

# Krisenmanagement und Business Continuity

Jossé

2020  
ISBN 978-3-8006-6426-9  
Vahlen

schnell und portofrei erhältlich bei  
[beck-shop.de](https://beck-shop.de)

Die Online-Fachbuchhandlung [beck-shop.de](https://beck-shop.de) steht für Kompetenz aus Tradition. Sie gründet auf über 250 Jahre juristische Fachbuch-Erfahrung durch die Verlage C.H.BECK und Franz Vahlen.

[beck-shop.de](https://beck-shop.de) hält Fachinformationen in allen gängigen Medienformaten bereit: über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird [beck-shop.de](https://beck-shop.de) für sein

umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.



## 4 Einführung in BCM: Störungen der Continuity – was nun?

### Befunde

Kein Unternehmen ist vor Cyberangriffen oder Naturkatastrophen gefeit. Politische Verwerfungen können Geschäfte massiv behindern. Genauso können aber auch interne Versäumnisse Störungen auslösen. Tatsächlich sind viele Störungen hausgemacht (und absolut vermeidbar).

Welche Bedrohung bzw. Störung eine Organisation am meisten fürchtet und was sie objektiv am ehesten treffen kann, mögen zwei paar Stiefel sein – und jedenfalls mögen sich die Einschätzungen im Zeitablauf ändern, gerade auch durch neue Themen auf der Agenda. Dies zeigen die Befunde des „Allianz Risk Barometer“ aus den Jahren 2013 vs. 2019 und 2020 im Vergleich:

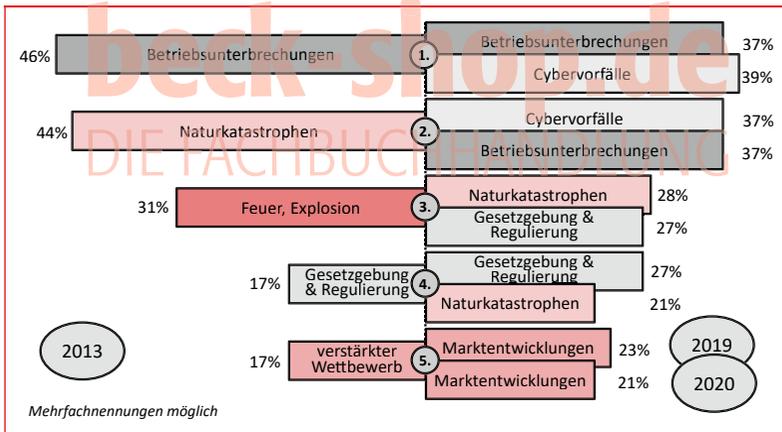


Abb. 11: Top-5 der erwarteten Geschäftsrisiken (weltweit)<sup>50</sup>

Klammern wir Cyberattacken und IT-Ausfälle kurz aus, die eine reale Gefahr darstellen, aber auch als Fokusthema anzusehen sind und in den letzten Jahren eine steile Karriere hingelegt haben: Oft stehen sie heute auf Platz 1 oder 2 der befürchteten Bedrohungen. Davon abgesehen gelten Betriebsunterbrechungen weltweit nach wie vor als die wichtigste Gefahr.

**In Deutschland gilt eine Betriebsunterbrechung als Risiko Nr. 1** (und kletterte gar von 48% im Jahr 2019 auf 55% im Jahr 2020)! Das gilt auch für andere

<sup>50</sup> Vgl. Allianz Global Corporate & Specialty SE (2013), (2019) und (2020)



Länder, wie z.B. für Polen, Italien, Österreich oder die Niederlande. Für viele Branchen ist die Betriebsunterbrechung die größte Bedrohung, so z.B. für Chemie und Pharma, Lebensmittel, Automobil- und Schwerindustrie, Energie, Groß- und Einzelhandel sowie Transport. Ein ähnliches Ergebnis zeigt sich bei der Befragung nach *Unternehmensgröße*: Für die großen und die mittelgroßen Unternehmen (ab 250 Millionen \$ Umsatz) sind Betriebsunterbrechungen die Gefahr Nr. 1.<sup>51</sup>

