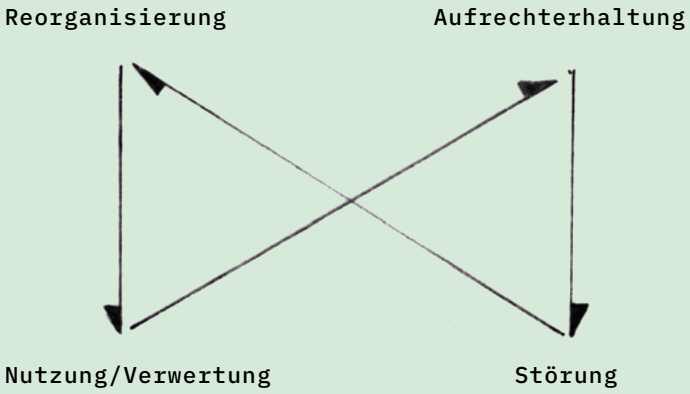


Zusammenspiel der Gesellschaft für resilientere Infrastrukturen

Frank Fischer
Institut für Business Continuity & Resilience Management e.V. (IBCRM)

Kurzvita

Frank Fischer

Frank Fischer ist Geschäftsführer der FCMS GmbH, die auf Beratung in den Bereichen BCM, ITSCM, Krisenmanagement und Resilience Management spezialisiert ist. Als Diplom-Kaufmann war er ab 2007 für eine Big Four Wirtschaftsprüfung und zwei spezialisierte Beratungsunternehmen tätig, bevor er sich 2013 selbständig machte und 2019 die FCMS GmbH gründete. Neben zahlreichen Projekten bei Banken und Versicherungen, Behörden, öffentlichen Verwaltungen und Unternehmen der kritischen Infrastruktur - sowohl national als auch international - hat er sein fundiertes Wissen bei Zertifizierungen unter Beweis gestellt. Seit 2009 ist er Mitglied im Business Continuity Institute. 2020 wurde er in den Vorstand des Instituts für Business Continuity & Resilience Management e.V. gewählt, dessen Vorsitz er seit 2022 innehat. In seinem Beitrag teilt er seine Sichtweisen auf die An- und Herausforderungen für resilientere Infrastrukturen und Resilienzmanagement. Alle URLs wurden zwischen dem 16.10.-23.10.2023 (erneut) abgerufen.

1. Einleitung

Mit dem Start der COVID-19-Pandemie im Jahr 2020, der Blockade des Suez-Kanals durch das Containerschiff Ever Given im März 2021, dem Jahrhundert-Hochwasser im Ahrtal im Juli 2021, dem russischen Angriffskrieg in der Ukraine seit Februar 2022 und seinen Auswirkungen auf die Verfügbarkeit von Gas und Erdöl sowie den Sabotageakten bei der Bahn im Oktober 2022 wächst das Bewusstsein in der Gesellschaft wieder, wie fragil die als selbstverständlich wahrgenommenen, alltäglich genutzten Systeme und deren Infrastrukturen sind. Der Bedarf nach ihrem Schutz, ihrer Sicherheit und Resilienz ist wie nie zuvor gestiegen.

Nicht erst seit den oben genannten Krisenfällen entwickeln sich Fachthemen, die jeweils auf ihren Bereich fokussierte Lösungsansätze beinhalten. Bereits um die Jahrtausendwende wurde das Business Continuity Management (BCM)

aus dem angelsächsischen Raum in das Bewusstsein der hiesigen Unternehmen zurückgeholt – und dort nach den Anschlägen des 11.September 2001 zumindest für eine Weile gehalten. Zur weiteren historischen Betrachtung sei an dieser Stelle auf das Werk von Rolf von Rössing „Betriebliches Kontinuitätsmanagement“ [1] verwiesen.

Leider verschwinden selbst die größten Katastrophen und ihre – zuvor - unvorstellbaren Folgen immer wieder aus dem kollektiven Gedächtnis. Statt die Erkenntnisse aus der Vielzahl an Ereignissen zu nutzen und in präventiven Maßnahmen zur Absicherung einzusetzen, ist man immer wieder erst im Nachhinein über die enormen Auswirkungen und Kosten der entstandenen Schäden erstaunt. Sollten diese Ereignisse nicht Anlass genug für eine Art „intrinsische Motivation“ bei allen Teilnehmern der Gesellschaft sein?

