UNIVERSITÄT KOBLENZ
FACHBEREICH INFORMATIK

Diplomarbeit

Business Continuity Planning

vorgelegt von
Sascha Rutenbeck

zur Erlangung des akademischen Grades eines
Diplom-Informatikers
im Studiengang Informatik

Erstgutachter:
Prof. Dr. Rüdiger Grimm
Institut für Wirtschafts- und Verwaltungsinformatik
Fachbereich 4: Informatik

Zweitgutachter:
Anastasia Meletiadou
Institut für Wirtschafts- und Verwaltungsinformatik
Fachbereich 4: Informatik

Koblenz, 24. September 2008

Erklärung

Hiermit versichere ich, dass ich die vorliegende Diplomarbeit selbstständig und ohne fremde Hilfe verfasst habe und keine als die angegebenen Quellen und Hilfsmittel genutzt habe. Alle Ausführungen der Arbeit, die wörtlich oder sinngemäß übernommen wurden, sind als solche kenntlich gemacht.

Mit der Einstellung dieser Diplomarbeit in die Bibliothek bin ich einverstanden.

Der Veröffentlichung dieser Arbeit im Internet stimme ich zu.

Koblenz, 24. September 2008

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

BC	Business Continuity
BCI	Business Continuity Institute
BCM	Business Continuity Management
BCP	Business Continuity Planning
BR	Backup and Restore
BRP	Business Resumption Planning
BS	Betriebssystem
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI (brit.)	British Standards Institute
CDP	Continous Data Protection
CP	Contingency Planning
DPC	Draft for Public Comment
DR	Disaster Recovery
DRP	Disaster Recovery Planning
DRII	Disaster Recovery Institute International
E/I/C	Emergency, Incident, Crisis
GbR	Gesellschaft bürgerlichen Rechts
IR	Incident Response
IT	Information Technology
ITCP	IT Contingency Planning
ITDR	IT Disaster Recovery

ITRM	IT Risk Management
IS	Information Security
KMU	Kleine und mittlere Unternehmen
RAID	Redundant Array of Independent Disks
RM	Risk Management
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SOX	Sarbanes Oxley Act
TIE Workstation	True Image Echo Workstation, Produktbezeichnung der Workstation-Software von Acronis
TIE Server	True Image Echo Server, Produktbezeichnung der Server-Software von Acronis
VBM	Value Based Management
VHD	Virtual HD, virtuelle Festplatte
VSS	Volume Shadow Copy Service

1 Einführung ins Business Continuity Planning (BCP)

Business Continuity Planning und eine Berufsunfähigkeitsversicherung haben zwei Dinge gemeinsam: Beide erkennen potentielle Risiken proaktiv und verfügen über festgelegte Maßnahmen für den Fall eines ungeplanten Notfalls. Der Unterschied ist, das Business Continuity Planning setzt sich auch über das 67. Lebensjahr hinaus kontinuierlich fort.

Notfälle passieren ständig. Meist häufiger als man denkt. Privat und geschäftlich. Wenn namenhafte Unternehmen wie die Gartner Group belegen, dass „zwei von fünf Unternehmen, deren Systeme als Folge einer Katastrophe zerstört werden oder längere Zeit nicht verfügbar sind, innerhalb von fünf Jahren Konkurs anmelden", dann liegt hier ein ernst zu nehmendes Problem vor. Liegen zusätzlich Zahlen auf dem Tisch, die die Kosten von IT-Ausfallzeiten westeuropäischer Unternehmen auf fünf Milliarden jährlich summieren, dann besteht sogar großer Handlungsbedarf.

Die Bedrohung der „Berufsunfähigkeit" eines ganzen Unternehmens (Geschäftsfortführung) kommt zudem von zahlreichen weiteren Stellen neben der IT. Abbildung 1.2 zeigt eine einfache Übersicht, wo diese Gefahren liegen. Dabei wird eines ganz deutlich: Der Aufwand der betrieben werden muss – und damit die Anforderungen an das Risikomanagement eines Unternehmens – sind enorm. So wird es passieren, dass ein Fehler, eine Nachlässigkeit oder eine schleichende Zuspitzung der Ereignisse die goldene Regel des Business Continuity Plannings bestätigt: „Es ist nicht die Frage *ob*, sondern *wann* ein Notfall eintreffen wird." Hurricanes im Südosten der USA, Überschwemmungen in der Outsourcing-Metropole Indien, politische Produktionsstilllegungen in China oder undichte Atomkraftwerke in Frankreich: nur einige Beispiele, die in jüngster Zeit den Trend zur Vorsorgeplanung vorangetrieben haben.

Der Druck zur Kostenoptimierung führt dabei zu wirtschaftlichen Verpflechtungen, die viele Bereiche eines Unternehmens in interne und externe Abhängigkeiten stellen. Ein Resultat dieser Entwicklung zeigt der Weltkatastrophenbericht 2008: Innerhalb nur eines Jahres haben sich die Kosten, die durch Katastrophen entstanden sind, fast verdoppelt.[1] Zugleich hat sich die Anzahl der gezählten Katastrophen aber verringert. Eine plausi-

[1] [Sch08]

ble Erklärung dieses bedeutenden Anstiegs ist in der Konzentration von Menschen und Vermögenswerten auf dicht besiedelte Gebiete zu sehen. Eine Effizienzsteigerung, die durch einseitige Kostenorientierung die Balance von Risiko (Verlust von Flexibilität) und Chance (Gewinnsteigerung) gefährdet.

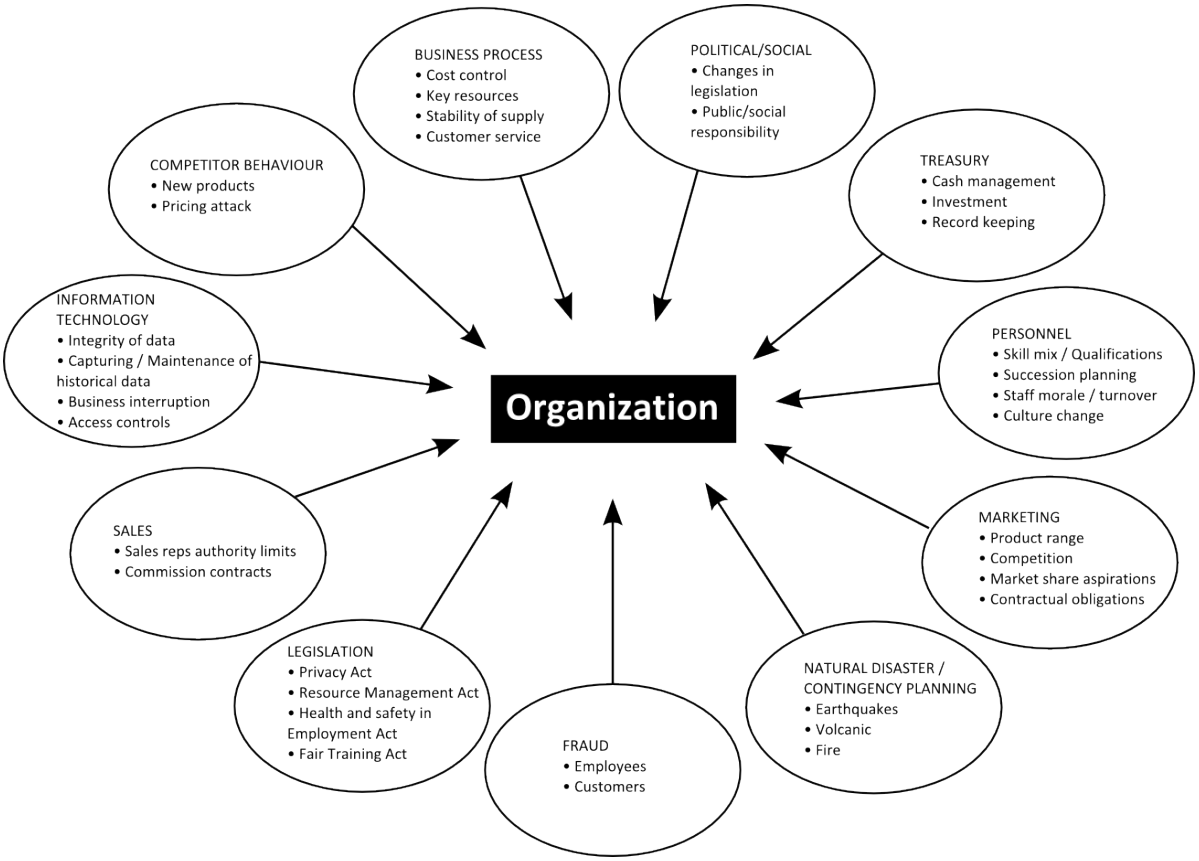


Abb. 1.1: Die zahlreiche Geschäftsrisiken eines Unternehmens, meist geprägt von Interdependenzen. (Quelle: vgl. [Hil07a])

Im Business Continuity Planning geht es darum, diese Flexibilität wieder zu erhöhen. Die IT ist dabei nicht das einzige, aber ein zentrales Thema, wie das folgende Beispiel zeigt: 69 Prozent der befragten Unternehmen in einer aktuellen Symantec-Studie vom Januar 2008 rechnen jeden Monat mit mindestens einer Störung ihrer IT und ganze 63 Prozent halten sogar einen größeren IT-Ausfall im Jahr für wahrscheinlich.[2] Dabei sind nur rund die Hälfte aller IT-Störungen tatsächlich auf Schwierigkeiten mit der eingesetzten Technologie zurückzuführen. Die anderen 50 Prozent verantworten die Menschen und

[2] [Sym08]

Prozesse im Unternehmen, die mit immer neuen Herausforderungen einer zusammenwachsenden Welt konfrontiert werden. Extrapoliert man diese Werte auf die etwa drei Millionen Unternehmen in Deutschland und geht nur von einem halben Prozentpunkt aus, bei denen ein großer IT-Ausfall als echter Notfall zu bezeichnen ist – die Wahrscheinlichkeit dafür liegt in Zeiten zunehmender Abhängigkeit von Informationen und einer 24/7-Verfügbarkeit mitunter um einiges höher – dann wären jährlich 10.000 Unternehmen existentiell gefährdet. Nach der Gartner Group stünden 40 Prozent davon vor dem wirtschaftlichen Aus. Das Resultat schlechter Vorsorgeplanung (einschließlich IT-Vorsorge) zeigt die Statistik in Abbildung 1.2.

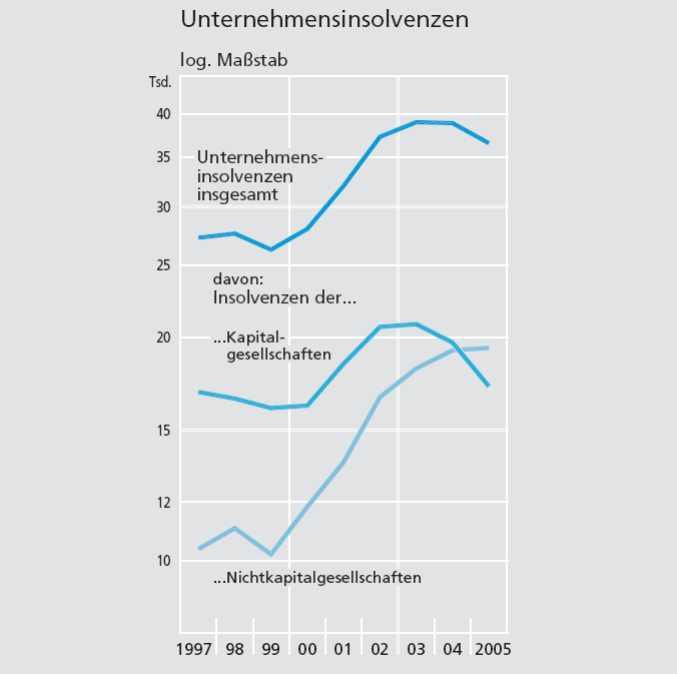


Abb. 1.2: Unternehmensinsolvenzen in Deutschland (Quelle: Deutsche Bundesbank)

Groß- und Kleinunternehmen sind in der Entwicklung einer Vorsorgementalität angesprochen. So geben zwar 90 Prozent der kleinen und mittleren Unternehmen an, auf ein funktionierendes Netzwerk und Emailverkehr wirtschaftlich angewiesen zu sein, aber nur bescheidene acht Prozent sehen darin einen Anlass, die Resistenz der IT gegen unvorhergesehene Ereignisse zu erhöhen – wohlwissend, dass selbst kleinere Defizite in diesem Bereich sich durch die Wertschöpfungskette fortsetzen können und Millionenverluste verursachen.[3] Die Dauer eines Ausfalls ist mitentscheidend. In vielen Organisationen ist ein Ausfall der gesamten Internetverbindung für 15 Minuten nicht gleich eine Katastrophe. Ein Ausfall, der den ganzen Tag dauert, kann schon gravierendere Folgen haben. Diese Sichtweise wird ein Aktienhändler, der Daytrading betreibt, nicht teilen, wenn er Wertpapiere innerhalb von 15 Minuten verkaufen muss. Ein Widerspruch findet sich auch beim Thema Datenverlust: Fast zwei Drittel aller Unternehmen werten Datenverlust als Ereignis mit „ernsten Folgen“[4], gleichzeitig planen aber nur 40 Prozent mit einer ausreichend langen Ausfallzeit[5]. Dem Test von Notfallplänen wird generell wenig Beachtung geschenkt, was die Anwendbarkeit im Ernstfall in Frage stellt.[6] Die Prioritäten operati-

[3] vgl. [Lei07]
[4] vgl. [Sym08]
[5] vgl. [Lei08]
[6] vgl. [Sid05] und Abbildung 4 in [Abe08]

ver Geschäftsprozesse harmonieren in vielen Fällen sehr gut mit dem zufriedenstellenden Gefühl, einen einmal angefertigten (theoretischen) Plan in der Schublade zu haben – oft zum Nachteil im Notfall.

Diese Diplomarbeit leistet einen Beitrag dazu, den Einstieg in das Thema Business Continuity Planning zu erleichtern und die Umsetzung von Notfallmaßnahmen erfolgreich zu gestalten. Aus dem Blickwinkel der IT geben die folgenden Kapitel wertvolle Definitionen und Abgrenzungen und greifen die Problemstellungen und Lösungswege einer individuellen Notfallvorsorge auf. Fokussiert wird ein umfassender Überblick über die zentralen Teilbereiche des Planungsprozesses (und ihrer Erfolgskriterien) und ein praktischer Einblick in das Krisenmanagement. Das Ziel besteht darin, durch Evaluation und Vergleich eine solide Basis zum Notfallmanagement zu erschaffen, die kritischen Faktoren des Prozesses hervorzuheben und gleichzeitig auf die Schwierigkeiten der meist geheimen, (weil) Unternehmen-individuellen Kontinuitätsmaßnahmen zu verweisen. Auf Aktualität wird dabei großen Wert gelegt, weswegen die Diplomarbeit auch eng an den neuen deutschen BSI-Standard 100-4 des Bundesamtes für Sicherheit in der Informationstechnik angelehnt ist.

In dem nun folgenden **Kapitel 2** wird erarbeitet, was Business Continuity Planning heutzutage bedeutet. Es wird gezeigt, wie von den verschiedenen Autoren und Institutionen des Notfallmanagements der Begriff definiert wird, ob es Unterschiede gibt und wo die Grenzen des Business Continuity gesehen werden. Begrifflichkeiten werden unter besonderer Berücksichtigung der deutschen Position abgegrenzt, für eine inhaltlich eindeutige Terminologie.

Kapitel 3 untersucht den Anwendungsdruck zur Notfallvorsorge. Es wird beschrieben, welche äußeren Zwänge zur Anwendung von Vorbereitungsmaßnahmen bestehen, wie sich diese ausdrücken und welche konkreten Pflichten damit für eine Organisation verbunden sind.

Die Aspekte des Business Continuity Planning sind in **Kapitel 4** unter die Lupe genommen. Dabei geht es um die verschiedenen Aufgaben, die jeder der drei Bereiche Personal, Technik und Organisation in sich trägt und welche besonderen Maßnahmen dabei zu beachten sind.

Dass die umfangreichen Vorbereitungen der Notfallplanung in einem zentralen Dokument, dem Notfallplan, zusammenfließen sollten, ist naheliegend. Wie dieser Business Continuity Plan aufgebaut ist, worauf dabei zu achten ist und welche Phasen der Erstellung dabei zu unterscheiden sind, wird in **Kapitel 5** beschrieben.

Auf die Hilfe von speziellen Werkzeugen kann mit steigender Unternehmensgröße nicht mehr verzichtet werden. **Kapitel 6** vergleicht unterschiedliche Alternativen, die den

praktischen Ablauf des Notfallmanagements in vielen Unternehmen unterstützen.

Kapitel 7 verfolgt anschließend einen praktisch-orientierten Ansatz. Die Informationen der vorangegangenen Kapitel werden aktiv verarbeitet und sind in einem beispielhaften Szenario eines fiktiven Kleinunternehmens wiederzufinden. Der Fokus liegt auf der Disaster Recovery – dem erfolgreichen Wiederanlauf und der Wiederherstellung nach einem Notfall-Ereignis.

Einige zusammenfassende Schlussfolgerungen sind in **Kapitel 8** dargestellt. Es werden einzelne Teile der Diplomarbeit aufgegriffen, die eine besondere Bedeutung innerhalb des Themas gewonnen haben. Ein Blick auf die zukünftigen Entwicklung im Business Continuity Planning schließt das Thema ab.

2 Definition und Abgrenzung

Business Continuity bezeichnet die (Überlebens-) Fähigkeit einer Institution, auf Notfälle angemessen zu reagieren um jederzeit ein vordefiniertes Maß an Geschäftsbetrieb aufrecht erhalten zu können[1]. Angelehnt an das Bundesamt für Sicherheit in der Informationstechnik (BSI)[2] sei für dieses Dokument festgelegt:

1. Als Institution gelten Unternehmen, Behörden und sonstige öffentliche oder private Organisationen.

2. Ein Notfall ist eine Situation in der wesentliche Bereiche, Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren und bei denen innerhalb der geforderten Zeit deren Verfügbarkeit nicht wieder hergestellt werden kann. Notfälle verursachen hohe Kosten für das Institut, können nicht im allgemeinen Tagesgeschäft abgewickelt werden und erfordern besondere Vorsorge.

Die Festlegung von angemessenen Reaktionsmaßnahmen und eines vordefinierten Geschäftlevels ist eine Aufgabe der strategischen Geschäftsleitung[3], welche ein besonderes Interesse an einem kontinuierlichen Dienstleistungsangebot des Instituts hat[4]. Als funktionsübergreifende Managementaufgabe betrachtet Business Continuity eine Institution stets als Ganzes und ist für eine erfolgreiche Durchführung auf einen Prioritätsstatus angewiesen. Die zentrale Aufgabe des Business Continuity ist die Vorsorge und Planung zur Bewältigung von Notfällen - das Notfallmanagement oder Business Continuity Planning (BCP).

Im Folgenden werden die BCP-Definitionen von vier der bedeutensten Akteure und Interessensgruppen auf diesem Gebiet vorgestellt, darunter zwei amerikanische Vertreter, das Business Continuity Institute[5] (BCI) und das Disaster Recovery Institute International[6] (DRII), die britische Normungsorganisation British Standards Institution[7] (BSI (brit.)) sowie das zuvor erwähnte deutsche Bundesamt BSI.

---

[1] vgl. [Bri06] und „Business Continuity“ in [Dis07]
[2] Internetadresse: `http://www.bsi.de`
[3] vgl. [Bri06]
[4] [Dis07]
[5] Internetadresse: `http://www.thebci.org`
[6] Internetadresse: `http://www.drii.org`
[7] Internetadresse: `http://www.bsi-global.com`

Das BCI erklärt, „*[Business Continuity Management Planning[8] are] the advance planning and preparations that are necessary to identify the impact of potential losses; to formulate and implement viable recovery strategies; to develop recovery plan(s) which ensure continuity of organisational services in the event of an E/I/C [Emergency, Incident, Crisis]; and to deliver a comprehensive training, testing and maintenance programme.*“[9]

Das DRII formuliert es anders und sieht BCP als „*Process of developing and documenting arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period of time and return to performing its critical functions after an interruption.*“[10]

Das Disaster Recovery Institute International beschreibt Business Continuity Planning als einen Prozess der Erarbeitung von Reaktionsmaßnahmen auf geschäftsunterbrechende Ereignisse und betont dabei insbesondere den zeitkritischen Aspekt solcher Ereignisse. Detailierter auf die Durchführung dieses Prozesses ausgerichtet liest sich die BCI Definition. Sie spricht die einzelnen Phasen der Erstellung eines Business Continuity Plans an und konzentriert sich dabei auf den Managementgedanken im Hintergrund.

Aufbauend auf den Definitionen des BCI und DRII entwickelte die British Standards Institution eine eigene Definition des Terms Business Continuity Plan mit der Absicht, die wesentlichen Gedanken beider Versionen in einer prägnanten und aktuellen Definition zu vereinen. Deren Entwurf des Standards BS 25999-2 Business continuity management – Part 2: Specification, veröffentlicht im Juni 2007, enthielt in Folge dieser Bemühungen folgende Definition:

„*[A Business Continuity Plan is a] documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical activities at an acceptable pre-defined level.*“[11]

Ein genauer Blick auf diese Formulierung zeigt, welchen Einfluss die beiden Organisationen auf den Britischen Standard haben und greift die wichtigen Punkte der Definition auf:

„*[A BCP is a] documented collection of procedures and information that is developed, compiled and maintained ...* “ – Ein BC Plan enthält wertvolle Informationen und beschreibt detailiert geplante Maßnahmen, die in kritischen Situationen Schaden vermindern und die Geschäftsfähigkeit des Unternehmens sichern sollen. Dieser Plan wird

[8] entspricht Business Continuity Planning, siehe auch Abschnitt 2.2
[9] [Bus]
[10] [Dis07]
[11] [Bri07]

durch einen permanenten Revisionsprozess aktuell gehalten. BCI und DRII unterstützen diesen Ansatz, berücksichtigen sie doch beide den Planung- und Dokumentationsprozess in ihren Definitionen.

„*... in readiness for use in an incident ...* " – Ein Hauptargument für BCP ist die Fähigkeit eines Unternehmens, in einem Notfall angemessen reagieren zu können. Das DRII spricht in diesem Zusammenhang allgemein von Events, das BCI diversifiziert diese mit dem Akronym E/I/C (Emergency, Incident, Crisis) und betont damit die Berücksichtigung aller Arten von Ereignissen und die damit einhergehenden Unterschiede im zeitlichen Ausmaß. Weitreichenden Katastrophen, die kaum von einer Institution selbstständig behoben werden können, beispielsweise Naturkatastrophen, Seuchen oder intelligente Computerviren, im Gegensatz zu kleineren, geschäftsbeeinträchtigenden Situationen, z.B. Datenverlust durch Stromausfall, bewegen sich in einem zeitlich unterschiedlichen Rahmen zur Wiederherstellung des Normalbetriebs und benötigen ebenso unterschiedliche Maßnahmen.

„*... to enable an organization to continue to deliver its critical activities at an acceptable pre-defined level.*" – Die Kontinuität kritischer Geschäftsprozesse wird sowohl vom DRII („*return to performing critical functions*") als auch vom BCI („*ensure continuity of organisational services*") als Ziel definiert. Interessant zu erkennen ist die Entwicklung, die dieser letzte Abschnitt der Definition seit dem Release des ersten Teils des DPC[12] BS 25999 Standards Code of practice for business continuity management[13] – etwa ein Jahr zuvor im Juni 2006 – vollzogen hat: der vorherige Wortlaut „*[...] to continue to deliver its products and services*" wurde ersetzt durch „*[...] its critical activities at an acceptable pre-defined level*" Damit wird nicht nur die Kundenorientierung („*products and services*") um einen mehr ganzheitlichen Blickwinkel („*activities*") erweitert, die Formulierung unterstreicht auch die Planungsnotwendigkeit einer angemessenen Reaktion.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik definiert in der aktuellen Entwurfsversion 0.7 des neuen deutschen BSI-Standard 100-4 Notfallmanagement (auch betriebliches Kontinuitätsmanagement genannt) als Oberbegriff für die zwei (zeitlich-abhängigen) Teilbereiche Notfallvorsorge und Krisenmanagement (auch Notfallbehandlung genannt). Auf die Vorsorgemaßnahmen während des Normalbetriebs geht der Entwurf zum aktuellen Zeitpunkt nicht ein. Das Krisenmanagement wird beschrieben und beginnt mit dem Eintreten des Notfalls (Abbildung 2.1): Nach der Eskalation werden Sofortmaßnahmen ergriffen und der Wiederanlauf gestartet. Erst im etablierten Notbetrieb beginnt die Wiederherstellung des Normalbetriebs, der das Krisenmanagement beendet. Das Business Continuity Management (BCM) definiert das BSI als „*ganzheitliche[n] Managementprozess zur Fortführung der kritischen Geschäftsprozesse*

[12] Draft for Public Comment
[13] [Bri06]

bei Eintritt eines Notfalls“. Diese Definition wird dem deutschen Begriff Notfallmanagement zugeordnet.

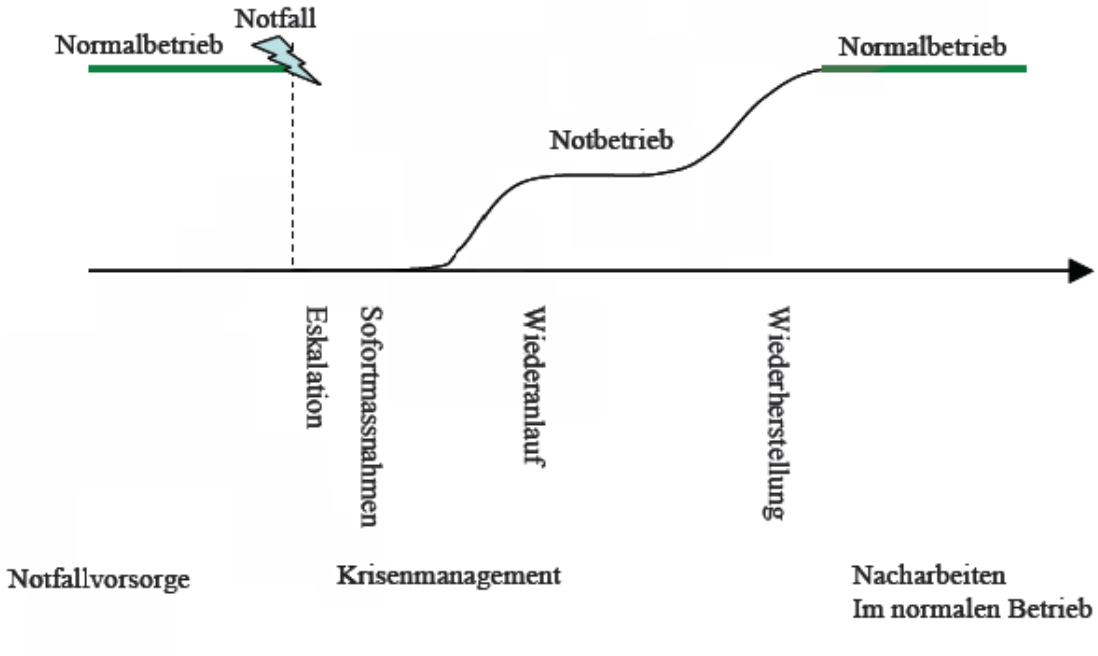


Abb. 2.1: Aufbau des Notfallmanagements im BSI-Standard 100-4 (Quelle: [Bun08])

Neben diesen Formulierungen finden sich in Büchern der Fachliteratur zahlreiche weitere von Autoren wie Susan Snedaker oder O'Hehir, die BCP betrachten als „*[...] methodology used to create and validate a plan [...]*“[14] mit dem Ziel Maßnahmen vorzubereiten „*[...] to ensure the survival of the organization in times of business disruption*“[15]. Festzustellen ist, dass die genannten Definitionen sich nur im Wortlaut unterscheiden. Alle Formulierungen betrachten das gleiche Thema und nur die eingenommene Position zwischen Detail und Abstraktion macht den Unterschied zwischen zwei Definitionen aus.

Für die weiteren Ausführung soll in Anlehnung an den deutschen Standard zum Notfallmanagement Folgendes festgelegt sein: Business Continuity Management und Notfallmanagement werden als Synonyme genutzt. Wird von „*Notfall*“ gesprochen, so sei auch immer „*Krise*“ und „*Katastrophe*“ als Steigerung eines Notfalls gemeint. Die Beziehung zwischen BCM und BCP soll in einem weiteren Abschnitt untersucht werden.

[14] [Sne07], S. 3
[15] [O'H07], S. 27

2.1 Business Continuity Planning und Disaster Recovery

Im Englischen entspricht der Begriff „*Contingeny Planning*“ (CP) dem, was im Deutschen als „*Notfallmanagement*“ bezeichnet wird[16]. BCP, die „*Incident Response*“ (IR) und „*Disaster Recovery*“ (DR) sind untergeordnete Teilaufgaben des CP. Für IR und DR sei Folgendes definiert[17]:

1. „*[The incident response is] the response of an organization to a disaster or other significant event that may significantly impact the organization, its people, or its ability to function productively*“
2. „*[Disaster Recovery is] the ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.*“

Abbildung 2.2 zeigt die zeitliche Anordnung dieser Aufgabenbereiche, die sich direkt aus den Definitionen ableiten lässt:

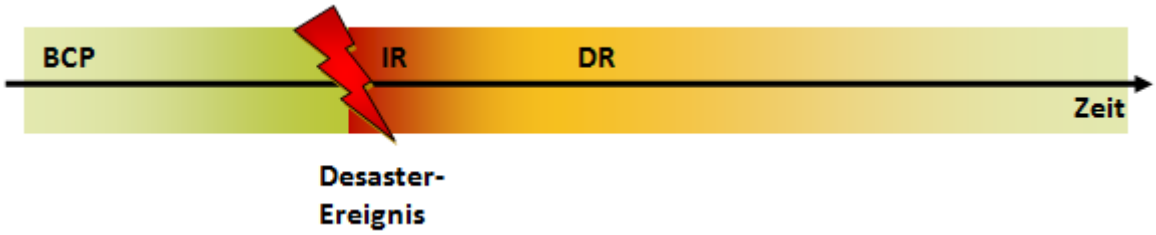


Abb. 2.2: Desaster unterbrechen die Notfallvorsorge und müssen durch Sofort- (IR) und Wiederherstellungsmaßnahmen (DR) in den Ausgangszustand gebracht werden. (Quelle: Eigendarstellung)

BCP und DR sind eng miteinander verbunden, liegen aber in der Abbildung auf verschiedenen Seiten einer Desaster-Situation. Als Desaster gilt jedes plötzlich auftretendes Ereignis, dass die Fähigkeit einer Institution zur Aufrechterhaltung von kritischen Funktionen, Prozessen oder Diensten über einen inakzeptabel langen Zeitraum beeinträchtigt[18]. BCP und DR teilen das gemeinsame Ziel, durch die Aufrechterhaltung solcher kritischen Geschäftsprozesse wirtschaftliche Schäden auf ein Minimum zu reduzieren. Wie der vorherige Abschnitt gezeigt hat, beschäftigt sich BCP dabei mit der Notfallvorsorge und ist proaktiv. Die IR, also Sofortmaßnahmen direkt nach dem Eintreten eines

[16] siehe [Rüd08] und [Dis07]
[17] [Dis07]
[18] [Dis07]

Desasters, und die Disaster Recovery sind reaktiv und folgen unter optimalen Bedingungen nur den Instruktionen des vorbereiteten Plans.

Disaster Recovery ist ein zentraler Wiederherstellungsprozess während und nach einem Desaster. Die Literatur ist unentschlossen, ob es der einzige ist. [Mic07] schreibt, dass obwohl Backup-Strategien ein integraler Teil eines DR Plans sind, gehört das gesamte Spektrum an Wiederherstellungsaktivitäten zu Disaster Recovery [19]. [Dou01] hingegen bezeichnet das Disaster Recovery Planning (DRP) als den technologischen Aspekt des BCP[20]. Er nennt Business Resumption Planning (BRP) („*the operational piece*“) als Komplement zu DRP, welche zusammen die Planungsaufgaben abdecken, die im Rahmen der Notfallplanung notwendig sind. Auch das DRII sieht DRP als die „*technische Komponente*“ des BCP an[21]. Das BCI verweist von DR direkt auf „*Information Technology Disaster Recovery*“ (ITDR) und definiert es als Teil eines BC Plans „*to recover and restore [...] IT and telecommunications capabilities after an E/I/C*“. Weitere Quellen[22] unterstützen die Sichtweise, dass Disaster Recovery eine ausschließlich technische Ausrichtung besitzt und wesentliche Planungen des BCP nicht integriert.

Ich denke Folgendes ist möglich: Business Continuity Planning, Incident Response und Disaster Recovery stehen einer zeitlichen Abhängigkeit wie in der oberen Abbildung ABC dargestellt. Das BCP übernimmt in Anlehnung an die Bezeichnung im BSI-Standard 100-4 die Notfallvorsorge. Dazu zählt zum einen das DRP, welches sich mit der Planung der Wiederherstellung von Daten und IT- / Netzwerkinfrastrukturen beschäftigen soll, zum anderen das BRP als Oberbegriff für alle anderen Aufgaben, die im Rahmen des BCP bearbeitet werden müssen und nicht zum DRP zählen. Der gesamte Prozess (BCP) orientiert sich an und priorisiert die kritischen Geschäftsfunktionen (Prozesse, Dienste) einer Institution.

Tritt ein Desaster ein, so werden die ersten Minuten der Sofortmaßnahmen als Incident Response bezeichnet. Neben Evakuierungen u.Ä. gehört die Aktivierung des Notfallplans zur IR. Die darauf folgende Phase wird als Disaster Recovery bezeichnet und stellt unter Zuhilfenahme des DR Plans den Wiederanlauf der Geschäftsaktivitäten her. Sollte ein Desaster einen Umfang haben, dass die Fähigkeiten des DR Plans übersteigt, so wird für eine kompletten Wiederherstellung in der gleichen Phase der Business Recovery / Resumption Plan initiiert. Spätestens mit der Aufnahme des Normalbetriebs ist die Disaster Recovery Phase beendet.

Im Hinblick auf das deutsche Vokabular soll zusätzlich gelten: Der Notfallbehandlung / dem Krisenmanagement seien die Aufgaben der IR und DR gleichgesetzt, wobei die IR

[19] [Mic07], S. 160
[20] „Introduction“, S. XII
[21] [Dis07]
[22] siehe bspw. [Dav] und [Coo]

alle Sofortmaßnahmen übernimmt und während der DR der Wiederanlauf zum Notbetrieb sowie die Wiederherstellung des Normalbetriebs umgesetzt wird.

