BUSINESS CONTINUITY MANAGEMENT – WIDERSTANDSFÄHIGKEIT ZU KRISENZEITEN

Laut dem Allianz Risk Barometer 2022, bei dem mehr als 2700 Risikomanagement-Experten zu ihren wichtigsten Unternehmenssorgen befragt wurden, ist die «Initiierung oder Verbesserung von BCM» (62%) die wichtigste Massnahme, die Unternehmen jetzt ergreifen, um ihre Lieferketten risikoärmer und angesichts der globalen Pandemie widerstandsfähiger zu machen.

- **Von Prof. Dr. Claus W. Gerberich**

Mit Business Continuity Management Krisen aktiv managen

Was ist Business Continuity Management?
Unter Business Continuity Management wird ein ganzheitlicher Prozess verstanden, dem das Ziel zugrunde liegt, Unterbrechungen des IT-Betriebs oder Anlagenverfügbarkeit in einem Unternehmen oder einer Organisation zu minimieren. Besonders Unterbrechungen, die dem Unternehmen ernsthaft Schaden zufügen würden, sollen so vermieden werden.

• HINWEIS

Im Kern des Business Continuity Managements stehen daher die Entwicklung und Dokumentation von Strategien, Plänen und Massnahmen für die Erreichung dieses Ziels. So soll bestmögliches, strukturiertes und fehlerfreies Handeln im Krisenfall ermöglicht werden.

Definieren von Notfallplänen: Nach Vollendung der Analyse erstellen Sie sogenannte Notfallpläne

In diesen wird definiert, wie im Falle der verschiedenen Krisenszenarien konkret zu reagieren ist. Dabei werden sowohl die sofort durchzuführenden Massnahmen beschrieben als auch der Übergang in den Notfallbetrieb sowie der Übergang vom Notfallbetrieb zurück in den Normalbetrieb. Auch die Nachbereitung eines solchen Vorfalls ist Teil der Notfallpläne.

Notfallübungen
Die Notfallpläne testen Sie in regelmässigen Abständen, um ihre Wirksamkeit zu überprüfen. Erkenntnisse aus diesen Tests fliessen dann als Verbesserungen in die Notfallpläne ein.

Stetige Optimierung der Pläne und Massnahmen
Die einmalige Erstellung der Pläne und Massnahmen reicht nicht aus, da sich die Rahmenbedingungen laufend ändern können. Neben den Notfallübungen sollten Sie auch bei Änderungen der Geschäftsprozesse oder der Rahmenbedingungen überprüfen, ob diese Einfluss auf die Notfallpläne haben und dementsprechend Änderungen vorgenommen werden müssen. Zudem sollte die Kritikalität der Geschäftsprozesse in regelmässigen Abständen neu bewertet werden.

• HINWEIS

Wichtig zu beachten ist, dass für die unterschiedlichen Krisenszenarien auch unterschiedliche Massnahmen definiert werden müssen, um bestmöglich reagieren zu können.

Wie funktioniert BCM?

Grundlegend für BCM-Konzepte ist der sogenannte PDCA-Zyklus. PDCA steht für «Plan», «Do», «Check», «Act».

Plan – Welche potenziellen Bedrohungen gibt es, wie kann ein Unternehmen diesen vorbeugen, und was muss im Fall der Fälle passieren? Wichtig: Die in dieser Phase entwickelten Handlungspläne sollten regelmässig getestet und von allen Beteiligten beherrscht werden. Nur so lässt sich beispielsweise sicherstellen, dass bei einem Feueralarm im Unternehmen alle wissen, was zu tun ist.

Do – In dieser Phase wird das für den Ernstfall Geplante umgesetzt. Die Akteure befolgen die in Phase 1 erarbeiteten Handlungspläne und stellen so die betriebliche Kontinuität sicher. Beispielsweise, indem sie verloren gegangene Daten aus einem Back-up wiederherstellen.