Erst die gesetzliche Regulierung und deren konsequente Prüfung durch die verantwortlichen Aufsichtsbehörden schafft es, zumindest bei Unternehmen den nötigen Druck zu entfalten und zu einer tieferen und nachhaltigeren Auseinandersetzung mit den Governance, Risk und Compliance-Themen (GRC) zu bewegen. Ohne die MaRisk, später die BAIT etc. und die teilweise noch immer „gefürchteten“ §44er-Prüfungen (KWG) der BaFin/Bundesbank wäre vermutlich auch der deutsche Finanzsektor noch nicht so resilient aufgestellt, wie er es jetzt schon überwiegend ist.[2]

Doch wer prüft eigentlich die Prozesse der Notfallvorsorge in den staatlichen Strukturen, auf Basis welcher Rechtsvorschriften? Das Spannungsfeld der Verantwortlichkeiten kann hier vom Bund und den Ministerien und seinen Behörden, über die 16 Bundesländer bis zu den 294 Landkreisen aufgezogen werden.

Und wie kann man das Bewusstsein für eine Notfallvorsorge bei Bürgerinnen und Bürgern schaffen, welche zahlenmäßig die größte Gruppe stellen und insgesamt die am meisten Betroffenen sein dürften?

1 Rolf von Rössing (2005): Betriebliches Kontinuitätsmanagement

2 Die bedeutenderen Institute werden seit 2014 direkt von der EZB beaufsichtigt.

2. Rollen und Verantwortlichkeiten bzw.: Welche Teilnehmer der Gesellschaft müssen eigentlich im Austausch miteinander stehen, um resilientere Strukturen zu bilden?

Bevor später eine vielleicht einfach anmutende Antwort auf diese Frage gegeben wird, sollen die Teilnehmer kurz klassifiziert werden.

Die **Behörden** repräsentieren den Staat, ihnen kommen u. a. hoheitliche Verwaltungsakte zu und sie tragen eine gesamtgesellschaftliche Verantwortung. Einige von ihnen sind bereits zur Erstellung einer nationalen Resilienz-Strategie, zur Übertragung von EU-Vorgaben in nationale Gesetze sowie zur Überwachung und Kontrolle der Einhaltung dieser Gesetze durch die regulierten Unternehmen und Organisationen verpflichtet.

Der originäre Zweck der **Hilfsorganisationen** (THW, DRK, Malteser, Johanniter und viele weitere) ist bereits die Hilfe und Unterstützung in Not- und Krisensituationen im Alltag. Solange diese Situationen regional begrenzt sind, kann dieser Aufgabe – Dank einer Vielzahl von ehrenamtlichen Helfenden – im Wesentlichen im Rahmen des Regelbetriebes nachgegangen werden. Doch wie sieht es bei bundeslandübergreifenden oder sogar bundesweiten Katastrophenfällen aus? Der noch zum Jahresende 2022 befürchtete Blackout scheint vorerst abgewendet; des BCMers Motto ist jedoch „be prepared"! Denn selbst rollierende Abschaltungen der Stromversorgung („Brown outs") gilt es zu vermeiden, da die Schäden an technischen Geräten nicht abschätzbar und ihr Wiederanlauf nicht sicher sind.

Die **öffentlichen und privaten Unternehmen** stellen die Infrastrukturen zur Verfügung bzw. gewährleisten/ermöglichen als Motor der deutschen Wirtschaft deren Nutzung. Sie werden zur Einhaltung der Vielzahl an Regelungen verpflichtet.

Die **Bürgerinnen und Bürger** sind auf Grund Ihrer Anzahl der größte Stakeholder in dieser Auseinandersetzung. Gegenwärtig jedoch – im Vergleich zu Unternehmen – am wenigsten zu (Eigen-) Verantwortung verpflichtet. Auch hier ist eine Zeitenwende erforderlich. Von mündigen und wirtschaftlich fähigen Bürgerinnen und Bürgern sollte erwartet werden können, dass sie ein Mindestmaß an Eigenvorsorge betreiben und sich auf Notfallsituationen vorbereiten, statt nach Eintreten von Ereignissen „zu hamstern". Zudem nehmen sie eine Doppelrolle im gesellschaftlichen System ein, da sie auch Mitarbeitende oder Beamte sind.

Die **Bundeswehr** nimmt eine Sonderrolle ein, da ihr Einsatz im Inland nur unter besonderen Voraussetzungen stattfinden darf. Hier sollten weitere Szenarien

und ggf. Schwellwerte definiert werden, welche in Krisen- und Katastrophensituationen eine schnellstmögliche humanitäre Unterstützung der Hilfswerke und der Bürgerinnen und Bürger gewährleisten.