Anmerkung: Viele der anderen Bedrohungen (wie z.B. Naturkatastrophen, politische Instabilität, Cyberattacken etc.) führen oft ebenso zu Betriebsstörungen, sind dort aber nicht inkludiert! **Das Gesamtrisiko für eine Betriebsunterbrechung ist daher als deutlich höher anzusehen.**

Allerdings sind solche Einschätzungen nur Annahmen und müssen die tatsächliche Bedrohungslage nicht wiedergeben. Wenige Wochen vor der Corona-Krise galt: Auf Platz 17 und nur von 3 % weltweit befürchtet stehen gesundheitliche Bedrohungen – inkl. Pandemien! Es ist davon auszugehen, dass diese bei der nächsten Befragung ein deutlich höheres Gewicht bekommen.

## Argumente für BCM

Die britische Wirtschaft verliert durch Großstörungen aufgrund von nicht vorhandenem BCM pro Jahr über 11 Mrd. Pfund. Durch bestehende Notfallpläne können die Kosten der Wiederbeschaffung, der Wiederingangsetzung und des Ersatzes von Anlagevermögen und Vorräten teilweise um bis zu 90 % gesenkt werden. Sofern Unternehmen ohne effektive BCM-Pläne von einer Großstörung betroffen werden, so die Erfahrung, schaffen es rund 50 % nicht, sich innerhalb der nächsten zwölf Monate wieder zu erholen und verschwinden von der unternehmerischen Landkarte. Weitere Befunde:

Bei einer Studie in Deutschland ergab sich, dass im Jahr 2018 knapp 49 % der Befragten bestehende BC-Pläne aktivieren mussten, 20 % der Befragten verzeichneten gleich mehrere Störungen – so selten sind diese also gar nicht! Betroffen waren vor allem die IT-Infrastruktur und -Sicherheit, der Ausfall von Personal, Gebäuden, externen Dienstleistern oder die Produktion.<sup>52</sup>

Nach einem Disaster...

- eröffnen 25 % der betroffenen Unternehmen nie wieder,
- schließen 80 % der Unternehmen, die es nicht schaffen, binnen eines Monats wieder zu eröffnen, mit großer Wahrscheinlichkeit endgültig, und
- 75 % der Unternehmen ohne BC-Pläne scheitern binnen 3 Jahren.

<sup>51</sup> Vgl. Allianz Global Corporate & Specialty SE (2020), S. 4 ff.

<sup>52</sup> BCM Academy (2019), S. 32. Weiterer interessanter Befund: rund 44 % sind mit dem eigenen BCM zufrieden oder sehr zufrieden, das Mittelfeld kommt auf rund 30 %, die weniger oder nicht Zufriedenen auf zusammen knapp 22 %. Hier besteht noch Verbesserungsbedarf! vgl. ebd., S. 20



Umgekehrt bestätigt eine weltweite Befragung des Business Continuity Institute (BCI) den Nutzen von BCM:

- Bei 82% der Unternehmen wurden durch BCM die Auswirkungen einer Störung gemildert und
- 74% waren in der Lage, ihre Schlüsselprodukte und -dienste weiterhin auszuliefern.

Und eine Umfrage aus dem Jahr 2019 bestätigt die wachsende Bedeutung von BCM: Knapp 70% der Praktiker finden BCM sehr bis überaus wichtig, im Jahr zuvor waren es noch 60% gewesen.

Bezogen auf Datenpannen werden immer wieder ähnliche Zahlen vorgelegt. 2,2 Mio. US-Dollar Verlust – je Stunde! So hoch wurde der Schaden eines App-Stores geschätzt, dessen Dienst bis zu elf Stunden ausfiel. Störungen in der IT können richtig teuer werden; gut, wenn man ein funktionierendes BCM hat...