Check – Ist eine akute Krisensituation erst mal überwunden, steht die Frage nach den Ursachen auf dem Programm. Der Vorfall sollte von den BCM-Verantwortlichen im Unternehmen ausgewertet und es sollten entsprechende forensische Analysen durchgeführt werden.

Act – Zu guter Letzt geht es um die Rückkehr zum Normalbetrieb und das Ziehen etwaiger Konsequenzen aus einem Vorfall. Sollten für den nächsten PDCA-Zyklus schon in Phase 1 neue Massnahmen geplant und Verbesserungen eingeführt werden? Oder ist die Wahrscheinlichkeit, dass sich die Bedrohungslage wiederholt, so gering, dass im Business Continuity Management keine Anpassungen erforderlich sind?

Auf welche Risiken und Bedrohungen zielt BCM ab?

Diesbezüglich gibt es keinerlei Einschränkungen. BCM hat alle Risiken im Fokus, die in irgendeiner Weise den Betrieb eines Unternehmens stören könnten. Zu den möglichen Ursachen zählen Pandemien und Elementargefahren wie Überschwemmungen, Erdbeben, Brände, Stürme und Vulkanausbrüche, aber auch technische Pannen wie Stromausfälle oder Internet-Blackouts und alle nur denkbaren Cyber-Vorfälle – vom einfachen Datenverlust über Ransomware-Attacken bis hin zum Server-Ausfall ohne Fremdeinwirkung.

Nutzen von Business Continuity Management

Wie zuvor schon beschrieben, ist ein etabliertes Business Continuity Management eine gute Möglichkeit, das eigene Unternehmen gegen Bedrohungen oder Störungen zu rüsten. So können Sie die Ausfallzeiten und somit auch die daraus resultierenden Umsatzeinbussen für Ihr Unternehmen möglichst gering halten.

BCM schafft mehrere Nutzenkategorien:

- Die Kosten von Betriebsunterbrechungen sinken.
- Bei Schadenseintritt findet ein planmässiges Handeln statt.
- BCM sorgt dafür, dass der Betrieb so schnell wie möglich wieder aufgenommen werden kann.
- Die gesetzlichen Anforderungen werden erfüllt.
- Der Wettbewerbsvorteil kann gesichert werden.

Vorteile von BCM

Von hoher Qualität ist ein BCM dann, wenn es alle potenziellen Bedrohungen und Risiken berücksichtigt und nichts übersehen hat. Verbindliche Kriterien gibt es aber nicht – allenfalls Anhaltspunkte und Best-Practice-Vorgaben im Rahmen der bekannten ISO-Zertifizierungen für Qualitätsmanagement (ISO 9001) und Informationssicherheit (ISO 27001). Den Fokus legen die Standards auf den Schutz, das Funktionieren und die Verfügbarkeit von Personen, Prozessen und Daten eines Unternehmens.

Folgende konkrete Vorteile kann man durch ein Business Continuity Management erwarten:

- Stabilität der Geschäftsprozesse erhöhen
- Ausfall und Wiederherstellzeiten von Anwendungen reduzieren
- strukturierte und schnelle Vorgehensweise bei Zwischenfällen
- ganzheitliche Risikobetrachtung auf allen Geschäftsebenen
- Compliance-Anforderungen sicherstellen und internationale Standards erfüllen
- Engagement der Leitung bei Notfallmanagement
- höhere Transparenz gegenüber interessierten Parteien und der Öffentlichkeit

Unabhängig davon gilt: Entscheidend für die BCM-Qualität ist es, alles im Blick und an alles gedacht zu haben. Ob beides gelingt, ist in der Praxis schwierig messbar. Business Coninuity Management muss je nach Unternehmen individuell und risikoabhängig umgesetzt werden. Das ist die eigentliche Herausforderung.

Wer ist verantwortlich für den BCM-Aufbau?