2.2 Business Continuity Planning und Business Continuity Management

Neben BCP ist Business Continuity Management (BCM) ein häufig genutzter Begriff. BCM ist definiert als „*holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.*“[23]

Vergleicht man diese Definition mit den Definitionen von BCP, so können deutliche Parallelen aufgezeigt werden, sowohl in der Art (Prozess), der Aufgabe (Aufbau eines Frameworks mittels Planung und Dokumentation) und dem Ziel (Krisensicherheit). Daraus folgt, dass BCP und BCM die gleiche Funktion erfüllen und somit synonym verwendet werden können. Auch das BCI unterstützt diese Ansicht und kombiniert beides zu einer Definition von Business Continuity Management Planning.

Das DRII geht noch einen anderen Weg und hält an einem Zusatz zur o.g. Definition des britischen Standards[24] fest. Dieser besagt u.a., dass BCM auch „*the management of recovery or continuity in the event of a disaster*“ ist. Diese Auslegung erstreckt den Umfang von BCM über den Bereich, den wir zuvor als Disaster Recovery (inkl. Incident Response) festgelegt haben – und setzt es so mit Contingency Planning gleich (Abbildung 2.3).

Es ist wichtig, eine Entscheidung für die Begriffseindeutigkeit zu treffen. Für die weiteren Ausführungen soll folgendes gelten: Auf Grund der Definitionsähnlichkeit von BCP und BCM auf Basis des Vergleichs von BS 25999 (brit. Standard, zukünftig möglicherweise internationaler Standard[25]) und den Definitionen des BCI[26] soll unter BCP und BCM dasselbe verstanden werden. Der Begriff BCM kann insbesondere dazu genutzt werden, die Bedeutung des kontinuierlichen Steuerungsprozesses von BCP zu betonen. Da die Definitionen und Erläuterung Business Continuity Planning bereits mehrfach als einen solchen Prozess (und nicht einmaligen Aufwand) beschrieben haben, wird in der weiteren Arbeit zum besseren Verständnis ausschießlich von BCP gesprochen.

[23] [Bri07]
[24] Entwurfsversion
[25] [Häm]
[26] Vereinigung professioneller BC-Experten

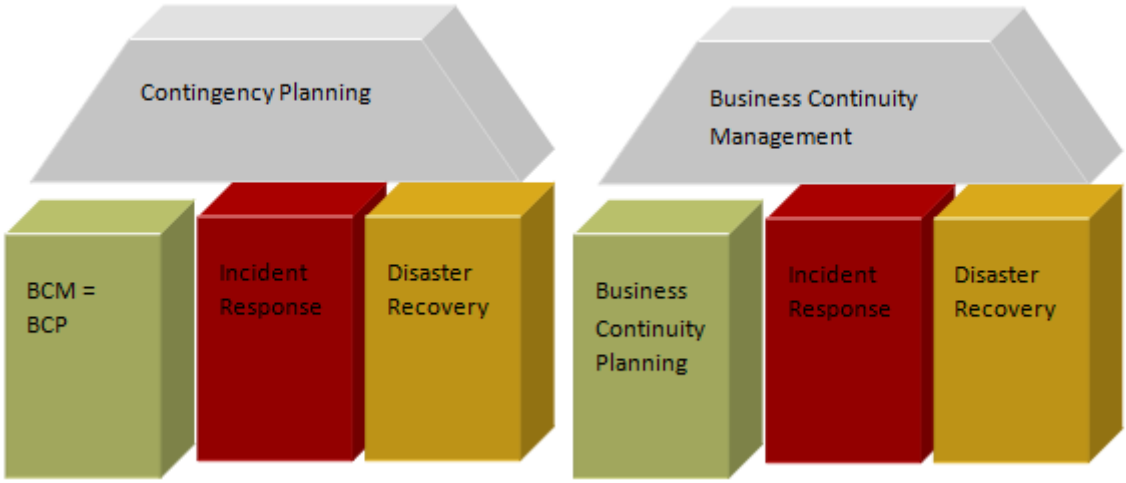


Abb. 2.3: Die Stellung von BCM zu BCP (Quelle: Eigendarstellung)

2.3 Business Continuity Planning und Notfallmanagement

In den USA und in Großbritannien ist Business Continuity bereits seit längerem ein etabliertes Thema. Die ersten Entwicklungen begangen bereits in den 50er Jahren und die zuvor zitierten BCI und DRII beschäftigen sich seit 14 Jahren, respektive 20 Jahren, mit diesen Fragestellungen. Eine Großzahl von Referenzwerken besteht nur in englischer Sprache. Spätestens aber seit der Hochwasserkatastrophe in Dresden 2002 oder den Anschlägen in London[27], Madrid[28] und New York[29] ist das Interesse an diesem Thema bei deutschen Managern erheblich gewachsen, die seit Januar 2008 auf den ersten eigenständigen deutschen Standard zum Notfallmanagement zurückgreifen können[30]. Neben Definitionen für verschiedene Arten von Geschäftsunterbrechungen – Störung, Notfall, Krise und Katastrophe – gibt das BSI den anfangs dargestellten formalen Aufbau des Notfallmanagements vor (siehe Abbildung 2.1, Seite 9). Bis auf die Gleichsetzung von Business Continuity Management und Notfallmanagement bleibt ein Abgleich des deutschen mit dem englischen Vokabular dem Dokument zum jetztigen Zeitpunkt vorenthalten. Eine Überlegung zu dieser Situation möchte ich im Folgenden darlegen:

Wenn gilt, was bisher festgestellt und/oder definiert wurde, d.h.

[27] Londoner U-Bahn Bombe in 2005, siehe [Krö]
[28] Madrider Zuganschläge in 2004, [Wag08]
[29] Anschläge auf das World Trade Center in New York und das Pentagon in 2001, [Sue01]
[30] Seit Februar 2008 nach einer ersten Überarbeitung in der Version 0.7 verfügbar, siehe [Bun08]

1. „*Contingency Planning*“ bedeutet „*Notfallmanagement*“ und
2. „*Notfallmanagement*“ bedeutet „*Business Continuity Management*“ und
3. „*Business Continuity Management*“ ist „*Business Continuity Planning*“

dann folgt daraus, dass BCP = BCM = CP = Notfallmanagement. Wenn man zudem und angelehnt an den BSI-Standard 100-4 annimmt, dass sich ein Notfallmanagement immer in eine Planungsaufgabe (Vorsorge, Vorbereitung, Planung) und eine Aktionsaufgabe (Notfallbehandlung, Einsatz und Durchführung des Plans) unterteilt, dann ergibt sich eine Situation wie in der unteren Abbildung 2.4 dargestellt.

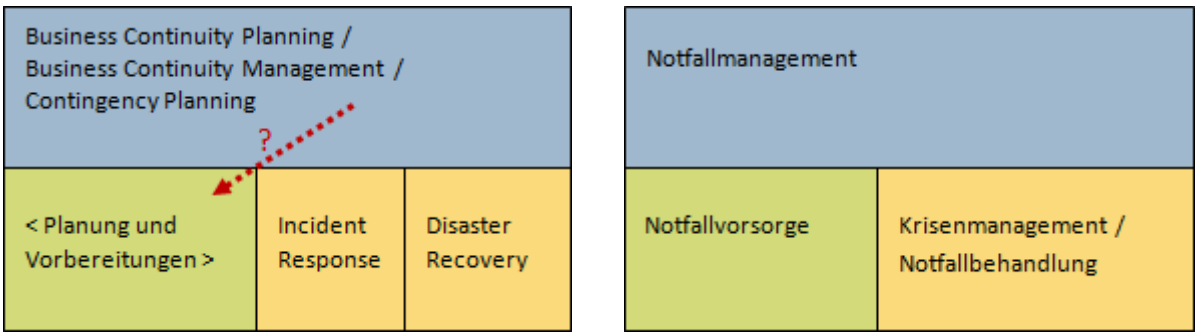


Abb. 2.4: Wie können die engl. Begriffe (links) den deutschen Begriffen (rechts) eindeutig zugeordnet werden? (Quelle: Eigendarstellung)

Es entsteht also eine gewisse Problematik, wie die Planungsaufgabe des BCP formal bezeichnet werden soll, um das „*Notfallmanagement*“ und das „*Business Continuity Planning*“ konfliktfrei zu verbinden. Ich schlage daher folgendes vor: BCP, BCM und CP können synonym für das deutsche „*Notfallmanagement*“ benutzt werden. Bei der Übersetzung von „*Notfallvorsorge*“ können jedoch verschiedene Schwerpunkte ausgedrückt werden. BCP und CP betonen gleichermaßen die Planungs- und Vorbereitungsaufgaben. Der Begriff BCM kann insbesondere dazu genutzt werden, die Bedeutung des kontinuierlichen Steuerungsprozesses von BCP zu betonen. Da die Definitionen und Erläuterung in dieser Arbeit bereits mehrfach Business Continuity Planning als einen solchen Prozess (und nicht einmaligen Aufwand) beschrieben haben, wird in der weiteren Arbeit zum besseren Verständnis ausschießlich von BCP für die Notfallvorsorge und von Contingency Planning für das Notfallmanagement gesprochen (Abbildung 2.5).

2.4 Contingency Planning und Risk Management

Das Verhältnis zwischen Contingency Planning und Risk Management (RM) entwickelt sich in einem organisatorischen Umfeld, in dem traditionelle Vorgehensweisen mit modernen Sichtweisen konfrontiert werden. Die relative Stellung beider Disziplinen zueinander

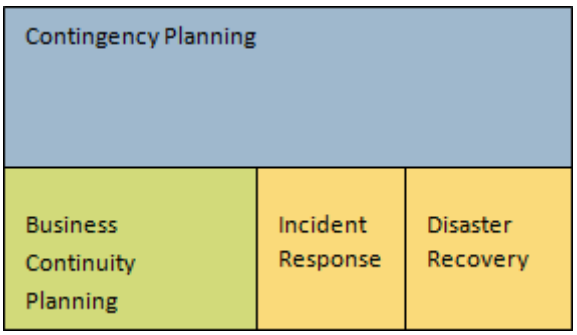


Abb. 2.5: BCP als Teil des Contingency Planning (Quelle: Eigendarstellung)

muss spätestens bei der Einführung eines Notfallmanagements festgelegt werden. Dabei gibt es drei verschiedene Sichtweisen[31]:

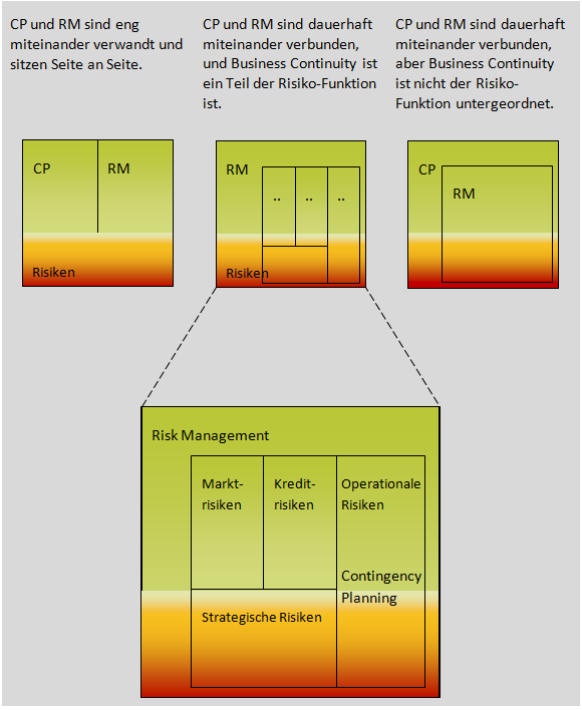


Abb. 2.6: Die relative Stellung des Contingency Planning (Quelle: Eigendarstellung)

Wie die obere Abbildung 2.6 zeigt, können CP und RM sowohl nebeneinander als auch in einer Hierarchie angeordnet sein. Risk Management ist definiert als „*process of identifying risks, evaluating their potential consequences and determining the most effective methods of controlling them or of responding to them [...] to reduce the frequency of risk*

[31] vgl. [McC04] und [Gal03]

events occurring [...] and to minimize the severity of their consequences [...]", wobei diese Risiken entweder als Markt-, Kredit- und operationale Risiken[32] oder als strategische und operationale Risiken klassifiziert werden können. So argumentiert [Gal03] beispielsweise, dass das Contingency Planning hauptsächlich von den operationalen Risiken des RM beeinflusst werde und ordnet es somit dem Risk Management unter.

Um eine begründete Entscheidung über die relative Stellung zu treffen, muss auf die Funktionen und Ziele von RM und CP geschaut werden. Abbildung 2.7 stellt die wichtigsten Merkmale beider Disziplinen gegenüber. Zwei dieser Unterschiede sind dabei besonders hervorzuheben:

1. Während sich das Risk Management generell alle Arten von Risiken analysiert, die die Geschäftsziele beeinflussen können, behandelt das Continuity Planning nur solche, die eine erhebliche Unterbrechung eines kritischen Geschäftsprozesses bedeuten können.

2. Während sich das Risk Management neben dem Ausmaß eines Ereignisses die Wahrscheinlichkeit seines Eintretens analysiert, konzentriert sich das Continuity Planning an Stelle der Wahrscheinlichkeit auf die zeitliche Dauer eines Vorfalls, die das Bestehen eines kritischen Prozesses oder im Extremfall die Existenz einer Institution gefährdet.

Die uneingeschränkte Betrachtung aller Arten und Größen von Risiken der Geschäftsziele durch das RM, einschließlich jener, welche auch vom CP behandelt werden, führt zu der Ansicht, das CP als Teil des RM unterordnen zu müssen. In [Gal03] vertritt Andrew McCrackan die interessante Meinung, dass diese Ansicht als generelles Missverständnis der Funktion von Business Continuity (BC) zu sehen ist. Dies ist ansatzweise in einer falschen Erweiterung der Risk Management Aktivitäten zu begründen, der größte Fehler liegt aber in Auffassung von Business Continuity als Neuerfindung alter Disaster Recovery Funktionen, laut McCrackan. Er argumentiert weiter, dass Experten, die bereits die Zeiten der Vorgänger des modernen Business Continuity miterlebt haben, Disaster Recovery, Emergency Planning und Co. nur als Maßnahmen für spezielle Risikotypen kennen. Aus diesem Blickwinkel sei es nicht unverständlich zu glauben, dass BC ein Teil von Risk Management ist.

RM kann entweder Teil eines durchgehenden Geschäftsprozesses sein oder eine übergeordnete Funktion, die auf die Bedrohungen der Ausführung dieses Prozesses ausgerichtet ist. Zwei Beispiele:

1. Kurssicherungsgeschäfte[33], z.B. Wechselkurs-Hedging oder Rohstoff-Hedging ist Teil des Wirtschaftsgeschäfts und hat mit Contingency Planning wenig zu tun. Es

[32] [Bas04]
[33] engl. Hedging

	Risk Management	Business Continuity Management
Key method	Risk Analysis	Business Impact Analysis
Key parameters	Impact & Probability	Impact and Time
Type of incident	All types of events - though usually segmented	Events causing significant business disruption to critical services and capabilities
Size of events	All sizes (costs) of events - though usually segmented	For strategy planning: "survival" threatening incidents only
Scope	Focus primarily on risks to core-business objectives	Mostly outside the core competencies of the business
Intensity	All from gradual to sudden	Sudden or rapid events (though response may also be appropriate if a creeping incident becomes severe)

Abb. 2.7: Risk Management und Contingency Planning im Vergleich (Quelle: [Roy08])

ist Risk Management. Das Contingency Planning stellt die Fähigkeit des Unternehmens sicher, die Funktion „Kurssicherungsgeschäft" weiter ausführen zu können. Damit sind eine Vielzahl von Risiken verbunden, die analysiert werden müssen. Dies übernimmt der Risk Management Aspekt innerhalb des Contingency Planning.

2. Die Risiken von Betrug und Unterschlagung[34] können durch das Risk Management (Analyse des Geschäftsprozesses) identifiziert werden und durch die Implementierung von Kontrollsystemen behandelt werden. Ein möglicher Ausfall dieser Systeme liegt jedoch im Bereich des Contingency Planning.

Das Fehlen einer klaren Definition des funktionalen Umfangs von RM und BCM[35] ist die Wurzel der anhaltenden Argumentationen auf diesem Gebiet. Im Allgemeinen ist Risk Management dann eine Funktion des Contingency Planning, wenn es um die Risiken (z.B. Ausfall, Verlust) von Besitz, Personal oder sonstigen Ressourcen geht, auf die das Unternehmen zur Existenzsicherung angewiesen ist. Die RM Funktion innerhalb des CP identifiziert und evaluiert diese Risiken und ergreift entsprechende Maßnahmen. Diese

[34] engl. Fraud
[35] vgl. [Roy08]

Betrachtungsweise führt zu der Schlussfolgerung, dass Contingency Planning nicht dem Risikomanagement untergeordnet werden sollte.

RM und CP sind zwei komplementäre Disziplinen. Ob sie auf einer Stufe stehen oder ob die RM Funktion innerhalb von Contingency Planning stärker zu werten ist als der größere Umfang des RM, der sich auch mit den alltäglichen Risiken der Geschäftsleitung befasst, muss jede Institution im Rahmen von Rollen- und Verantwortlichkeitsdefinitionen individuell beantworten.

Für den weiteren Verlauf dieser Arbeit lege ich Folgendes fest: Wie in Abbildung 2.8 dargestellt, sei das IT Contingency Planning (ITCP) Teil des IT Risk Managements (ITRM). Information Security (IS) ist ein zweiter Teil des ITRM auf der selben Ebene wie das ITCP steht. Es beschäftigt sich mit den täglichen IT-Risiken des operativen Geschäfts. IS und ITCP überschneiden sich dann in ihren Verantwortlichkeiten, falls ein schleichender Vorfall ein bedrohliches Ausmaß annimmt.

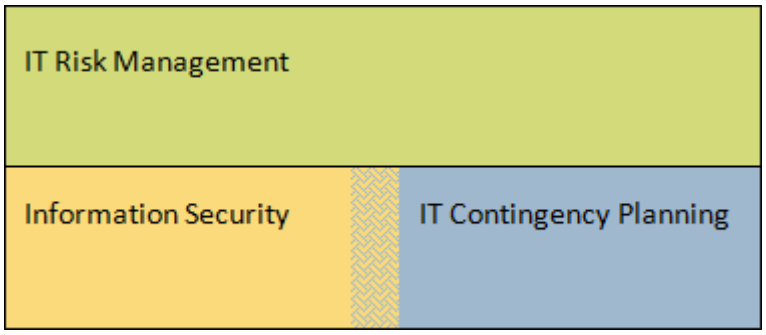


Abb. 2.8: IT Contingency Planning als Teil des IT Risk Managements (Quelle: Eigendarstellung)

2.5 Schlussfolgerung

Abbildung 2.9 fasst die besprochenen Begriffe der vorherigen Abschnitte in einer Übersicht zusammen. Die Diplomarbeit wird sich in den nachfolgenden Teilen auf den informationstechnischen Aspekt des BCP konzentrieren. Hervorgehoben ist daher die Eingliederung des Contingency Planning in das IT Risk Management. Das CP behandelt in dieser Taxonomie alle Risiken, die vom ITRM nicht vermieden werden können und welche eine Gefahr von technischer Seite für die kritischen Geschäftsprozesse einer Institution darstellen. Untergliedert ist es in die eigentliche Planungsphase, das BCP, welches alle Aufgaben der Notfallvorsorge und -planung übernimmt, und die Aktionsphasen Incident Response und Disaster Recovery, welche für die Sofortmaßnahmen (IR) und die

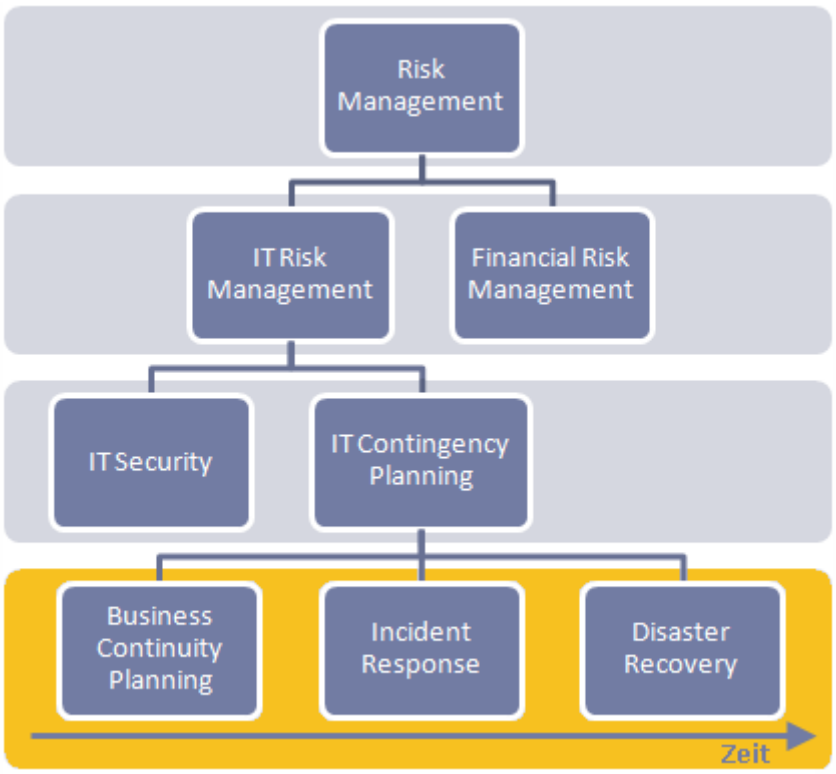


Abb. 2.9: Die Taxonomie des BCP (Quelle: Eigendarstellung)

Durchführung der Notfallpläne (DR) verantwortlich sind.

Der zeitliche Ablauf der Aktionsphase veranschaulicht Abbildung 2.10: Die IR greift sofort nach Eintritt eines Desasters und löst u.a. den DRP aus. Unterscheidet man DRP und BCP, wie bspw. in [Mic07], so wird nachfolgend der BCP aktiviert „*when the scope or scale of a disaster exceeds the ability of the DRP to restore operations*“[36] Der Abgleich mit den deutschen Begriffen des BSI-Standards 100-4 gilt wie zuvor beschrieben. Notfallmanagement wird als Alternativbegriff zu Contingency Planning genutzt werden.

Die Notfallplanung ist ein geschäftsgesteuerter Prozess, der ein weites Spektrum von Managementdisziplinen in sich vereint (Abbildung 2.11 auf Seite 21). Der Ausfall von Schlüsselzulieferern oder Hauptabnehmern, industrielle Auseinandersetzungen, die zu Ressourcenmangel führen, der Verlust von Führungspersonal und sonstigen Fachkräften, infektiöse Epidemien, Missbrauch, Erpressungen, Umweltverschmutzung und Rufbeschädigung sind nur einige der Aspekte, die im Contingency Planning berücksichtigt werden

[36] [Mic07], S. 160

Abb. 2.10: Die Pläne der IR, DR und des BC greifen geordnet ineinander. (Quelle: Eigendarstellung)

müssen[37]. Ein Unternehmen muss fähig sein, sowohl auf externe Umstände (z.B. Flut, Stromausfall, Sabotage, Terrorismus), welche den Verlust von Teilen des Unternehmens bis hin zur gesamten operativen Einsatzfähigkeit bedeuten können, als auch auf interne Situationen – unabsichtliche (z.B. versehentliches Löschen wichtiger Unternehmensdaten) und absichtliche (z.B. Brandstiftung durch verärgerte Mitarbeiter) – angemessen reagieren zu können. Nur komplett integriert in ein Unternehmen, eine Behörde oder eine sonstige Organisation und unterstützt von der Geschäftsführung können dauerhaft diese Aufgaben erfüllt und ein aktueller und zielgerichteter Business Continuity Plan aufrecht erhalten werden. Die Entwicklung einer „*Kontinuitätskultur*“ ist dabei ebenso wichtig wie die Erarbeitung des eigentlichen Plans.

Ansporn für ein erfolgreiches IT-BCP – die Aufrechterhaltung der operationalen Kernprozesse – ist die Verantwortung der Unternehmensleitung für das langfristige Interesse von Mitarbeitern, Kunden und weiterer Stakeholder. Denn auch wenn es annähernd möglich ist, die finanziellen Verluste einer (Zer-)Störung im Vorfeld zu kalkulieren, sind die größten Auswirkungen eines schlecht behandelten Vorfalls meist im angeschlagenen Ruf des Unternehmens und im Vertrauensverlust auf Kundenseite zu finden. Der Schutz von Image und Markenname kann dabei weder durch internes noch externes Sourcing versichert werden. Umgekehrt hingegen kann eine gut durchgeführte Vorfallbehandlung den Ruf von Organisation und Management verbessern.

ITCP bedeutet nicht nur Kosten, sondern Wertsteigerung. Effektives CP ist Teil einer

[37] siehe [Hil07a], S. 484

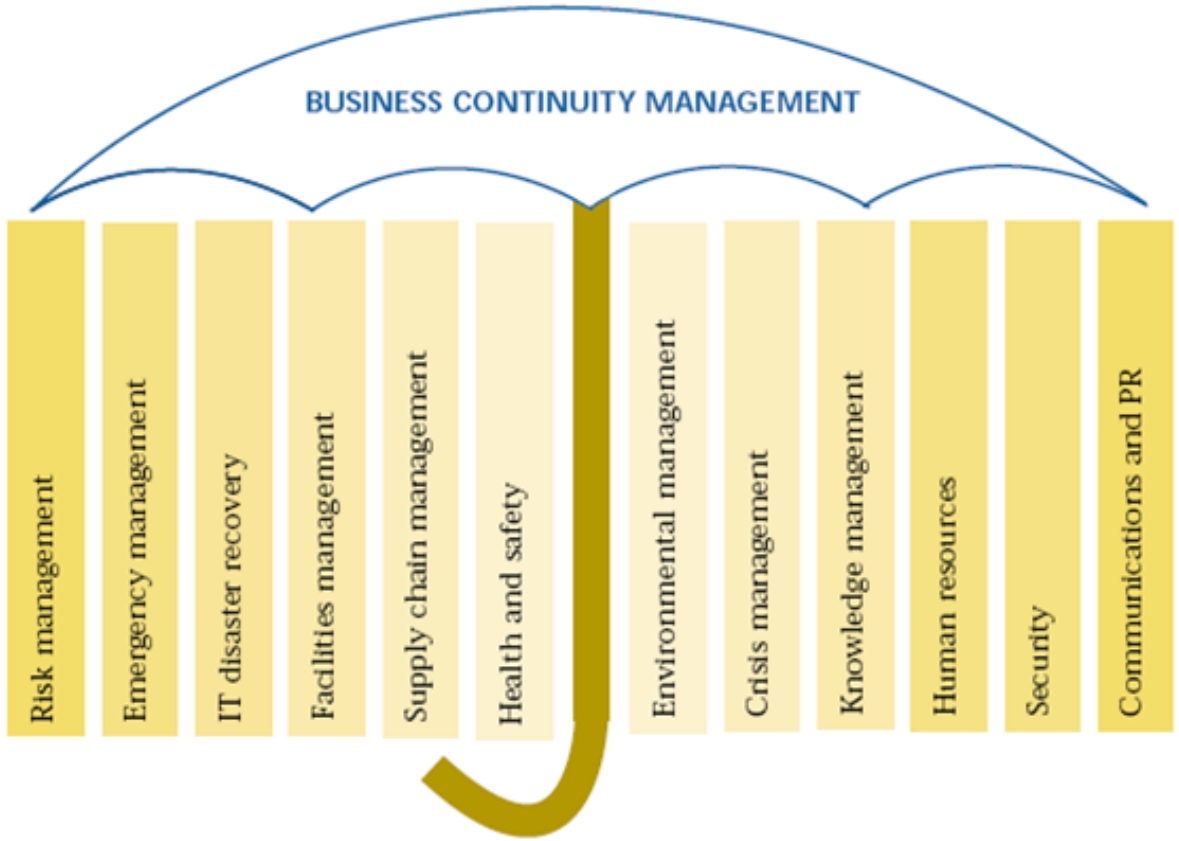


Abb. 2.11: Notfallmanagement als ein übergreifender Prozess mit vielen Disziplinen (Quelle: [Smi03])

dauerhaft erfolgreichen Unternehmensstrategie und optimiert als Value Based Management (VBM) Prozess[38] jederzeit die Kosteneffizienz. Manche Geschäftsführer erkennen dies nicht und setzen Contingency Planning auf die Liste der Nice-to-have Extras. „*Wir hatte noch nie einen solchen Notfall, also wir brauchen kein Notfallmanagement*“ lautet der Irrglaube. Die Diplomarbeit soll ihren Teil dazu beitragen, die Notwendigkeit einer angemessener Notfallplanung zu unterstreichen und Hilfestellungen in den praktischen Fragen der Umsetzung zu geben.

[38] siehe [Bus02]

3 Forderung nach Contingency Planning in Gesetzen und Standards

Jedes Unternehmen agiert in einem Rahmen, der von zahlreichen gesetzlichen und regulatorischen Vorgaben geprägt ist. Dieses Faktum ist unabhängig von der geografischen Lage und führt zu der wertvollen, wenn auch trivialen Einsicht: Die Nichtbeachtung relevanter Gesetze geht stets strafrechtlichen Reaktionen voraus. Der Umfang solcher Reaktionen basiert stets auf dem individuellen Fall und ist bis zu einem gewissen Punkt finanziell im Vorfeld einzuschätzen; beim Verhalten von Stakeholdern, insbesondere Kunden, sind gute Vorhersagen eine seltene Ressource und Image oder Markenname stehen schnell auf dem Spiel. Dieses Kapitel untersucht, inwieweit Contingency Planning (CP) in gesetzlichen Vorschriften verankert ist und zeigt einige Beispiele auf, die in der Planung beachtet werden müssen.

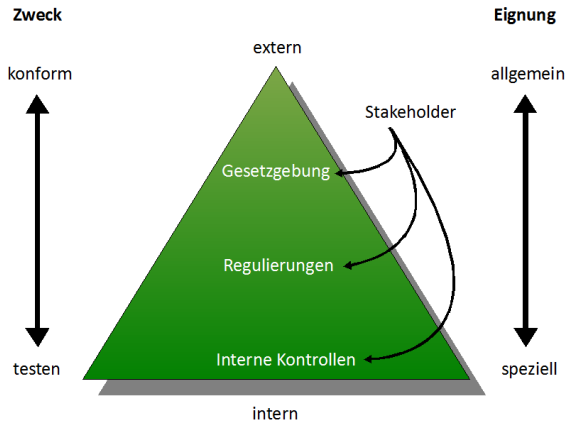


Abb. 3.1: Hierarchie der Kontrolltypen, vgl. [Dom01], S. 20

Anwendungsdruck kann auf verschiedenen Ebenen geschaffen werden. Der Einfluss von Stakeholdern auf unternehmens- und BCP-relevante Gesetzgebung, Richtlinien und interne Kontrollen (Selbststeuerung) ist dabei nicht zu unterschätzen. Abbildung 3.1 zeigt eine Hierarchie drei verschiedener Kontrolltypen. Dabei wird zwischen extern entwickelten (Gesetze und Richtlinien) und intern entwickelten (administrative Systeme, Prozeduren, Überwachungen, Bewertungssysteme, Budgets und Belohnungen) Quellen unterscheiden. Interne Kontrollen sind äußerst spürbar und variieren zwischen einzelnen Organisationen, wohingegen externe Kontrollen eine eher allgemeine Basisfunktion erfüllen. Die Kontrolltypen können auch anhand ihre Eignung und ihres Zwecks differenziert werden. Die Eignung eines Kontrolltypes ist die Deckung des Kontrolltypes mit den Eigenschaften eines Unternehmens, darunter Ressourcen, Geschäftsfunktionen und Historie. Dies variiert von generellen Ge-

setzen, die für alle Unternehmen gelten, über Richtlinien speziell für einzelne Industrien, Aktivitäten oder Prozesse bis zu jenen individuellen internen Kontrollen, die von Unternehmen eigenständig aufgestellt werden. Das Zweck-Kriterium betrachtet die Absichten hinter dem Kontrolltyp, ob die Organisation von außen auferlegte Erwartungen erfüllt (Konformität) oder ob die Aktivitäten dazu dienen, interne Zielsetzungen zu erreichen (Testdurchführung). Stakeholder haben großen Einfluss auf jeden Level dieser Hierarchie und spielen meist eine zentrale Rolle bei der Entwicklung von Selbstregulierungen nach Krisen. Oft ist es der Druck jener Stakeholder, der die Organisationen zu einer mehr proaktiven Vorgehensweise bewegt.

Grundsätzlich gilt für jedes Unternehmen ein gewisses Maß an Achtsamkeit, gesetzlich aber auch ethisch. Wobei Letzteres ausschließlich vom persönlichen Verantwortungsgefühl abhängt und in entsprechender Fachliteratur diskutiert wird[1], ist die BCP-relevante Gesetzgebung (äußerer Druck) nach [Sch01] in sechs Themengruppen zu unterscheiden:

- **Contingency Planning Statutes** beziehen sich auf die Entwicklung von Notfall- und Wiederherstellungsplänen für kritische Systeme.
- **Liability Statutes** bestimmen Sorgfaltspflichten und Haftungsgrundlagen für Manager eines Unternehmens.
- **Life-Safety Statutes** enthalten Anordnungen zum Schutz der Angestellten am Arbeitsplatz.
- **Risk Reduction Statutes** legen notwendige Risk-Management Bereiche zur Reduzierung und Milderung der Konsequenzen von Desastern fest.
- **Security Statutes** umfassen Betrug und Missbrauch von digitalem Besitz.
- **Vital Records Management Statutes** regeln die Behandlung und Aufbewahrung von Unternehmensdaten, sowohl in elektronischer als auch in Papierform.

Diese Kategorisierung basiert auf der US-Gesetzgebung. Bspw. Liability Statutes (Grundlagen zur persönliche Haftbarkeit von Unternehmern) spielen dort eine größere Rolle als in Deutschland – dennoch kann diese Klassierung als internationale Vorlage herangezogen werden. Im Vergleich dazu stammen Vorschriften zum CP in Deutschland ausschließlich aus den Bereichen Arbeitsrecht, Arbeitsschutzbestimmungen (entspricht den Life-Safety Statutes) und Produkthaftpflicht[2]. Die Identifizierung und Beachtung relevanter Vorschriften ist wichtig, um deren Auswirkungen und Einflüsse auf die eigene Handlungsfähigkeit während einer Störung oder Krise zu erkennen. Das deutsche BSI formuliert in seinem neuesten Standard[3]: „*Es gibt eine Vielzahl von bereichsspezifischen*

[1] siehe z.B. [BNG03] und [All06]
[2] [Dom01], S. 22
[3] BSI-Standard 100-4 „Notfallmanagement“

Gesetzen, Richtlinien und Vorschriften, die hierzu je nach Art der Institution zu beachten sind. Welche das jeweils sind, hängt beispielsweise von der Organisationsform der Institution, der Branche und der Art der Geschäftsprozesse ab. [...] Um die rechtlich relevanten Anforderungen identifizieren zu können, sollte daher zunächst immer die aktuelle Gesetzeslage geprüft werden. Gegebenenfalls sind branchenspezifische relevante Standards oder Vorgaben der kontinuierlichen Geschäftsfortführung zu berücksichtigen bzw. können als Vorlagen herangezogen werden"[4]. Nicht nur Banken und Großunternehmen sind hierbei angesprochen – der Standard adressiert bewusst auch kleine und mittlere Unternehmen (KMU) und Behörden[5].