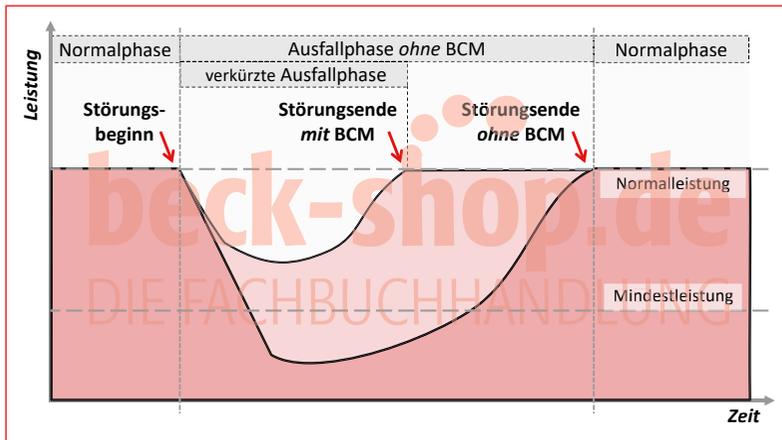


Abb. 12: Schneller wieder zum Normalzustand mit BCM

In den letzten Jahren wurde Toyota von einer ganzen Reihe von Pannen gebeutel, oft mit teuren Produktrückrufen verbunden. Als Konsequenz wurde das Qualitätsmanagement neu aufgestellt; neu geschaffene, regionale Kompetenzzentren sollten künftig näher am Kunden schneller reagieren. Obwohl das in der Summe mehrere Millionen Fahrzeuge betraf, gab es ein weiteres Thema, wie Toyota schmerzlich erfahren musste:

Japan liegt am pazifischen Feuerring – Erdbeben und Tsunamis stehen dort quasi auf der Tagesordnung. Im März 2011 war es wieder soweit: Aufgrund der Erdbeben mit nachfolgendem Tsunami sowie der Reaktorkatastrophe von Fukushima (klassische Kettenreaktion!) gab es über mehrere Wochen große Produktionsausfälle. Allein im April 2011 sank die Produktion von Toyota weltweit auf rund 50%, in Japan sogar auf nur 25%. Zwei Gründe gab es dafür: Zum einen waren zahlreiche Produktionsanlagen beschädigt, zum



anderen konnten wesentliche Zulieferer Toyota nicht mehr beliefern: rund 150 verschiedene Autoteile fehlten.

Daraufhin wurde die Supply Chain überarbeitet – weg von einem zwanghaften Kaputtsparen mit Lagerabbau und Skaleneffekten durch Single Sourcing.<sup>53</sup> Die Analyse erkannte 300 der 1500 Lieferantenwerke als riskant, das betraf 1000 verschiedene Teile. Deren Lieferanten wurden verpflichtet, die Teile an mehreren Standorten zu produzieren und/oder Lager anzulegen sowie ihrerseits BC-Pläne zu implementieren. Toyota selbst organisierte sein BCM-System neu, in enger Koordination mit lokalen Behörden, mit dem Ziel, in der Region eine höhere Katastrophenresistenz zu erreichen.

Toyota hat es offensichtlich kapiert: Die Augen vor der Realität zu verschließen ist keine Krisenprophylaxe. Und: Kosteneinsparungen sind *eine* Sache – wenn solche Programme aber im Fall X vielfach höhere Kosten (und entgangene Umsätze) bewirken, dann sind sie fehl am Platz. Nur einseitig Kosten senken vergrößert oft die Risikoposition. Und: Ein solides BCM lässt sich nicht von Kostensenkungsprogrammen verführen, sondern identifiziert ungeschminkt mögliche Großstörungen und entwickelt dafür unvoreingenommen wirksame Maßnahmen – und im Zweifelsfall auch unpopuläre, wie z.B. Städte unter Hausarrest zu stellen (Coronakrise) oder das Einrichten eines alternativen Produktionsstandortes beim ärgsten Konkurrenten (Pharma).