3. Regulierung - kontinuierlich steigender Umfang mit Vor- und Nachteilen

In den beiden folgenden Kapiteln soll ein grober Überblick über die wichtigsten Gesetze und Vorschriften gegeben werden.

3.1. Regulierung bei Behörden und Organisationen mit Sicherheitsaufgaben (BOS)

Das Verwaltungsverfahrensgesetz (VwVfG) regelt das Verwaltungsverfahren und enthält Bestimmungen zur Vorkehrungs- und Gefahrenabwehrplanung, die bei der Vorbereitung auf Notfälle und Krisensituationen einzuhalten sind.

Das Gesetz über den Zivilschutz und die Katastrophenhilfe (ZSKG) regelt die Zusammenarbeit des Bundes und der Länder sowie der Kommunen im Zivilschutz- und Katastrophenfall und definiert die Aufgaben und Befugnisse des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe.

Das Gesetz über den Brand- und Katastrophenschutz (BrKG) legt die Aufgaben und Befugnisse der Feuerwehren und des Katastrophenschutzes fest. Es enthält Bestimmungen zur Vorbereitung auf und die Bewältigung von Bränden, Katastrophen und anderen Notfällen. An dieser Stelle sei unbedingt auf den Leitfaden Krisenmanagement für Behörden und Unternehmen des VFDB[3] und die Feuerwehrdienstvorschrift 100 hingewiesen.

Der Katastrophenschutz „ist Ländersache“. Er wird von jedem Bundesland in einem eigenen Gesetz geregelt, welches die Organisation und Verantwortlichkeiten in Bezug auf die Vorbereitung und Bewältigung von Katastrophen und Notfällen regelt.

Auch die genauen Anforderungen an das Notfallmanagement für Behörden können in den Landesgesetzen und -verordnungen variieren. Jedes Bundesland kann spezifische Regelungen erlassen, die auf die örtlichen Gegebenheiten zugeschnitten sind.

Wie vor diesem Hintergrund eine Überprüfung der Notfall- und Krisenmanagementfähigkeiten in allen Bereichen des öffentlichen Sektors - ähnlich den Überprüfungen bei den Unternehmen - stattfinden kann und welche Behörde dies umsetzen soll, scheint fraglich. Damit Behörden und weitere Organisationen mit Sicherheitsaufgaben ihren Auftrag gerade auch in Krisensituationen

3 https://www.vfdb.de/media/doc/technischeberichte/TB_09_Leitfaden_Krisenmanagement.pdf

erfüllen können – und damit einhergehend resiliente staatliche Infrastrukturen gewährleisten - liegt es auf der Hand, dass sie nicht von weiteren Regulierungen im Bereich kritische Infrastrukturen - namentlich, dem KRITIS-Dachgesetz[4] - ausgenommen werden dürfen.

Im Juli 2022 wurde von der Bundesregierung die Nationale Resilienzstrategie[5] beschlossen. Sie ist das Instrument, mit dem auf Bundesebene die Widerstandsfähigkeit der Gesellschaft und der staatlichen Institutionen gegenüber verschiedenen Bedrohungen gestärkt werden soll. Während sie Maßnahmen für den Bund beinhaltet, adressiert sie alle Mitglieder der Gesellschaft zur Teilnahme.[6]

3.2. Wesentliche Regulierung von Unternehmen

Seit der ersten Veröffentlichung der MaRisk im Jahre 2005 wurde dem Bankensektor ein Rahmen zur Ausgestaltung seines Risikomanagements zur Verfügung gestellt. Mit der im Juni 2023 veröffentlichten 7. Novelle[7] und den seit 2017 spezifizierten Bankaufsichtlichen Anforderungen an die IT (BAIT)[8] – wenig später von den VAIT[9] für Versicherungen gefolgt – liegen transparente Anforderungen vor, welche mit den 44er Sonderprüfungen durch BaFin bzw. Bundesbank für eine gewisse Resilienz im Finanzwesen gesorgt haben.
Mit in Kraftsetzung des Digital Operational Resilience Act (DORA)[10] im Januar 2023 wurden nun auf EU-Ebene Anforderungen geschaffen, welche die Sicherheit von Netzwerken und Informationssystemen zur Unterstützung von Geschäftsprozessen im Finanzbereich fordern und ebenso logische als auch physische Risikoreduzierungen adressieren. Über die enthaltenen Vorschriften zu Auslagerungen und dem Bezug von Dienstleistungen wird DORA auch außerhalb der Finanzindustrie relevant und Resilienz steigern.