Im globalen Kontext sind landesübergreifende Kategorisierungen oder Vorschriften zu Business Continuity Planning mangels noch fehlender internationaler Standards (und damit Gesetzesgrundlagen) kaum zu finden. Tatsächlich sind die kulturellen Differenzen in der Wahrnehmung von BCP sogar sehr groß. In den Vereinigten Staaten hat das Contingency Planning eine wichtige Schlüsselrolle in Krisenplanung, Heimatschutz und (staatlicher) Notfallvorsorge eingenommen. Die Europäische Union stellte in den letzten Jahren das Thema zunehmend in den Vordergrund und wird dem Notfallmanagement voraussichtlich eine vergleichbar verantwortungsvolle Schlüsselposition einräumen. In Großbritanien beispielsweise ist BCP durch den Civil Contingency Act[6] bereits fest integriert. Japan hingegen fasst BCP nur als Planungsaufgabe von Naturkatastrophen auf und vertraut ganz auf die eigenen Managementfähigkeiten im Falle eines Desasters[7]. Israel sieht BCP als untergeordneten Teil einer Sicherheitsfunktion anstelle einer eigenen Managementdisziplin, Singapore konzentriert ausschließlich IT-BCP, Korea nur auf den Finanzsektor. Afrika setzt ebenfalls den Fokus auf IT, meist jedoch nur auf Regierungsebene. Die BRIC-Staaten (Brasilien, Russland, Indien und China) befinden sich noch auf einem niedrigen Level, der nicht über IT-Wiederherstellung hinausgeht, jedoch ist eine Entwicklung in nächster Zeit abzusehen[8].

Die überwiegende Abwesenheit von (einheitlichen) Regelungen im Business Continuity Planning ist jedoch nicht unbedingt überraschend. Ganz abgesehen von dem individuellen Charakter des BCP und den Regionen, in denen die Notfallplanung noch eine sehr junge Disziplin ist, fokussiert die Gesetzgebung meist auf das *Ergebnis* anstelle des Prozesses, nicht zuletzt um sich in Fragen der Schuldzuweisung darauf stützen zu können. Wenn Contingency Planning aber als wertgewinnende (und weniger als wertmindernde) Aktivität angesehen werden soll, muss darüber hinaus ein breiteres Set unternehmerischer Kontrollen in Betracht gezogen werden, um Krisen (sowohl gesetzliche als auch finanzielle) und deren Konsequenzen im Voraus zu verhindern. Dafür muss selbstständ-

[4] [Bun08], S. 16
[5] [Bun08], S. 5
[6] Seit 2006, relevant für die Notfallplanung einer Vielzahl staatlicher und privater Organisationen
[7] Seit April 2008 ist ein Gesetz in Anlehnung an den amerikanischen Sarbanes-Oxley Act in Kraft.
[8] [Hil07a], S. 569-571

dig eine höhere Integration von Geschäftsfunktionen (Marketing, F&E[9], Produktion, Beschaffung) und externen Körpern (Behörden und Selbstregulierende Organisationen (SROs)) geschaffen werden[10].

In den folgenden Abschnitten werden einige der wichtigsten Gesetze und Vorschriften zum Business Continuity Planning behandelt. Wie oben angesprochen, muss die aktuelle Rechtslage von jeder Institution individuell untersucht werden, um die relevanten Anforderungen zu identifizieren. Neben zahlreichen Vorschriften und Standards zu Business Continuity werden zwei gesetzliche Verankerungen ausführlich dargestellt, welche eine direkte Forderung von Contingency Planning formulieren: der amerikanische Sarbanes-Oxley Act und die Zweite Basler Eigenkapitalverordnung.

3.1 Sarbanes-Oxley Act

Der Sarbanes-Oxley Act (SOX)[11] ist ein US-Bundesgesetz zur verbindlichen Regelung der Unternehmensberichterstattung in Folge zahlreicher Bilanzskandale[12], US-amerikanischer Unternehmen wie Enron[13], Worldcom[14], Tyco International[15] und Peregrine Systems[16]. Das Gesetz wurde am 30. Juni 2006 vom US-Kongress erlassen, um das Vertrauen der Öffentlichkeit in die Transparenz und Vollständigkeit der veröffentlichten Finanzdaten wiederherzustellen.

Weitere Ziele bestehen in der Förderung und Verbesserung von ethischen Geschäfts- und Führungspraktiken. SOX gilt für alle inländischen und ausländischen Unternehmen, deren Wertpapiere an US-Börsen gehandelt werden. Andere private Unternehmen außerhalb des öffentlichen Interesses sind nicht direkt von diesen Anforderungen betroffen, wenngleich auch hier die Tendenz zur Erfüllung besteht – aus Gründen der Wettbewerbsfähigkeit, der Attraktivität für Investoren und Partner und zum besseren Schutz der Unternehmenswerte.

Das Gesetz ist in insgesamt 68 Abschnitte gegliedert. Obwohl SOX nicht ausdrücklich auf die Anforderungen von Business Continuity oder Informationssicherheit eingeht, sind diese Vorkehrungen jedoch eine entscheidende Voraussetzung für die Einhaltung der

[9] Forschung und Entwicklung
[10] [Dom01], S. 22,44
[11] [U.S02]
[12] [Pat02]
[13] [Fre03]
[14] [RA02]
[15] [The05]
[16] [Wei03]

H. R. 3763

One Hundred Seventh Congress of the United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Wednesday, the twenty-third day of January, two thousand and two

An Act

To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Sarbanes-Oxley Act of 2002".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Abb. 3.2: „An act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes." Titelseite des Sarbanes-Oxley Act.

SOX-Richtlinien. Die vier bedeutensten Bestimmungen in diesem Zusammenhang sind[17]:

- Abschnitt 302: Die Richtigkeit der Bilanzen muss vom Geschäftsführer und Leiter der Finanzabteilung beglaubigt werden. Die Finanzdaten müssen fehlerfrei und vollständig sein.
- Abschnitt 404: Der Geschäftsführer, der Leiter der Finanzabteilung und der Abschlussprüfer müssen die Effektivität interner Kontrollen bestätigen. Unternehmen müssen die Effektivität der Kontrollen erhalten, überwachen und entsprechende Berichte erstellen.
- Abschnitt 409: Unternehmen müssen eine wesentliche Veränderung ihrer Finanzsituation in Echtzeit offen legen. Verstöße oder Abweichungen, die auf mögliche erhebliche Veränderungen hinweisen, müssen frühzeitig erkannt werden.
- Abschnitt 802: Unternehmen müssen die Unterlagen der Abschlussprüfung aufbewahren und schützen. In Übereinstimmung mit den Unternehmensrichtlinien muss sichergestellt werden, dass die Unterlagen verfügbar sind und nicht verändert werden.

Abschnitt 404 „Management Assessment of Internal Controls“ wird als einer der meist diskutierten und weitreichensten Bestimmungen angesehen. In dem originalen Wortlaut des Gesetzestextes heisst es, „*[...] requiring each annual report [...] to contain an internal control report, which shall- (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.*“ Die daraus abzuleitende Bedeutung in der Vorbereitung von Wiederherstellungsmaßnahmen und Notfallplanung besteht aus zwei Teilen:

1. Es müssen (technische) Vorkehrungen vorhanden sein, die zu jedem Zeitpunkt die Sicherheit aller finanziellen und sonstiger Daten garantieren, die zur Erfüllung der Vorschriften zur Berichterstattung notwendig sind. Diese Daten müssen für zukünftige Kontrollen von Finanzaufsichtbehörden archiviert werden und jederzeit zugänglich sein.
2. Alle damit zusammenhängenden Maßnahmen und Prozeduren müssen transparent und vollständig dokumentiert werden, sodass während eines SOX-Audits die Existenz und die Qualität von Vorsorgemaßnahmen (z. B. ein Business Continuity Plan) festgestellt werden kann.

[17] [Com06]

Die Erfüllung dieser Anforderungen bedeutet oft kostenintensive Investitionen für die Unternehmen. Erfahrungen haben jedoch bereits gezeigt, dass eine direkte Verbindung zwischen effektiver Compliance und langfristiger Wertschaffung besteht, die sich nicht zuletzt im Shareholder Value widerspiegelt[18]. Neben potentiellen Wettbewerbsvorteilen ist vor allem die persönliche Haftbarkeit [19] von CFOs und CEOs bei Verstößen ein besonderer Ansporn für ein erfolgreiches Business Continuity Management.

Für die Kontrolle der Umsetzung der SOX-Anforderungen hat sich das COSO-Framework[20] etabliert. Zur Unterstützung dieses Frameworks werden zusätzlich COBIT[21] (IT) und ISO 27002[22] verwendet[23].

Der Sarbanes-Oxley Act spricht Contingency Planning nur indirekt an. Daher gibt es offene Aspekte, die jedes (Beratungs-) Unternehmen individuell beachten muss. Nachfolgend sind fünf dieser Aspekte dargestellt[24].

- Wiederanlaufzeit: SOX schreibt keine Messung der Datenwiederherstellungszeit vor. Die Zeit, die zwischen Desaster und einer vollständigen Wiederherstellung vergeht, bleibt somit auch im SOX-Audit unberücksichtigt.
- Wiederherstellungsstrategie: SOX gibt keine Hilfestellung, welche Strategien für ein Unternehmen (oder Applikation) geeignet sind.
- Notfallplan: Das Gesetz schreibt nicht wörtlich einen umfassenden und aktuell gehaltenen Business Continuity Plan vor, sondern spricht nur von der Sicherung belegrelevanter Daten. Ein effektives BCP ist damit vom Gesetzgeber lediglich impliziert.
- Wiederherstellungsprioritäten: SOX definiert keine Abhängigkeiten oder eine Wiederherstellungshierarchie. Welche Netzwerke, Server oder Anwendungen zuerst wiederhergestellt werden bleibt unbestimmt, solange dies nicht bestimmt Sicherheits-, Verfügbarkeits- und Integritätskontrollen der zu schützenden Daten betrifft.
- Entgangene Einnahmen: SOX betrachtet lediglich die Wiederherstellungsfähigkeit von Daten. Die dafür aufgewendete Zeit sowie finanzielle Verluste einer langwierigen Wiederaufnahme der Geschäftsprozesse wird nicht direkt bedacht.

[18] [The06], [The04], [Con06]
[19] Multi-Millionen Dollar Strafen oder bis zu 20 Jahre Haft, siehe SOX-Abschnitt 802
[20] Committee of Sponsoring Organizations of the Treadway Commission, `http://www.coso.org` (Stand: 23.06.2008)
[21] Control Objectives for Information and Related Technology, `http://isaca.org/cobit` (Stand: 23.06.2008)
[22] International Organization for Standardization, siehe [Int07]
[23] vgl. [Com06]
[24] vgl. [Dor05]

Besonders diese letzten Anmerkungen machen deutlich, dass eine SOX-Compliance alleine kein Unternehmen vor dem wirtschaftlichen Aus schützt. SOX ist die Brille des Gesetzgebers, um einen schärferen Blick auf die Unternehmenstransaktionen werfen zu können und die Nachvollziehbarkeit durch größere Transparenz der Geldwirtschaft in den Chefetagen amerikanischer Organisationen zu erhöhen. Ein wirtschaftliches Unternehmen muss über diese spezifische Datensicht hinausgehen und auch die Prozesse in die Planung fest integrieren.

3.2 Zweite Basler Eigenkapitalverordnung (Basel II)

Das Regelwerk „Internationale Konvergenz der Eigenkapitalmessung und der Eigenkapitalanforderungen“, besser bekannt unter dem Namen Basel II, bezeichnet die Summe aller Eigenkapitalvorschriften für Kreditinstitute, die vom Basler Ausschuss für Bankenaufsicht in den letzten Jahren vorgeschlagen wurden. Basel II[25] beschreibt die Neuregelungen des Bankenaufsichtsrechts, die erstmals im Juni 2004 veröffentlicht wurden. Ziel des Ausschusses ist die Schaffung einheitlicher Wettbewerbsbedingungen im internationalen Bankensystem sowie die Reduzierung des Insolvenzrisikos der Finanzinstitute. Der Basler Ausschuss für Bankenaufsicht setzt sich aus Vertretern der nationalen Bankenaufsichtsbehörden oder der Zentralbanken der führenden Industrienationen zusammen[26] und ist ein reines Beratungsgremium ohne gesetzgeberische Kompetenzen. Die ausgesprochenen Empfehlungen hingegen dienen meist als Basis für die Gesetzgebung der EU und finden so Eingang in das nationale Recht der Mitgliedstaaten.
staaten.

Die so genannten Säule 2 von Basel II verlangt die Einführung eines Internal Capital Adequacy Assessment Process (ICAAP)[27]. Dieser bankinterne Prozess muss Verfahren zur Identifizierung, Messung, Steuerung und zum Reporting von Risiken im Kreditinstitut enthalten und soll proportional zum Geschäftsvolumen des jeweiligen Instituts ausgelegt sein. In Deutschland ist ICAAP durch die nationale Gesetzgebung in den „Mindestanforderungen an das Risikomanagement“ (MaRisk)[28] verankert. Die Institute der deutschen Kreditwirtschaft hatten ihr bestehendes internes Risikomanagement spätestens bis zum 1. Januar 2008 an die MaRisk anzupassen[29].

[25] [IS06]

[26] darunter Belgien, Deutschland, Frankreich, Italien, Japan, Kanada, Luxemburg, Niederlande, Schweden, Schweiz, Spanien, USA und Großbritannien, siehe auch „Regulators“ unter `http://www.basel2.hk/index.html` (Zugriff am 29. März 2008)

[27] Methoden zur Bestimmung der regulatorischen Eigenmittelanforderungen, des Risikomanagements und der integrierten Gesamtbankrisikosteuerung

[28] [Bun07a] oder direkt online unter [Bun07b]

[29] [Deu07]

Für die Notfallplanung in Deutschland ist Artikel 7.3 „Notfallkonzept“ von MaRisk von besonderer Bedeutung. Der Artikel setzt sich aus zwei Teilen zusammen.

> *AT 7.3 – Textziffer 1*
>
> *Für Notfälle in zeitkritischen Aktivitäten und Prozessen ist Vorsorge zu treffen (Notfallkonzept). Die im Notfallkonzept festgelegten Maßnahmen müssen dazu geeignet sein, das Ausmaß möglicher Schäden zu reduzieren.*
>
> *Die Wirksamkeit und Angemessenheit des Notfallkonzeptes ist regelmäßig durch Notfalltests zu überprüfen.*
>
> *Die Ergebnisse der Notfalltests sind den jeweiligen Verantwortlichen mitzuteilen.*

Die Aussagen formulieren prägnant die Anforderung von und an ein angemessenes Business Continuity Planning. Es muss in der Lage sein, für Notfälle in allen kritischen Aktivitäten und Prozessen ein Konzept zu entwickeln und fortzuführen (Aktualität), dessen festgelegte Maßnahmen zur Reduzierung des (zeitlichen) Ausmaßes möglicher Schäden geeignet sind. Da Basel II die wesentlichen Einflussfaktoren auf die Gesamtrisikosituation eines Instituts fokussiert, gilt auch in MaRisk, dass sich der Begriff „Notfall“ nicht ausschließlich auf den Ausfall von IT-Systemen bezieht, sondern die IT nur soweit betrachtet, wie sie im Rahmen der Aufrechterhaltung primärer Geschäftsprozesse oder Standorte zum Einsatz kommt. Im Fall der Auslagerung von Prozessen oder Diensten haben das auslagernde Institut und der Dienstleister über aufeinander abgestimmte Notfallkonzepte zu verfügen. Die Textziffer 1 besagt weiterhin, dass die Dokumentation aller Maßnahmen des Notfallkonzepts ein essentieller Bestandteil der Notfallvorsorge ist. Ein entsprechendes Notfallhandbuch muss so gestaltet sein, dass auch ein sachverständiger Dritter die spezifizierten Maßnahmen verstehen, einleiten und ausführen kann (Verständlichkeit). Dies erfordert eine strukturierte Darstellung notwendiger Informationen, darunter Verantwortlichkeiten, Eskalationsstufen, Handlungsanweisungen zu speziellen Notfallereignissen oder temporären Datenaufbewahrungsrichtlinien, Wiederanlaufverfahren, Listen zur Wiederbeschaffung defekter IT-Komponenten bis hin zu vertraglichen Regelungen mit Partner, Lieferanten oder Kunden, die in einer solchen Situation von zentraler Bedeutung sind. Die Verfügbarkeit des Notfallplans ist ebenso sicherzustellen und gegebenenfalls von den verantwortlichen Mitarbeitern bestätigen zu lassen (Verfügbarkeit). Die Definition von Ausfallszenarien, die einer Geschäftsprozessanalyse folgen sollte, gehört ebenfalls zur Dokumentation. In regelmäßigen Abständen muss der Notfallplan getestet und geübt werden. Die Häufigkeit der Notfallübungen soll sich an der Gefährdungslage des Instituts orientieren, da der normale Betriebsablauf dabei gestört werden kann. Die Tests sollten bevorzugt in einem Backup-System durchgeführt werden und mit den Notfallkonzepten eventueller Dienstleister abgestimmt sein. Deren Ergebnisse sind den jeweiligen Verantwortlichen mitzuteilen.

> *AT 7.3 – Textziffer 2*
>
> *Das Notfallkonzept muss Geschäftsfortführungs- sowie Wiederanlaufpläne umfassen.*
>
> *Die Geschäftsfortführungspläne müssen gewährleisten, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen. Die Wiederanlaufpläne müssen innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen.*
>
> *Die im Notfall zu verwendenden Kommunikationswege sind festzulegen. Das Notfallkonzept muss den beteiligten Mitarbeitern zur Verfügung stehen.*

Textziffer 2 fordert für die Umsetzung von MaRisk, respektive Basel II, Geschäftsfortführungs- und Wiederanlaufpläne, die effiziente Maßnahmen zur Vermeidung bzw. zur schnellen Weiterführung kritischer Geschäftsprozesse umfassen. Alle darauf einwirkenden Faktoren, im Speziellen IT, müssen erfasst und dokumentiert werden. Dazu ist auch die Koordination von IT Disaster Recovery (IT-DR) und Business Continuity Plan gefordert: Aus Risikoanalysen und Schadenseinschätzungen des BCP ergeben sich maximal tolerierbaren Ausfallzeiten für die IT-DR. Daraus sind die entgültigen Notfallpläne zu erarbeiten. Teil dieser Pläne sind zudem verlässliche Kommunikationskonzepte, die eine Benachrichtigungsreihenfolge der verantwortlichen Personen (oder deren Vertreter bei Nichterreichbarkeit) beinhalten sowie die Alternativen und Verfügbarkeiten von Kommunikationsmitteln (z. B. Festnetz, Fax, Mobilfunk, E-Mail, Funk, Kurier) regeln. Es ist hingegen nicht erforderlich, dass für ausgelagerte Funktionen ein eigenständiger Notfallplan ausgearbeitet werden muss, sofern der Dienstleister einen eigenen Notfallplan besitzt und seine Prüfungsberichte zur Verfügung stellt[30].

Die o.g. Textziffern zum Notfallkonzept stehen mit ihren Formulierungen in einem deutlichen Kontrast zum Sarbanes-Oxley Act. Daten und IT werden nur im Zusammenhang mit Geschäftsprozessen adressiert, Kommunikationslösungen und Notfalltests werden fokussiert. Eine direkte Haftbarkeitsklausel für einzelner Personen gibt es nicht. SOX und Basel II im Vergleich führen zu dem persönlichen Eindruck, dass mit SOX ein Unternehmen und mit Basel II der Erfolg eines Unternehmens kontrolliert werden soll.

3.3 Weitere Regularien

Neben dem Sarbanes-Oxley Act und Basel II gibt es zahlreiche weitere Gesetze, Richtlinien und Standards, die Anforderungen an ein Notfallmanagement stellen oder den Aufbau des Notfallmanagements beeinflussen. Der Großteil der bekanntesten und bedeutensten Vorschriften besteht in den USA und in Europa. Nur durch eine sorgfältige Analyse der individuellen Unternehmenssituation können alle rechtlich relevanten Vorschriften

[30] [Bun07a], S. 75

identifiziert werden. Die nachfolgende Liste ist daher ein Ausschnitt der aktuellen Gesetzeslandschaft, der einen Einblick in deren Inhalte gibt.

3.3.1 Weitere Vorschriften in Amerika

New York Stock Exchange (NYSE) 446[31]

Regel 446 fordert ein Notfallmanagement für alle Mitglieder und Mitgliedorganisationen[32] der New York Stock Exchange (NYSE) seit August 2004. Es muss ein umfassender BCP aufgestellt sein, der alle geschäftskritischen Bereiche der jeweiligen Organisation abdeckt. Dieser BCP muss sowohl online, falls möglich, in jedem Fall aber durch ein entsprechendes (E)Mail-System zugänglich sein.

Joint Commission on Accreditation of Healthcare Organizations (JCAHO)[33]

Die JCAHO-Kommission schreibt für alle US-Gesundheitsorganisationen einen Notfallplan vor. BCP wird ausdrücklich als wichtige Vorkehrung für den Fall einer (landesweiten) Krisensituation und eine damit verbundene erhöhte Nachfrage nach medizinischer Behandlung bezeichnet. Als integrale Teile dieses Plans nennt JCAHO: Risikoeinschätzung (Chemikalien, Ansteckungsgefahren), die Zusammenstellung von Notfallteams, die Erstellung von Eskalationsprotokollen und Wiederaufnahmeprozeduren sowie regelmäßige Überwachung und Tests.

Health Insurance Portability and Accountability Act (HIPAA)[34]

HIPAA ist ebenfalls ein allein für den medizinischen Bereich gültiges Gesetzeswerk, das für organisatorische Vereinfachungen sowie Datenschutz und Datensicherheit im amerikanischen Gesundheitssystem sorgen soll. Die Anforderungen beinhalten einen Datensicherungsplan (data backup plan), einen Wiederherstellungsplan (disaster recovery plan) und ein Konzept zur Vorgehensweise in Krisensituationen (emergency mode operation plan). Des Weiteren sind, falls angemessen, zusätzliche Test- und Revisionsprozesse sowie Datenanalysen durchzuführen und zu dokumentieren.

Federal Financial Institutions Examination Council (FFIEC)[35]

Der FFIEC wird auf Grund seiner hohen Anforderungen an die Unternehmensführung (Verantwortlichkeit) und an das Business Continuity Planning als einer der aggressivsten Standards des US Marktes angesehen. Diese Anforderungen umfassen Risk Assessment, BIA, Tests und Kontrollen. Der Standard propagiert einen angemessenen BCP und kann von jedem Unternehmen herangezogen werden.

[31] [New04]
[32] [New08]
[33] [Joi]
[34] [Dep03]
[35] [Fed08]

3.3.2 Weitere Vorschriften in Europa

Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)[36]

Bereits seit 1995 bestehend, beschreiben die steuerrechtlichen Vorschriften zur ordnungsmäßigen Buchführung konkret den empfohlenen Umgang mit aufbewahrungspflichtigen Daten und Belegen in elektronischen und nicht-elektronischen Buchführungs- und Archivsystemen. Ein Kernpunkt ist das interne Kontrollsystem, welches Aspekte der Datensicherheit, Dokumentation, Prüfbarkeit und Datenwiedergabe integriert, und damit unmittelbar Einfluss auf das Notfallmanagement hat.

ISO 27002 und BS 25999[37]

Der internationale Standard ISO 27002 (vor April 2007 inhaltlich als ISO 17799 bzw. BS 7799 bekannt) sowie der British Standard 25999 sind keine rechtlich verankerte Gesetze, nehmen aber auf Grund ihrer internationalen Bedeutung[38] eine wichtige Rolle ein. Gegenseitige Referenzen deuten den komplementären Charakter dieser Standards an, wobei das ISO Werk ein Framework beschreibt, welches vom Britischen Standard umfassend ausgefüllt wird. Konkret wie möglich und allgemeingültig wie nötig – so formen die Standards aufbauen auf „best practices“ der BC-Community einen BC-Lifecycle Ansatz, der als breit aufgestelltes Grundgerüst für ein erfolgreiches BCM definiert wird. Zu den Themen dieses Ansatzes gehören:

- Business continuity programme management,
- Strategy determination,
- Understanding the organization,
- Developing a business continuity response,
- Exercise, maintenance and review,
- Embedding BCM in the organizational culture.

Hazard Analysis Critical Control Point (HACCP)[39]

Für die europäische Lebensmittelindustrie hat das HACCP-Konzept besonderen Einfluss auf das Risk-Assessment und die Vorsorgeplanung. Im deutschen Recht seit 1998 in der Lebensmittelhygiene-Verordnung verankert verlangt es u.a.

- eine umfangreiche Analyse aller Risiken, welche die Verträglichkeit von Lebensmitteln beeinflussen können,
- die Vorausplanung von Korrekturmaßnahmen bei Abweichungen,

[36] [Arb95]
[37] [Bri06], [Int07]
[38] Wie zuvor der British Standard 7799 kann auch BS 25999 zukünftig in die internationale ISO-Reihe aufgenommen werden.
[39] [Bun98]

- die regelmäßige Überprüfung des Systems zur Sicherstellung der Lebensmittelsicherheit und
- die Dokumentation aller geplanten Maßnahmen.

Seit Anfang 2006 führt die Nicht-Einhaltung dieser Vorschriften zum Handelsausschluss von Lebensmitteln in der Europäische Union.

Combined Code und Turnbull Report[40]

An der London Stock Exchange gelistete Unternehmen unterliegen dem Combined Code. Er wurde im Juni 2006 überarbeitet und beschreibt Good Practices zu den Themen Vorstandszusammensetzung, Entlohnungen, Rechenschaftspflicht, Audits und die Beziehung zu Shareholdern. „Comply or explain" ist die Devise dieser Vorschrift, welche als Konsequenz für die Unternehmen bedeutet, entweder die Umsetzung der Prinzipien bestätigen zu können oder eine Erklärung für die Nichtbefolgung vorlegen zu müssen. Der Code beinhaltet in Abschnitt C.2 ebenfalls Anforderungen an ein internes Kontrollsystem, darunter

- die Einführung und Aufrechterhaltung eines internen Kontrollsystems (IKS) zum Schutz der Shareholder,
- die regelmäßige Überprüfung der Effektivität des IKS, inkl. Kontrollen der Finanzen und Compliance, operationelle Kontrollen und Überwachung des Risk Management Systems (RMS)
- die Berichterstattung an Shareholder.

Der Turnbull Report wird in diesem Zusammenhang als wichtiges Dokument zur Hilfe genommen, da er sich eingehend mit dem IKS beschäftigt und einen entsprechenden Leitfaden für die Umsetzung entwickelt. Zudem sind die Turnbull Richtlinien als Rahmenwerk für die Erfüllung des SOX Abschnitt 404 von der U.S. Securities and Exchange Commission (SEC) anerkannt.

Die 8. EU-Richtlinie und Japan's Financial Instruments and Exchange Law[41]

Bis zum 29. Juni 2008 ist in allen EU-Mitgliedstaaten die 8. EU-Richtlinie über Abschlussprüfungen von Jahresabschlüssen umzusetzen. Die Richtlinie weist markante Parallelen zum Sarbanes-Oxley Act auf und wird im allgemeinen Sprachgebrauch oftmals als EuroSOX referenziert. Diese Bezeichnung ist jedoch umstritten, da die inhaltlichen Gemeinsamkeiten nur auf einen Teilbereich beschränkt sind. Im Vordergrund der EU-Richtlinie stehen Anforderungen an die Jahresabschlussprüfung, um das Vertrauen in die Unternehmen öffentlichen Interesses[42] weiter zu stärken. Gemeinsamkeiten mit dem amerikanischen SOX finden sich in den Zielen,

[40] [Fin06], [Fin05a]

[41] [Eur06], umgesetzt in deutsches Recht durch das Berufsaufsichtsreformgesetz (BARefG) vom 5. September 2007 ([Bun07c])

[42] börsennotierte Unternehmen, Banken, Versicherungen und Unternehmen besonderer Größe oder Stellung[43]

- die Abschlussprüfer unabhängiger zu machen,
- Prüfungsausschüsse einzurichten und
- das Vertrauen in die Bilanzen durch den Schutz der Anleger zu gewährleisten.

Zwei Konsequenzen ergeben sich direkt aus diesen Zielen: Zum Schutz der Shareholder wird der Rechnunglegungsprozess zukünftig durch einen Prüfungsausschuss zu überwachen sein, das heisst muss ein internes Kontroll- und Risikomanagementsystem eingeführt werden, das durch regelmäßige Dokumentation, Tests und Dokumentation der Tests diesen Schutz garantiert.
In Asien führt Japan zur selben Zeit eine Adaption des SOX ein: der Japanease Sarbanes-Oxley (JSOX) ist im April 2008 in Kraft getreten und verfolgt bis auf wenige Ausnahmen das gleiche Ziel wie sein amerikanisches Pendant (Abschnitt 3.1).

BSI-Standard 100-4[44]

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Januar 2008 erstmals eine Diskussionsgrundlage für einen deutschen Standard des Notfallmanagements veröffentlicht. Der technische fokussierte IT-Grundschutz Baustein 1.3 „Notfallvorsorge-Konzept“ wurde überarbeitet und verweist seitdem auf den komplexeren BSI-Standard 100-4 „Notfallmanagement“. Die Absicht des BSI bestand nicht darin, den zuvor von britischer Seite entwickelten British Standard 25999 zu übersetzen, sondern ein äquivalentes Werk zu schaffen, das Grundschutzspezifika mit Aussagen aus verschiedenen Standards rund um das Thema Contingency Planning verbindet. Die Philosophie des Grundschutzes, eine schnelle Umsetzungshilfe durch konkrete Beispiele zu geben, soll auch in diesem Standard fortgeführt werden.
Die Aufgaben im Rahmen der Erstellung eines BCP sind verständlich und anwendungsorientiert formuliert. So beschreibt der Standard folgende Aufgaben:

- Planung & Konzeption zur Notfallvorsorge
  - Leitlinie zum Notfallmanagement
  - Durchführung einer Business Impact Analyse
  - Durchführung einer Risikoanalyse (gemäß BSI 100-3)
  - Definition einer Notfallmanagementstrategie
  - Erstellung eines Notfallvorsorgekonzepts
- Erstellung Notfallhandbuch zur Notfallbewältigung
  - Sofortmaßnahmen / Alarmierung
  - Wiederanlauf
  - Geschäftsfortführung

[44][Bun08]

  - Wiederherstellung
  - Rückführung in den Normalbetrieb
  - Aufarbeitung, Nachbereitung, Analyse
  - Krisenmanagement
  - Öffentlichkeitsarbeit
- Etablierung und Pflege einer Notfallmanagement-Kultur
  - Sensibilisierung
  - Schulung
- Planung und Durchführung von Übungen und Tests
  - Übungsplan
  - Übungskonzept
  - Testarten / Übungsarten
  - Durchführung / Nachbereitung
- Permanente Aufrechterhaltung
  - Wartung (Aktualisierung)
  - Überprüfung (Review)
  - Kontinuierlicher Verbesserungsprozess
  - Software-Unterstützung

Die anwendungsnahe Formulierung von Aufgaben und Maßnahmen wird den Unternehmen, Behörden und sonstige öffentlichen oder privaten Organisationen bei der Umsetzung der Empfehlungen entgegenkommen. Durch die vollständige Implementation von BSI 100-4 erhalten größere Unternehmen ein mit allen (internationalen) Standards und Regulatorien konformes Notfallmanagement.

4 Aspekte des BCP

In dem vorherigen Kapitel wurde gezeigt, dass Business Continuity Planning bereits in vielen Bereichen verpflichtend ist, um gesetzlichen Anforderungen und Industriestandards gerecht zu werden. Dieser Trend entwickelt sich zunehmend weiter: Euro-SOX und Japan-SOX sind nur zwei Beispiele, dass ein Geschäftsprozess-orientiertes Contingency Planning in Zukunft weitere Länder und Industrien erreichen wird. In diesem Kapitel soll gezeigt werden, was die Aufgaben des BCP tatsächlich sind. Dazu betrachte ich die Teilbereiche Personal, Organisation und Technik. Am Schluss soll ein Überblick geschaffen worden sein, welche Teildisziplinen in einem guten Notfallplan bearbeitet und umgesetzt werden müssen.

Zuvor jedoch sollte ein kurzer Blick darauf geworfen werden, warum ein funktionierendes Notfallmanagement auch ohne äußeren Anwendungsdruck empfehlenswert ist. Denn die rechtlichen Aspekte (externer Druck) alleine formen nur einen Teil der Gründe, die Notfallplanung zu einem integralen Bestandteil priorisierter Managementdisziplinen zu machen. Das existentielle, ureigene Interesse eines jeden Unternehmers, zu jeder Zeit seine Geschäftsaktivitäten uneingeschränkt aufrecht erhalten zu können, bildet das Komplement (interner Druck).

Dieses Interesse steht in direktem Zusammenhang mit dem Wert und dem Ansehen eines Unternehmens. Den oft breit aufgestellten Vorschriften, deren Relevanz für das Unternehmen analysiert werden muss und durch angemessene Strategien geplant sein sollte, steht so die effiziente Umsetzung individueller Lösungen und Optimierungsprozesse gegenüber. Diese Umsetzung berücksichtigt u.a.

- die Sicherung des Unternehmenswertes (z.B. Aktienwert) und die Gewährleistung der Shareholderinteressen,
- die Demonstration vorbildlichen Managements gegenüber Medien und Öffentlichkeit,
- die Sicherung von Arbeitsplätzen und
- das Management und den Schutz von Reputation und Markenname.

Diese ausgewählten Elemente gehören zu den Ansätzen, die gerne als Good Corporate Goverance zusammengefasst werden. Ob Marktanteilstrategie, Umsatzwachstum oder

eine andere Unternehmensstrategie: BCP kann – richtig etabliert – das Rückgrat eines Unternehmens sein, das jegliche Strategie unterstützt – sowohl operativ als auch gegenüber der Öffentlichkeit. Die Vorteile bei Zertifizierungen oder Versicherungensverträgen sollten auch nicht unterschätzt werden. Auditoren befürworten stets mehr Sicherheitsvorsorge und Versicherungen offerieren bessere Konditionen. Indirekte Effekte können ebenso auftreten. So ist es nicht unwahrscheinlich, dass Unternehmen, die BCP etabliert haben, bspw. auch von ihren Lieferanten Planungsvorsorge fordern. Dadurch wird ein nachhaltiger Schutz geschaffen, der nicht nur der eigenen Strategie entgegen kommt, sondern alle Stakeholdern von den Mitarbeitern und Kunden bis zu den Aktionären und Umweltorganisationen, die in irgendeiner Weise besonderes Interesse an der Kontinuität der Organisation zeigen.