## BCM-Lücke in Unternehmen

Das BCM-Barometer 2018/2019 zeigt einige Lücken in deutschen Unternehmen auf: Demnach geben rund zwei Drittel der Befragten an, BCM habe für sie *keine Priorität* und leiste keinen bzw. *zu wenig Wertschöpfungsbeitrag* (rund 69 % bzw. 63 %). Die Hälfte nennt *Kosten* als Grund, kein BCM zu haben, und je 31 % *Ressourcen- bzw. Zeitmangel*. Und das, obwohl gleichzeitig mehr als die Hälfte einen Störfall hatte! Vielleicht sollte man sich die Zeit endlich einmal nehmen?

Tatsächlich gibt es mehrere Gründe, warum BCM trotz offensichtlichem Nutzen in einer Mehrzahl der Unternehmen nicht implementiert ist und ein entsprechendes Bewusstsein oft noch Mangelware ist:

1. **Zu wenig Bewusstsein** für krisenartige Störungen und deren potenzielle destruktive Gewalt – ein vorausschauendes Denken ist insgesamt zu wenig ausgeprägt. Doch Festhalten an überkommenen Denkschemata ist ein schlechter Ratgeber! Und falls doch ein BCM eingerichtet wird, dann ggf. nur als oberflächliche Anwendung und ohne tiefergehendes Verständnis von Nutzern und Verantwortlichen.
2. **Mangelnde Unterstützung** seitens der Unternehmensleitung, mangelhafte Einbeziehung von BCM in andere Disziplinen (z.B. Notfallplanung, IT-

<sup>53</sup> Nichts gegen sinnvolle Einsparungen – aber die Produktions- und Lieferfähigkeit muss gewahrt bleiben, auch im Fall X.



Sicherheit, Strategisches Management) und zu wenig Ressourcen sowie Zeitmangel.

3. **Skepsis**, im Sinne von „BCM taugt nichts, schützt uns nicht“. Ein Förderer dieser Haltung sind frühere falsche Prognosen, z.B. das aufgebauschte Jahr-2000-Problem oder auch SARS: Da die angekündigte Ausbreitung der Pandemie glücklicherweise viel geringer ausfiel, führt das leicht zu der Annahme, Behörden und Institute würden übertreiben. Wozu sich also jetzt darauf vorbereiten?
4. **Verharmlosen und sich in Sicherheit wiegen**: Die Sicht, „uns wird das Ereignis nicht treffen“ oder dass sich die Störung nicht so drastisch auswirken wird. Grund: Bestehende Versicherungen und Statistiken gaukeln Sicherheit vor bzw. der Störung und ihren Auslösern wird schlichtweg insgesamt eine zu niedrige Wahrscheinlichkeit beigemessen. Mit anderen Worten, das Problem wird idealisiert und verharmlost – ein klassischer Abwehrmechanismus im Sinne der kognitiven Dissonanz.
5. **„Das Tagesgeschäft geht vor, keine Zeit.“** Auf den Abgrund zugehen und einfach weitermachen anstatt innezuhalten, um sein Geschäft auf Schwachstellen abzuklopfen. Das ist fatal, aber leider gängig. Natürlich ist das operative Geschäft leichter greifbar und insgesamt vertrauter; bei strategischen Überlegungen und Krisenvorsorge ist Vorstellungsvermögen gefordert. Das hat nicht jeder. Und sich mit möglichem Negativen zu befassen, klingt nicht sexy. Dann lieber Ausblenden und Verletzbarkeiten ignorieren.
6. **Erfahrungspragmatismus**, nach dem Motto „es bringt nichts, es kostet zu viel, wir sind schon mit ganz anderen Sachen fertig geworden, wir schaffen das.“

Zum letztgenannten Aspekt zählt auch, dass oft kein direkter Nutzen gesehen wird. Und in der Tat sind ersparte Schadenskosten – und noch dazu für einen gänzlich unvorstellbaren Fall X! – viel weniger gut zu kommunizieren wie erzielte Erlöse, und seien die Kosten der Störung auch noch so exorbitant hoch.