Für die Betreiber Kritischer Infrastrukturen liegen erst seit der Verabschiedung des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

4 https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html
5 Original: Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen
6 An dieser Stelle muss dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zu diesem Kompetenz-gewinn gratuliert werden! Resilienzstrategie und KRITIS-Dach-Gesetz unterstützen die Neuausrichtung.
7 https://bit.ly/3Q0TZlB
8 Letzte Überarbeitung August 2021: https://bit.ly/3FotrpG
9 Letzte Überarbeitung März 2022: https://bit.ly/3FnKYyb
10 https://eur-lex.europa.eu/eli/reg/2022/2554/oj

(IT-Sicherheitsgesetz; zur Stärkung des BSI-Gesetzes, welches seit 1991 in Kraft ist) im Jahr 2015 branchenübergreifende gesetzliche Regelungen vor. Sie zielen jedoch primär auf den Schutz der Sicherheit und Verfügbarkeit der kritischen IT-Systeme bzw. Anlagen ab. Waren denn Aufbau-, Ablauforganisation und Risikomanagement der IT oder der Geschäftsbereiche unserer KRITIS-Unternehmen nicht „schützenswert" oder deren Notfallvorsorge relevant für eine Regulierung? Oder haben die branchenspezifischen Rechtsverordnungen und Vorschriften die Anforderungen an Business Continuity Management hinreichend geregelt?

Das Energiewirtschaftsgesetz (EnWG) und die dazugehörige Verordnung über die Meldung von Störungen und Angriffen auf die Verfügbarkeit und Integrität von Energieversorgungssystemen (EnergieStörV) erfordern Störungs- und Notfallmanagement im Energiebereich.

In der Telekommunikationsbranche gelten besondere Anforderungen an das Notfallmanagement gemäß dem Telekommunikationsgesetz (TKG). Diese Vorschriften regeln unter anderem die Pflicht zur Meldung von sicherheitsrelevanten Vorfällen an die Bundesnetzagentur.

Im Verkehrssektor, insbesondere im Bereich des Schienenverkehrs und der Luftfahrt, gibt es spezifische Notfallmanagement-Anforderungen gemäß dem Allgemeinen Eisenbahngesetz (AEG) und dem Luftverkehrsgesetz (LuftVG).

Im Gesundheitswesen unterliegen Krankenhäuser und Gesundheitseinrichtungen Vorschriften zum Notfallmanagement. Diese Vorschriften können je nach Bundesland variieren und werden von den jeweiligen Landesgesundheitsbehörden erlassen.

Mit Blick auf die Erkenntnisse aus der Einleitung verwundert es daher nicht, dass die KRITIS-relevanten Unternehmen mit weiteren EU-Richtlinien zur Steigerung ihrer Resilienz konfrontiert werden. Zeitgleich mit DORA wurde im Dezember 2022 die Richtlinie über die Resilienz kritischer Einrichtungen (Directive on the Resilience of Critical Entities - RCE[11]) veröffentlicht, welche nun auch die Dienstleistungen und die Risikobewertung in den Fokus nimmt. Außerdem wurden die Neuerungen in der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2), welche – neben vielen anderen – ebenfalls Risikomanagementmaßnahmen für die Cybersicherheit beinhaltet.

Ob Betreiber von öffentlichen Telekommunikationsnetzen dann noch immer von den Regelungen des §8a BSIG befreit werden[12], wird sich mit dem KRITIS-Dachgesetz zeigen, welches die nationale Umsetzung der RCE-Direktive sein wird. Der im Juli 2023 veröffentlichte Referentenentwurf lässt dies aktuell jedoch nicht vermuten. Dass der Telekommunikationssektor klare Vorgaben

11 https://eur-lex.europa.eu/eli/dir/2022/2557/oj
12 Siehe §8d (2) 1. BSIG

auf Basis von bundespolitischen Entscheidungen benötigt, hat er in seinem Strategiepapier Resilienz der Telekommunikationsnetze[13] deutlich gemacht.

Eines ist diesen Regulierungen gleich: Sie heben die Verantwortlichkeit des Managements hervor und verpflichten die Mitgliedsstaaten zur Einführung von Sanktionen bei Nichtbefolgung. Es könnten dann der DSGVO[14] ähnliche Prozentsätze des gesamten weltweit erzielten Umsatzes fällig werden. Statt die Eigenkapitalquote für Risiken zu erhöhen oder Rückstellungen für Strafzahlungen zu bilden, sollte man sich also nun gerade im Bereich der Kritischen Infrastrukturen nicht nur den Cyber-und Informationssicherheitsmanagement (ISM)-Themen, sondern auch den weiteren GRC-Themen mit mehr Interesse widmen und für angemessene Ressourcenausstattung Sorge tragen.