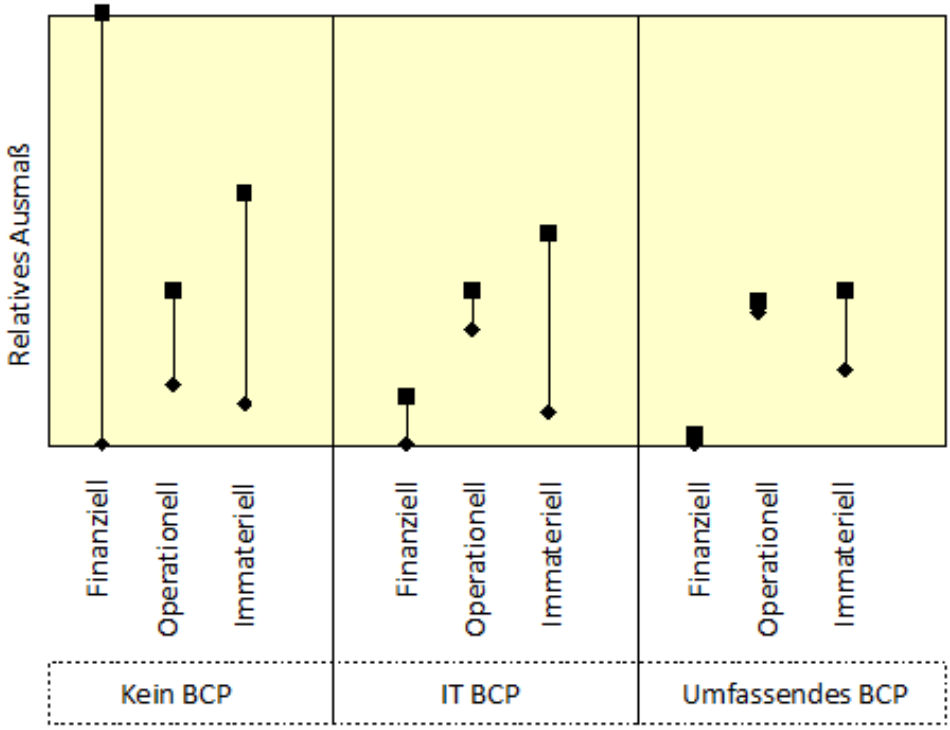


Abb. 4.1: Das relative Ausmaß eines Notfalls hängt von dem umfang des etablierten BCP ab. (Vgl. [Hil07a], S. 482)

Statistiken zeigen, dass schon ein einfacher Ansatz eines BCP bereits mit Abstand wertvoller ist als die Ignoranz des Themas. Als am 11. September 2001 zwei Flugzeuge in die Zwillingstürme des World Trade Centers stürzten hatte keines der dort ansässigen Unternehmen einen Notfallplan für ein solches Szenario entwickelt. Dass dennoch einige Unternehmen wie Morgan Stanley, Cantor Fitzgerald oder American Express innerhalb weniger Stunden wieder den Geschäftsbetrieb fortsetzen konnten, verdanken sie der Vor-

bereitung auf verschiedene Zwischenfälle, die neben einem Ausfall der IT beispielsweise auch den Verlust von Betriebsgebäuden berücksichtigten[1]. Auch die Studien der Stromkrise im Geschäftsbezirk von Auckland, Neuseeland, drei Jahre zuvor im Februar 1998 kamen zu einem ähnlichen Ergebnis: Vorausgehende Planung half bei der Wiederherstellung und der Reduzierung des Ausmaßes. Es scheinte bereits geholfen zu haben, einen Plan nur zu überdenken und die ersten Schritte einer Notfallplanung durchzugehen, sodass Alternativen bereits identifiziert und bewertet wurden[2].

Abbildung 4.1 stammt aus einer dieser Rückblicke und zeigt tendenziell die relativen Auswirkungen auf Finanzen, Geschäftsbetrieb und immaterielle Werte (z.B. Kundenservice, Kommunikation, Sicherheit), abhängig von dem Umfang des BCP in den Unternehmen.

Generell muss bei jeglicher Planung ein angemessener finanzieller Aufwand berücksichtigt werden. Ein gewisser Level an Risiko ist unvermeidbar. Eine vernünftige Notfallstrategie kann nur durch die Gegenüberstellung von Eintrittswahrscheinlichkeit und Ausmaß auf der einen Seite und Kosten für die Implementierung der Strategie auf der anderen Seite erreicht werden.

Im Folgenden werden nun die IT-Notfallplanung und die organisatorischen und personellen Aspekte des Business Continuity Plannings gegenübergestellt. Der Personalaspekt beschreibt dabei die Vorkehrungen und Maßnahmen im Bereich Human Resources. Der IT-Abschnitt befasst sich mit den technischen Aufwendungen, die zur Umsetzung einer BCP-Strategie nötig sind. Im organisatorischen Aspekt werden die Risiken und Maßnahmen identifiziert, die neben dem Personal- und IT-Aspekt das Unternehmen als Ganzes betreffen.

4.1 Personal

Das Personal muss im Vordergrund stehen, wenn man über Business Continuity spricht. Genauso stark wie ein Unternehmen heute auf Technik und Informationstechnologie angewiesen ist, hängt es in einem mindestens gleichen Maße von qualifiziertem und talentiertem Fach- und Führungspersonal ab. Dennoch zeigt eine Umfrage von IBM, dass mehr als die Hälfte aller befragten Unternehmen keine Vorkehrungen für Personalausfall oder Personalverlust getroffen haben[3]. Eine sehr optimistische Grundhaltung wenn man bedenkt, dass die Einstellung und Ausbildung von neuen Mitarbeitern mitunter sehr viel mehr Zeit in Anspruch nimmt als die Neubeschaffung von IT-Komponenten, welche weitaus häufiger in der Planung berücksichtigt wird.

[1] [Boe07])
[2] [Hil07a], S. 482
[3] [IBM06]

Gute Gründe für die Personalplanung sind naheliegend. Humankapital ist mehr als nur eine intelligente Investition, ganz besonders in innovativen und beratenden Unternehmen. Mitarbeiter bringen ein Unternehmen nach vorne und sichern dessen Existenz, sind aber auch gleichzeitig die kritische Quelle für Fehlentscheidungen, Ausfälle und somit wirtschaftliche Schäden. Dies führt zu zwei unterschiedlichen Szenarien: Erstens, die Mitarbeiter können nicht handeln. Pandemien können schnell ganze Belegschaften gesundheitlich belasten und außer Gefecht setzen. Terroranschläge oder Naturkatastrophen machen Angehörige auf psychologische Unterstützung angewiesen und effiziente Arbeit unmöglich. Und zweitens, die Mitarbeiter handeln falsch. Menschliche Fehler sind einige der Hauptursachen für die Entstehung von Notfällen, wie Fallstudien belegen, und können kleine Störungen zu großen Krisen werden lassen.

Typische Aufgaben des Personalaspektes im Rahmen des Business Continuity Planning sind eine grundlegende Kommunikations- und Vorsorgeplanung, Mitarbeiterschulungen sowie die Ersatz- und Nachfolgeplanung.

Die grundlegende Kommunikations- und Vorsorgeplanung beschäftigt sich mit der Identifizierung und Behandlung von Personalrisiken, die kurzzeitige Störungen in den Geschäftsabläufen hervorrufen können. Mit zunehmender Größe eines Unternehmens muss zudem auf langfristige Trends reagiert werden, wie z.B. ein Fachkräftemangel aus wirtschaftlichen oder politischen Gründen oder die demographische Entwicklung bei den Mitarbeitern und im Kaufverhalten der Kunden. Die Entwicklung und Fortführung von aktuellen Kommunikationsstrategien muss eindeutige Anleitungen für die Kontaktaufnahme und Informationsverbreitung beschreiben und stellt somit ein wichtiges Mittel für den Krisenfall dar. Neben der Festlegung der zu benutzenden Medien oder Leitungen ist eine klare Kommunikation von Rollen und Verantwortlichkeiten unerlässlich. Im gleichen Schritt müssen die Regelungen für Fehlzeiten angepasst werden. Zur grundlegenden Notfallplanung im Personalbereich zählt auch Mitarbeitervorsorge für Ausnahmesituationen zu treffen. Dazu gehört in erster Linie sicherzustellen, dass die Lohn- und Gehaltsabrechnung im Business Continuity Plan berücksichtigt wird, um die Mitarbeiter z.B. während einer Katastrophe nicht zusätzlich zu belasten. Es sollte sogar weiter gegangen und Unterstützungsleistungen geplant werden, darunter psychologische, medizinische oder materielle Hilfe. Ziel der Personalplanung im Rahmen von Business Continuity sollte es sein, qualifizierte Mitarbeiter in Krisenzeiten persönlich soweit zu entlasten, dass sie ihrer Tätigkeit im Unternehmen bestmöglich nachgehen können.

Wie wichtig regelmäßige Schulungsmaßnahmen dabei sind wird noch zu oft unterschätzt. Aktuelle Nachrichten und Fallstudien bestätigen das immer wieder[4]. Unvorbereitete Mitarbeiter sind in solchen Situationen überfordert, zögern zu lange oder treffen die falschen Entscheidungen. Falsche Entscheidungen können nicht nur in Krankenhäusern oder Al-

[4] [Hil07b], [Hil07c]

tenheimen lebensbedrohlich sein. Fälle, in denen ein engagierter Mitarbeiter nach einem Feueralarm vorschnell ohne die genaue Situation zu kennen die gesamte Sprinkleranlage auslöste und damit Wasserfluten über kritische IT-Komponenten niederkamen, sind unangenehme und millionenschwere Realität[5]. Oder es ist die mangelnde Kenntnis über die eigenen Befugnisse, die Vorfälle eskalieren lässt. Wichtig ist, dass aus vorangegangenen Fehlern (Störung, Desaster) gelernt wird und entsprechende Schulungen dies widerspiegeln. Ein effektives Schulungsprogramm muss die Mitarbeiter auf verschiedene Arten von Katastrophen vorbereiten. Dabei ist die Ausbildung des Personals (Fokus auf die Mitarbeiter) nicht gleichzusetzen mit dem Testen von BC-Plänen (Fokus auf die Methoden). Ein solches Programm muss sensibilisieren und gutes Teamverhalten in den Vordergrund stellen. Die Mitarbeiter sollten durch entsprechende Entwicklungsmöglichkeiten auf die Übernahme weiterer Verantwortungsbereiche vorbereitet werden. MaRisk spricht in diesem Zusammenhang von einem Grundsatz der Proportionalität. Dies bedeutet, es müssen angemessene Maßnahmen zur quantitativen und qualitativen Personalausstattung geschaffen werden, die sich aus den betriebsinternen Erfordernissen, den Geschäftsaktivitäten und der Risikosituation ergeben[6]. Dieser Grundsatz, der in MaRisk nur für Kreditinstitute verpflichtend ist, kann von jedem Unternehmen als Basis für Aus- und Weiterbildungsprogramme aufgenommen werden. Zur nachhaltigen Unterstützung aller Schulungsmaßnahmen liegt es aber auch im Rahmen des Personalaspekts der Notfallplanung, eine Unternehmenskultur zu etablieren, die die vermittelten Seminarinhalte fördert, darunter Fachwissen und Verhaltensweisen[7].

Eng mit den Schulungsmaßnahmen verbunden ist die Ersatz- und Nachfolgeplanung. Bspw. ist in MaRisk festgelegt: „Die Abwesenheit oder das Ausscheiden von Mitarbeitern sollte nicht zu nachhaltigen Störungen der Betriebsabläufe führen“.[8]Für Schlüsselpositionen und geschäftskritische Rollen (Spezialisten oder Führungskräfte) sollte frühzeitig potentieller Ersatz gefunden und Vertretungspläne erarbeitet werden. Ansätze können dabei in zwei Richtungen gehen: Zum einen kann in die Verfügbarkeit des Unternehmens investiert werden, um Mitarbeitern bspw. durch Heimarbeit die Möglichkeit zu geben, ihre Aufgaben zu erfüllen. Dies wäre in dem Fall von Wert, wenn der Arbeitsplatz auf Grund physischer Blockaden nicht erreichbar ist, z.B. wegen Bahnstreiks oder Epidemierisiken. Zum anderen kann aber auch die Verfügbarkeit von qualifizierten Fachkräften verbessert werden. Dazu sollten gute Beziehungen zu Geschäftspartnern aufgebaut werden, um im Notfall auf deren (personelle) Unterstützung zählen zu können. Eine personelle Krise in Folge einer Explosion oder eines Busunfalls während eines Betriebsausflugs sind tragische Beispiele eines solchen Notfalls. Strategien und Maßnahmen in der Personalplanung sollten stets sowohl auf kurzfristige als auch auf langfristige Störungen der Geschäftsabläufe ausgerichtet sein. Die Etablierung einer Datenbank mit aktuellen Informationen zu den Fähigkeiten jedes Mitarbeiters kann dabei als Anfang dienen.

[5][Hil07a], S. 43
[6][Bun07a], AT7.1-Textziffer 1
[7][Hil07d], [Hil07e]

4.2 Technik

Die Notfallplanung für IT-Systeme (IT-BCP) ist häufig der Einstieg eines Unternehmens in das Kontinuitätsmanagement. Da kritische Geschäftsfunktionen meist stark von IT- und Telekommunikationssystemen abhängig sind, beschäftigt sich das IT-BCP mit Lösungen zur Datensicherheit und Datenverfügbarkeit in Notfallsituationen. Die derzeit jüngste[9] Studie der Aberdeen Group hebt die wichtigsten Gründe von Unternehmen zur Implementierung eines BCP hervor (Abbildung 4.2).

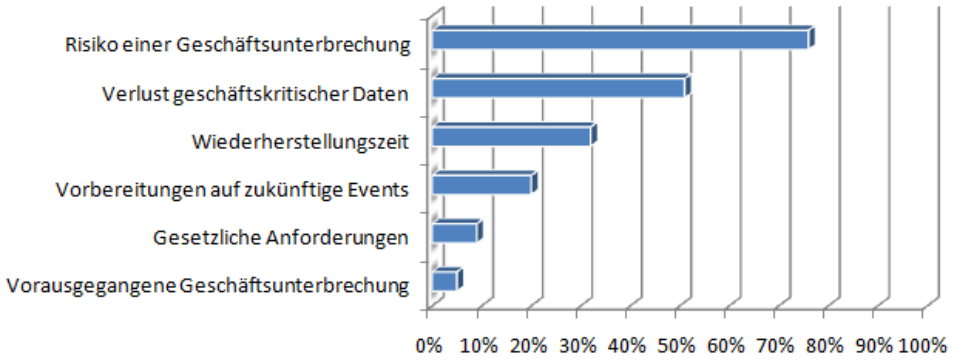


Abb. 4.2: Die Aberdeen-Studie enthüllt die Gründe zur Einführung einer Notfallvorsorge (Quelle: [Abe08])

Es hat mehrere Gründe, warum die Risiken von Geschäftsunterbrechungen, Datenverlust und zu langen Wiederherstellungszeiten an der Spitze dieser Liste stehen. Die Bedeutung von integeren und zuverlässigen IT-Systemen für die Geschäftsfortführung ist ein ganz wesentlicher Teil dieser Begründung.

Die technische Notfallplanung (IT-BCP) orientiert sich an den kritischen Geschäftsprozessen eines Unternehmens. Wenn man in der IT von einem Desaster spricht, so ist häufig ein Ausfall des IT-Betriebes in seiner Gesamtheit oder wesentlicher Teile davon gemeint. Dabei gilt es zu bedenken, dass IT-Dienste heutzutage stark miteinander verzahnt sind. Fällt beispielsweise der interne LDAP- oder DNS-Dienst aus, so ist es Benutzern praktisch nicht mehr möglich, File- und Print-Sharing sowie E-Mail zu nutzen, da die Server nicht mehr erreichbar sind, obwohl sie einwandfrei funktionieren.[10] Der Erfolg der Planung für IT-Systeme ist daher in hohem Maße abhängig von einer korrekten Identifizierung dieser Zusammenhänge zwischen Prozessen und Funktionen. Daraufhin müssen die Anforderungen an die benötigten Hardware, Software und Daten für die einzelnen Funktionen ermittelt und angemessene Lösungen umgesetzt werden.

[8] [Bun07a], AT7.1-Textziffer 3
[9] März 2008, [Abe08]
[10] [Bau08]

Geeignete Hardware zur Erfüllung der Geschäftsfunktionen muss zu jeder Zeit verfügbar sein. Dazu zählen beispielsweise Server, Mainframes oder verteilte LAN-Netzwerke, die essentielle Dienste oder Ressourcen bereit stellen. Auch Anforderungen an die Kapazitäten (Speicher, Datendurchsatz) sind zu beachten. Generell besteht die Möglichkeit, entsprechendes Notfallinventar selbstständig bereitzuhalten oder Serviceleistungen spezialisierter Anbieter einzukaufen. Die Lagerung von Notfallinventar (häufig Duplikate) ist mit wachsender Unternehmensgröße eine zunehmende, finanzielle Belastung (Lagerhaltungskosten, Logistik etc.). Je nach DR-Strategie kann dies aber die kostengünstigste Alternative darstellen. Neben der reinen Hardware sollte auch für eine Ausweich-Arbeitsumgebung vorgesorgt sein (Standortsicherheit). Dies empfiehlt sich insbesondere deshalb, da durch bestimmte Ereignisse (Feuer, Explosion, Überschwemmung, giftige Gase, Streiks etc.) der Zugang zu den gewöhnlichen Arbeits- und Geschäftsräumen gesperrt sein kann. Servicedienstleister bieten hier sowohl mobile als auch stationäre Lösungen an, die als Hot Site, Warm Site und Cold Site unterschieden werden. Eine Hot Site ist eine Kopie der normalen Arbeitsräume innerhalb der Organisation mit allen IT-Systemen, Infrastrukturen, Applikationen und (beinahe allen[11]) Datenbeständen für minimale Verluste während eines Notfalls. Die Warm Site enthält ebenfalls Duplikate der Hardware, aber keine Kopien des Datenbestands. Diese werden erst im Notfall aufgespielt. Eine Cold Site hingegen ist nicht mehr als ein klimatisierter Arbeitsraum, ohne jegliche vorinstallierte Hardware. Die Cold Site ist damit die einfachste und günstigste Variante eines Ausfall-Standorts. Im starken Kontrast dazu die Hot Site, die durch permanente Einsatzfähigkeit und Echtzeit-Datenspiegelung hohe Kosten verursacht. Die Auswahl hängt vom Kosten-Nutzen-Verhältnis – Umsatzverlust durch Ausfalldauer vs. Unterhaltungskosten der Backup Site – und der Strategie des Unternehmens ab (Die Flugleitzentrale am Frankfurter Flughafen sichert sich bspw. mit mehreren Hot-Sites ab, ein junges Grafikdesign-Startup hat sicher geringere Anforderungen).

Wie zuvor angesprochen, müssen neben Maßnahmen zur Verfügbarkeit der Hardware auch die Software- und Datenbestandsanforderungen des BCP umgesetzt werden. Eine Lösung ist beispielsweise die Echtzeitspiegelung aller Daten zu einer Hot Site. Kostengünstigere Alternativen reichen von regelmäßigen Sicherungen auf permanenten Datenträgern (z.B. Bänder, CD, BlueRay etc.) über elektronisches Data Vaulting (Offsite Datenlagerung) und Continous Data Protection bis zu Virtualisierungsstrategien. Letztere haben zudem den Vorteil, durch Erweiterungen der virtuellen Infrastruktur die Möglichkeit zur Remotesteuerung und -arbeit zu schaffen. Auf diese Weise kann das Personal in entsprechenden Notfallsituationen entlastet und, bspw. falls physische Anwesenheit am Arbeitsplatz nicht möglich ist, durch Heimarbeit seine Funktion erfüllen. Solche Strategien richten sich wiederum direkt an die Hardware.

Die Umsetzung von IT-Lösungen sind so individuell wie die Anforderungen und das

[11] abhängig von DR-Strategie und RPO, siehe Abschnitt 6.2

Unternehmen selbst. Fragestellungen der Sicherungsstrategie beschäftigen sich mit den Charakteristiken unterschiedlicher Backup-Optionen, dem Bedarf an unterstützender (BCP-) Software (siehe Kapitel 6) und der Effektivitätssteigerung umgesetzter Strategien. Diese Strategien werden insbesondere von zeitlichen Anforderungen bestimmt, wie Reaktionszeiten sowie Ausfall- bzw. Wiederherstellungszeiten. Benutzer- und Synchronisierungsmanagement sind weitere Aufgaben des IT-Aspekts. Ebenfalls müssen die rechtlichen Anforderungen an die IT (siehe Abschnitt 4.3) eines Unternehmens im Rahmen von Business Continuity ermittelt werden. In MaRisk ist für den Finanzsektor festgelegt, dass die „IT-Systeme (HW, SW) und die zugehörigen IT-Prozesse die Integrität, Verfügbarkeit, Authentizität sowie die Vertraulichkeit der Daten sicherstellen“[12] müssen. Damit einhergehend ist die Planung eines Programms zum Test und zur Verbesserung der technischen Sicherungs- und Wiederaufnahmeprozesse.

4.3 Organisation

Neben der personellen Notfallplanung und der technischen Notfallplanung (v.a. IT-Systeme) umfasst Business Continuity Planning auch ein breites Feld organisatorischer Aufgaben, die nicht in diese Kategorien eingeordnet werden können. Diese Aufgaben haben häufig einen unterstützenden oder übergeordneten Charakter und fördern durch eine unternehmensweite Implementierung eine BC Kultur, die sowohl Mitarbeiter und Management als auch externe Institutionen wie Lieferanten oder Notrufdienste (Polizei und Feuerwehr) betreffen.

Eine der Basisaufgaben ist die Analyse von Auswirkungen regionaler Katastrophen. Beispielsweise Naturkatastrophen bedrohen Unternehmen abhängig von ihrem Standort. Generell sind die zu erwartenden Auswirkungen von Überschwemmungen nahe Flüssen oder Meeren größer als im höher gelegenen Inland. In Bergregionen hingegen ist auf Lawinen zu achten, die nicht nur die Unternehmensgebäude direkt beschädigen können, sondern auch Straßen oder Tunnel zu blockieren drohen und damit die Versorgung eines Unternehmens. Neben den Naturkatastrophen sind es auch von menschlicher Hand geschaffene Standortvorgaben, die bei Erstellung eines Kontinuitätsplans berücksichtigt werden müssen. Krisen in einem nahegelegenen Chemieunternehmen, einer Produktionsstätte für biologische Schädlingsbekämpfungsmittel oder einen Atomkraftwerk können schnell zu einer eigenen Krise werden.

Auf die Vielfältigkeit an denkbaren Szenarien, die die wirtschaftliche Existenz eines Unternehmens gefährden können, sollte mit einen modularen Aufbau eines BC Plans reagiert werden In enger Zusammenarbeit mit dem Risikomanagement des Unternehmens sollten die kritischen Geschäftsprozesse identifiziert und in funktionale Bausteine zerlegt werden. Ein Notfallmodul eines Handelsunternehmens kann zum Beispiel sein:

[12] [Bun07a], AT7.3

„Beladen an der Hauptladerampe nicht möglich“, anstatt mehrere Szenarien von Sturmschäden zu beschreiben. Modulare Pläne sparen Zeit sowohl in der Anwendung (geringere Reaktionszeit wegen höherer Flexibilität) als auch in der Entwicklung (Vermeidung von Redundanzen in Szenarien und Orientierung an Funktionen). Verschiedene Krisen haben oftmals ähnliche Auswirkungen. So könnte in dem obigen Beispiel die Hauptladerampe auch wegen Hagelschäden oder einem Kabelbrand betriebsunfähig sein. Szenariobeschreibungen für diese Fälle sind mit einem deutlichen Mehraufwand in der Entwicklung verbunden. In der Anwendung sind modulare Pläne von großem Vorteil, da reale Notfälle nicht notwendigerweise mit Szenariobeschreibungen identisch sind und so flexibler und schneller eine Wiederherstellung von (Geschäfts-) Funktionen unternommen werden kann.

Eine vorausschauende Organisation sollte auch stets die praktische Einsatzfähigkeit der Notfallpläne sicherstellen. Dies bedeutet zum einen, dass ein ständiger Prozess zur Aktualisierung der Pläne etabliert werden muss, der die Änderungen im Unternehmen und Schadensauswirkungen auf Geschäftsprozesse realistisch widerspiegelt. Dazu gehört auch jederzeit zu wissen, wie im Notfall zugangsbeschränkte Räume betreten werden können. Zum anderen können es katastrophengefährdete Gebiete notwendig machen, auch für den Ausfall von Wasserversorgung, Abwasserentsorgung, Elektrizität oder Benzin vorzusorgen, um Ersatzmaschinen weiter zu betreiben. Bspw. ist ein Notstromaggregat nur dann eine gute Lösung für Stromausfälle, wenn auch (genug) Treibstoff vorhanden ist, um das Aggregat zu betreiben.

Die Sicherstellung der sofortigen Handlungsfähigkeit auf Basis des BCP geschieht durch die Organisation und Durchführung von Trainings und Tests. James Royds[13] betonte auf der BC Expo im April 2008, dass „training [and] exercising incident management teams in the art of incident / crisis management“ als reine Business Continuity Aufgabe eine Schlüsselanforderung des BCP-Prozesses ist[14]. Trainierten Notfallteams muss gleichzeitig die nötige Authorität eingeräumt werden, um Maßnahmen einzuleiten und durchzuführen. Neben qualifiziertem Personal ist für die Bereitstellung nötiger Ressourcen zu planen. Case Studies[15] haben gezeigt, dass „Hilfe zu Selbsthilfe“ in Notfallsituationen dazu beiträgt, Personal zu entlasten und so zur Fokussierung der Mitarbeiter auf die Wiederherstellung der Unternehmensprozesse beitragen. Solche „Disaster Packs“ beinhalten bspw. die Versorgung mit Verpflegung und Wohnraum für die Notfallzeit. Auch die Suche nach Parkplätzen oder andere Verzögerungen müssen in der Planung berücksichtigt werden. Für erfolgreiche Tests ist es erforderlich, dass Kommunikationsressourcen (Telefone, Computer, Übertragungskapazitäten etc.) definiert sind und bereitstehen. Der BSI-Standard 100-4 empfiehlt zudem eine verantwortliche Person („Prozesseigentümer

[13] Zertifiziert durch das BCI
[14] [Roy08]
[15] Bspw. in [Hil07a]

Notfallplanung“) der Unternehmensleitung zu bestimmen – für kurze Entscheidungswege in der Vorbereitung und im Notfall.

Zur Unterstützung der Maßnahmen im Rahmen von Business Continuity sollte darauf geachtet werden, dass ausreichend Sicherheitsvorkehrungen installiert sind. Dazu zählen u.a. Rauchdetektoren, Feuersprinkler und Notausgänge, welche leicht erkennbar sein müssen und im BCP dokumentiert sein sollten. Auch Arbeitsrichtlinien gehören in diesen Bereich: Zur Vermeidung von Diebstahl und Schutz unternehmenseigener Informationen sind Papierstapel am Arbeitsplatz oder ungesperrte PCs kritisch zu betrachten.

Ein weiterer Teil der organisatorischen Aufgaben ist die Kommunikation nach außen. Dabei sind drei Gruppen von Stakeholdern zu unterscheiden. Erstens sollte eine gute Zusammenarbeit mit lokalen Behörden wie Feuerwehr, Polizei, Krankenhaus und Verwaltung etabliert werden, um im Notfall bestmögliche Unterstützung zu bekommen. Zweitens sollten die Kontaktdaten der Lieferanten jederzeit verfügbar sein, um durch intensive Kooperation eine optimale Abstimmung der eigenen BC Planung und den dokumentierten BC Plänen der Lieferanten zu erzielen. Drittens sollte die Kommunikation mit den weiteren Interessensgruppen und der Öffentlichkeit vorbereitet sein. Einzelne PR-Sprecher oder ganze PR-Unternehmen können engagiert werden, eine Notfallsituation oder Krise in den Medien nicht zum Schaden des Unternehmens, der Mitarbeiter und Stakeholder eskalieren zu lassen.

Weitere Risiken, die den Planungsprozess beeinflussen, sind generell jene, auf die das Risikomanagement zeitlich nicht reagieren kann (vgl. Abschnitt 2.4). Solche Risiken können in allen wichtigen Bereichen liegen und durch unerwartete oder schlagartige Ereignisse herbeigeführt werden. Ein Beispiel: Die Risiken der Kundenbeziehungen sind Teil des Risikomanagements. Ist ein Hauptabnehmer von medizinischem Spezialequipment aber auf Grund neuer Forschungserkenntnisse gezwungen, seine bisherigen Behandlungsmethoden zu ändern und einen wirtschaftlichen Schaden durch eine drastische Reduzierung der Einkäufe zu minimieren, hat dies große Auswirkungen und bedeutet eine mögliche existenzielle Bedrohung für den Lieferanten.

Im Rahmen des organisatorischen Aspekts der BC Planung müssen geeignete Verträge für die Personalplanung (Schulungen), IT-Planung (Recovery Sites) und Geschäftsplanung (PR-Agentur) ausgehandelt und abgeschlossen werden. Ziel sollte immer die Erhöhung der Wiederherstellungseffizienz bzw. die Verringerung der Komplexität der Maßnahmen sein, wobei auch hier ein wirtschaftlich plausibler Kostenrahmen eingehalten werden muss (Abbildung 4.3).

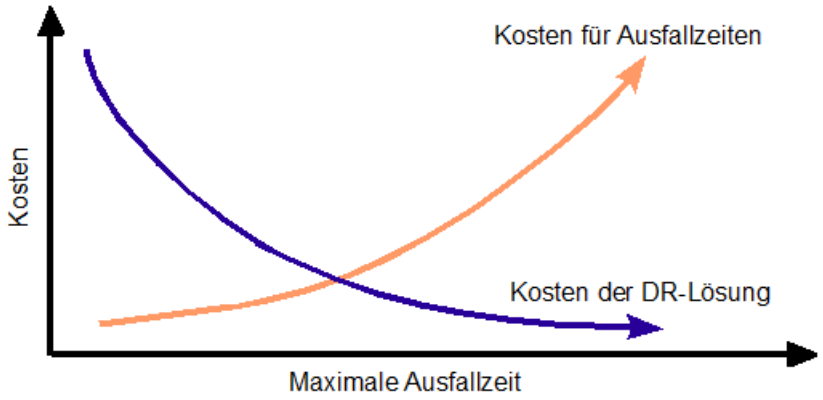


Abb. 4.3: Eine von vielen Herausforderung des BCP: Kosteneffizienz. (Quelle: [Hil07a], S. 240)

5 Der Business Continuity Plan

Das Contingency Planning umfasst wie bereits gesehen eine große Anzahl an präventiven und reaktiven Maßnahmen, die ihrerseits auf technischen, organisatorischen und personellen Gegebenheiten oder auf entsprechenden Annahmen über die Geschäftsprozesse beruhen. Ziel muss es sein, diese Fülle an Informationen auf aktuellem Stand in einer Notfallsituation schnellstmöglich zugänglich und anwendbar zu machen. Diese Aufgabe soll durch das Business Continuity Planning (BCP) erfüllt und das Resultat in dem Business Continuity Plan (BC Plan) dargestellt werden.

Der BC Plan dient somit als Leitfaden der Disaster Recovery. Drei Grundanforderungen müssen dabei beachtet werden[1]:

Der Plan muss aktuell sein! Ein veralteter Notfallplan ist nicht nur nutzlos, sondern führt zu einer trügerischen Sicherheit und zu selbstbewussten (aber unbewussten) Fehlentscheidungen, die mehr Schaden anrichten können als Entscheidungen aus der Gewissheit heraus, nicht vorgesorgt zu haben.

Der Plan muss verfügbar sein! Der Vorteil eines aktuellen Plans ist verloren, wenn er nicht schnell herangezogen werden kann; bspw. wenn er in Hamburg benötigt, aber nur als Druckexemplar im München gelagert wird. Der Plan sollte in elektronischer Form auf den mobilen Geräten (USB Sticks, CDs/DVDs, PDAs, Notebooks, etc.) der Schlüsselpersonen[2] stets mitgeführt werden. Es können auch Aufgabenbeschreibungen zusammen mit den dafür notwendigen kritischen Informationen im Brieftaschenformat individuell für einzelne Personen (Individual Default Response (IDR)) angefertigt werden, die jederzeit leicht mitzutragen sind[3].

Der Plan muss leicht verständlich sein! Aufbau und Inhalt müssen so strukturiert sein, dass jede Person ohne Verzögerung erkennt, was ihre Aufgaben sind und welche Schritte wie und wann eingeleitet werden müssen. Gleichzeitig muss der Zusammenhang zwischen den einzelnen Rollen und Aufgaben in einem größeren Kontext dargestellt werden, wobei besonders auch die Annahmen deutlich beschrieben sein sollten, um die geplanten Strategien bestmöglich auf eine reale Notfallsituation anwenden zu können.

[1] Vgl. [Mar02], S. 142f

[2] Sicherheitsaspekt: Ein BC Plan enthält sensible Informationen, die missbraucht werden können. Teile des Plans sollten daher nur an verantwortliche Personen kommuniziert werden.

[3] [Luc04]

5.1 Aufbau und Inhalt

Der Business Continuity Plan ist kein einzelner, zusammengeschriebener Plan – und noch weniger eine Business Continuity Strategie. In Kapitel 2 wurde der BC Plan bereits als „documented collection of procedures and information“ definiert und in Abschnitt 2.1 wurde gezeigt, dass diese Sammlung („collection“) zumindest einen IT- und einen Geschäftsaspekt besitzt. Tatsächlich ist der BC Plan eine Zusammensetzung aus mehreren spezialisierten Teamplänen, welche die Notfallvorsorge- und Krisenmanagementstrategien dokumentieren, die zuvor basierend auf Anforderungs- und Auswirkungsanalysen (BIA[4]) festgelegt wurden. Diese Pläne und Teams können bspw. als Business Resumption Plan/Team und Disaster Recovery Plan/Team unterschieden werden, oder in großen Organisationen weiter differenziert sein, zum Beispiel in Geschäftseinheiten, IT Recovery, Logistik, Kommunikation, allgemeine Koordination etc.[5] Informationen über Grundsätze oder zurückliegende Versionen bleiben diesen Teamplänen bewusst vorenthalten, um nur die direkt für die Notfallsituation erforderlichen Handlungsschritte zur Vermeidung weiterer Eskalation und zur Wiederherstellung von System- und Geschäftsaktivitäten darzustellen. Sie beinhalten also ausschließlich die Informationen, die das entsprechende Team zur Erfüllung seiner Funktion benötigt.