Desinteresse, Unkenntnis, vermeintlich zu hohe Kosten für BCM oder zu geringer Vorteil sowie zu wenig Erfahrung im Umgang mit Störungen bzw. der Implementierung von BCM sind wesentliche Verhinderungsgründe. Gleiches gilt für die Annahme, dass es reiche, sich Großstörungen erst dann zu widmen, wenn sie bereits aktiv entstanden sind. Doch das funktioniert nicht. Jedenfalls ist wertvolle Zeit verschenkt. Getreu dem Motto „Zeitablauf vernichtet Handlungsmöglichkeiten“ fehlt zum einen wertvolle Zeit, die benötigt wird, um Maßnahmen zu entwickeln; zum anderen ist die Auswirkung bis dato stärker angewachsen. (vgl. Abb. 6, S. 24)

Nicht weniger fatal ist die trügerische Sicherheit, wenn Pläne halbherzig entwickelt werden, aber mittlerweile längst veraltet sind, weil das Personal gewechselt hat, ungeübt ist oder z.B. Ersatzoptionen nicht mehr funktionieren.

Und schließlich ein fatales Dilemma, das so genannte *Verletzlichkeitsparadoxon*: Gerade, weil Vorsorge betrieben wird und die Anzahl und Wahrscheinlichkeit eines Störfalls sinken, ist man weniger darauf vorbereitet (und



auch ungeübt im Umgang mit den schädlichen Folgen): Die Folgen eines „Dennoch-Störfalls“ sind daher überproportional hoch.

## Hintergrund

Die Idee hinter BCM ist uralte: Je komplexer und größer die Vorhaben, desto dramatischer sind die Folgen von Unterbrechungen. Ob beim Pyramidenbau oder einem Feldzug in der Antike oder einem global agierenden Unternehmen heute: Nachschublücken, politische Aufstände oder Seuchen waren und sind Störungen (oder deren Auslöser), die das ganze Unternehmen scheitern lassen können.

Schon früh<sup>54</sup> erkannte man beim *Militär*, dass eine strategische Voraussicht und die Kontinuität unter Gefechtsbedingungen (Waffen, Verpflegung, Menschen, Sold, Finanzen usw.) für den Erfolg ausschlaggebend sind. Was nützt die Eroberung einer Stelle, wenn dann der Nachschub abreißt? Oder wenn ein reiner Unterstützungsprozess wie Versorgung mit warmer Kleidung ausfällt? Nicht nur Napoleon hat das in seinem Russlandfeldzug erfahren... Auch die berühmte Varusschlacht im Teutoburger Wald könnte man als (geländebedingte) Störung sehen, in der die römischen Truppen nicht in der üblichen Schlachtordnung marschieren und sich formieren konnten; damit konnten sie ihre Stärke nicht ausspielen, gleichzeitig aber boten sie dem germanischen Gegner eine lange, verletzbarke Flanke.

Nach Ansätzen bei *Großprojekten* und im *Zivil- und Katastrophenschutz* war es in jüngerer Zeit zunächst die *IT*, die per BCM abgesichert werden sollte. Ereignisse wie der weltweite Börsencrash von 1987, das Y2K-Problem und die Anschläge auf das World Trade Center am 11. September 2001 förderten eine intensivere Absicherung gegenüber (IT-)Störungen. In der Folge wurde der Ansatz auf *Unternehmen* insgesamt und all ihre Funktionen ausgeweitet, schließlich auch auf Kommunen und andere *Gebietskörperschaften* oder sogar ganze *Regionen* (z.B. touristische Destinationen).<sup>55</sup>

Das *Notfallmanagement* war ebenfalls eine Keimzelle des BCM; während bei Ersteren meist operative Schadensereignisse vor allem Anlagen bedrohen, geht es beim BCM vorrangig um die Aufrechterhaltung der Geschäftsprozesse – mithin ein anderer und deutlich weiterer Blickwinkel.