4. Themenvielfalt und Herausforderungen bei der Ausrichtung an Standards

Um resilientere Infrastrukturen schaffen zu können, muss man sich mit einer Vielzahl an Organisationsthemen auseinandersetzen.[15] Nach einer Ermittlung von Defiziten bzw. Risiken steuern gerade die GRC-Themen die entsprechenden Maßnahmen zur Reduzierung/Härtung bei. Grundsätzlich sollte man diese aber nicht nur aus Compliance-Gründen umsetzen, sondern ihren Mehrwert für eine ordentliche Geschäftsorganisation erkennen und nutzen.

4.1. GRC-Themen

Das BCM liefert die grundlegenden Mechanismen zur Aufrechterhaltung des geschäftlichen Regelbetriebes. In einem ganzheitlichen Ansatz, welcher die Verzahnung mit Risikomanagement, Informationssicherheit, physischer Sicherheit (Unternehmenssicherheit insgesamt) und den anderen GRC-Themen gewährleistet und die internationalen Standards ISO 22301:2019 [16] und ISO 22313:2020 [17] - in Deutschland gegebenenfalls den jüngst veröffentlichten BSI 200-4 [18] - berücksichtigt, kann es bei strategischem Einsatz eine Führungsrolle in der Schaffung von Resilienz nach ISO 22316:2017 [19] einnehmen.

13 https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Resilienz/start.html
14 https://eur-lex.europa.eu/eli/reg/2016/679/oj
15 Siehe insbesondere Seite 9, Annex A der ISO 22316:207, zu den relevanten Managementdisziplinen.
16 https://www.iso.org/standard/75106.html
17 https://www.iso.org/standard/75107.html
18 https://bit.ly/48VJ5pU
19 https://www.iso.org/standard/50053.html

Das ITSCM setzt nach ISO 27031:2011[20] die Elemente des BCM LifeCycles mit spezifischer Ausrichtung auf die IT um - und gewährleistet damit in einer transformierten und digitalisierten Welt die Erreichung der Ziele des BCM. Für die Berücksichtigung von BCM in der Supply Chain sollte ISO/TS 22318:2021[21] verwendet werden. Krisen werden unter Zuhilfenahme von ISO 22361:2022[22] mit einer Schatten-Organisation gemanaged und bewältigt, die bei Eskalation von Notfällen (einschlägiger internationaler Standard hierfür ist ISO 22320:2018[23]), Bedrohungen für Leib und Leben und weiteren unplanbaren Vorfällen aktiviert wird.

ISM nach ISO 27001:2022[24] ermittelt mit so genannten Schutzbedarfsanalysen die physischen und digitalen Risiken von Informationen/Assets, um deren Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten. Mit der Berücksichtigung des Qualitätsmanagement nach ISO 9001:2015, deren Anforderungen und Ziele – gerade zum Prozessmanagement - in einem engen Zusammenhang[25] zur BCM-Norm ISO 22301 stehen, sollte sich für das Change-Management an ISO 10020:2022[26] ausgerichtet werden. Risikomanagement nach ISO 31000:2018[27] sollte als übergreifender Ansatz zur Ermittlung, Bewertung und Festlegung von angemessenen Vorgehensweisen zur Reduzierung von Schadensereignissen verwendet werden.

Zwischen den meisten der genannten Themen bestehen Schnittstellen, welche initial abgestimmt und durch regelmäßigen Austausch gepflegt werden sollten.

Zu beachten ist: diese Standards geben einen Rahmen vor. Jedes Unternehmen und jede Organisation muss für sich entscheiden, wie genau dieser Rahmen ausgefüllt und umgesetzt werden soll.

4.2. Non-GRC-Themen

Um auf Veränderungen und Herausforderungen reagieren zu können, diese zu bewältigen und sich gerade von Krisensituationen erholen zu können, bedarf es der Berücksichtigung weiterer Themen. Sie liegen tief in der „DNA“ einer jeden Organisation, eine Ausrichtung an formal dokumentierten internationalen Standards ist hier nicht möglich. Denn dazu gehören alle Themen, die auf die Unternehmenskultur einzahlen.