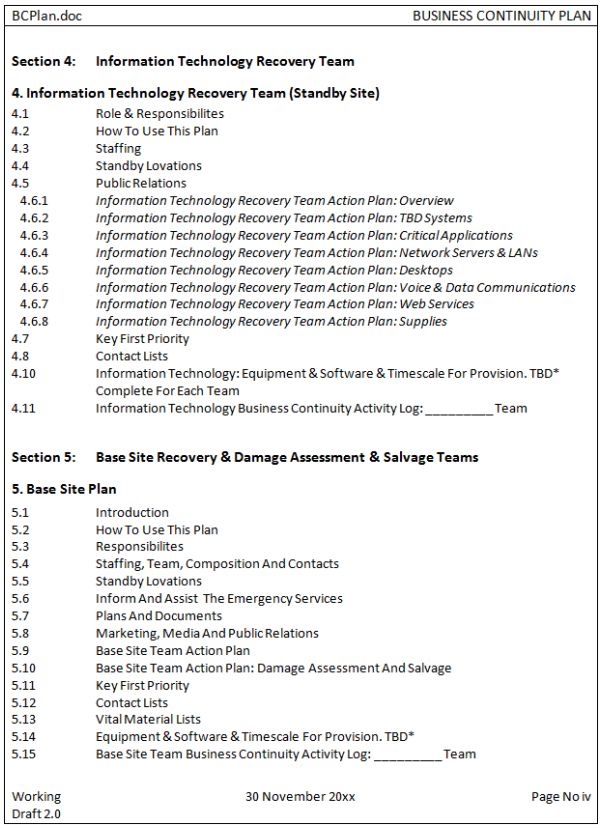
Präsentiert wird der BC Plan in einer leicht verständlichen Struktur, wenn er sowohl nach Rollen und Teams, aber auch nach den Namen der Mitarbeiter sortiert und durchsucht werden kann. Auf diese Weise kann jede Schlüsselperson schnell ihre individuellen Zuständigkeiten und Befugnisse erkennen und angemessen agieren. Baumstrukturen, die bei einer Rollenbetrachtung erwachsen und später oftmals als Telefonbäume genutzt werden, haben sich in einer realen Notfallsituation selten als besonders effizient herausgestellt. Obwohl manches Unternehmen daher ein IT-gestütztes Nachrichtensystem vorzieht[6], sind dennoch die Kontaktdaten von Teammitgliedern und Schlüsselpersonen obligatorisch in jedem Teamplan aufzunehmen.

[Hil07a] nennt weitere Punkte, die in einem Business Continuity Plan nicht fehlen sollten: Neben einem selbstverständlichen Inhaltsverzeichnis, einer Beschreibung des Umfangs und den bereits angesprochenen Annahmen, auf denen der Plan basiert – neben ineffektiven Tests die Hauptursache, warum BC Pläne misslingen[7] – gehört außerdem eine Gebrauchsanleitung ins Repertoire sowie eine Auflistung der bekannten Schwächen des Plans zusammen mit einer Liste der Personen, die für deren Behebung verantwortlich sind. Bei den Aktionsplänen für die einzelnen Teams darf nicht fehlen:

- Namen aller Teammitglieder und Ersatzkräfte inkl. Kontaktdaten

[4] Business Impact Analysis
[5] [Luc04]
[6] [Luc04]
[7] [Var05]

- Prioritätenliste für die Wiederherstellung
- Zielsetzungen für Wiederherstellungszeiten (RTO[8])
- Zielsetzungen für Sicherungszeitpunkte (RPO[9])
- Anforderungen an Berichte
- Liste wesentlicher Dokumente und Materialien inkl. der Beschreibung, wie/wo diese zu bekommen sind (darunter Passwörter, Schlosskombinationen, etc.)
- Zeitrahmen zur Bereitstellungen benötiger Ressourcen
- Relevante Verträge (interne und externe)
- Sonstiges unterstützendes Material wie Prozeduren, Pläne, Karten usw.



BCPlan.doc BUSINESS CONTINUITY PLAN

Section 4: Information Technology Recovery Team

4. Information Technology Recovery Team (Standby Site)

4.1 Role & Responsibilites
4.2 How To Use This Plan
4.3 Staffing
4.4 Standby Lovations
4.5 Public Relations
4.6.1 *Information Technology Recovery Team Action Plan: Overview*
4.6.2 *Information Technology Recovery Team Action Plan: TBD Systems*
4.6.3 *Information Technology Recovery Team Action Plan: Critical Applications*
4.6.4 *Information Technology Recovery Team Action Plan: Network Servers & LANs*
4.6.5 *Information Technology Recovery Team Action Plan: Desktops*
4.6.6 *Information Technology Recovery Team Action Plan: Voice & Data Communications*
4.6.7 *Information Technology Recovery Team Action Plan: Web Services*
4.6.8 *Information Technology Recovery Team Action Plan: Supplies*
4.7 Key First Priority
4.8 Contact Lists
4.10 Information Technology: Equipment & Software & Timescale For Provision. TBD* Complete For Each Team
4.11 Information Technology Business Continuity Activity Log: _____ Team

Section 5: Base Site Recovery & Damage Assessment & Salvage Teams

5. Base Site Plan

5.1 Introduction
5.2 How To Use This Plan
5.3 Responsibilites
5.4 Staffing, Team, Composition And Contacts
5.5 Standby Lovations
5.6 Inform And Assist The Emergency Services
5.7 Plans And Documents
5.8 Marketing, Media And Public Relations
5.9 Base Site Team Action Plan
5.10 Base Site Team Action Plan: Damage Assessment And Salvage
5.11 Key First Priority
5.12 Contact Lists
5.13 Vital Material Lists
5.14 Equipment & Software & Timescale For Provision. TBD*
5.15 Base Site Team Business Continuity Activity Log: _____ Team

Working Draft 2.0 30 November 20xx Page No iv

Abb. 5.1: Auszug eines Teamplans (Quelle: vgl. [Hil07a], S. 294ff)

[8] Recovery time objective
[9] Recovery point objective

5.2 Erstellung des Plans innerhalb des Notfallmanagement-Prozesses

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt im BSI-Standard 100-4 die Erstellung des Plans innerhalb eines vier Phasen Notfallmanagement-Prozesses. Dieses systematische Vorgehen orientiert sich wie bereits die anderen Standards des IT-Grundschutzes am PDCA-Modell[10]. Abbildung 5.2 stellt den Ablauf grafisch dar.

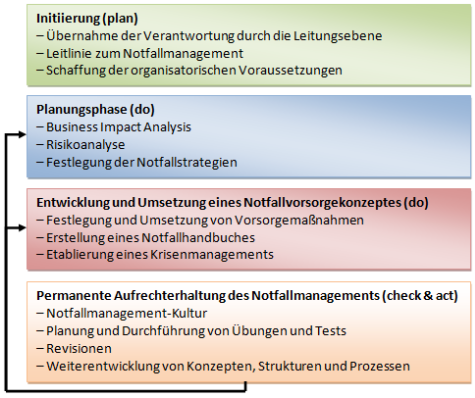


Abb. 5.2: Der Notfallmanagement-Prozess des BSI (Quelle: [Bun08])

Initiierung Zu Beginn muss Business Continuity als ernst genommenes Thema innerhalb einer Organisation etabliert werden. In der Initiierungsphase ist daher für die Unterstützung und Einbindung der Unternehmens- oder Behördenleitung zu sorgen und eine Leitlinie zu entwickeln, die die nötigen Rahmenbedingungen klärt. Dazu gehört die Bereitstellung von qualifiziertem Personal und ein ausreichend großes Budget.

Planungsphase Bevor der Business Continuity Plan geschrieben werden kann, müssen verstreute Daten erhoben und Informationen daraus gewonnen werden. Kernstücke sind die Business Impact Analyse und eine darauf aufbauende Risikoanalyse für die kritischsten Prozesse und Ressourcen. Sind alle Geschäftsprozesse identifiziert, deren Abhängigkeiten untereinander erkannt und deren Kritikalität eingeschätzt, so können auf dieser Basis RPOs, RTOs und weitere Mindestanforderungen festgelegt und zu einer kosteneffizienten Notfallstrategie zusammengestellt werden.

Entwicklung und Umsetzung eines Notfallvorsorgekonzeptes In der dritten Phase („Do“) wird der BC Plan erstellt. Im Rahmen der ausgewählten Strategie werden dazu angemessene Vorsorgemaßnahmen umgesetzt. Diese Angemessenheit ergibt

[10]Plan-Do-Check-Act – Modell zur Unterstützung eines kontinuierlichen Verbesserungsprozesses

sich aus den Aspekten, die bereits in Kapitel 4 beschrieben sind und individuell für jede Organisation betrachtet werden müssen.

Permanente Aufrechterhaltung des Notfallmanagements Der PDCA-Ansatz betont grundsätzlich die Kontinuität eines Prozesses. Dazu ist es notwendig, eine organisationsweite Kultur zu etablieren, in der eine Sensibilität für die Aufgabe und das Ziel jenes Prozesses herrscht. Auch beim Notfallmanagement kann dies durch Schulungen und themenbezogene Trainings erreicht werden – zum einen um alle Mitarbeiter über die Existenz eines Business Continuity Programms zu informieren, zum anderen um speziellen Mitarbeitern Spezialwissen für Schlüsselrollen in dem Prozess zu vermitteln. Die Entwicklung einer optimalen Notfallvorsorge ist ein langer Prozess, an dem aktiv gearbeitet und dessen Maßnahmen regelmäßig zu testen und in wiederholten Durchläufen der Planungs- und/oder Umsetzungsphase weiterzuentwickeln sind.

Neben dem hier dargestellten Prozessablauf des deutschen BSI-Standards gibt es andere Ansätze, auf die an dieser Stelle verwiesen sein soll. Hervorzuheben sind dabei die Ausführungen des amerikanischen National Institute of Standards and Technology (NIST)[11], beschrieben in [Mar02], und der BCM Lifecycle des British Standard Institute, der einen zentralen Bestandteil des BS25999-1 ausmacht. Differenzen sind auf den ersten Blick in der reinen Anzahl an Phasen zu erkennen, in die der Prozess unterteilt ist. Ein zweiter Blick auf die dahinter stehenden Funktionen zeigt, dass der deutsche Standard inhaltlich die gleichen Absichten verfolgt wie seine britischen und amerikanischen Pendants. Alle Beschreibungen haben zudem gemein, dass Business Continuity Planning als Kreislauf dargestellt wird.

[11] Internetseite: `http://www.nist.gov`

6 Tools zur Unterstützung im BCP Prozess

Ein komplexer Prozess wie das Notfallmanagement kann neben den Dienstleistungen eines spezialisierten Anbieters durch ein einzelnes oder mehrere geeignete Software-Werkzeuge unterstützt werden. Die am Markt verfügbaren Tools reichen von den proaktiven Aufgaben der Notfallvorsorge bis zu den reaktiven Maßnahmen des Krisenmanagements. Die Tools sollten sich dabei stets an den Anforderungen des Prozesses richten – nicht umgekehrt. Lange Zeit bestand der Konflikt, dass den sehr individuellen Anforderungen des BCP Werkzeuge gegenüber standen, die eine bestimmte Vorgehensweise zu stark diktierten oder aber zu allgemein gehalten waren, dass sie nicht auf die Bedürfnisse des Unternehmens ausreichend angepasst werden konnten.[1] Heutzutage sind diese Kinderkrankheiten weitgehend beseitigt, sodass der Einsatz eines Software-Werkzeuges die Tätigkeiten der an der Notfallorganisation beteiligten Personen erheblich erleichtern kann.

6.1 Tools der Notfallvorsorge

Das Business Continuity Institute (BCI) hat zusammen mit dem Disaster Recovery Institute International (DRII) zehn Kompetenzbereiche des BCP identifiziert. Diese sind[2]:

1. Project Initiation and Management
2. Risk Evaluation and Control
3. Business Impact Analysis
4. Developing Business Continuity Strategies
5. Emergency Response and Operations
6. Developing and Implementing BC Plans
7. Awareness and Training

[1] [Hil07a], S. 369
[2] [Dis03]

8. Maintaining and Exercising the BC Plan
9. Public Relations and Crisis Coordination
10. Coordination with External Agencies

Alle Bereiche können durch Werkzeuge unterstützt werden. Die Bereiche sechs (Developing and Implementing BC Plans) und acht (Maintaining and Exercising the BC Plan) stehen im Fokus der verfügbaren BCP Tools – aus historischen Gründen (Kernbereich) und da sie die tatsächliche Entwicklung und Dokumentation des BC Plans verbessern. Die Bereiche zwei, drei und fünf können ebenfalls von Software unterstützt werden, die speziell für das BCP entwickelt und implementiert wurde. Die Bereiche eins, vier, sieben, neun und zehn spielen eine wichtige Rolle als BCP-Kompetenz, die dabei verwendeten Tools sind aber meist nicht ausschließlich für diesen Zweck entwickelt und können daher auch in anderen Projekten und Abteilungen einer Organisation eingesetzt werden.

Abb. 6.1: Phasen der Notfallvorsorge (Quelle: Eigendarstellung)

Für eigenständige Softwareapplikationen im BCP-Kernbereich muss auf kommerzielle Produkte zurückgegriffen werden. Zwar lässt sich Open Source Unterstützung finden, jedoch zeigt sich diese bisher nur in Form von Templates, die sehr häufig auf Microsoft Word oder Microsoft Excel basieren. Templates, die nicht nur als Open Source, sondern auch zahlreich gegen Entgelt in Paketen zwischen 30 € bis 300 € angeboten werden, haben generell den Nachteil, dass sie nicht als Unterstützung eines kontinuierlichen Prozesses wahrgenommen werden. Des Weiteren betrachten sie nur einen kleinen Ausschnitt des gesamten Prozesses, decken keine internen Abhängigkeiten oder Referenzen auf und sind umständlich in der Pflege. Templates können jedoch als Hilfestellung zum Einstieg in die Notfallvorsorge dienen, da sie bspw. im Bereich Risikoanalyse und -bewertung sowie Planentwicklung auf wichtige Aspekte aufmerksam machen können.

Die großen Software-Suiten beinhalten neben dem Kernprodukt (Analyse, Entwicklung, Darstellung und Verwaltung eines BCP) viele Zusatzfunktionen in den Bereichen Datenbankanbindung, Visualisierung, Benachrichtigungssysteme, Datenschutz, Mandantenfähigkeit, Schnittstellen, Online-Erreichbarkeit u.v.m. Die nachfolgenden Tools sollten bei der Auswahl in Betracht gezogen werden[3]:

[3] Internetseite: `www.softguide.de`

Continuity Manager CM ist eine flexible, auf Lotus Notes basierende BCP-Software mit aktiver Online-Begleitung der Plandurchführung im Übungs- und Echtfall.

Hersteller: HEINEUNDPARTNER GmbH – **BS:** Windows
Nettopreis: ca. 10000 € – `www.heine-partner.de/CM.130.0.html`

Continuity Action Planning Tool CAPT ist eine etablierte Datenbankanwendung zur Verwaltung von Informationen und zur Erstellung von Notfallhandbüchern.

Hersteller: HEINEUNDPARTNER GmbH – **BS:** Windows
Nettopreis: ca. 10000 € – `www.heine-partner.de/CAPT.249.0.html`

Incident Manager Der Incident Manager verwaltet vernetzte Informationen und hilft beim Aufbau eines effektiven Risiko- und Notfallmanagements.

Hersteller: elementec – **BS:** Windows
Nettopreis: ca. 2350 € – `www.elementec.com/imanager.htm`

XENCOS Die modulare Software Suite XENCOS besitzt ein BCP, BIA und Risk Analysis Modul und unterstützt den gesamten Notfallmanagement-Prozess.

Hersteller: HEINEUNDPARTNER GmbH – **BS:** Windows
Nettopreis: ca. 15000 € – `www.heine-partner.de/XENCOS.272.0.html`

Living Disaster Recovery Planning System LDRPS ist das weltweit am häufigsten eingesetzte Planungstool für BCP, inkl. einen umfangreichen Zugriffs- und Datenschutz, großem Schnittstellenumfang, flexibel, aktuell und Internetfähig.

Hersteller: Strohl Systems – **BS:** Windows
Nettopreis: ca. 15000 € – `www.strohlsystems.com/Software/LDRPS`

alive-IT Alive-IT ist eines der innovativsten Notfallplanungsprodukte, das heute erhältlich ist mit einem Einsatzspektrum von der Dokumentation Ihrer Notfallprozesse bis hin zu prozessorientierten Betriebskonzepten für die Produktion. Webbasiert und plattformunabhängig (Java) unterstützt es bei der Planung, Dokumentation und dem Wiederanlauf.

Hersteller: Controll-IT GmbH – **BS:** Windows, Linux, Solaris
Nettopreis: ca. 2000 € – `www.controll-it.de/de/software/index.html`

Eine Übersicht weiterer Tools zum Notfallmanagement kann unter [BCM08] eingesehen werden.

6.2 Tools der Notfallbehandlung

Für die Notfallbehandlung gibt es eine nochmals breitere Palette an Softwareangeboten, die von Eskalationsmaßnahmen über Wiederanlauf bis Wiederherstellung alle Bereiche

des Krisenmanagements unterstützen. Die Tools unterscheiden sich dabei in dem Ziel der Sicherung (Sicherungsobjekt: Daten, Anwendungen, Standort), der Methodik bzw. Funktionalität (Ablauf, Zuverlässigkeit, Geschwindikkeit, Sicherheit) und daraus resultierend auch im Preis. Recherchen im Rahmen dieser Diplomarbeit haben ergeben, dass die Kosten für Basisprodukte (keine Zusatzfunktionen, keine optionalen Upgrades etc.) zwischen ca. einhundert bis mehreren zehntausend Euro liegen. Der Endbetrag ergibt sich immer aus den eigenen Anforderungen und der Entscheidung für eine angemessene Lösung, zu welcher auch Serviceleistungen wie Schulungen oder Updates gehören.

Fehlender Service ist u.a. ein Grund, warum Open Source Lösungen außerhalb des Home Office / Privatnutzer DR-Bereiches nicht anzutreffen sind. Zwar gibt es Software, die zur Synchronisation oder zur Wiederherstellung einzelner Festplatten geeignet ist, allerdings fehlt diesen Tools bisher die nötige Reife oder schlicht die Funktionalität, die bereits ein junges Startup zur Sicherung von Daten und Anwendungen benötigt. Selbst wenn es gelingt, in einem gewissen Rahmen (diverse) freie Software zu finden, die einfachen Ansprüchen an Funktion, Zuverlässigkeit und Backup- / Wiederherstellungszeit genügt, so sind es im Gegensatz zu dieser Menge an unterschiedlicher Funktionssoftware die kommerziellen Tools des Disaster Recovery, die durch eine einfachere Bedienung und Übersicht hervortreten.

Unterschieden werden können Methoden zur Datensicherung, zur Applikations- und Systemsicherung sowie zur Standortsicherung.[4] Zur Sicherung von Daten werden drei Techniken auf dem Markt angeboten: RAID-Systeme, das klassische Verfahren der Backup-and-Restore Systeme (BR) und die Continous Data Protection Methode (CDP).

RAID-Systeme organisieren mehrere physische Laufwerke zu einem logischen Laufwerk, um eine höhere Datensicherheit bei Ausfall einzelner Festplatten zu erhalten. RAID-Techniken sind immer ein Kompromiss aus Sicherheit, Geschwindigkeit und Kosten. Hersteller empfehlen zur Datensicherheit die RAID-Level 5E und 6. Redundanzen werden stets nur von den gespeicherten Daten und Anwendungen angelegt. RAID dient weder zur Sicherung von Betriebssystemen und Hardware oder zur Standortsicherung.

BR-Systeme sichern periodisch Daten und Anwendungen, in Einzelfällen zusammen mit dem gesamten Systemzustand. Als Medium gelten Bänder oder Bandbibliotheken. Man spricht von virtuellen Bandbibliotheken oder Virtual-Tape-Libraries, wenn an Stelle von Bändern Festplatten benutzt werden, die sich über eigene Treiber als Bandlaufwerke darstellen. Bibliotheken können große Mengen an Speicher verwalten, sind aber langsam in der Wiederherstellung und für eine schnelle Recovery (wenige Minuten oder Stunden) kaum zu gebrauchen. Durch die Auslagerung der Bänder wird die Trennung von Quell- und Sicherungsdaten erreicht, wobei in einer Notfallsituation ein physikalischer

[4] Weitere Ausführungen basieren auf [Bau08] und [Com07]

Rücktransport unvermeidbar und zeitintensiv ist. Virtuelle Bibliotheken machen Bänder überflüssig, verzichten aber auf diese Trennung von Quelle und Sicherung. Größter Nachteil der periodischen Datensicherung ist ihre Trägheit: Datenverlust und Wiederherstellungszeiten können sich über einen ganzen Tag erstrecken. In diesem Zusammenhang werden heute meist zwei Ziele definiert: „Recovery Point Objective“ (RPO) und „Recovery Time Objective“ (RTO). RPO bezeichnet das Intervall zwischen den einzelnen Sicherungen. Mit dem RPO wird damit auch festgelegt, wie viele Daten und Transaktionen maximal verloren gehen dürfen. Bei nächtlicher Sicherung kann der Recovery Point also bis zu 24 Stunden oder einen Arbeitstag zurückliegen. Mit dem RTO wiederum wird die maximal zulässige Zeitspanne für die Wiederherstellung der Dienste definiert. Beide Zielvorgaben sollten so niedrig wie möglich sein, denn prinzipiell gilt: Je niedriger RPO und RTO, desto schneller der Wiederanlauf.

Um den relativ langen Recovery Szenarien der Backup-and-Restore Techniken zu begegnen, gibt es die CDP-Varianten. Diese Alternativen basieren auf einer Snapshot-Technik (z.B. auf dem Volume Shadow Copy Service (VSS) ab Windows 2003) mit einer deutlich höheren Sicherungsfrequenz und niedrigerem RPO. Ein „Backupfenster“ in der Nacht wird damit hinfällig und ein ernsthafter 24x7-Betrieb erst möglich. Als Sicherungsmedium dienen stets Plattensysteme, die sich über beliebige IP-Strecken anbinden lassen und alle Daten permanent sichern. Hat ein Benutzer während eines Backupfensters eine Datei exklusiv im Zugriff, so muss sie von der Sicherung ausgeschlossen werden. Beim Backup mittels eines CDP-Systems müssen zwei grundsätzliche Methoden unterschieden werden: synchrone und asynchrone. Bei einer synchronen Lösung wird jede Änderung unmittelbar auf das Backupsystem mitgeschrieben (leistungsintensiv)[5]. Bei einem asynchronen System werden Änderungen an einer Datei zunächst protokolliert. Das Backupsystem kopiert die geänderten Dateien je nach Auslastung mit einer Verzögerung von wenigen Sekunden bis hin zu einigen Minuten[6]. Vom Standpunkt der Wiederherstellung haben CDP-Systeme eindeutig Vorteile. So schnell wie die Snapshots erzeugt sind, so schnell sind sie auch wieder zurückzuholen. Die Benutzer können Dateien häufig selbst rücksichern, wodurch der RTO-Wert im günstigsten Fall gegen null tendiert.

Geht es um die Prozessabsicherung, so sind andere Techniken nötig. Nicht die Daten, sondern die Systeme, die diese Daten verarbeiten, stehen hierbei im Fokus der Aufrechterhaltung und Sicherung. Imaging, Failover- und Cluster-Systeme sind bekannte Lösungen zur Prozessabsicherung. Beim Imaging wird die gesamte Partition eines Rechners auf Sektorebene kopiert. Dies bietet einen enormen Geschwindigkeitsvorteil gegenüber der Dateiebene und eignet sich insbesondere für eine schnelle Wiederherstellung eines kompletten Rechnersystems („Bare Metal Restore“). Inkrementelle Verfahren

[5] Bekannte, synchrone CDP-Lösungen: DoubleTake, everRun FT, Neverfail und WANSync.
[6] Oft als Add-on für klassische Backup-Lösungen angeboten, z.B. von CA, Symantec oder Microsoft.

sparen Speicherplatz und Tools wie bspw. Acronis' Universal Restore[7] bieten Lösungen für das generelle Probleme des Imaging, Rücksicherungen ausschließlich auf beinah identische Hardware machen zu können. Beim Clustering von Systemen werden einem Serververbund Load Balancer vorgeschaltet, die Anfrage auf die einzelnen Server entsprechend ihrer Auslastung und Verfügbarkeit verteilen. Dies bedeutet gleichzeitig mehr Performance und höhere Verfügbarkeit. Clustering bietet sich bspw. bei Webservern an, wenn Daten nur gelesen werden – oder bei Diensten wie DNS, WINS und Active Directory. Bei schreibendem Zugriff sind an die Applikation besondere Anforderungen gestellt. In Failover-Lösungen steht für jedes zu schützende System ein Zweitsystem bereit, das beim Ausfall des Primärsystems einspringt und dessen Funktion übernimmt. Durch Heartbeat-Signale wird so bspw. der Zustand von DHCP-, Datei-, Druck-, Mail- und Datenbankserver überwacht und automatisch oder manuell auf das nebenstehende Passivsystem umgeschaltet. Standortsicherheit kann durch den Einsatz von geeigneten Replikationstechniken (bspw. synchrone Fibre-Channel-SANs oder kostengünstigere SAS und iSCSI Lösungen) erzielt werden. Ausfall-Rechenzentren und die Duplizierung aller Hard- und Software sind mit Abstand die teuersten Extreme zur Sicherung der Unternehmensprozesse.

Da Failover- und Clusterlösungen teilweise sehr kompliziert zu realisieren sind, setzt man als Alternative immer häufiger Virtualisierungslösungen ein. Neuste Lösungen wie PlateSpin Forge[8] und VM Infrastructure 3[9] haben großes Zukunftpotential. Der VMware ESX-Server 3i[10] beispielsweise lässt sich bereits von einem USB-Stick mit 32 MByte Speicher booten und innerhalb weniger Minuten installieren. In einer virtuellen Maschine laufende Server können mit Technologien wie VMotion von VMware im laufenden Betrieb ohne Reboot auf eine andere physikalische Hardware gebracht werden. Virtuelle bootfähige Disks laufen unter jeder Hardware, da alle Komponenten von der Virtualisierungslösung emuliert werden. Die Zeit für die Wiederherstellung eines ausgefallenen Servers reduziert sich drastisch. Verfügbarkeit und Geschwindigkeit gehören damit zu den großen Vorteilen der Virtualisierung. Ihr großer Nachteil ist allerdings, dass Virtualisierung beim heutigen Stand der Technik eine Menge an I/O-Performance kostet. Performancekritische Datenbankanwendungen lassen sich mit aktueller Technologie oft nicht virtualisieren.

Fazit: RAID Systeme können Daten und Applikationen absichern und stellen eine gute Lösung für einen kontinuierlichen Betrieb dar, bieten aber keine Standortsicherung. Klassische Backup-Systeme sind besonders für die Langzeitspeicherung von Daten geeignet. Auch kostengünstige Sicherungenin regelmäßigen Intervallen lassen sich damit

[7] Internetseite: `www.acronis.de/enterprise/products/ATIES/universal-restore.html` (Stand: Juli 2008)
[8] Internetseite: `www.platespin.com/forge` (Stand: Juli 2008)
[9] Internetseite: `www.vmware.com/products/vi` (Stand: Juli 2008)
[10] Internetseite: `www.vmware.com/products/esxi` (Stand: Juli 2008)

realisieren. Für eine besonders schnelle Wiederherstellung und geringstmöglichen Datenverlust sind CDP-Techniken die bessere Wahl.

Es gibt viele Konzepte im Bereich des Disaster Recovery und es ist eine sehr komplexe Herausforderung, eine gute Lösung für die individuellen Anforderungen einer Organisation zu finden. Rational betrachtet müssen wie schon im Business Continuity Planning die Kosten und Konsequenzen für den Ausfall eines Prozesses über einen bestimmten Zeitraum (Wiederanlaufzeit, Wiederherstellungszeit), z.B. durch den Verlust von Daten, gegen die Kosten für die Toolunterstützung der DR Lösungen abgewogen werden.

7 BCP in der Anwendung

Notfallmanagement braucht *proaktives* Vorgehen für eine bestmöglich *Reaktion* im Notfall. Bisher wurde in den vorangegangenen Kapiteln meist diese geforderte Proaktivität fokussiert: in den Definitionen und Gesetzen sowie im Aufbau und in den Inhalten rund um das Business Continuity Planning. Dabei wurden solide Grundlagen geschaffen, die für das Verständnis und somit zur Anwendung von BCP unerlässlich sind. Dieses Kapitel wendet sich nun der reaktiven Seite des Contingency Planning zu. Am Beispiel eines fiktiven Unternehmens wird das Event eines Notfalls simuliert und analysiert. Ziel ist die Beschreibung der Disaster Recovery – ihre Durchführung, ihre Probleme und ihre Lösungen. Die folgenden Abschnitte behandeln Fragen, die sich bei der Durchführung einer Backup-Planung und der Wiederherstellung von verlorenen Daten stellen. Die Lösungen basieren dabei auf eigenen Erfahrungen, die mit der Acronis Security Suite gesammelt wurden.[1]

Als Grundlage eines solchen Szenarios sind drei virtuelle Maschinen auf einem physischen Serversystem in Betrieb. Der Acht-Kern-Prozessor von Intel mit einer Taktung von jeweils 2,33 GHz schafft zusammen mit 16 GB RAM und mehreren SATA-Platten im RAID 10 Verbund eine solide Ausgangssituation für eine realistische IT-Umgebung. Die virtuellen Maschinen (VM) sind mit VMware erstellt und konfiguriert: VM1 (Rechnername: WorkstationXP) besitzt einen der acht Prozessorkerne (2,33 GHz Intel Xeon CPU), 512 MB virtuellen Arbeitsspeicher und eine 8 GB Festplatte. Die VM1-Konfiguration simuliert im folgenden Szenario einen klassischen Windows-Client mit XP Professional SP2 als Betriebssystem. VM2 (BackupStorage) ist als Klon des VM1-Designs als Auslagerungsort für Sicherungsdateien vorbestimmt. Ein Unterschied zur VM1 besteht jedoch in der verfügbaren Festplattenkapazität: VM2 besitzt eine zweite (virtuelle) Festplatte mit einer Größe von 35 GB. Die dritte VM (Server2003) baut ebenfalls auf einem CPU-Kern auf. Sie verfügt über 1 GB RAM und drei Partitionen à 15 GB. Die VM3 simuliert den zentralen Server des Szenarios mit Windows Server 2003 als Betriebssystem. Die SCSI-Festplatten der virtuellen Maschinen sind im NTFS-Format organisiert. Zu jeder VM kann zur Szenariodurchführung ferngesteuert (Remote-Verbindung) werden. Alle

[1] Die Produktentscheidung basiert auf den Softwareanforderungen des Szenarios, welche im Abschnitt 7.1 „Szenariobeschreibung“ und zu Beginn von Abschnitt 7.2.2 (Frage 2) beschrieben werden. Die Vorteile kommerzieller Produkte für unternehmenskritische Daten im Gegensatz zu Open Source Alternativen konnte bereits in Abschnitt 6.2 im Rahmen der BCP-Tools dargelegt werden und gilt in den Hauptargumenten (Datensicherheit, Service und Missbrauchschutz) entsprechend für alle DR-Lösungen.

Rechner befinden sich in der gemeinsamen Arbeitsgruppe „Safe&Secure“. Das Szenario der Real Fiction GbR soll als Ausgangspunkt und praktische Hilfe für vergleichbare Situationen herangezogen werden können.

7.1 Real Fiction GbR: Szenariobeschreibung

Die Real Fiction GbR ist ein junges Unternehmen aus Koblenz, das virtuelle 3D-Software für die nächste Generation von Konsolensteuerungen erstellt. Weitere Chancen für diese Art von Software liegen im Bereich der Medizin sowie in der Luft- und Raumfahrt. Als ambitioniertes Unternehmen hat die Real Fiction GbR schon früh die Potentiale am amerikanischen Markt erkannt und möchte zu gegebener Zeit auch dort Neukunden gewinnen. Die Entwicklung der gesetzlichen Rahmenbedingungen für ein Notfallmanagement hat das Unternehmen im Blick und interessiert sich schon von Beginn an für eine angemessene Lösung zur Sicherheit ihrer Daten und Geschäftsaktivität.

Das drei Mann starke Kleinunternehmen kam bisher ohne jegliche Notfallvorsorge aus. Die Sicherung von Fortschritten bestand in der unregelmäßigen Auslagerung relevanter Daten auf DVD oder eine dateibasierte Synchronisation auf externen Festplatten. Das Unternehmensgebäude, eine Büroetage in der Innenstadt, ist ausgestattet mit einer Küche, Arbeitsraum und belüftetem Serverraum zur Wärmeabfuhr. Durch die Nähe zum Arbeitsplatz (durchschnittlich fünf Kilometer) verließen sich die Mitarbeiter auf eine schnelle Reaktion im Notfall und die Qualität ihrer Hardware. Auf den Einsatz von Notebooks als Arbeitsmittel zu Gunsten der Mobilität (gelegentlich Heimarbeit und Präsentationen beim Kunden) und dem persönlichem Wohlgefühl wollen die Entwickler nicht verzichten und nehmen den beschränkten Speicherplatz im Vergleich zu Desktop-Systemen in Kauf. WLAN wird jedoch nicht verwendet, da sie auf die Übertragungsraten eines Gigabit-Netzwerks angewiesen sind. Ein Festnetz-Telefon gibt es nicht, was die grundsätzlich Favorisierung von Funksystemen unterstreicht. Der Kontakt mit den Auftraggebern erfolgt daher über Mobiltelefone oder in persönlichen Treffen. Von speziellen Lieferanten ist das Team unabhängig, nicht zuletzt durch die Entscheidung für Standardsoftware. Das Entwicklerteam ist hingegen sehr sensibel gegenüber personellen Ausfällen und setzt sich derzeit intensiv mit dem Thema Ersatzplanung auseinander.

Die Entwicklungsumgebung der Real Fiction GbR basiert auf einem reinem Windows Netzwerk. Ein Windows Server 2003 R2 bildet das Zentrum der angeschlossenen Rechner. Der Server dient zur zentralen Koordination und Speicherung aller wichtigen Unternehmensdaten, darunter auch die Entwicklungsdaten, die von einem SQL Server 2005 verwaltet werden. Des Weiteren befinden sich drei Notebooks (im Folgenden als Workstations bezeichnet) in Unternehmensbesitz, die jeweils mit Windows XP Professional als

Betriebssystem ausgestattet sind. Der Anschluss ans Internet ist über eine DSL16000[2] Leitung geregelt.