<sup>54</sup> Allen voran der chinesische Militärtheoretiker Sun Tzu (ca. 500 v.Chr.), bei uns vor allem Clausewitz. Sicherlich sind solche Erkenntnisse aber zigttausend Jahre älter.

<sup>55</sup> In Großbritannien bspw. existiert seit 2004 der sog. Civil Contingencies Act (CCA), der eine Art BCM für Großstädte und Grafschaften vorsieht: deren Verletzbarkeiten durch Störungen und ihre Folgewirkungen sollen vorausschauend erkannt und gehandhabt werden. Die UNO fährt schon seit 1999 ein Programm namens UNDRR (UN Office for Disaster Risk Reduction; bis 2019: UNISDR), das z.B. Störungen aufgrund von Migration (ausgelöst durch z.B. Klimawandel, Dürre, Erdbeben, Tsunamis oder Krieg) handhaben und insgesamt die Widerstandskraft von Nationen und Gemeinwesen gegenüber solchen Katastrophen und deren Folgen stärken soll. Vgl. hierzu UNDRR (2019). Ein vom UNDRR unterstütztes Programm „Making Cities Resilient“ promotet den BCM-Gedanken für Städte; vgl. Wagner (2020), S. 8 ff.



Die *BWL* steuerte grundlegend den strategischen Kontext bei, außerdem Ansätze wie Kontingenz- bzw. Alternativplanung, zahlreiche Analyseinstrumente und Erkenntnisse aus dem Risikomanagement. Tatsächlich gab das *Risikomanagement* wichtige Anstöße für das BCM (auch aufgrund gesetzlicher Vorgaben wie dem KonTraG);<sup>56</sup> mittlerweile aber hat sich das BCM emanzipiert und grenzt sich vom Risikomanagement deutlich ab.

Der wesentliche Treiber für eine Weiterentwicklung und Verbreitung von BCM ist das in London ansässige *Business Continuity Institute (BCI)* mit Mitgliedern aus der ganzen Welt.<sup>57</sup> In Deutschland sind u.a. zwei Bundesämter involviert: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BKK).

## Normen und Standards

Von den zahlreichen Normen und Standards seien die wichtigsten kurz genannt: Seit 2012 existiert für BCM die weltweit anerkannte Norm ISO 22301. Davor waren vor allem die beiden britischen Standards BS 25999-1 und -2 eine hervorragende Hilfe. Gleiches gilt für die Good Practice Guidelines (vom BCI), die auch auf Deutsch erschienen sind und regelmäßig neu aufgelegt werden. Alle diese Regelwerke bzw. Hilfestellungen können Sie zu Rate ziehen, wenn Sie Ihr eigenes BCM entwickeln.

Doch beachten Sie bitte: Die verschiedenen Standards verleiten ggf. dazu, dass Analysen, Templates und BC-Pläne nach Schema F abgearbeitet werden, aber kein Bewusstseinsprozess stattfindet. BCM ist aber kein starres Korsett, sondern eher ein Rahmenkonzept, in das sich unterschiedliche Bausteine der Absicherung gegen das Unbekannte und drastisch Schädigende einbauen lassen. Sofern nicht ein Geschäftspartner anderes fordert, ist es daher ratsam, dass jedes Unternehmen unter Einbindung seiner Mitarbeiter seine eigenen Assessments durchführt und seine eigenen BC-Pläne entwickelt. Wie das grundsätzlich geht, lesen Sie in Kap. 5.<sup>58</sup>

## Wer braucht BCM?

Die Antwort ist einfach: Grundsätzlich jede Institution, die sich Störungen mit gewaltigem Schadenspotenzial ausgesetzt sieht, also nicht nur große Konzerne, sondern gerade auch der Mittelstand. Wenn nachfolgend vor al-

---

<sup>56</sup> Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich verpflichtet kapitalmarktorientierte Gesellschaften zu einem Risikomanagementsystem; eine Verpflichtung für ein BCM ergibt sich nicht explizit, aber implizit schon.