Zum Beispiel Führung und Kommunikation, da sie die Bereitschaft zu Flexibilität und Anpassungsfähigkeit der Mitarbeitenden beeinflussen, ihr Vertrauen

20 https://www.iso.org/standard/44374.html
21 https://www.iso.org/standard/79001.html
22 https://www.iso.org/standard/50267.html
23 https://www.iso.org/standard/67851.html
24 https://www.iso.org/standard/27001
25 https://www.iso.org/standard/62085.html
26 https://www.iso.org/standard/82213.html
27 https://www.iso.org/standard/65694.html

stärken können und Verständnis für die Ziele der Organisation schaffen. Genauso beeinflussen die Art und Weise, wie das Thema organisationale Resilienz in einem ganzheitlichen, koordinierten, interdisziplinären Ansatz durch das Management unterstützt, mit Ressourcen ausgestattet und in die Unternehmensstrukturen eingebettet wird und sich um das Wohlbefinden, die Gesundheit[28] und schlussendlich auch die Arbeitsplatzsicherheit der Mitarbeitenden[29] gekümmert wird, deren Widerstandsfähigkeit.

4.3. Verwendung von einheitlichen Begriffen und weitere nationale Herausforderungen

In Deutschland wird in den GRC-Themen häufig ein „sprachlicher Spagat" gelebt, der für ein gemeinsames Verständnis aller Beteiligten aufgelöst werden muss. Zum einen führt die wörtliche Übersetzung von Begriffen aus dem Englischen teilweise zu Verwechslungen in der Bedeutung. So ist der Notfall oftmals kein „Emergency" und wird auch nicht in den Kontext des „Major Incident" in der IT gebracht.

Dies trifft wohl auch auf den Resilienz-Begriff zu. Während dafür umgangssprachlich Widerstandsfähigkeit verwendet oder die Rückkehr zu einem Ausgangszustand verstanden wird, definiert ISO22300 ihn als Fähigkeit, ein sich wandelndes Umfeld aufzunehmen und sich anzupassen. Im Idealfall nutzt man also den Wandel als Chance, wie zum Beispiel die gerade stattfindende Transformation im Rahmen der Digitalisierung. Nicht nur um effizienter in seiner Organisation und Marktausrichtung zu werden, sondern gleichzeitig resilientere Strukturen zu schaffen.

Weitere Herausforderungen können in der Vielfalt der immer spezialisierteren Themen (siehe 4.1), seinen unterschiedlichen Anwendern und den Überarbeitungszyklen der Standards liegen.

Während Behörden, Hilfsorganisationen, öffentliche bzw. halb-staatliche Unternehmen sowie kleine und mittlere Unternehmen (KMU) in Deutschland für die Themen ISM und BCM überwiegend die nationalen Standards des BSI[30] zur Informationssicherheit umsetzen, orientieren sich die global tätigen Unternehmen überwiegend an den oben aufgeführten ISO-Standards, da sie so die Vielzahl weiterer – insbesondere strengerer - Regulierungen anderer nationaler Aufsichtsbehörden besser erfüllen. Ein zweiter Kreis von Anwendern kann in den unterschiedlichen Funktionen innerhalb der Unternehmen und Organisationen identifiziert werden. Während die internen Vorgaben zumeist in der sogenannten 2nd-Line erstellt werden (siehe Exkurs Three Lines-Modell), die

28 Siehe auch: Wolfgang Roth, Die resiliente Führungskraft, insb. Kapitel 4, Seite 95ff.

29 Siehe auch: Frank T. Meyer, Destination Resilienz, insb. Kapitel 12, Seite 47f.

30 Bundesamts für Sicherheit in der Informationstechnik

sich dabei an der Vielzahl der Standards orientiert, haben sich gerade in den IT-Bereichen Begriffe und Prozesse nach ITIL[31] etabliert.

Exkurs Three Lines-Modell: Nach diesem Modell liegt die Umsetzungsverantwortung grundsätzlich innerhalb der Organisationseinheiten, zu denen alle Bereiche der Geschäftsorganisation zählen – also auch die Finanzabteilung, das Personalwesen, die IT usw. und nicht ausschließlich die Geschäftsbereiche. Die Vorgaben werden unternehmensspezifisch von einer zentralen fachlichen Einheit anhand der rechtlichen Regelungen und branchenspezifischen Standards in der 2nd-Line[32] erstellt. Deren ordnungsgemäße Umsetzung wird durch eine direkt der Geschäftsleitung unterstellten, unabhängigen Einheit als 3rd-Line überprüft. Ggf. kann diese Überprüfung auch durch fachlich versiertere externe Prüfungen erfolgen. Auf diesem Wege scheint die Umsetzung auch für KMUs möglich zu sein.