Des Weiteren legen immer mehr Unternehmen Wert auf Business Continuity Management und setzen ggf. ein entsprechendes Konzept für eine Zusammenarbeit voraus. Selbst wenn ein solches Konzept nicht vorausgesetzt wird, kann BCM genutzt werden, um das Vertrauen von Partnern und Kunden Ihrem Unternehmen gegenüber zu stärken.

Der Aufbau eines Managementsystems für Business Continuity ist immer und zuerst eine Managementaufgabe. Die Situation ist vergleichbar mit der beim Aufbau eines ISMS (Information Security Management System). Bei grösseren Unternehmen und in Konzernen wird die Verantwortung daher beim Chief Information Security Officer (CISO) liegen. Dieser sollte ein geeignetes Team intallieren, bestehend aus BCM-Experten und Risikomanagern, das sich um alle BCM-Aufgaben kümmert. Erfolgreich kann BCM aber nur sein, wenn alle im Unternehmen die konkreten Massnahmenpläne kennen und deren Umsetzung regelmässig üben.

BCM und Risikomanagement

Risikomanagement ist die Grundlage für Business Coninuity Management. Aufgabe und Ziel des Risikomanagements ist es, die Risiken für ein Unternehmen zu identifizieren, deren Eintrittswahrscheinlichkeiten zu bestimmen und den möglichen Impact zu analysieren. Auf dem Fundament dieses Wissens können im Rahmen des Business Continuity Managements dann entsprechende Pläne und Massnahmen entwickelt und etabliert werden.

Welche Kriterien hat BCM zu erfüllen?

Von hoher Qualität ist ein BCM dann, wenn es alle potenziellen Bedrohungen und Risiken berücksichtigt und nichts übersehen hat. Verbindliche Kriterien gibt es aber nicht – allenfalls Anhaltspunkte und Best-Practice-Vorgaben im Rahmen der bekannten ISO-Zertifizierungen für Qualitätsmanagement (ISO 9001) und Informationssicherheit (ISO 27001). Den Fokus legen die Standards auf den Schutz, das Funktionieren und die Verfügbarkeit von Personen, Prozessen und Daten eines Unternehmens.

Unabhängig davon gilt: Entscheidend für die BCM-Qualität ist es, alles im Blick und an alles gedacht zu haben. Ob beides gelingt, ist in der Praxis schwierig messbar. Business Coninuity Management muss je nach Unternehmen individuell und risikoabhängig um-

gesetzt werden. Das ist die eigentliche Herausforderung.

Welche Entwicklungen verändern das Business Continuity Management

Die Digitalisierung ist auch in diesem Bereich der mit Abstand stärkste Veränderungsmotor – nicht nur im Hinblick auf Cyber-Vorfälle.

Beispiel Cloud-Speicher: Ein Unternehmen, das seine geschäftsrelevanten Daten nicht mehr physisch auf Servern im eigenen Haus speichert, sondern in der Cloud, muss sich vor Datenverlust durch Hochwasserschäden am eigenen Gebäude nicht mehr fürchten. Aber: Das Risiko ist nicht verschwunden, es wurde nur auf den Cloud-Anbieter verlagert. Dieser kann das Risiko im Idealfall besser managen, komplett verschwinden wird es jedoch nicht. Darüber hinaus bringt die fortschreitende Digitalisierung als solche auch wieder neue Risiken mit sich. Die Anfälligkeit für Cyber-Kriminalität steigt weiter, und ohne funktionierendes Internet und zuverlässige Stromversorgung geht heute kaum noch etwas.

Die drei Schritte, um Ihr Business-Continuity-Management-System zu entwickeln

In nur wenigen Schritten ermitteln wir den Reifegrad Ihrer Business Continuity, entwickeln ein gemeinsames Vorgehen, um Ihre Business Continuity stetig zu verbessern und erarbeiten gemeinsam Notfallstrategien und Notfallpläne:

1. GAP-Analyse

Wir analysieren bereits vorhandene Aspekte Ihres Business Continuity Managements bzw. IT-Notfallmanagements und damit dessen Umsetzungsgrad.