Nach einem Festplattencrash auf einem der Notebooks im letzten Monat, verursacht durch einen Virus[3], musste viel Zeit und Geld in die Wiederherstellung kritischer Daten investiert werden, die auf keinem der Backup-DVDs in aktueller Form erhalten waren. Der Vorfall ließ das Unternehmen schnell handeln, um die täglich wachsende Datenmenge (500 MB täglich, 30-40 GB an temporären Daten) mit einem Minimum an zeitlichem Verlust rekonstruieren zu können. Eine angestrebter RPO-Wert von einer Stunde und ein RTO-Wert[4] von zwei Stunden dient als Ausgangssituation für eine angemessene Lösung. Die Real Fiction GbR erzeugt täglich in einem fünfstündigen Prozess ein neues 3D-Modell, das als Arbeitsgrundlage für den Folgetag benötigt wird. Da der Prozess sehr ressourcenaufwendig ist und nicht nur außerhalb der Arbeitszeiten ausgeführt werden kann, muss auf ein intelligentes Zeitmanagement geachtet werden. Der Kostenrahmen wird auf einmalige Anschaffungskosten von 1500 € und jährlichen Ausgaben von maximal 3000 € festgelegt. Darin soll eine Standortsicherheit eingeschlossen sein, inklusive aller anfallender Neben-, Wartungs- und Leitungskosten. Diese Beträge sind in einer Analyse der Geschäftssituation erarbeitet und in Abstimmung mit Vertragsstrafen bei Verzögerungen und Wiederherstellungsalternativen nach einem Vorfall als akzeptabel beschlossen.

Für die Sicherung der Unternehmensdaten hat sich die Real Fiction GbR für die Security Suite des Sicherheitsspezialisten Acronis entschieden. Mit dem Acronis True Image Echo Server for Windows (TIE Server) und Acronis True Image Echo Workstation (TIE Workstation) soll der Schutz der Daten zu jederzeit[5] gewährleistet sein. Die bisher unregelmäßige Sicherung der Notebooks soll automatisiert werden, wobei Wert auf eine einfache, aber zuverlässig Bedienung gelegt wird. An die Server-Software wird die Anforderung gestellt, mit einer sicheren Übertragungstechnik auch den Standort gegen Ausfälle absichern zu können, ohne dabei das Budget für Vorsorgemaßnahmen zu überdehnen. Die Acronis Software erfüllt diese Anforderungen. In den Vorbereitungen möchte sich das Unternehmen an dem BSI-Standard 100-4 orientieren und eine dedizierte Rolle „Notfallmanager“ im Team einführen.

[2] Downspeed 16000 Kb/s, Upspeed 1024 Kb/s

[3] vgl. `http://www.heise.de/ct/05/08/172` (Stand: 19.08.2008), z.B. verbreitet über die Tochter / den Sohn im Heimnetz

[4] siehe Definitionen auf Seite 57

[5] o.g. Bedingungen gelten

7.2 Lösungen im Business Continuity Planning

Als erfolgsversprechende Grundlage für das Notfallmanagement bestimmt die Real Fiction GbR zu Beginn eine Person für die Aufrechterhaltung der Kontinuitätsstrategie (Aktualisierungen, Anpassungen, Tests und Trainings). Die Verantwortungsübernahme durch diesen Notfallmanager wird zwar nicht die Teamarbeit an allen Themenstellungen des Business Continuity Planning ersetzen, aber (spätestens) in Notfällen kann ein erfahrener Ansprechpartner mit Expertenwissen zeitraubende Diskussionen vermeiden und Entscheidungen können schnell getroffen werden.

Eine Lösung für die Real Fiction GbR wird in den nachfolgenden Abschnitten erarbeitet. Es werden Antworten auf die Fragen gegeben, was dieses Unternehmen zu sichern hat (7.2.1), welche Architektur aus Hard- und Software es dabei verwenden kann (7.2.2 auf der nächsten Seite), und wie die kritischen Parameter Zeit (7.2.3 auf Seite 70) und Datensicherheit (7.2.4 auf Seite 73) in dieser Vorsorgefunktion wirken.

7.2.1 Welche Daten und Funktionen müssen gesichert werden?

Der Entwicklung einer Kontinuitätsstrategie geht immer der Abgleich von Soll-Zustand und Ist-Zustand voraus. Daraus ergeben sich auf Prozessebene die Daten und Funktionen, die gesichert werden müssen. Bei der Real Fiction GbR ist bisher noch kein Sicherheitskonzept vorhanden. Eine BIA hat die Entwicklung neuer Softwarekomponenten als Kernprozess des Unternehmens bestätigt[6]. Alle Ressourcen, zu denen dieser Kernprozess in Abhängigkeit steht, und die Prozesse zur Sicherstellung dieser Ressourcen sind als kritisch einzustufen und müssen in der Notfallvorsorge behandelt werden. Dazu zählt die Aufrechterhaltung des Serverbetriebs, die Sicherstellung dessen Verfüg- und Erreichbarkeit sowie der Zugang zu benötigter Hard- und Software (Rechner, Betriebssysteme und Entwicklungsumgebungen). In dem kleinen Unternehmen ist die Gesamtheit der gespeicherten Daten unersetzbar, sowohl auf dem Server als auch auf den genutzten Notebooks, da Programmmodule verteilt bearbeitet werden. Da in dem Unternehmen nur drei Personen beschäftigt sind, kann die Einhaltung der Wiederherstellungszeit (RTO = zwei Stunden) durch Personalausfall gefährdet sein. Aus diesem Grund empfiehlt sich neben einer Datenspiegelung auch ein gleichzeitiges Abbild (Image) der gesamten Server- und Workstation-Betriebssystemkonfiguration anzufertigen. Damit ist eine schnelle (personalschonende), hardwareunabhängige Wiederaufnahme des Geschäftsprozesses ermöglicht. Für eine effektive Standortsicherheit werden diese Abbilder auf lokalen Kopien sowie auf Backup-Festplatten eines Storage-Services in Bonn gespeichert (siehe nächster Abschnitt).

[6] Annahme

Durchzuführende Schritte in der **Übersicht:**

1. Durchführung einer Business Impact Analyse (Abgleich von Soll- und Ist-Zustand)
2. Identifizierung kritischer Prozesse
3. Abhängigkeiten ermitteln (Prozesse, Ressourcen, Daten)
4. Sicherungsstrategie entwickeln (Umfang, RPO, RTO, Standortsicherheit)

7.2.2 Welche Vorbereitungen sind für Hardware und Struktur zu treffen?

Mit dem Ziel, für die reine Operativumgebung der Real Fiction GbR eine angepasste Notfallstrategie zu implementieren, wurde in eine neue Disaster Recovery Software von Acronis investiert. Die Acronis Security Suite lässt sich leicht in das bestehende Windows-Netzwerk integrieren und unterstützt die verwendete MS SQL Server 2005 Datenbank-Applikation. Die Software besteht aus sieben relevanten Komponenten:

- Server Software, zentrale Applikation für Serversysteme, von der Backup- und Wiederherstellungsaufgaben ausgeführt und verwaltet werden.
- Workstation Software, Verwaltungsapplikation vergleichbar mit der Server-Software, aber für Client-Betriebssysteme.
- Universal Restore, Zusatzmodul zur hardwareunabhängigen Wiederherstellung von Systemabbildern.
- Backup Server, Tool zur Verwaltung lokal angeschlossener Speichergeräte.
- Group Server, Tool zur Gruppierung von Rechnern.
- License Server, Tool zur Verwaltung von Workstation-Lizenzen.
- Managementkonsole mit Remote-Agents, zur zentralen Verwaltung aller Steuerungs- und Sicherungsaufgaben auf entfernten Unternehmensrechnern.

Der True Image Echo Server for Windows (im Folgenden als „TIE Server“ bezeichnet zur klaren Unterscheidung zwischen dem Acronis (Software-) Server und der physikalischen Unternehmensrechner mit Windows 2003 Server als Betriebssystem („im Folgenden ‚Server‘ genannt“)) ist auf dem Windows 2003 Server installiert, das True Image Echo Workstation Paket (nachfolgend „TIE Workstation“ genannt) läuft auf den Notebooks des Unternehmens. Die weiteren Tools können unabhängig von bereits installierter Acronis-Software im Netzwerk installiert werden, bspw. auf einem dedizierten Rechner

für Verwaltungsaufgaben. Im Fall der Real Fiction GbR befinden sich der Gruppenserver und der Lizenzserver neben dem TIE Server auf dem gleichen System. Ebenfalls ist die Managementkonsole auf dem ständig aktiven Server installiert, sodass Clientaktivitäten zentral gesteuert werden können. Die Verwendung der Werkzeuge direkt auf dem Server hat den Vorteil, dass diese Tools jederzeit verfügbar sind.[7] Bei zunehmender Auslastung des Servers ist jedoch ein Zweitsystem in Betracht zu ziehen, dass die zusätzlichen Unterhaltungskosten mit der Entlastung des Primärservers rechtfertigen kann. Der Backupserver ist an alle Windows-Installationen zu knüpfen, die über lokal angeschlossene Speichergeräte verfügen, welche für die Speicherung der Backupdateien genutzt werden sollen. Dazu können später bspw. Bandlaufwerke gehören, die zur Langzeitaufbewahrung rechtlich relevanter Daten (siehe Kapitel 3) eingesetzt sind. Bei der Real Fiction GbR wird dieses Tool auf einem entfernten Sicherungsserver eingesetzt (siehe weiter unten). Sowohl lokal als auch zentral über die Managementkonsole und den Gruppenserver (nach Installation der Remote Agents) können so die Backup- und Wiederherstellungsoperationen gesteuert werden. Die Verteilung der Softwarekomponenten zeigt Abbildung 7.2 auf Seite 69.

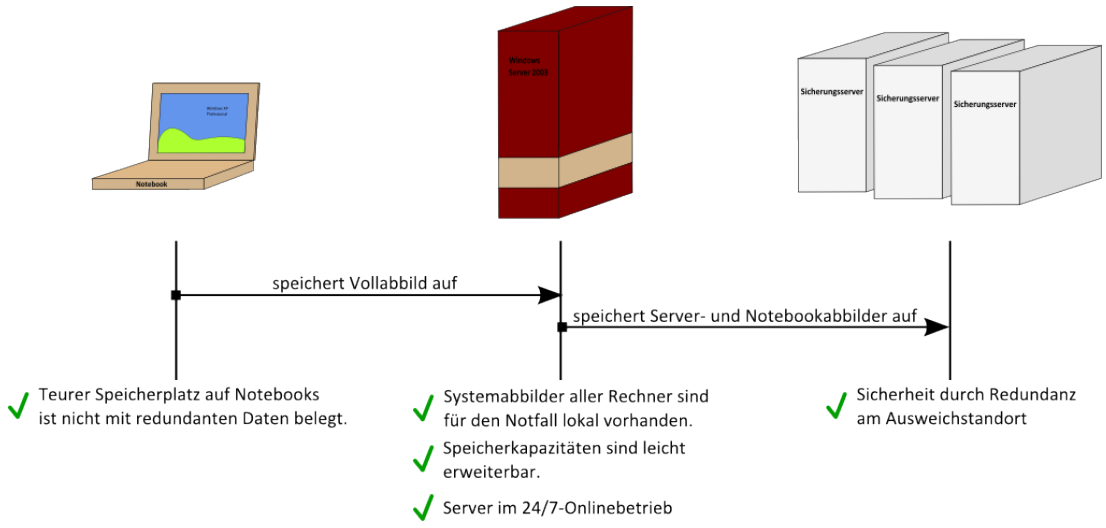


Abb. 7.1: Ablauf des Backupprozesses (Quelle: Eigendarstellung)

Server und Workstations (Hardware) sind innerhalb des Hauses in einem Gigabit-Netzwerk verbunden, um die großen Datenmengen zu bedienen, die während der Erstellungen virtueller 3D-Umgebungen übertragen und gespeichert werden müssen. Anstatt direkt auf dem Sicherungsserver zu speichern, werden die Systemabbilder der Notebooks zuvor automatisch nach einem festgelegten Zeitplan in einer separaten Partition des Servers abgelegt (vgl. Abbildung 7.2). Erst von dort werden sie, zusammen mit dem Plattenab-

[7] Verfügbarkeit des Servers vorausgesetzt

bild des Servers, auf dem entfernten Sicherungsserver ausgelagert (siehe Abbildung 7.1). Der Vorteil dieser Lösung besteht darin, dass immer eine lokale Kopie jeder Workstation im Netzwerk vorhanden ist und somit eine Wiederherstellung nach einem Ausfall zeitnah durchgeführt werden kann. Gleichzeitig wird der beschränkte Speicherplatz der mobilen Geräte für andere Anwendungen freigehalten. Möglich ist dies auf der vorhandenen Hardware durch die geringe Anzahl an zu sichernden Rechnern – sollten weitere Workstations in die Entwicklung zukünftig mit einbezogen werden, müssen die Speicherkapazitäten entsprechend erweitert werden.

Der lokale Speicherort des Serverabbildes wird als Secure Zone bezeichnet. Dieser geschützte Bereich auf der Festplatte ist technisch eine primäre Partition, die von der Acronis Software[8] angelegt und als Backupspeicher verwaltet wird, aber herkömmlichen Windows-Anwendungen keinen Zugriff erlaubt. Wie auch die Workstation-Images werden die Daten des Servers auf Sektorebene erfasst und gespeichert, sodass die Archivgröße nur die tatsächlich belegten Sektoren beinhaltet und von informationslosen Daten befreit bleibt. Die Secure Zone ist so bemessen, dass zwei komprimierte Vollbackups und dazugehörige inkrementelle Backups darin gespeichert werden können. So ist sichergestellt, dass stets ein Serverabbild auf Unternehmensseite vorhanden ist, selbst wenn wegen eines unterbrochenen Backupprozesses das älteste Systembackup unvollständig überschrieben wird.[9]

Als weitere technische Maßnahme wird der Server mit einem RAID 10 Verbund aufgewertet. Zwei Ziele sollen damit erreicht werden: Zum einen soll die lokale Verfügbarkeit der Backups erhöht werden (Ausfallsicherheit). Die Secure Zone des Servers hält zwar grundsätzlich ein aktuelles Backup bereit, jedoch kann die Softwarelösung keinem Festplattenausfall vorbeugen. Um wegen eines einzelnen Plattencrashs nicht direkt den vollen Umfang des Notfallplans durchführen zu müssen, soll durch die Duplikation von Festplatten höhere Datensicherheit und langfristige Kostenersparnis erreicht werden. Das zweite Ziel dieser Investition liegt in dem angestrebten Geschwindigkeitsvorteil (Datendurchsatz). Da durch die (Voll-)Backups von Server und Workstations neben der Geschäftsaktivität der 3D-Modellerstellung ein weiterer zeit- und ressourcenintensiver (Schreib-/Lese-Operationen) Prozess von dem Server durchgeführt werden muss, sollen durch die Parallelisierung der Operationen Engpässe vermieden werden.[10] Die RAID-Technik zusammen mit der Secure Zone bilden so einen wichtigen Schutz der Möglichkeit zur zeitnahen Wiederherstellung von System und Daten im Notfall, bevor zweistellige Gigabyte-Größen an Backups über das Internet zurückgespielt werden müssen.

[8] TIE Workstation oder TIE Server

[9] Das Speichermanagement der Secure Zone kann im Handbuch des Acronis TIE Server auf Seite 13 nachgelesen werden

[10] Eine umfangreiche Übersicht über die RAID-Technologie gibt `http://de.wikipedia.org/wiki/RAID`

Für den Notfall hat sich das Unternehmen für das entschieden, was vom BSI beispielhaft als „kleine Lösung“ bezeichnet wird.[11] Da keine Hochverfügbarkeitslösung angestrebt ist, um im Kostenrahmen zu bleiben, wird ein Service-Vertrag abgeschlossen, der folgende Punkte beinhaltet: Auf Basis einer kalten Standby-Lösung (Cold-Site) garantiert der Dienstleister bei Ausfall des gesamten Standorts der Real Fiction GbR die Fortführung der Geschäftsaktivitäten. Die vertraglich festgelegte Ausstattung umfasst die sofortige Bereitstellung eines klimatisierten Rechnerraumes mit eingerichtetem Internetzugang. Die verfügbare Leitungskapazität entspricht dabei mindestens der Originalleitung des Unternehmens. Des Weiteren werden der Real Fiction GbR drei Rechner und ein Server in vergleichbarer Qualität der Originalsysteme vernetzt bereitgestellt[12]. Sowohl Server als auch Workstations müssen ein Standard-Betriebssystem nicht älter als Windows 2000 Professional SP4 bzw. Windows 2000 (Advanced) Server eingerichtet haben, um die Kompatibilität zu der Acronis Software zu gewährleisten. Durch das Zusatzmodul Acronis Universal Restore wird identische Hardware nicht benötigt: Bei der Wiederherstellung besteht damit die Möglichkeit, die gesicherten Abbilder entweder direkt auf der physischen Hardware aufzuspielen oder als virtuelle Festplatten (VMware, VMware ESX-Server, Parallels, XenServer und Microsoft Virtual PC) zu mounten. Dadurch ist die Flexibilität des Dienstleisters erhöht (Freiheit in der Bereitstellung passender Hardware), was sich in einer reduzierten Servicerate widerspiegelt. In Verbindung mit der Standortsicherheit wird außerdem ein Storage-Service vereinbart. Das Unternehmen bekommt einen effektiven Speicherplatz von einem Terabyte zur permanenten Verfügung gestellt, um die eigenen Backups in sicherem Abstand von der Produktivstätte zu lagern. Die Kombination von Backup-Ort und Ausweichstandort erreicht neben einem günstigen Paketpreis des Anbieters große Geschwindigkeitsvorteile bei der Wiederherstellung der Images, die nicht über große Entfernungen, sondern direkt über das lokale Netzwerk adressiert werden können.

Die Verbindung zum Sicherungsserver wird durch eine Erhöhung der Leitungskapazität verbessert. Gesucht war eine skalierbare und preisgerechte Lösung, die unabhängig von teurer Hardware und weiteren Anschaffungskosten auskommt. Die neuen Anforderungen an die Upstream-Bandbreite haben zu einem Providerwechsel geführt.[13] So werden die zuvor asymmetrischen Bandbreiten für Down- und Upstream[14] auf eine symmetrische Backup-Leitung mit einer Kapazität von 6 Mbit/s umgestellt, die zusammen mit den Anforderungen des Unternehmens wachsen kann. Damit ist die Übertragungsgeschwindgikeit des Upstreams versechsfacht und die Backupdauer drastisch reduziert. Da sich damit gleichzeitig aber auch die Downstream-Rate verringert hat (längere Wiederherstellung), ist die Bedeutung lokaler Sicherheitskopien nochmals gewachsen (siehe dazu mehr im nächsten Abschnitt 7.2.3 auf Seite 70). Das Unternehmen hat mit dem Wech-

[11] siehe Tabellen 7 und 8 des BSI-Standards 100-4
[12] inkl. Routing und Netzwerkkabel
[13] Für dieses Szenario denkbar (Beispiel): IQom ([iQo08])
[14] Up/Down: 1/16 Mbit/s, siehe Abschnitt 7.1

sel eine maßgeschneiderte und höchst skalierbare Verbindung zur Verfügung, mit einer garantierten Bandbreite und einem vorteilhaften Abrechnungssystem.[15]

Kein Mehraufwand ist bei der Behandlung der Datenbanken entstanden: Durch die VSS[16]-Unterstützung von Acronis kann der MS SQL Server für einige Sekunden automatisch anhalten, um ein Abbild der Datenbanken zu erstellen.

Abbildung 7.2 fasst die DR-Lösung für die Real Fiction GbR in einem Vorher-/Nachher-Vergleich zusammen.

Durchzuführende Schritte in der **Übersicht:**

1. Auswahl von geeigneter Hard- und Software zur Unterstützung der Notfallvorsorge und/oder Disaster Recovery (Kriterien: Kompatibilität, Funktionsumfang, Preis).
2. Installation und Konfiguration der Acronis Security Suite Komponenten auf Workstations, Unternehmensserver und Sicherungsserver.
3. Hardwareerweiterungen/Neuanschaffungen sind zu prüfen, falls eine zu hohe Auslastung der bestehenden Systeme droht.
4. Einrichtung der Partitionsstruktur: auf dem Server sind Workstation-Partition und Secure Zone anzulegen.
5. Installation des RAID Systems auf dem Server.
6. Abschluss von Dienstleistungsvereinbarungen (SLA) unter Berücksichtigung von Ausweichstandort (kalt, warm, heiß), Storagelösung, Konfiguration und Kapazitäten.
7. Anpassung der Leitungskapazitäten an geänderte Anforderungen.

[15] „Burstable – volle Bandbreite zu Spitzenzeiten nutzen, aber nur den Durchschnitt zahlen“, Quelle IQom (Stand: 20.08.2008)

[16] Volume Shadow Copy Service, Erklärung unter `http://www.microsoft.com/germany/technet/datenbank/articles/600448.mspx` (Stand: 19.08.2008)

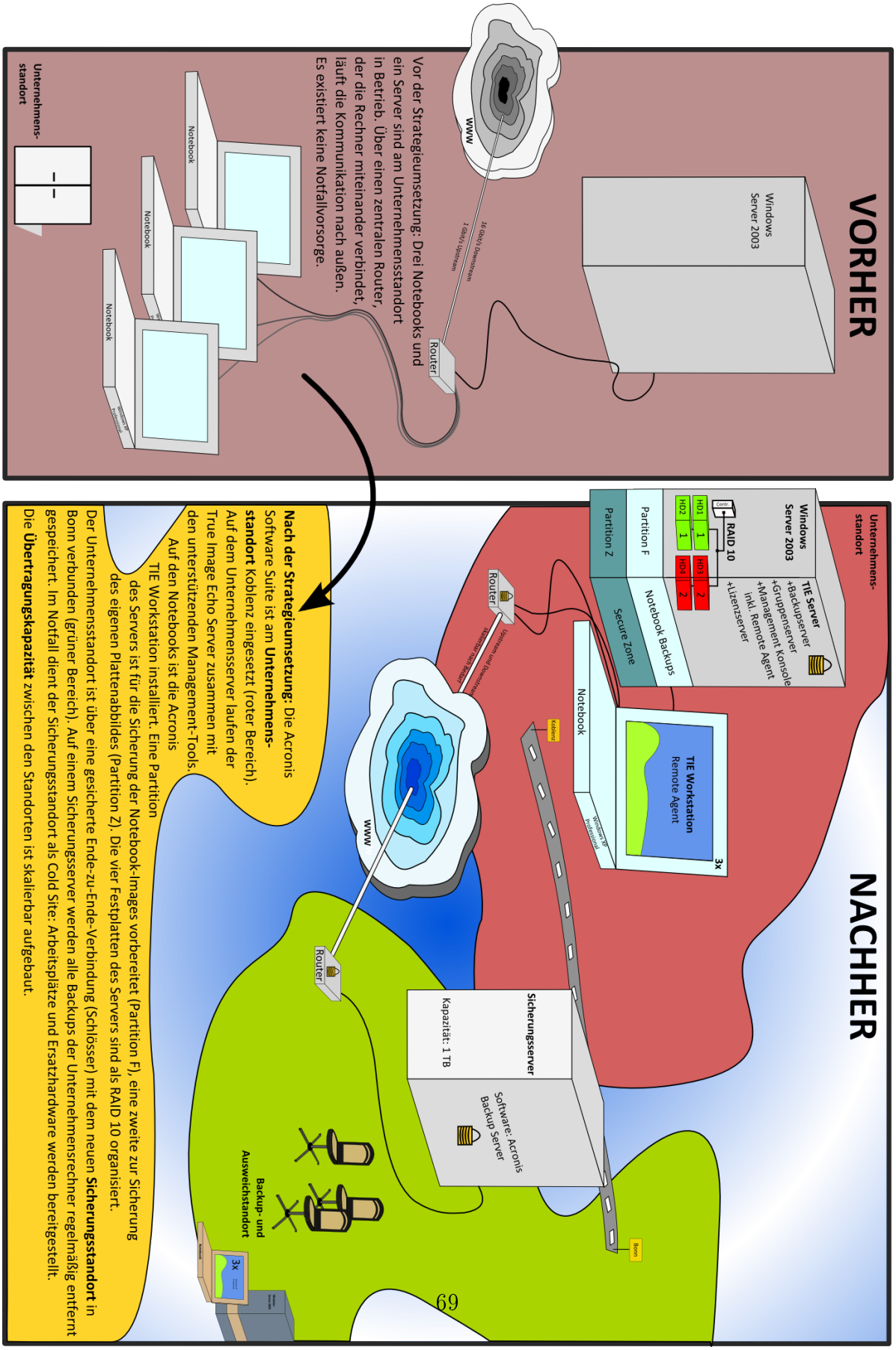


Abb. 7.2: Aufbau der DR-Lösung bei Real Fiction (Quelle: Eigendarstellung)

7.2.3 In welchen Zeitabständen wird die Sicherung vorgenommen?

An Stelle einzelner Daten ist die zeitintensive Sicherung einer ganzen Partition zu empfehlen. Der Grund dafür klingt zumindest für viele Finanzexperten paradox: Sicherheit durch Flexibilität. Um diesen Ansatz zu verstehen muss ein Blick auf drei entscheidende Faktoren im Unterschied zwischen Datenarchiv und Partitionsabbild geworfen werden. Diese Faktoren sind Komplexität (des Archivzugriffs und der Wiederherstellung von Informationen), Speicherplatz und Zeit. Als unterschiedlich schwierig kann die Wiederherstellung beider Archivtypen nicht bezeichnet werden, verwenden sie doch die gleiche Maske innerhalb der Acronis Security Suite (Wiederherstellungsassistent). Jedoch praktischer erweist sich die Datenwiederherstellung aus dem Partitionsabbild, da eine Einbindung des Images als virtuelles Laufwerk („mounten“) und somit gleichzeitig eine Wiederherstellung einzelner Dateien als auch der ganzen Partition möglich ist. Neben dem Mounten (auch in andere Virtualisierungstools) bildet auch das Bare Metal Restore Feature (Erzeugung von Bootmedien aus dem Partitionsabbild) einen Vorteil im Zugriff auf die Daten. Der Faktor Speicherplatz ist nur auf den ersten Blick ein Fürsprecher des Datenarchives. So ist es leicht verständlich, dass ein Partitionsabbild neben ausgewählten Dateien auch Anwendungen und Anwendungskonfigurationen (inkl. Betriebssystem (BS)) mitspeichert, somit also ein Plus an Daten im Archiv gespeichert ist, jedoch speichert Acronis nur die Teile der Festplatte, die wirklich Daten enthalten. Außerdem wird der Inhalt der Auslagerungsdatei[17] und der Ruhezustandsdatei[18] nicht gesichert. Die Sicherung auf Dateibasis ist demnach nur dann sinnvoll, wenn die Differenz zwischen Sicherungsgröße und belegtem Speicherplatz der Partition signifikant ist. Der wichtigste Faktor *für* das Partitionsabbild ist jedoch der zeitliche Aspekt, der von zwei Seiten betrachtet werden sollte:

1. Während der Erstellung des Backups ist die benötigte Zeit auf Grund der optimierten Sicherungsgröße so gering wie möglich gehalten. Wie beim Speicherplatz ist ein zeitlicher Vorteil des Datenarchives nur bei verhältnismäßig kleinen Sicherungsgrößen gegeben, welche in der Real Fiction GbR jedoch vollständig auszuschließen sind – der Datenbestand der Rechner dient ausschließlich geschäftlichen Zwecken, woraus automatisch Sicherungsbedarf aller Daten resultiert (Mehrwert an Informationen bei vergleichbarem Zeitaufwand).

2. Während der Wiederanlaufphase in einer Notfallsituation kann allein das Partitionsabbild eine flexible – und damit schnelle – Reaktion auf die situativen Umstände ermöglichen. Zudem erfüllt es die gesetzten Anforderungen (siehe Abschnitte 7.1 und 7.2.1) an Wiederherstellungszeit und Standortsicherheit. Nur durch die Charakteristik des Plattenabbildes, auch Konfigurationen, Anwendungen, Lizenzen,

[17] pagefile.sys, falls vorhanden (bis Windows XP)
[18] hiberfil.sys, falls vorhanden (Aktivierung des Ruhezustands optional)

Updates, Firewall-Einstellungen, Treiber, Registry und mehr in den Backups zu erhalten, kann das 2h-RTO-Ziel der Real Fiction eingehalten werden. Die hardwareunabhängige Wiederherstellung per Bootdisk ohne auf ein bestimmtes Betriebssystem, eine spezielle Formatierung der Platte oder die Installation des Acronis-Tools angewiesen zu sein, verschafft Zeitersparnis durch Flexibilität und finanzielle Sicherheit durch schnelle Geschäftsfortführung. Ein alternativer Weg über die Erweiterung des SLA[19] (vordefinierte Rechnerkonfigurationen am Ausweichstandort, Lizenzkosten für Acronis Software) steht in einem wirtschaftlich ungünstigen Verhältnis zu den Zusatzkosten für die Sicherung der BS-Dateien. Die Vorteile der Partitionssicherung überwiegen für das Unternehmen.

Um optimale Sicherungsintervalle für die Real Fiction GbR zu bestimmen, muss die exakte Dauer für die Anfertigung eines Vollbackups sowohl für Clients als auch für Server beachtet werden. Hinzu kommt die Übertragungsdauer zum externen Speicherort, wobei dieser neben der Hardware (Festplatte) auch den Netzverkehr stark auslastet.

Der Server besitzt mit der RAID-Architektur eine effektive Speicherkapazität von einem Terabyte. Davon werden 300GB für die Systemabbilder der drei Notebooks und 420 GB für die Acronis Secure Zone (1,5-fache der Quelle[20]) genutzt. Mit einer normalen Kompressionsrate von durchschnittlich 60% bei den zugrunde liegenden Daten(typen) und einer 95%-igen Speicherplatzbelegung ist eine Größe von etwa 160 GB[21] für ein komprimiertes Vollbackup des Servers zu erwarten. Zeitlich wird das Backup dafür fünf Stunden benötigen.[22] Eine Workstation mit einer 200 GB großen Festplatte benötigt mit gleichen Einstellungen etwa 75% der Server-Backupzeit. Für die Übertragung der Clientabbilder zum Server ergeben sich in Tests mit dieser Konfiguration Kopierzeiten unter 40 Minuten. Durch die Einführung der RAID-Technik wird jedoch mit Geschwindigkeitsvorteilen gerechnet, die die interne Kopierzeit auf maximal eine halbe Stunde reduzieren sollen. Durch die skalierbare Gestaltung der Backupleitung (siehe 7.2.2) kann unabhängig von der tatsächliche Sicherungsgröße ein vollständiger Backupvorgang in einem nächtlichem Zeitfenster von etwa acht Stunden durchgeführt werden.

Neben den Vollbackups ist mit Acronis auch die Erstellung differentieller und inkrementeller Backups möglich.[23] Inkrementelle Backups brauchen nur ein Vollbackup und speichern danach jeweils nur die Änderungen zum letzten (inkrementellen) Backup, um Speicherplatz, Festplattennutzung und Netzwerkauslastung zu reduzieren. Die Inkre-

[19] vorheriger Unterabschnitt 7.2.2

[20] Trotz Komprimierung der Vollbackups ist laut Hersteller das 1,5-fache an freiem Speicherplatz für die Sicherung einzuplanen (für inkrementelle/differentielle Backups)

[21] Rechnung: $1TB - 720GB \cdot 0{,}95\% \cdot 0{,}6\%$

[22] Schätzung beruht auf Erfahrungswerten: durchschnittlich werden 18 Minuten pro 10 GB Daten benötigt

[23] zur Unterscheidung von differentiellem und inkrementellem Backup siehe Acronis Handbuch, S. 12, oder unter `http://de.wikipedia.org/wiki/Datensicherung` (Stand: 03.08.2008)

mente werden eingesetzt, um die Fortschritte (Dateiänderungen) der täglichen Arbeit zu sichern. Per Dual Destination werden im laufenden Betrieb die Serverinkremente gleichzeitig in der lokalen Secure Zone und auf dem Sicherungsserver hinterlegt. Die Clients speichern ihre inkrementellen Erweiterungen ausschließlich und direkt auf dem Sicherungsserver, da die Datenänderungen auf den Clients während des Tages verhältnismäßig gering sind und sehr schnell von dem Sicherungsort wiederhergestellt werden können. Für die Real Fiction ist eine stündliche Sicherung ein angemessenes Intervall (RPO, siehe Abschnitt 7.1), das durchgehend umgesetzt werden kann. Der Sicherungsprozess kann mit der Acronis Software automatisch durchgeführt werden, nicht zuletzt um menschliche Fehler dabei zu vermeiden. Im Taskplaner des TIE Server bzw. der TIE Workstation werden dazu entsprechende Aufträge angelegt, welche auch über die Management Konsole und den Gruppenserver eingerichtet werden können. Sollte einer der Clients zur geplanten Zeit ausgeschaltet sein, wird die Sicherung beim nächsten Einschalten automatisch nachgeholt. Per WinPopup oder Email informiert die Software über Erfolg, Fehler oder nötige Benutzereingaben des Prozesses.

Die Sicherungsvorgänge haben auf diese Weise einen Platz zusammen mit den anderen zeit- und ressourcenintensiven Prozesse des Unternehmens. In der Real Fiction GbR ist vor allem die 3D-Modellerstellung ein Prozess, der die Serverhardware konstant auslastet. Die sechsstündige Modellerstellung wird täglich manuell gestartet. Die untenstehende Abbildung 7.3 fasst die Situation in einem zeitlichen Ablaufplan zusammen.

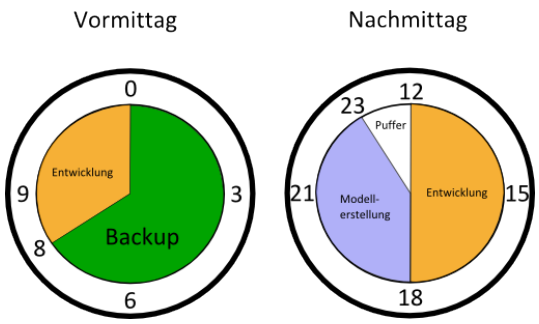


Abb. 7.3: Für einen überschneidungsfreien Ablauf werden zeitkritische Prozesse aufeinander abgestimmt.

Auf diesem Weg ergeben sich zwei Vorteile: Erstens werden alle ressourcenintensiven Prozesse außerhalb der normalen Arbeitszeiten vollautomatisch durchgeführt. Da in dem Unternehmen kein 24/7-Geschäftsbetrieb gefordert ist, kann an kostenintensiveren Hard- und Softwarelösungen eingespart werden. Zweitens ist durch die zeitliche Anordnung sichergestellt, dass das täglich neue 3D-Modell nach Erstellung direkt gesichert wird und so im Notfall eine komplette Neuerstellung vermieden werden kann. Obwohl asynchron Lösungen wie die Acronis Suite immer ein gewisses Maß an Zeit- und Datenverlust bedeuten, kann durch die inkrementellen Erweiterungen im Hintergrund ein niedriges RPO und eine hohe Aktualität der Abbilder gewährleistet werden.

