden und Betreiber

Kritischer Infrastrukturen werden. Nur so können – wenn es ganz konkret um bevorstehende Störungen oder Ausfälle geht – noch rechtzeitig relevante Maßnahmen ergriffen werden, um kurzfristig entstehenden Risiken entgegenwirken zu können (bspw. DIN SPEC 91390, *Integriertes Risiko-management für den Schutz der Bevölkerung*).

Dieser Austausch ist auch erforderlich damit die gewonnen Erkenntnisse in den Normungs- und Standardisierungsprozess einfließen können. Nur so können die Standardisierungs-dokumente die geeigneten präventiven Maßnahmen aufzeigen und allen interessierten Stellen zugänglich gemacht werden.

Während mit einem KRITIS-Dachgesetz lediglich "Leitplanken" in der Regulierung Kritischer Infrastrukturen gesetzt werden können, bedarf es weitergehender Detaillierungen zum Beispiel durch Normen oder weitergehende gesetzliche Vorgaben. Die beteiligten Akteure bekräftigen die **Empfehlung der Europäischen Union in der CER-Richtlinie (Art. 16)**, dass Mitgliedsstaaten die **Anwendung und Weiterentwicklung von Normen und Standards fördern** sollten, um höhere Schutzniveaus sicherzustellen.

6 Einen institutionellen Rahmen schaffen

Kernstück eines KRITIS-Dachgesetzes muss die Schaffung eines institutionellen Rahmens und entsprechender Verantwortlichkeiten sein. An dies angeknüpft wird es erforderlich werden, eine **zentrale KRITIS-Meldestelle** für Betreiber Kritischer Infrastrukturen zu schaffen, die möglichst dauerhaft erreichbar ist. Eine zerstückelte Zuständigkeit bei Fragen zu "KRITIS" muss der Vergangenheit angehören, da diese im tatsächlichen Krisenfall eher behindert als förderlich ist.

Durch das KRITIS-Dachgesetz muss diese zentrale KRITIS-Meldestelle in die Lage versetzt werden, standardisierte, einheitliche und idealerweise **digitalisierte Meldeprozesse**, wie auch den standardisierten prozessualen Umgang mit diesen Meldungen (inklusive der Verteilung und Nachverfolgung) zu etablieren sowie die einheitliche Kommunikation zu allen relevanten Playern sicherzustellen. Dazu muss die Möglichkeit geschaffen werden, **umfassend relevante Informationen** zu den Meldungen mit **anderen Akteuren auszutauschen**. Zudem müssen konkret zu **nutzende Kommunikationsmittel und -wege vorgegeben und beübt** werden können.

Bei der Formulierung eines KRITIS-Dachgesetzes sollten eventuell bestehende Regelungen auf Länderebene oder auf Kommunalebene berücksichtigt werden.

7 Ausblick

Die oben genannten Punkte und Beispiele machen deutlich, dass das KRITIS-Dachgesetz und die Normung und Standardisierung Hand in Hand gehen müssen, um die nationalen KRITIS-Sektoren auf stabile Füße stellen zu können. Dabei gibt das KRITIS-Dachgesetz die Richtung vor. Im Bereich der Sicherheit und des Bevölkerungsschutzes gibt es bereits einige wichtige Normen und Standards, wie bereits oben erwähnt. Im Zusammenhang mit der Corona-Pandemie wurde bereits eine KRITIS-Normen-Matrix erstellt, die sektorenbezogen einen Überblick über relevante Management-Normen gibt. Diese Übersicht muss nun auf alle Gefahrenlagen ausgeweitet und ggf. um technische Normen ausgeweitet werden.

Dabei muss identifiziert werden, wo sich noch Lücken in der Normung und Standardisierung befinden, die schnellstmöglich geschlossen werden sollten. DIN bietet durch seine vielen Normenausschüsse die Expertise, den transparenten Bearbeitungsprozess und das Einbinden der wichtigen interessierten Kreise die ideale Plattform, diese Normungs- und Standardisierungsprojekte umzusetzen.

Geschäftsstelle
DIN e. V. · Am DIN-Platz · Burggrafenstraße 6 · 10787 Berlin
Telefon: 030 2601-0 · Telefax: 030 2601-1231
E-Mail: info@din.de · **www.din.de**