<sup>57</sup> Schauen Sie mal rein auf [www.thebci.org](http://www.thebci.org)

<sup>58</sup> Eine Ausführliche Darstellung mit dem kompletten BC-Prozess, Methodenanwendungen, zahlreichen Praxisbeispielen und einem Glossar erwartet Sie in Jossé: Business Continuity Management (BCM), Störungen im Unternehmen vorausschauend managen, Verlag Vahlen, München 2021 (ISBN 978-3-8006-6293-7).



lem Unternehmen fokussiert werden, so sollten auch Städte (Dresden bei Elbehochwasser; Duisburg bei der Loveparade), touristische Destinationen (Galtür beim Lawinenunglück; Ischgl bei Pandemie) oder ganze Regionen und Staaten<sup>59</sup> (bei Unruhen, Tsunamis oder Pandemien) vorausschauend BCM betreiben und Maßnahmen zur Immunisierung betreiben.

Bei Unternehmen sind es mehr Aspekte wie Abbau von Redundanzen, globale Lieferbeziehungen, große Abhängigkeiten aufgrund komplexer Prozesse, lagerlose Produktion oder strategisch relevante Marktveränderungen, die ein *BCM unumgänglich* machen: „**Eine Kette ist so stark wie ihr schwächstes Glied.**“ Das allein sollte schon zum Nachdenken anregen! Betrachtet man die oft extrem vulnerablen Prozesse, noch dazu ohne Ersatzoptionen, dann gleicht das einem Herausfordern des Schicksals. Solche Unternehmen brauchen dringend ein BCM.

### Definition BCM

Die Kernaufgabe von BCM ist, die **Fortführung der Geschäftstätigkeit** und den wirtschaftlichen Erfolg von Unternehmen sicherzustellen trotz angespannter Situation. Damit soll BCM die Wertschöpfung stabilisieren und so die Unternehmensinteressen schützen, wie z.B. Prozesse, Marke und Reputation.

Zu diesem Zweck identifiziert und analysiert BCM existenzbedrohende Störungen und entwickelt grundsätzliche Abwehr- und Bewältigungsstrategien sowie konkrete Maßnahmen.

### Ziel von BCM

Gegenstand von BCM sind Störungen (vgl. Abb.13, S.41), und zwar jene **Beeinträchtigungen oder Unterbrechungen**,<sup>60</sup> die nicht mit den gegebenen Mitteln im Rahmen der *operativen Routine* bewältigt werden können.<sup>61</sup> Solche

<sup>59</sup> Weil nicht nur Unternehmen angesprochen werden, ist der deutsche Begriff des „*Betrieblichen Kontinuitätsmanagements (BKM)*“ mittlerweile als zu eng gefasst anzusehen und die englische Bezeichnung „Business Continuity“ vorzuziehen; „business“ wird dort in weiterem Sinn verstanden.

<sup>60</sup> Ein einfaches Bild erklärt den Unterschied: Bei Straßenbauarbeiten können Sie beide Fahrspuren sperren (Unterbrechung bzw. Ausfall) oder nur eine Fahrspur, während die andere geöffnet bleibt (Beeinträchtigung); wahrscheinlich dauern die Bauarbeiten im 2. Fall etwas länger und sind aufwendiger. Weitere Option wäre z.B. eine zeitweise Sperrung (z.B. nachts).

<sup>61</sup> Beispiele: Eine defekte Maschine kann binnen zwei Stunden vom eigenen Team im Werk repariert werden → Routine. Ein kurzfristiger Stromausfall → Routine, also kein Fall für BCM. Falls allerdings durch die kleine Ursache eine Kettenreaktion in Gang gesetzt werden kann, sieht es anders aus: Es kommt im Werk zu einer Überlast (Ursache: Stromnetz von außen) und Überhitzung, daraufhin entzündet sich ein biologisches Schmiermittel, es kommt zu einem Brand: Maschinen und Teile werden beschädigt bzw. zerstört, es kann wochenlang nicht produziert werden, Kunden