Die Überarbeitungszyklen der ISO-Standards liegen im Schnitt bei 5 Jahren. Damit sollen methodische Weiterentwicklungen berücksichtigt und Konsistenz zwischen den verschiedenen Standards gewährleistet werden.

Die deutschen BSI-Standards 200-1/2/3 zur Informationssicherheit und dessen Management haben ihre 2008 veröffentlichten Vorgänger der 100-x-Serie im Oktober 2017 abgelöst. Der BSI 100-4 Notfallmanagement wurde im Juni 2023 als BSI 200-4 Business Continuity Management - an der ISO 22301 orientiert - neu veröffentlicht[33]. BCM-Verantwortliche aller Interessengruppen können ihn nun für die BCM-Umsetzung verwenden, solange sie keinen (internen und externen) Bedarf an einer Zertifizierung haben. Diesen formellen Nachweis der BCM-Fähigkeiten kann man nur mit dem internationalen Standard erreichen.

Die einheitliche Verwendung von Begriffen ist daher von zentraler Bedeutung für alle Themen und bei Abstimmung der Schnittstellen zu berücksichtigen. Für eine bessere und Resilienz fördernde Zusammenarbeit müssen die Themenverantwortlichen in den Unternehmen und Organisationen heutzutage daher - noch mehr als früher - enger zusammenarbeiten.

31 Information Technology Infrastructure Library

32 https://www.diir.de/fileadmin/fachwissen/downloads/Three-Lines-Model-Updated-German.PDF

33 Vor dem Hintergrund der bisherigen Tätigkeiten des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe als Kontaktstelle für das Sendai Rahmenwerk sowie der Neuausrichtung im Krisenmanagement und der anstehenden Veröffentlichung des KRITIS-Dachgesetz könnte geprüft werden, inwiefern das Prozess- und Resilienz-orientierte BCM aus dem Informationssicherheits-orientierten Kontext herausgelöst wird.

5. Abschließende Empfehlungen und Impulse zur Diskussion

Und wer trägt nun die Verantwortung für die Schaffung resilienterer Strukturen und vernetztem Risiko- und Resilienzmanagements? In einer vernetzten Gesellschaft: alle zusammen!

Bundesregierung und Behörden müssen einen verlässlichen, stabilen, transparenten und die Leistung der Wirtschaft anerkennenden Rahmen und entsprechende staatlichen Strukturen schaffen. Um resilientere Infrastrukturen schaffen zu können, müssen zeitnah Entscheidungen zur Umsetzung der Maßnahmen aus den bisher veröffentlichten Strategien getroffen werden. Denn die Auseinandersetzung mit der Vielzahl von Regelungswerken sowie deren Umsetzung – mit Hilfe von nationalen und internationalen Standards sowie praxisorientierten Leitfäden – erfordert gut ausgebildete Mitarbeitende, Ressourcen und Zeit. Ohne Investment keine Resilience!

Auch sollte es einen branchenbezogenen und -übergreifenden Austausch mit den Hilfswerken und Unternehmen geben. Beim in Deutschland gerade erst gestarteten Cell Broadcast hat dies bereits gut funktioniert. Mit weiteren Lösungen und Kampagnen müssen auch die Bürgerinnen und Bürger aufgeklärt und motiviert werden, ihren Beitrag zu leisten. Ehrenamtliches Engagement könnte dabei auf staatliche Anerkennung treffen.

Die Unternehmen sollten ihre eigenen BCM- und Krisenmanagementübungen mit mehr interdisziplinär besetzten Teams und insbesondere zusammen mit den Behörden und Organisationen mit Sicherheitsaufgaben durchführen. Die Unternehmen der kritischen Infrastruktur sollten zeitnah in die Länder- und Ressortübergreifende Krisenmanagementübung (LÜKEX) eingebunden werden.

Darüber hinaus ist bei den Unternehmen eine Zeitenwende in der Wahrnehmung der GRC-Themen erforderlich. Diese sollten nicht um der Compliance willen in einem Minimum-Ansatz umgesetzt werden, sondern – für die Schaffung resilienterer Unternehmen - auch aus einer der Unternehmenskultur entsprechenden intrinsisch-motivierten Position heraus. Dazu gehört auch die Verantwortungs-Übernahme beim Top-Management: je nach Größe und Bedeutung des Unternehmens sollte es einen Risk & Resilience-Verantwortlichen direkt in der Geschäftsleitung geben!