2. Massnahmenplanung

Auf Grundlage der Analyse erkennen wir die notwendigen Massnahmen zur Erhöhung des Reifegrads Ihres Business-Continuity-Management-Systems. Wir entwickeln pragmatische Herangehensweisen und Massnahmen, die Ihnen helfen, ein zweckmässiges Business Continuity Management zu etablieren, das sich stetig weiterentwickelt und verbessert.

3. Implementierung

Gemeinsam setzen wir die geplanten Massnahmen um und coachen die BCM-Verantwortlichen bei der Umsetzung und Etablierung von Regelaufgaben. Dadurch verfügen Sie über das notwendige Handwerkszeug im Schadensfall und können im Notfall zielgerichtet und effektiv agieren sowie reagieren.

Was macht einen guten Business-Continuity-Plan (BCP) aus?

Bei der szenariobasierten Planung werden die eigene Aufstellung des Unternehmens und die Belastbarkeit der Lieferketten kritisch geprüft. Der BCP, der von der obersten Führungsebene mitgetragen werden sollte, ist ein ganzheitlicher Ansatz, der wesentliche Abläufe, kritische Ausrüstung, Schlüsselpersonal, funktionale Schwachstellen, Gefährdungen der Lieferkette und Lösungsvorschläge berücksichtigt. Ein effektiver BCP wird Schlüsselpersonen aus jedem kritischen Funktionsbereich, Abteilungsleiter und Standortmanager einbeziehen. Sowohl Mitarbeitende als auch Manager sollten den Planungsprozess und die Implementierung erleichtern, verstehen und, wenn möglich, selbst übernehmen. BCPs sollten gut dokumentiert sein, um den Anforderungen von Audits zu genügen, und sollten aus vier Schlüsselschritten bestehen:

- Durchführung einer Business-Impact-Analyse (BIA), die die Folgen einer Unterbrechung einer Geschäftsfunktion und eines Prozesses vorhersagt
- Bewertung von Risiken durch Definition wahrscheinlicher Bedrohungen oder Schwachstellen und deren Auswirkungen auf das Geschäft
- Festlegung von Recovery Point Objectives (RPOs), die beschreiben, bis zu welchem Zeitpunkt die Wiederherstellung des Geschäftsprozesses erfolgen kann
- Festlegung von Wiederherstellungszeitzielen (Recovery Time Objectives, RTOs), die definieren, wie viel Zeit nach der Benachrichtigung über die Unterbrechung des Geschäftsprozesses für die Wiederherstellung benötigt wird; und die Übungs- und Wartungszeit, die erforderlich ist, um den Plan anhand verschiedener Szenarien zu testen und Anpassungen vorzunehmen

QUELLEN

Data Guard, 2022.

Allianz Szenarioplanung für künftige Unterbrechungen, 2022.

AUTOR

Prof. Dr. Claus W. Gerberich, Studium des Maschinenbaus und der Betriebswirtschaft in Karlsruhe, Mannheim und am MIT Cambridge/Boston. Er führt Trainings und Beratungen durch und hat sich dabei auf die Bereiche Unternehmensführung und -strategie sowie Controlling spezialisiert.

Impressum

Verlag	WEKA Business Media AG Hermetschloostrasse 77 CH-8048 Zürich www.weka.ch	Layout/Satz	Dimitri Gabriel/Sarah Rutschmann
Herausgeber	Stephan Bernhard	Publikation	10 × jährlich, Abonnement: CHF 98.– pro Jahr, Preise exkl. MWST und Versandkosten. Als digitale Publikation erhältlich unter: www.weka-library.ch
Redaktion	Carla Seffinga	Bildrechte	www.istockphoto.com
		Bestell-Nr.	9150