Durchzuführende Schritte in der **Übersicht:**

1. Entscheidung für Daten- oder Partitionsabbild

2. Dauer zur Durchführung eines Vollbackups ermitteln
   a) Kompressionsraten bestimmen
   b) Maximale Speicherplatznutzung sicherungsrelevanter Daten ermitteln
   c) Übertragungsdauer zum Sicherungsserver ermitteln
3. Parallelisierungsoptionen prüfen
4. Sicherungsablaufreihenfolge einhalten
5. Entscheidung für differenzielle oder inkrementelle Backups treffen
6. Zeitliche Abstimmung mit anderen ressourcenintensiven Prozesse im Unternehmen durchführen. Kann keine zufriedenstellende Lösung mit den ermittelten Vorgaben gefunden werden, so müssen die Anforderungen an das Vollbackup überarbeitet werden, gegebenenfalls in Verbindung mit weiteren Investitionen. Danach sollte mit Schritt 2 fortgesetzt werden.
7. Umsetzung der Sicherungsstrategie mit der Acronis Software Suite durch Einrichtung von Tasks

7.2.4 Wie kann Übertragungssicherheit beim Backup hergestellt werden?

Eine bestmögliche Sicherheit der Partitionsabbilder wird durch die Kombination verschiedener Ansätze erreicht. Die Acronis Software bringt einige Schutzvorkehrungen mit, die aber alleine noch kein zufriedenstellendes Ergebnis liefern können. Welche dies sind und warum die Ansätze des Tools nicht ausreichen, wird in den nachfolgenden Paragraphen beschrieben. Denn um die Backups wiederherstellbar zu speichern und dabei vor Missbrauch zu schützen, müssen in der Strategie der Real Fiction GbR *alle* Schwachstellen der Backupsicherung (meist Schnittstellen) abgedeckt sein. Abbildung 7.4 illustriert die kritischen Stellen, die sich auf physischer Ebene (grüne Markierungen), auf Anwendungs- und Betriebssystemebene (orangene Markierungen) und auf der Übertragungsebene (rote Markierungen) in der Lösung für das Unternehmen ergeben.

Beginnt man in einer chronologischen Reihenfolge, so ist von Anfang an Vorsorge zu tragen, dass die zu sichernden Systeme gegenüber potentiellen Angreifern von außen geschützt sind (physischer Schutz). Dieser Schutz umfasst hierbei alle Hard- und/oder Softwarelösungen, die nicht direkt in den eigentlichen Backupprozess involviert sind. Dazu zählen die Bereiche Gebäudeschutz und physische Zugangskontrolle, Hardwareintegrität, Firewalls, Intrusion Detection Systeme, Spyware-Schutz, Applikationen- und Firmware-Updates, Virenscanner etc. In gleichem Maße ist dafür zu sorgen, dass auch

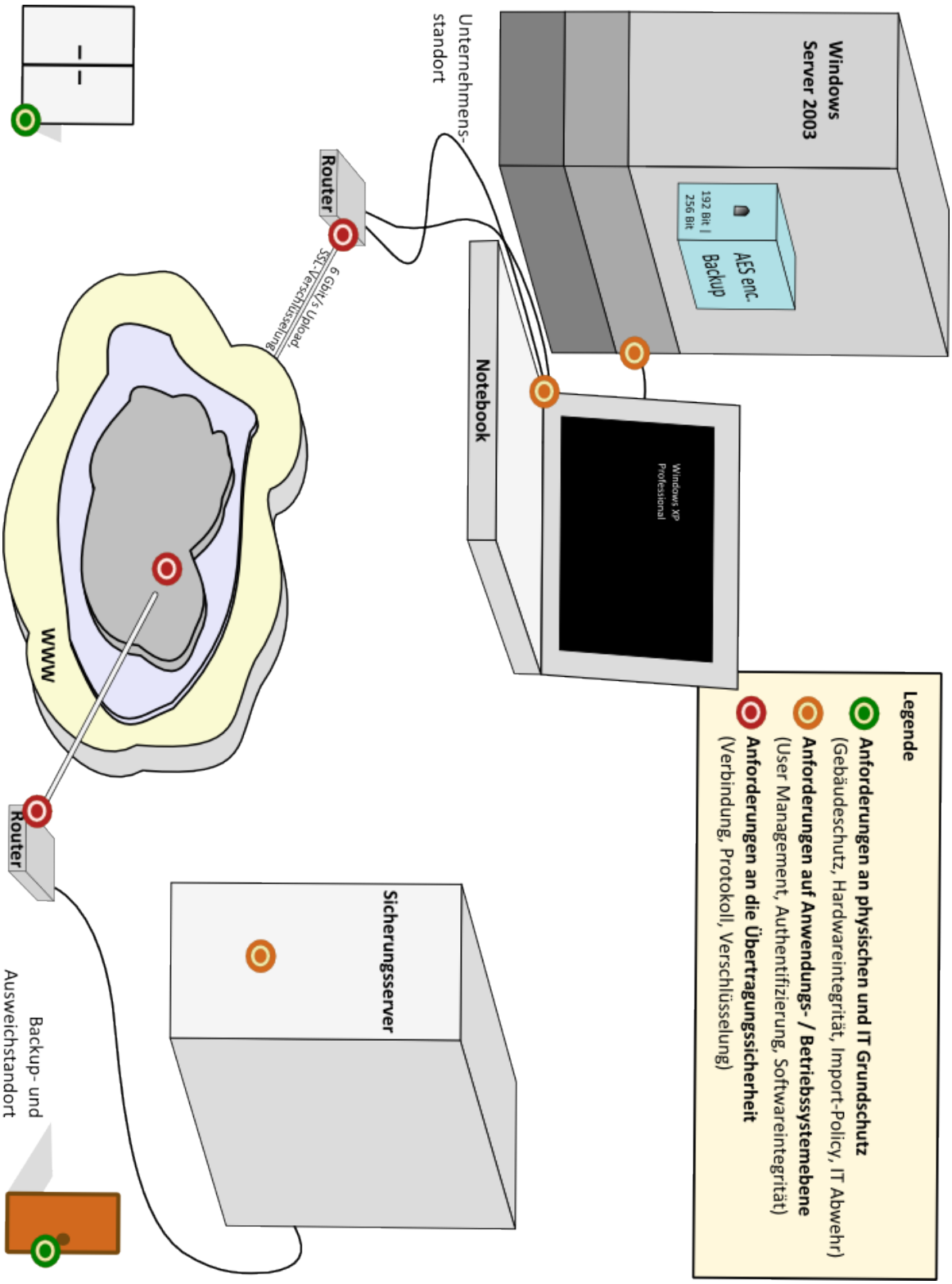


Abb. 7.4: Potentielle Angriffspunkte müssen frühzeitig erkannt und behandelt werden. (Quelle: Eigendarstellung)

von anderen Quellen (z.B. DVDs, USB-Speicher u.ä.) keine Gefährdung der Betriebssysteme, der Anwendungen oder der Daten in das Unternehmen getragen wird. Diese Themen der IT-Security errichten einen grundlegenden Level an (IT-) Sicherheit.[24]

Auf Anwendungsebene bieten die primären Disaster Recovery Tools TIE Server, TIE Workstation und die Management Konsole (Remote Zugang) keinen eigenen Zugriffschutz. Der Zugang zu den Programmen kann nur über Gruppenrichtlinien und Benutzerkonten auf Betriebssystem- und Netzwerkebene (bspw. bei vorhandenem Funknetz) geregelt werden.[25] Bei der manuellen Einrichtung solcher Regeln ist konsequent darauf zu achten, dass den unauthorisierten Benutzern das Installationsrecht (der Acronis Suite) auf dem Rechner ebenfalls entzogen wird. Da die Serialnummern auf dem Lizenzserver im Netzwerk leicht zugänglich sind, können kritische Daten so unbemerkt entwendet werden. Ein denkbares Szenario: Ein Aggressor erhält Zugang zum Netzwerk per WLAN[26] (bspw. nur WEP-Verschlüsselung / unsicherer WPA-Key), bekommt Remotezugriff auf den Server per Management Konsole, führt ein Backup und Komprimierung von Projektdateien aus und schickt es an seinen Fremdrechner. Dann löscht er alle Log-Dateien. Ähnlicher Datenklau ist über Ethernet denkbar, falls die oben angesprochene IT-Security Schwachstellen ausgenutzt werden. Ein Schutz der Daten bei Diebstahl des Rechners ist mit Benutzerkonten und Gruppenrichtlinien zwar nicht gegeben (u.a. weil die Originaldaten auf dem gleichen physischen Laufwerk frei liegen), aber ein solcher Fall liegt dann auch nicht mehr im Bereich der IT-Notfallplanung.

Unmittelbar vor der Erstellung des Backups kann optional ein Virencheck der Sicherungsdaten durchgeführt werden. Sollte auf den Systemen generell kein Virenscanner permanent aktiv sein oder auf einer nur geringen Sicherheitstufe laufen, so kann ein zusätzlicher Intensivscan vor dem Backup zu empfehlen sein. Dies verlängert zwar die ohnehin langwierige Backupprozedur, jedoch ist diese Zeit besser beim Backup als bei der Wiederherstellung investiert.

Bei den Archiv-Optionen (Abbildung 7.5) gibt es neben der Fehlerbenachrichtigung per Email zwei weitere sicherheitsrelevante Aspekte: die Sicherheitseinstellungen auf Dateiebene und die Verschlüsselung der Archive. Auf Dateiebene kann bestimmt werden, ob spezielle Ordner- oder Dateirechte im Backup mit aufgenommen werden. Auf einem Ersatzsystem müssen bei Erhalt genau diese Benutzerkonten existieren, um den Zugriff zu gestatten. Grundsätzlich ist die Einbeziehung der Rechte beim Backup zu empfehlen, da die Entscheidung zur Wiederherstellung der Rechte auch nochmals bei

[24] Die Anforderungen an physischen Schutz und grundlegenden IT-Schutz sind in Abbildung 7.4 symbolisch dargestellt (grüne Markierungen).

[25] Die Anforderungen auf Anwendungs- und Betriebssystemebene sind in Abbildung 7.4 symbolisch dargestellt (orange Markierungen).

[26] Auch wenn das Funknetz in der Regel nicht genutzt wird (siehe Abschnitt 7.1), ist die Verwendung zu Präsentationszwecken nicht auszuschließen.

der Wiederherstellung des Backups getroffen werden kann. Da diese Option bei einer kompletten BS-Partitionssicherung keinen Sinn macht (und daher nicht zur Verfügung steht), ist sie im Fall der Real Fiction GbR ohne Bedeutung. Sehr wertvoll hingegen und im Rahmen der Backupstrategie angewendet ist die Möglichkeit zur passwortgeschützten AES-Verschlüsselung[27] des Archives. Sofern ein ausreichend starkes Passwort benutzt wird[28] kann ein Zugriffs-/Missbrauchschutz des Systemabbildes sowohl bei der Übertragung[29] als auch während der Speicherung beim Storage-Dienstleister zuverlässig gewährleistet werden.[30] Es ist jedoch bei der Verwendung von Acronis darauf zu achten, dass der Passwortschutz samt Verschlüsselung nicht bei der Speicherung in die Secure Zone – und damit mit dem Dual Destination Feature[31] – zur Verfügung steht. Der Secure Zone kann jederzeit ein eigenes Passwort zugewiesen werden, sollte jedoch per Dual Destination auf einem freigegebenen Windows-Netzwerkordner gesichert werden, muss sowohl die Verbindung als auch das fertige Archiv gesondert geschützt sein.

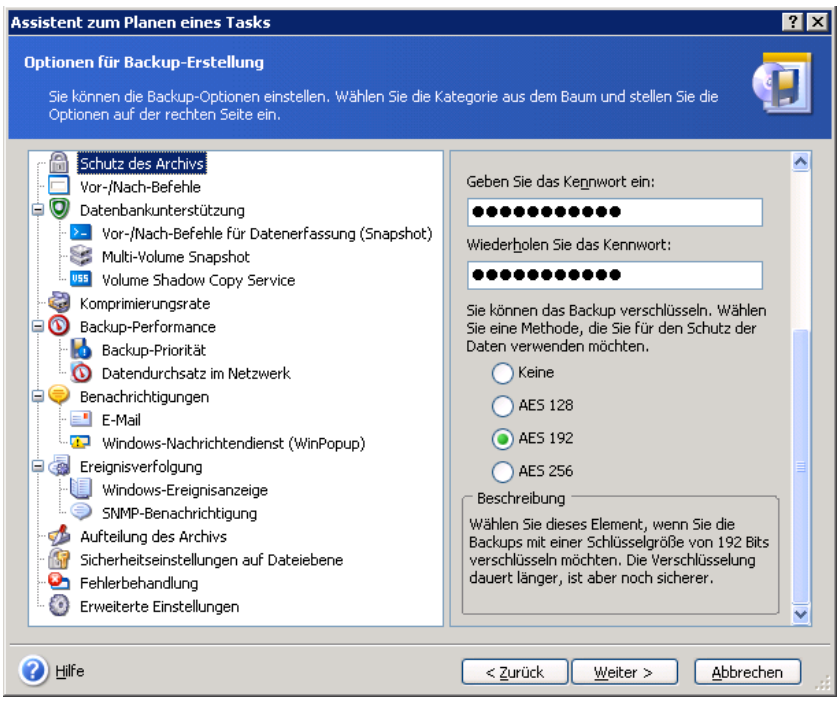


Abb. 7.5: Die Archivoptionen im Überblick (Quelle: Acronis True Image Echo Server)

[27] optional: Verschlüsselung mit 128 Bits, 192 Bits oder 256 Bits oder unverschlüsselt

[28] Tipps und Check unter `https://passwortcheck.datenschutz.ch/check.php?lang=de` (Stand: 18.08.2008)

[29] falls in einem freigegebenen Windows-Netzwerkordner gespeichert wird

[30] Zur Sicherheit des Advanced Encryption Standard (AES) siehe [Age05] und [Kra02].

[31] Speicherung in der Secure Zone mit automatisch anschließender Kopie des Backups an einen weiteren Ort

Wird eine Verbindung mit einem Acronis Serverdienst (Remote Agent, Gruppenserver, Backupserver) aufgebaut, so wird zur Übertragungssicherheit automatisch eine SSL-verschlüsselte Authentifikation/Kommunikation benutzt (vgl. Abbildung 7.4). Möchte man die Ende-zu-Ende Sicherheit zusätzlich erhöhen, kann der Server des Unternehmens (für die Notebook-Images) bzw. der Sicherungsserver (für Server- und Notebook-Images) zur Annahme von (authorisierten) VPN-Verbindungen konfiguriert werden. Vor allem bei einer unsicheren WLAN-Nutzung (z.B. WEP) innerhalb des Unternehmens sollte diese Maßnahme umgesetzt sein.[32]

Das übertragene Backup auf einem entfernten Server darf nur von einer authorisierten Person wiederherzustellen sein. Die verwendete Übertragungstechnik zusammen mit der AES-Verschlüsselung wird auch neugierigen[33] Dienstleistern den Zugang zu den Informationen vorenthalten. Einzig der oben angesprochene Fall „Dual Destination Backup auf einen Windows-Netzwerkordner per SMB-Protokoll“ muss bedacht werden: Da hierbei weder automatisch eine SSL-Verbindung etabliert noch ein Archivschutz von Acronis eingerichtet werden kann, werden die Abbilder unverschlüsselt übertragen und gespeichert. Neben einer zertifikatbasierten[34] VPN-Verbindung als manuelle Lösung für die Übertragung ist eine Kommandozeilenoption für den Zeitpunkt zwischen Fertigstellung der Backup-Operation und Transfer des Images nötig, die das Abbild nachträglich mit einem Passwort schützt, bspw. durch ein Archivmanager wie WinRAR[35]. Dieser Weg ist sehr ressourcen- und zeitintensiv und sollte nur in Ausnahmefällen (z.B. Acronis Backup Server hat eine Sicherheitslücke oder läuft dauerhaft unzuverlässig) gegangen werden.

Die Archive und der Wiederherstellungsprozess werden von der Real Fiction GbR als Teil der Sicherungsstrategie regelmäßig überprüft. Dazu zählt zum einen die automatische Validierung der Archive, bei der die Integrität der Daten überprüft wird. Dieser Task wir immer dann ausgeführt, wenn die Sicherungsintervalle der Vollbackups vergrößern (am Wochenende und zu Urlaubszeiten). Zum anderen lassen sich die erstellten Archive zu virtuellen Festplatten konvertieren. Damit kann im Rahmen einer virtuellen Umgebung wie VMWare oder Virtual Server die Einrichtung und Parametrierung der eingesetzten Produkte auf der vorhandenen Hardware getestet werden. Die Virtualisierung hält sich die Real Fiction GbR aber wegen der besonderen Anforderungen an Plattenplatz und manueller Steuerung nur für Ausnahmesituationen offen. Ändert sich die Konfiguration oder der technische Aufbau (Hardware) im Unternehmen, so müssen die Sicherheitseinstellungen erneut konsolidiert und gegebenenfalls angepasst werden.

[32] Die Anforderungen an die Übertragungssicherheit sind in Abbildung 7.4 symbolisch dargestellt (rote Markierungen).
[33] In diesem Fall wurden bei der Evaluation der Storage-Anbieter bereits Fehler gemacht.
[34] Durch eine zertifikatbasierte Authentifikation können Man-In-The-Middle-Angriffe verhindert werden.
[35] Im Internet: `www.winrar.de` (Stand: 18.08.2008)

Die Sicherheitsoptionen in der **Übersicht**:

Physischer Schutz / IT-Grundschutz	• Gebäudeschutz und Zugangskontrollen (physisch und technisch, z.B. WLAN) • Hard- und Software Sicherheitssysteme, darunter Firewall, Virenscanner, Erkennung von Abhörung und Eindringung, Update-Policy • Richtlinien im Umgang mit externen Datenträgern und der Verwendung von Unternehmensdaten
Schutz auf Betriebssystem- und Anwendungsebene	• Benutzermanagement auf BS- oder Netzwerkebene (Acronis startet ohne Authentifizierung): • Virencheck der Daten vor Erstellung des Backup-Archivs • Aktivierung und Konfiguration der Email-Statusbenachrichtigung (Fortschritt, Erfolg, Fehler) • Sicherung auf Dateiebene: Erhalt/Verwurf von Dateirechten • Verschlüsselung des Archives (bis zu 256 Bits AES-Verschlüsselung) • Passwortsicherung der Acronis Secure Zone
Übertragungssicherheit	• SSL verschlüsselte Kommunikation zwischen allen Komponenten der Acronis Security Suite • Konfiguration von VPN-Verbindungen zur Erhöhung der Ende-zu-Ende Sicherheit (v.a. bei Nutzung des Funknetzes)
Sonstige Schutzmaßnahmen	• Evaluierung von Dienstleistern anhand Erfahrungswerten von vergleichbaren Unternehmen (Größe, Budget, Anforderungen) und Referenzen • Backup-Sicherheit im Ausnahmefall durch alternativen Passwortschutz gewährleisten • Durchführung regelmäßiger Tests (Validierungen, theor. DR-Ablaufevaluierung, prakt. Datenwiederherstellung auf Testsystemen) • Änderungen von Ausgangsbedingungen sind in die Sicherungsstrategie einzuarbeiten

7.3 Umsetzung der Disaster Recovery

Business Continuity Vorfälle können nie zu 100% abgewendet werden, wenn das Prinzip der Wirtschaftlichkeit („Wirtschaftlichkeit ist das nachhaltig günstigste Verhältnis zwischen Nutzen und Kosten“[36]) im Aufbau des Notfallmanagements befolgt wird. Kommt es irgendwann zu einem Ereignis, das über das Ausmaß einer Störung hinausgeht (Notfall), so muss eine funktionierende (d.h. getestete) Disaster Recovery den eingetretenen Schaden auffangen, minimieren und unter Einhaltung zeitlicher Vorgabe (RTO) bis zum Normalbetrieb reduzieren. Die Gestaltung dieses Krisenmanagements basiert auf vielen Faktoren, maßgeblich sind die zuvor behandelten Aspekte Daten- und Funktionskritikalität, (vorhandene) Softwaresysteme (Kompatibilität), IT-Umgebung, verfügbares Budget (resultierend aus der BIA), qualifiziertes Personal, Standort, Kernkompetenzen, Geschäftsziele und Unternehmensgröße. Diese Faktoren weisen häufig enge Abhängigkeiten untereinander auf und müssen bei Änderung einer Komponente als Ganzes auf die fortlaufende Einhaltung des Sicherheitsniveaus überprüft werden.

Im bestmöglichen Fall ist während eines Notfalls nur den aktuellen Vorgaben des Business Continuity Plans zu folgen. Die praktische Handlungsfähigkeit sollte durch die darin beschriebenen Kontaktdaten, Zuständigkeiten und Ablaufplanungen zu einer schnellen (und richtigen) Reaktion von Unternehmensseite führen. Von Kundenseite sollten hausinterne Notfälle optimaler Weise nicht sichtbar sein.

Da die Real Fiction GbR ein forschendes Kleinunternehmen ist, welches momentan kein Webserver oder Kundencenter betreibt, unterscheidet sich die (IT-) Disaster Recovery in Aufwand und Lösungsansatz sehr stark von mittelständischen oder Großunternehmen wie bspw. das Haus Rabenhorst oder die United Internet AG. Der Erhalt und die Verfügbarkeit besonders wichtiger Daten hat in jedem der Unternehmen eine gleichermaßen existenzielle Bedeutung, eine einzelne universelle Vorgehensweise gibt es aber nicht. Allerdings beschreibt der BSI-Standard 100-4 eine gewohnt „konkrete Abstraktion“ zur Organisation und Vorgehen im Krisenmanagement, welche als Einstieg und Rahmen zu empfehlen ist. In den folgenden drei Abschnitten (vgl. Abbildung 7.6 auf der nächsten Seite) wird das Szenario der Real Fiction GbR weitergeführt und die individuelle Ablauforganisation dieses Unternehmens analysiert: durch einen Testlauf der Disaster Recovery.

7.3.1 Auf welche Weise kann eine rechtzeitige und authorisierte Aktivierung des Notfallplans erzielt werden?

Um die Entscheidung über die Aktivierung eines BCP treffen zu können, muss eine Meldung über einen (potentiellen) Notfall an die verantwortliche Person(-engruppe) gebracht

[36] Online Verwaltungslexikon ([Pro07])

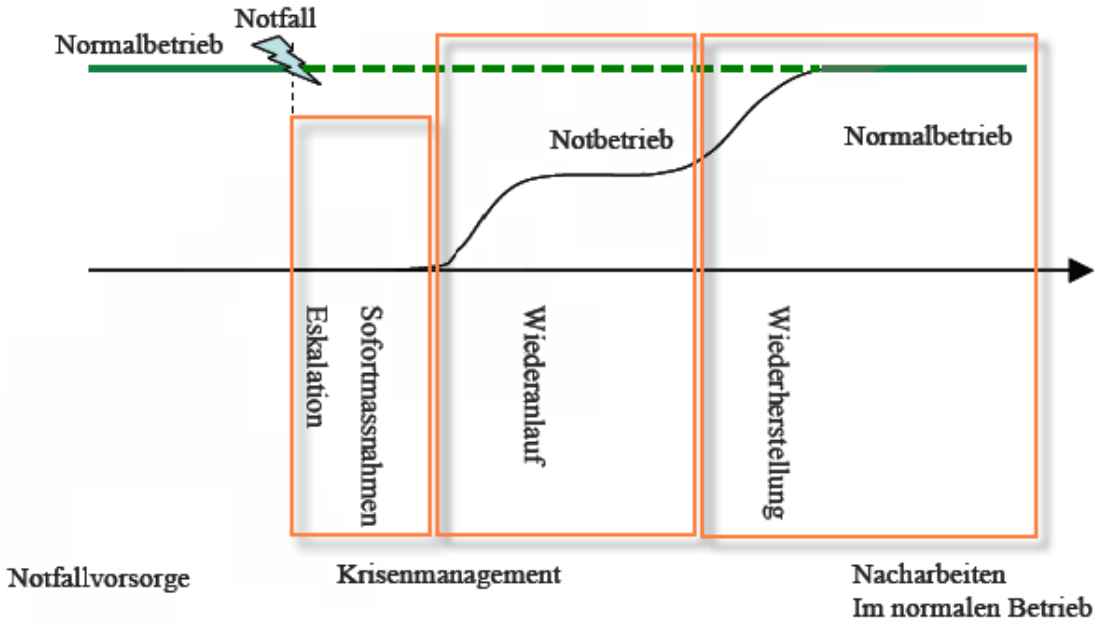


Abb. 7.6: Stufen der Disaster Recovery (Quelle: [Bun08])

werden. Rechtzeitigkeit bedeutet vor diesem Hintergrund, dass die zeitliche Differenz zwischen Feststellung des Notfalls (resp. Störung) und dessen Meldung so gering wie möglich ist. Die Schwierigkeit kann darin gesehen werden, dass das Ausmaß einer vermeintlichen Störung unterschätzt und damit zu spät mitgeteilt wird oder Kommunikationswege zu kompliziert gestaltet oder sogar den Mitarbeitern unbekannt sind. Authorisation, ein zweiter wichtiger Aspekt zur Aktivierung des Plans, impliziert die eindeutige Verteilung von Verantwortung und Zuständigkeiten. Eine Einzelperson oder einem Gremium obliegt die Vollmacht, auf Basis vorliegender Informationen das Krisenmanagement zu aktivieren, um einen Fehlalarm zu vermeiden und schnelle Handlungsfähigkeit im Notfall zu erreichen.

Die Real Fiction GbR folgt dem Aufbau des Krisenmanagements, wie er in Kapitel 2 bereits beschrieben wurde (dargestellt in Abbildung 2.1 auf Seite 9). Der Ablauf gestaltet sich in drei verschiedenen Phasen (Abbildung 7.7): Bei Eintritt einer Störung, die nicht in kurzer Zeit behoben werden kann, werden die Kollegen unverzüglich telefonisch informiert (Meldungsphase). Die Telefonnummern und Kontaktadressen des kleinen Teams sind sowohl im Notfallplan als auch in den mobile Geräten hinterlegt. In einer Konferenzschaltung wird die Situation diskutiert (Entscheidungsphase). Dabei wird festgelegt, ob eine sofortige Eskalation durchgeführt werden soll oder eine genauere Bewertung der Lage und möglicher Folgeschäden nötig ist. Im dritten Schritt wird der Notfallplan mitsamt seinen Maßnahmen umgesetzt und das Unternehmen über den Notbetrieb in den

Normalbetrieb zurückgeführt (Umsetzungsphase).

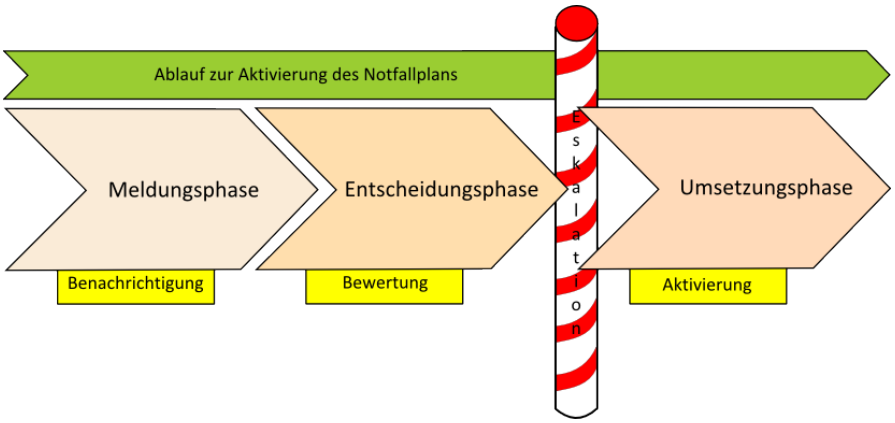


Abb. 7.7: Phasenmodell bei Eintreten eines Notfalls (Quelle: Eigendarstellung)

In der Meldungsphase stellt sich die Herausforderung, einen möglichst schnellen Übergang zwischen Störereignis und Entscheidung zu schaffen. Das BSI bezeichnet diesen Prozess als Alarm-Management. Dabei stehen zwei Aufgaben im Mittelpunkt: das Erkennen des potentiellen Notfalls zum einen, und die Kommunikation der Sachlage an die zuständigen Mitarbeiter zum anderen. Letzteres ist bei der Real Fiction GbR einfach geregelt, da die generelle Empfehlung, die Kontaktnummern enger Mitarbeiter stets verfügbar zu haben, schon auf Grund der kleinen Teamgröße gegeben ist. Die umgehende Erkennung eines Notfalls (insbesondere einer schleichend anwachsenden Störung) ist jedoch meist mit größeren Aufwendungen verbunden. Das Unternehmen hat in jedem Raum Rauchmelder installiert, in der Küche zusätzlich einen Wassermelder[37]. Server- und Arbeitsraum sind des Weiteren durch Bewegungsmelder und Magnetkontakte an den Fenstern und Türen gesichert, um Einbrüche zu verhindern. Diese einzelnen Komponenten sind an ein Sicherheitssystem angeschlossen, welches direkt mit dem bundesweiten Leitstellenservice verbunden ist und automatisch Meldungen an die eigene Mobilnummer und die Notrufzentrale weitergibt.[38] Damit folgt die Real Fiction GbR dem vom BSI empfohlenen Vorschlag zur Einrichtung einer Gefahrenmeldeanlage (GMA)[39] zur Reduzierung physischer Risiken der Unternehmensdaten.

Meldungen bezüglich Netzereignissen (bspw. Verbindungsabbrüche, Angriffe mit Viren oder Trojanern, Penetrationen) werden in dem Unternehmen durch Hard- und Softwarefirewalls sowie Virenscanner produziert und per SMTP-Funktion und PUSH[40] -

[37] Option: Feuer-Unterdrückungssysteme
[38] z.B. Protector-V, vgl. `www.protector-v.de` (Stand: 20.08.2008)
[39] hervorgehoben im BSI-Standard 100-4, bereits beschrieben im IT-Grundschutz
[40] Definition siehe `de.wikipedia.org/wiki/Push-Dienst`

Technologie direkt auf die Mobiltelefone (z.B. Blackberrys) des Teams übertragen.[41] Intrusion Detection und Intrusion Response Systeme sind bisher nicht eingeführt worden, werden aber mit dem Wachstum des Unternehmens und einer Webpräsenz zunehmend an Bedeutung gewinnen. Wird zum Beispiel der Backupvorgang des Servers unterbrochen und kann nicht automatisch wieder aufgenommen werden, so unterstützt die Acronis Software ebenfalls eine sofortige Email-Benachrichtigung. Stromausfälle, die diese Art der Notfallmeldung verhindern, können durch eine geeignete USV-Lösung[42] behandelt werden. Da die GMA netzspannungsunabhängig läuft (Batteriebetrieb), wird die Serviceleister-Vereinbarung für den Notfall als ausreichende Alternative gegenüber einer angemessenen (teuren) Notstromlösung angesehen.

Das BSI spricht von dem Alarm-Management als eigenständiger Prozess, durch den alle Meldungen zentral zusammen laufen und bewertet werden, bevor der Krisenstab(-leiter) informiert bzw. alarmiert wird – u.a. um Fehlalarme zu vermeiden. Eine geringe Mitarbeiteranzahl wie bei Real Fiction lässt das Alarm-Management und die Krisenstabsfunktion jedoch aus Gründen der Effizienz verschmelzen. Dennoch gilt für alle Teamgrößen, die Schwelle zur Formulierung einer Meldung möglichst niedrig zu halten.

In der Entscheidungsphase muss auf Basis der vorliegenden Informationen die Eskalation beschlossen werden oder alternativ reagiert werden. Das Team der Real Fiction bildet gemeinschaftlich den Krisenstab, wobei nur einer Person die endgültige Entscheidungskompetenz zugesprochen wurde. Dabei wird sich an dem Notfallhandbuch orientiert, in dem die Anforderungen zur Eskalation dokumentiert sind. Wenn die Arbeitsräume für eine Besprechung nicht genutzt werden können, bieten sich Hotels o.ä. Tagungsorte als Krisenstabsräume (inkl. benötigtem technischen Equipment) an.

Die stufenlose Eskalation und der Umzug zum Ausweichstandort erfolgt bei der Real Fiction direkt. Die Sofortmaßnahmen werden nicht schrittweise umgesetzt, sondern können parallel durchgeführt werden. Im Notfallplan stehen die dazu nötigen Kontaktinformation von Rettungsdiensten, Servicedienstleistern, Wegbeschreibungen zu Notfalltreffpunkten und Ausweichstandorten. Die Aufgaben für die einzelnen Teammitglieder sollten darin ebenfalls klar definiert sein (Öffentlichkeitsarbeit[43], Vorbereitung der Backup-Site(s), Ressourcenrettung soweit möglich), um den Notbetrieb ohne große Zeit- und Datenverluste aufnehmen zu können.

Durchzuführende Schritte in der **Übersicht**:

- Kommunikationswege und Authorisierung sind auf eine schnellstmögliche Aktivierung des Notfallplans abzustimmen.

[41] Mehr Informationen zum Push IMAP Protokoll siehe [Rei07], [Joh04].
[42] Definitionen und Übersicht gibt [Red08]
[43] einschließlich Lieferanten, Kunden, Polizei, Feuerwehr, Notarzt etc.

- Die Aktivierung des Plans ist in drei Phasen umzusetzen.
  - Meldungsphase: Erkennung eines Notfalls und Benachrichtigung des Krisenmanagements. Gefahrenmeldeanlagen und sonstige technische Hilfen sind zu empfehlen, um das geschulte und sensibilisierte Personal zu unterstützen.
  - Entscheidungsphase: Die Entscheidung über eine Eskalation ist zu fällen. Ist dies auf Grund der Informationslage nicht möglich, muss auf schnellstem Wege eine Bewertung mit zusätzlichen Informationen von dem Krisenstab durchgeführt werden.
  - Umsetzungsphase: Schrittweise oder direkte Umsetzung aller Sofortmaßnahmen anhand des Notfallhandbuchs. Eine klare Aufgabenverteilung ist wichtig.

7.3.2 Welche Faktoren beeinflussen einen möglichst effizienten Notbetrieb?

Im Krisenmanagement werden zwischen dem Ausführen der Sofortmaßnahmen nach Eintreten eines Notfalls und der Rückkehr zum Normalbetrieb zwei Phasen – Wiederanlauf und Notbetrieb – unterschieden, dargestellt in Abbildung 2.1 auf Seite 9. Die Faktoren, die den Wiederanlauf und die Durchführung des Notbetriebs in besonderem Maße beeinflussen, werden nachfolgend erläutert.