Die GRC-Themenvielfalt macht pragmatische Herangehensweisen insbesondere bei KMUs erforderlich, da auch hier die Umsetzungsverantwortung in den Organisationseinheiten der 1st Line liegt. Im Interesse einer nachhaltigen Ausrichtung sollte für alle GRC-Themen das Three-Lines-Model angewendet werden.

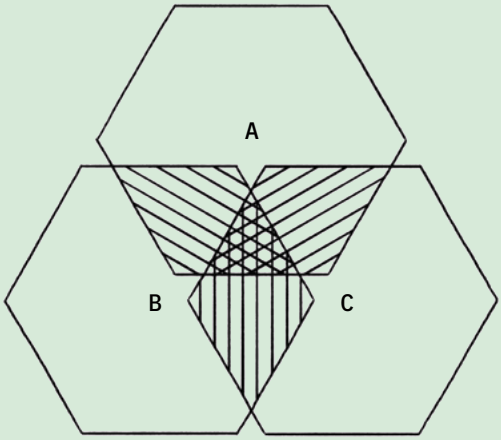
Im GRC- und Resilience-Gebiet gibt es mittlerweile eine unüberschaubare Anzahl von Veranstaltungen, bei denen Themenverantwortliche, Beraterinnen und Berater, Studierende, Wissenschaftlerinnen und Wissenschafter sowie Prüferinnen und Prüfer und viele weitere ihre Sichtweisen und Expertise

vermitteln. Was passiert mit diesen vielen wichtigen Impulsen? Wie kann man ihre Nachverfolgung übernehmen?

So dringlich die aktuelle Auseinandersetzung mit den Informationssicherheits-relevanten Cyber-Themen ist, darf nicht vergessen werden, sich auch mit den anderen Ressourcen-bedrohenden Ausfallrisiken zu beschäftigen. Während die Umsetzung eines BCM-Systems national und international anerkannten Prinzipien folgt und in der Literatur verankert ist, ist es noch immer nicht in allen weiteren Themen und Unternehmen ausreichend bekannt. Auch auf Grund der spezifischen Anforderungen aus dem ISM (so z.B. die Vorgaben der Schutzbedarfsfeststellungen aus §8a BSIG und §5 BAIT) wird es oft nur in Teilen berücksichtigt.

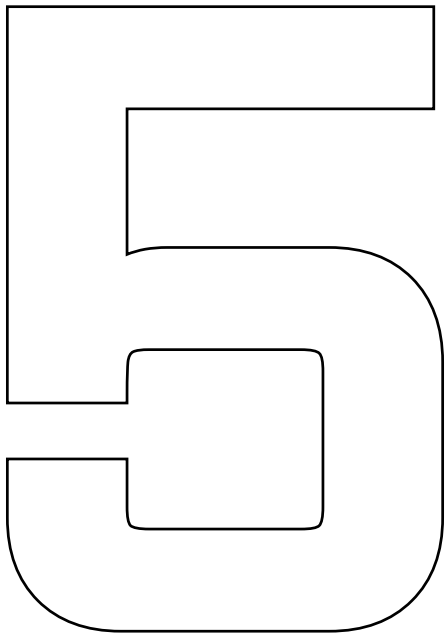
Weitere Unterstützung zur kontinuierlichen Verbesserung – für die vermutlich auch ein Wandel in der deutschen Fehlerkultur erforderlich ist - und Steigerung des Resilienz-Reifegrades könnte durch branchen-bezogenes Benchmarking der Resilienz-Fähigkeiten erzielt werden. Die Durchführung solcher Benchmarks sollte durch unabhängige Institutionen erfolgen.

Forschung, Wissenschaft, Normung und Interessenverbände haben die Krisen und Katastrophen der letzten Jahre analysiert, Erkenntnisse dokumentiert und stellen eine Vielzahl an Methodiken und Dokumenten zur Verfügung, wie gesetzliche Regelungen und Prävention, Detektion und Reaktion/Bewältigung umgesetzt werden können. Wann fangen wir als Gesellschaft an, diese zu berücksichtigen? Es gibt keine Erkenntnisdefizite mehr. Ein Scheitern liegt „nur noch“ an den Umsetzungsdefiziten in der Praxis.



A Behörden und Hilfsorganisationen
B Wirtschaft
C Zivilgesellschaft
||| + ✲ Stärkung der gesellschaftlichen Resilienz

Kapitel



Abschließende Betrachtungen