Der Wiederanlauf (Phase 1)

Die Qualität des Notbetriebs hängt stark von der Vorbereitung auf – und den Maßnahmen des – Wiederanlaufs ab. Die nächsten Schritte sind zudem sehr fehleranfällig, wodurch die zeitliche Sensibilität dieser Phase schnell an ihre Grenzen stoßen kann. Die Fähigkeiten der Real Fiction-Mitarbeiter sind jedoch geschult und das Team kann sich auf ein aktuelles Notfallhandbuch und Disaster Recovery Lösung verlassen – zwei wichtige Faktoren zur Einhaltung der vordefinierten Wiederherstellungszeit (RTO). Sobald die Sofortmaßnahmen eingeleitet sind (Notrufe und Strategieentscheidung), trifft sich das (Krisenmanagement-) Team an dem 30 Autominuten entfernten Ausweichstandort nahe Bonn. Der zuvor benachrichtigte Dienstleister hat die vertraglich geregelten Ressourcen bereits vorbereitet und übergibt bei Ankunft den Raum (Cold Site) schlüsselfertig.

Als nächstes wird die Disaster Recovery mit Acronis durchgeführt. Zur Wiederherstellung der Systemimages von der Backup-Site auf der nicht identischen Hardware der Recovery Site sind drei Möglichkeiten mit der genutzten Acronis Software denkbar. Der schnellste Weg wird mit der Acronis CD oder einer zuvor angefertigten Restore-CD gegangen. Diese bootfähigen Disks installieren sich automatisch im Hauptspeicher (Laufwerk nutzbar) und verbinden sich betriebssystemunabhängig mit dem Sicherungsserver, auf dem die Images gelagert sind. Über die sichere Verbindung zwischen den

Acronis Komponenten kann das letzte Systemabbild direkt wiederhergestellt werden. Dieser Weg des Bare Metal Restore (betriebssystemunabhängige Wiederherstellung mittels Boot-CD) entspricht dem optimalen Einsatz der Acronis Suite.

Ist eine Notfall-CD nicht am Ausweichstandort hinterlegt, weil sie bspw. nie angefertigt wurde, besteht eine weitere, aber komplizierte Alternative der Datenwiederherstellung. Steht ein Rechner mit installierter Acronis Management Konsole zur Verfügung, bspw. ein Heim-PC, so können unmittelbar nach der Eskalation virtuelle Festplatten (VHD) aus den Backups erzeugt werden. Am Ausweichstandort werden die VHDs in der entsprechenden Software gemountet (z.B. VMWare, XEN oder MS Virtual Server) und während des Notbetriebs damit betrieben. Die Vorteile von Virtualisierung sind allgemein bekannt: Plattformunabhängigkeit, gute Hardwareauslastung, Wirtschaftlichkeit – um nur einige zu nennen. In dem konkreten Fall ergeben sich aber zahlreich Hindernisse, die beachtet werden müssen. So ist es eine notwendige Voraussetzung, dass auch auf dem Sicherungsserver eine lizensierte Acronis True Image Echo Version installiert ist, da der Acronis Backup Server diesen Konvertierungstask nicht ausführen kann. Außerdem kann dieser Task nicht automatisiert werden. Das bedeutet, für eine aktuelle VHD muss stets manuell gesorgt werden – und zwar von jedem relevanten Backup. Sofern nicht mehrere physische Laufwerke bei der Konvertierung benutzt werden, muss die Konvertierung seriell erfolgen, was mit einem erheblichen Zeitaufwand verbunden ist.[44] Zudem steigen die Anforderungen an den verfügbaren Speicherplatz auf dem Sicherungsstandort um bis zu 300%, da die VHD kurzzeitig zusätzlich zum komprimierten Backup zwischengespeichert werden muss (unkomprimiert). Da die Übertragung einer VHD nicht über den Acronis Backup Server geschehen kann, muss über einen alternativen Weg für eine sichere Verbindung gesorgt werden (z.B. SFTP, VPN). Der zeitliche Bedarf für die Installation der Virtualisierungssoftware fällt dabei schon kaum mehr ins Gewicht. Aus den genannten Gründen ist der Weg über virtuelle Festplatten im Disaster Recovery Prozess daher nicht zu empfehlen. Sollten allerdings alle Notfall-CDs sowie alle Authentifizierungsdaten bspw. in einem Feuer verloren gegangen sein, kann diese zeitaufwendige Methode einen möglichen Ausweg darstellen.

Ohne Notfall-CD, aber mit vorheriger Registrierung beim Hersteller, besteht die Möglichkeit, über das Acronis-Webportal die Software erneut zu laden. Danach wird das Tool auf einem vorkonfiguriertem Betriebssystem installiert und man führt die Wiederherstellung über die Server bzw. Workstation-Applikation durch.[45]

Die Real Fiction GbR hat die Software-CDs und die Schlüsselnummern in einem Schließfach bei ihrem Recovery Site Dienstleister abgelegt. Recovery-Boot-CDs und Kopien der Installationscodes befinden sich gleichzeitig im Unternehmen (gesichert). Die größte Her-

[44] Im Test: Konvertierung von 4,5GB (Abbild): 22 Minuten. Größe der virtuellen Platte: 9GB

[45] Registrierungsdaten zum Webportal und eine BS-Lizenz müssen vorhanden sein

ausforderung für das Unternehmen besteht in der Erfüllung der Wiederherstellungszeit. Die Reihenfolge der Wiederherstellung ist durch eine Server-Priorität klar geregelt.[46] In komplexeren IT-und Geschäftsstrukturen sind die Abhängigkeiten dieser im Vorfeld zu analysieren und im Notfallhandbuch festzuhalten. Einflussstarke Faktoren auf die Wiederherstellungszeit sind für das Unternehmen neben der Größe der wiederherzustellenden Partitionen eine vollständige Personalverfügbarkeit (des Krisenteams und Schlüsselpositionen) und die Zuverlässigkeit des Dienstleisters. Insbesondere in einem kleinen Team müssen alle Mitglieder vor Ort sein, um den zusätzlichen organisatorischen Aufwand zu bewältigen. Bei der Auswahl des Dienstleisters sollte man nach Möglichkeit bereits auf Erfahrungswerte Anderer zurückgegriffen haben. Eine Verzögerung beim Zugang zu den zugesagten Räumlichkeiten und Ressourcen wird alle RTO-Vorgaben leicht gefährden.

Der Notbetrieb (Phase 2)

Sind die Abbilder wiederhergestellt, müssen die tatsächlichen Datenverluste festgestellt werden. In Forschungstätigkeiten gilt es, die durch das RPO nicht abgedeckten Fortschritte zu rekonstruieren. Da der Notbetrieb durch zahlreiche zusätzliche Belastungen gekennzeichnet ist, darunter Umleiten des Postverkehrs, Kontakt zu Versicherungen, Rücksprache mit Polizei, Kundenbeschwerdemanagement, etc., ist eine strikte Arbeitsteilung zur Aufrechterhaltung einer eingeschränkten Produktivität sinnvoll. Ebenfalls sollte sichergestellt werden, dass die kontinuierlichen Sicherungen zur Backup-Site nach der Wiederherstellung der Systeme automatisch weitergeführt wird.

Das BSI empfiehlt, mit der Planung zur Rückführung in den Normalbetrieb zu beginnen, „sobald die dringlichsten Maßnahmen für die Geschäftsfortführung umgesetzt sind“. Wegen der „Nicht-Planbarkeit vieler Umstände und Auswirkungen“ muss für einen „ausgedehnten Zeitraum“ geplant werden.[47] Der Vertrag mit dem Dienstleister ist daher so gestaltet, dass das Real Fiction Team auf unbeschränkte Zeit die Arbeitsplätze zur Verfügung gestellt bekommt.

[46] Die Workstation-Abbilder sind zudem im Server-Backup enthalten

[47] Für alle Zitate dieses Paragraphen vgl. BSI-Standard 100-4 ([Bun08]), Unterabschnitt 6.3.3 „Wiederherstellung“ (Seite 53)

Die alternative Schritte des Wiederanlaufs in der **Übersicht**:

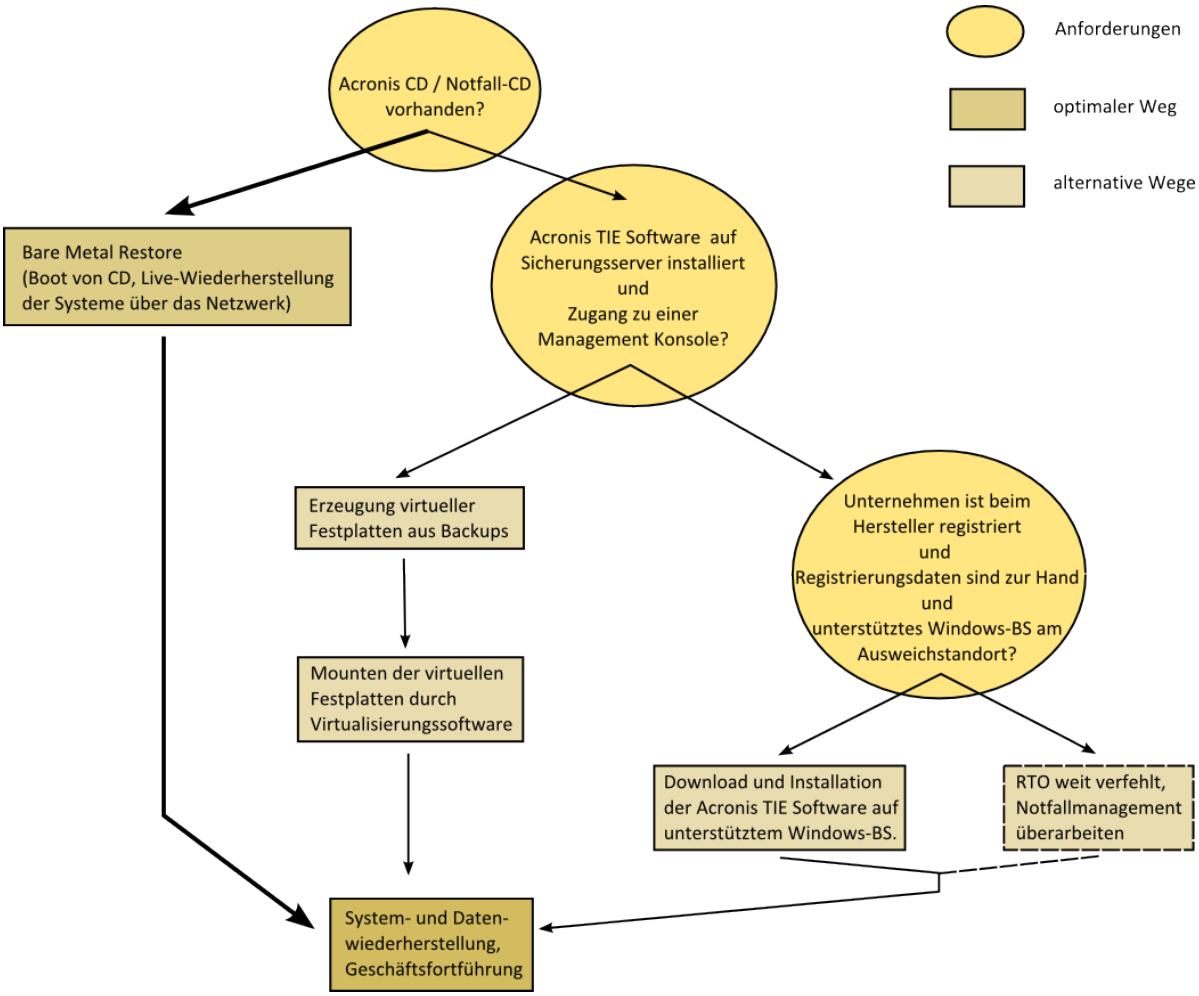


Abb. 7.8: Baumstruktur alternativer Wege zum Notbetrieb (Quelle: Eigendarstellung)

7.3.3 Wie können Fehler bei der Rückspielung aller Daten vermieden werden?

Die Rückkehr zum Normalbetrieb steht in der Regel unter einem ähnlich zeitlichen Druck wie der Wiederanlauf zum Notbetrieb. Das hängt damit zusammen, dass im Notbetrieb auf Grund von Ressourcenmangel (Personal, Technik, Budget) und zusätzlichen Belastungen (Arbeit, Verantwortung, Stress) die Produktivität der Geschäftsaktivitäten eingeschränkt ist. Eine schnellstmögliche Wiederherstellung zum Normalbetrieb ist

daher schon aus wirtschaftlicher Sicht angestrebt. Basis dieser Umsetzung sollten die vorab (vor dem Notfall) definierten Zeitpunkte bzw. Bedingungen sein, wann ein Notfall offiziell als bewältigt gelten soll. Zumindest alle kritischen Ressourcen müssen wieder verfügbar sein, die konkrete Ausgestaltung des Ablaufplans zur Deeskalation / Rückführung kann allerdings erst im Notbetrieb erarbeitet werden (anlehnend an die zuvor zitierte „Nicht-Planbarkeit“ im Notbetrieb.[48]

Für die Real Fiction GbR besteht die größte Aufgabe in der Wiederherstellung oder Wiederbeschaffung und Reinitialisierung der Hardwarekomponenten. Ist die Technik im Unternehmensgebäude erst einmal wieder aufgebaut, so läuft die Softwarerückspielung auf die gleiche Weise ab wie zuvor im Wiederanlauf. Die Möglichkeit zur Erstellung einer Recovery-CD sollte in jedem Fall genutzt werden, falls vorhandene Exemplare durch den Notfall unbrauchbar gemacht wurden. Vor dem Umzug in das Unternehmensgebäude werden für alle Rechner manuell ein inkrementelles Backup über den Acronis Group Server erstellt. Um nicht nur die Aktualität der Daten sicherzustellen, sondern auch mögliche Integritätsfehler auszuschließen, wird danach für alle gesicherten Archive (Vollbackups plus inkrementelle Backups) eine Validierung durchgeführt. Dieser Schritt kann auf allen Systemen parallel ausgeführt werden, da die Validierung immer eine hohe CPU-Auslastung mit sich bringt. Ist der Prozess auf allen Rechnern beendet, kann der Ausweichstandort verlassen und die Abbilder in den Unternehmensräume wieder aufgespielt werden. Es bietet sich an, die aktuellsten Backups auf einem mobilen Datenträger (z.B. eine ausreichend große Festplatte) mitzuführen. Mit Hilfe der Notfall-CDs und den lokalen Backups kann somit schnell eine komplette Wiederherstellung erreicht werden, ohne die Abbilder erneut von der Backup-Site übertragen zu müssen. Damit ist die Rückführung der Real Fiction GbR in den Normalbetrieb erreicht.

Es bleibt zu erwähnen, dass nach der Rückführung in den Normalbetrieb insbesondere bei mitarbeiterstarken Unternehmen auf die individuellen Belastungen während des Notbetriebs Rücksicht genommen werden sollte. Überstunden- und Urlaubsangelegenheiten während der Aufarbeitung des Notfalls im Normalbetrieb sollten daher bereits im Vorfeld mit dem Betriebsrat oder sonstiger Mitarbeitervertretung einvernehmlich geregelt worden sein. Zu den arbeitsintensiven Aufgaben der Aufarbeitung zählt insbesondere die Identifizierung von Schwachstellen des Krisenmanagements, zur Verbesserung des Ablaufs beim nächsten Notfall.

Durchzuführende Schritte in der **Übersicht**:

- Rückkehr zum Normalbetrieb, sobald vordefinierte Bedingungen bezüglich kritischer Ressourcen (notiert im Notfallhandbuch) erfüllt sind.

[48] siehe Unterabschnitt Notbetrieb auf Seite 85

- Wiederbeschaffung von Hard- und Software, die im Rahmen des Notfalls verloren ging.
- Aktuelle Sicherungskopien anfertigen und am Unternehmensstandort wiederherstellen.
- Ausfallzeiten wiederaufarbeiten bei Berücksichtigung der individuellen Mitarbeiterbelastungen.
- Schwierigkeiten der Disaster Recovery in Verbesserungen des Notfallmanagements umsetzen.

8 Folgerung und Ausblick

„Ist diese Notfallstrategie wirklich notwendig?“ Es gibt hunderte Fragen wie diese und tausende Antworten rund um das Thema Business Continuity Planning. Wahrscheinlich lässt sich sogar jede einzelne Fragestellung in eine von zwei Kategorien einordnen:

1. Fragen nach dem Gründen für BCP (Überzeugungsmangel)
2. Fragen nach der Angemessenheit im Notfallmanagement (Erfahrungsmangel)

Diese Diplomarbeit beantwortet diese Frage nicht. Das kann sie meiner Meinung nach auch gar nicht. Denn bei allem, was diese wissenschaftliche Arbeit vermitteln soll, wird eine Sache zu jeder Zeit in den Vordergrund gestellt: Die Etablierung eines Notfallmanagements kann nur dann erfolgreich sein, wenn jeder Prozess als unternehmensindividuelle Aufgabe bearbeitet wird. Wenn Rahmenwerke nicht als Bauanleitung, aber als unterstützende Hintergrundinformation gesehen werden und wenn die floskelhaften Begründungslisten, wie sie oft in Artikeln und Büchern zu finden sind, der Herausarbeitung nachweisbarer Vorteile für ein spezifisches Unternehmen weichen, *dann* können Überzeugungen und Erfahrungen verständlich vermittelt werden zum Vorteil von Arbeitnehmer und Arbeitgeber.

Durch die Kapitel hinweg in dieser Arbeit hat sich ein wichtiger Gedanke geformt: Business Continuity Planning ist ein sehr breites Thema, das nicht isoliert betrachtet werden kann und darf, sondern das auf oberster Ebene in alle Bereiche eines Unternehmens hineingreift. Ein Notfallplan spiegelt die vernetzten Strukturen eines Unternehmens oder einer Behörde wider. Je komplexer die Organisation, desto deutlicher muss der Notfallplan den sprichwörtlich „roten Faden“ darstellen.

Der zweite wichtige Punkt, der aus den zurückliegenden Betrachtungen folgt, ist, dass Business Continuity Planning ungleich vielen anderen bereichsübergreifenden Management-Themen ein sehr praxis- und oft erfahrungsorientiertes Thema ist. Zu Beginn habe ich BCP mit einer „Berufsunfähigkeitsversicherung“ verglichen – dieser Vergleich zeichnet im letzten Kapitel mehr noch als am Anfang deutliche Parallelen. *Existenzsicherung* ist ein Individualkonzept, aufbauend auf realen Situationen und praktischen Anforderungen, um im Ergebnis durch die Kombination von Best Practices und eigenen Erfahrungen einen zufriedenstellenden Level an Sicherheit zu erhalten.

Für die weiteren Schritte bedeutet dies, dass auf wissenschaftlicher Seite die Notfallplanung zunächst aktiv innerhalb von Universitäten oder in Kooperation mit aufgeschlossenen Unternehmen angewendet werden sollte. Dabei werden die gesetzlichen Vorgaben, die eingesetzten Werkzeuge und die speziellen Ziele des Unternehmens eine wichtige Rolle spielen. Als Resultat erhält man eine Wissensdatenbank, die für weitere wissenschaftliche Untersuchungen auf dem Gebiet genutzt werden kann. Auf übergeordneter Ebene könnte so langfristig Wissen generiert werden, das Organisationen in diesem Feld der Unternehmungssicherheit vor dem Hintergrund immer komplexerer Strukturen in ihren Vorsorge- und Planungsvorhaben unterstützt.

Die zukünftige Entwicklung des Notfallmanagements wird auch weiterhin in einem aktiven Rahmen stattfinden. Weltweit wird Business Continuity Planning noch stärker gefragt sein als es heute bereits ist. Ich denke mittelfristig (in drei bis fünf Jahren) werden Großunternehmen stärker in die Verantwortung genommen, Vorsorge zu betreiben. Denkbar wären auch regionale Auflagen oder weitere branchenspezifische Bestimmungen, wie es sie beispielsweise im Banksektor bereits gibt. In Deutschland wird man sich am BSI-Standard 100-4 orientieren, der erst jüngst in der letzten Entwurfsversion vor der Veröffentlichung im vierten Quartal 2008 herausgegeben wurde. Die Vorzeichen sind also positiv und der Aufschwung des Business Continuity Planning wird auch in den nächsten Jahren weiterhin anhalten.

Literaturverzeichnis

[Abe08] Aberdeen Group: *Business Continuity: Implementing Disaster Recovery Strategies and Technologies*. 2008. – Stand: 28. Juni 2008

[Age05] Agency, National S.: Fact Sheet NSA Suite B Cryptography. In: *Central Security Service* (2005). http://www.nsa.gov/ia/industry/crypto_suite_b.cfm. – Stand: 24. August 2008

[All06] Allinson, Robert E.: *Saving Human Lives. Lessons in Management Ethics*. 1. Auflage. Springer-Verlag GmbH, 2006 (Issues in Business Ethics). – ISBN 1402029055

[Arb95] Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.: *Bundesministerium der Finanzen: Grundsätze Ordnungsmäßiger DV-Gestützter Buchführungssysteme (GoBS)*, November 1995. http://www.bundesfinanzministerium.de/nn_53848/DE/Wirtschaft_&_und_%_Verwaltung/Steuern/Veroeffentlichungen__zu__Steuerarten/Abgabenordnung/005.html?__nnn=true. – Stand: 08. April 2008

[Bas04] Basel Committee on Banking Supervision: *Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework*, Juni 2004. http://www.bis.org/publ/bcbs107.htm. – Stand: 1. April 2008

[Bau08] Baumeister, Johann: Disaster Recovery: So beugt man dem Totalausfall vor. In: *ZDNet.de* (2008). http://www.zdnet.de/enterprise/server/0,39023275,39190194,00.htm. – Stand: 12. Mai 2008

[BCM08] BCM-News.de: *Market overview BCM-Tools*. http://bcm-news.de/tinc?key=ModQ0vfH\&formname=BCM_Tools. Version: 2008. – Stand: 11. Juli 2008

[BNG03] Badaracco, Joseph L. ; Nash, Laura L. ; Gellerman, Saul W.: *Harvard Business Review on Corporate Ethics*. Mcgraw-Hill Professional, 2003 (Harvard Business School Press). – ISBN 159139273X

[Boe07] Boerse, Jan-Hendrik: *Business Continuity Management bei Pandemien*, Fachhochschule Wiesbaden, Diplomarbeit, 2007

[Bri06] British Standards Institution: *BS 25999-1 Business Continuity Management – Code of Practice*. 2006 http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030157563. – ISBN 0580496015. – Stand: 10. April 2008

[Bri07] British Standards Institution: *BS 25999-2 Business Continuity Management – Specification for BCM*. 2007 http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030169700. – ISBN 0580599132. – Stand: 10. April 2008

[Bun98] Bundesministerium der Justiz: *Verordnung über Anforderungen an die Hygiene beim Herstellen, Behandeln und Inverkehrbringen von Lebensmitteln*, 1998. http://www.gesetze-im-internet.de/lmhv_2007/index.html. – Stand: 11. April 2008

[Bun07a] Bundesanstalt für Finanzdienstleistungsaufsicht: *Mindestanforderungen an das Risikomanagement*, Oktober 2007. http://www.bundesbank.de/bankenaufsicht/bankenaufsicht_marisk.php. – Stand: 1. April 2008

[Bun07b] Bundesanstalt für Finanzdienstleistungsaufsicht: *Rundschreiben 5/2007 (BA) - Mindestanforderungen an Das Risikomanagement*, Oktober 2007. http://www.bafin.de/cln_006/nn_721290/SharedDocs/Veroeffentlichungen/DE/Service/Rundschreiben/2007/rs__0705__ba.html?__nnn=true. – Stand: 1. April 2008

[Bun07c] Bundesministerium für Wirtschaft und Technologie: *Berufsaufsichtsreformgesetz, Siebte Novelle der Wirtschaftsprüferordnung, in Kraft*, September 2007. http://www.bmwi.de/BMWi/Navigation/Presse/pressemitteilungen,did=217290.html. – Stand: 11. April 2008

[Bun08] Bundesamt für Sicherheit in der Informationstechnik: *BSI-Standard 100-4 Notfallmanagement*, März 2008. http://www.bsi.bund.de/literat/bsi_standard/index.htm. – Stand: 1. April 2008

[Bus] Business Continuity Institute: *Glossary of the BCI*. http://www.thebci.org/Glossary.pdf. – Stand: 20. April 2008

[Bus02] Business Continuity Institute ; Smith, David (Hrsg.): *Business Continuity Management: Good Preactice Guidlines*. http://www.davislogic.com/bcm.htm. Version: 2002. – Stand: 20. April 2008

[Com06] Compliance-Magazin: Was ist SOX? In: *Compliance-Magazin.de* (2006), Oktober. http://www.compliancemagazin.de/gesetzestandards/usa/sox/symantec051006.html. – Stand: 1. April 2008

[Com07] Computerwoche: Ratgeber: Disaster-Recovery-Verfahren. In: *TecChannel* (2007). http://www.tecchannel.de/storage/backup/1728161. – Stand: 28. Juni 2008

[Con06] Connors, Tom: SOX Benefits. In: *Corporate Responsibility Officer* (2006). http://www.thecro.com/node/400. – Stand: 1. April 2008

[Coo] Cook, Rick: *DR, BC, BIA: What's the difference?* http://searchstorage.techtarget.com/tip/0,289483,sid5_gci892358,00.html. – Stand: 20. April 2008

[Dav] DavisLogic Inc.: *Business Continuity Management.* http://www.davislogic.com/bcm.htm. – Stand: 20. April 2008

[Dep03] Department of Health and Human Services: *The HIPAA Law and Related Information.* http://www.cms.hhs.gov/HIPAAGenInfo/02_TheHIPAALawandRelated%20Information.asp. Version: Februar 2003. – Stand: 12. April 2008

[Deu07] Deutsche Sparkassenakademie: *Deutsche Sparkassenakademie DSGV-Interpretationsleitfaden MaRisk*, Juni 2007. http://www.deutsche-sparkassenakademie.de/leitfaden/index.html. – Stand: 1. April 2008

[Dis03] Disaster Recovery Institute International: *Professional Practices.* http://www.drii.org/drii/ProfessionalPractices/about_professional_detail.aspx. Version: 2003. – Stand: 19. Mai 2008

[Dis07] Disaster Recovery Journal: *BC Glossary.* http://www.drj.com/glossary/drjglossary.html. Version: August 2007. – Stand: 20. April 2008

[Dom01] Dominic Elliott und Ethné Swartz und Brahim Herbane: *Business Continuity Management.* Routledge, 2001. – ISBN 0415204925

[Dor05] Dorion, Pierre: Go beyond SOX for business continuity. In: *Search400.com* (2005). http://search400.techtarget.com/tip/0,289483,sid3_gci1145397,00.html. – Stand: 1. April 2008

[Dou01] Doughty, Ken: *Business Continuity Planning: Protecting Your Organization's Life.* Auerbach Publishers Inc., 2001. – ISBN 0849309077

[Eur06] Europäische Parlament und der Rat der Europäischen Union: *8. EU-Richtlinie (RICHTLINIE 2006/43/EG)*, Mai 2006. http://www.cco-forum.de/wordpress/wp-content/uploads/2007/10/i-eu-richtlinie.pdf. – Stand: 10. April 2008

[Fed08] Federal Financial Institutions Examination Council: *Business Continuity Planning Booklet*, März 2008. `http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf`. – Stand: 14. April 2008

[Fin05a] Financial Reporting Council: *The Turnbull Guidance on Internal Control*, Oktober 2005. `http://www.frc.org.uk/corporate/internalcontrol.cfm`. – Stand: 10. April 2008

[Fin05b] Finanzmarktaufsichtsbehörde Österreich (FMA): *Stellungnahme der FMA Zum Entwurf eines Bundesgesetzes, mit dem das Qualitätssicherungsgesetz erlassen und das Wirtschaftstreuhandberufsgesetz (WTBG) geändert wird*, April 2005. `http://www.fma.gv.at/cms/site//attachments/9/9/5/CH0214/CMS1139401780611/050519_1.pdf`. – Stand: 12. April 2008

[Fin06] Financial Reporting Council: *Combined Code*, Juni 2006. `http://www.frc.org.uk/corporate/combinedcode.cfm`. – Stand: 11. April 2008

[Fre03] Frentz, Clemens von: Enron: Chronik Einer Rekord-Pleite. In: *Manager-Magazin* (2003), September. `http://www.manager-magazin.de/unternehmen/artikel/0,2828,178836,00.html`. – Stand: 14. April 2008

[Gal03] *Kapitel* What is business continuity management (BCM)? In: Gallagher, Michael: *Business Continuity Management – How to protect your company from danger*. Financial Times Prentice Hall, 2003 (Management Briefings Executive Series). – ISBN 0273663518, S. 8–12

[Hil07a] Hiles, Andrew: *The Definitive Handbook of Business Continuity Management*. Bd. 2. Wiley & Sons, 2007. – ISBN 0470516380

[Hil07b] *Kapitel* Case Study: Thirty seconds of terror! The California earthquake. In: Hiles, Andrew (Hrsg.): *The Definitive Handbook of Business Continuity Management*. Wiley & Sons, 2007. – ISBN 0470516380, S. 431–434

[Hil07c] *Kapitel* Case Study: A coutionary tale. In: Hiles, Andrew (Hrsg.): *The Definitive Handbook of Business Continuity Management*. Wiley & Sons, 2007. – ISBN 0470516380, S. 451–453

[Hil07d] *Kapitel* Case Study: Chicago Floods. In: Hiles, Andrew (Hrsg.): *The Definitive Handbook of Business Continuity Management*. Wiley & Sons, 2007. – ISBN 0470516380, S. 429–430

[Hil07e] *Kapitel* Case Study: It happened to them. In: Hiles, Andrew (Hrsg.): *The Definitive Handbook of Business Continuity Management*. Wiley & Sons, 2007. – ISBN 0470516380, S. 454–456

[Häm] Hämmerle, Matthias: *ISO Standard für Business Continuity Management veröffentlicht.* http://www.bcm-news.de/2007/12/12/iso-standard-fuer-business-continuity-management-veroeffentlicht. – Stand: 20. April 2008

[IBM06] IBM Deutschland GmbH: *Planung für den Notfall – BC unter Personalaspekten.* 2006

[Int07] International Organization for Standardization: *ISO/IEC 27002 (ISO17799) 2007*, April 2007. http://www.27001-online.com. – Stand: 10. April 2008

[iQo08] iQom Business Services GmbH: *Produktseite zu iQ.connect.line.datalink.* http://www.iqom.de/de/produkte-loesungen/iq-connect/iq-connect-line/iq-connect-line-datalink. Version: 2008. – Stand: 20. August 2008

[IS06] International Settlements, Bank for: *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework – Comprehensive Version*, Juni 2006

[Joh04] Johannessen, Bob: The Push-IMAP Protocol. In: *Internetseite des Johannessen Design Bureau* (2004). http://db.org/2004/02/12/push-imap. – Stand: 31. August 2008

[Joi] Joint Commission on Accreditation of Healthcare Organizations: *The Joint Commission.* http://www.jointcommission.org. – Stand: 9. April 2008

[Krö] Krönig, Jürgen: *Hauptverdächtigter: al-Qaida.* http://www.zeit.de/2005/28/london_terror. – Stand: 20. April 2008

[Kra02] Krafft, Martin: Gefahr für AES und RSA. In: *magnus.de* (2002). http://internet.magnus.de/sicherheit/artikel/aes-und-rsa-noch-sicher.html. – Stand: 24. August 2008

[Lei07] Leierseder, W.: IDC-Studie: Kleine Firmen vernachlässigen IT-Sicherheit. In: *Onlineportal ChannelPartner.de* (2007). http://www.channelpartner.de/zyxel-special/238138/index1.html. – Stand: 8. September 2008

[Lei08] Leierseder, W.: Hochwasser, Terror, Pandemie: Die wenigsten sind gegen einen IT-Ausfall genug gewappnet. In: *CIO Online-Magazin* (2008). http://www.cio.de/knowledgecenter/rm/848437/index1.html. – Stand: 5. September 2008

[Luc04] Lucey, Kathleen: Business continuity plan development explored. In: *Continuity Central* (2004). http://www.continuitycentral.com/feature0106.htm. – Stand: 12. Mai 2008

[Mar02] Martin Wieczorek, Uwe Naujoks und Bob Bartlett: *Business Continuity: Notfallplanung für Geschäftsprozesse*. Bd. 1. Springer Verlag, 2002. – ISBN 3540442855

[McC04] McCrackan, Andrew: *Is business continuity a subset of risk management?* http://www.sueddeutsche.de/ausland/schwerpunkt/893/9884. Version: 2004. – Stand: 20. April 2008

[Mic07] Michael Whitman und Herbert J. Mattord: *Management of Information Security*. Bd. 2. Cengage Learning Services, 2007. – ISBN 1423901304

[New04] New York Stock Exchange: *NYSE - Information Memos: Rule 446 - Business Continuity and Contingency Plans*. http://www.nyse.com/Frameset.html?displayPage=http://rules.nyse.com/NYSE/Help/Map/rules-sys463.html. Version: April 2004. – Stand: 3. April 2008

[New08] New York Stock Exchange Euronext: *NYSE Trading Licenses*. http://www.nyse.com/productservices/nyseequities/1167954368153.html. Version: 2008. – Stand: 3. April 2008

[O'H07] *Kapitel* What is a business continuity planning (BCP) strategy? In: O'Hehir, Michael: *The Definitive Handbook of Business Continuity Management*. Wiley & Sons, 2007. – ISBN 0470516380, S. 27–46

[Pat02] Patsuris, Penelope: The Corporate Scandal Sheet. In: *Forbes Magazine* (2002), August. http://www.forbes.com/2002/07/25/accountingtracker.html. – Stand: 14. April 2008

[Pro07] Prof. Dr. Burkhardt Krems: Wirtschaftlichkeit und Wirtschaftlichkeitsuntersuchungen. In: *Beitrag im Online-Verwaltungslexikon olev.de* (2007). http://www.olev.de/w/wirtsch.htm. – Stand: 31. August 2008

[RA02] Riva Atlas, Simon R.: Worldcom's Collapse: The Overview; Worldcom Files For Bankruptcy; Largest U.S. Case. In: *The New York Times* (2002), Juli. http://query.nytimes.com/gst/fullpage.html?res=9C04E6D81738F931A15754C0A9649C8B63. – Stand: 13. April 2008

[Rüd08] Rüdiger Grimm und Anastasia Meletiadou: Vorlesung IT-Risk-Management. In: *Sicherheitskonzepte*. Universität Koblenz-Landau, 2008

[Red07] Redaktion von Silicon.de: Japan strikt an eigenem SOX. In: *Silicon.de* (2007), März. http://www.silicon.de/software/business/0,39039006,39183008,00/japan+strickt+an+eigenem+sox.htm. – Stand: 13. April 2008

[Red08] Redaktion des Elektronik-Kompendium: *USV - Unterbrechungsfreie Stromversorgung.* http://www.elektronik-kompendium.de/sites/grd/0812171.htm. Version: 2008. – Stand: 30. August 2008

[Rei07] Reimann, Michael: IMAP-Push. In: *Internetseite der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen* (2007). http://www.gwdg.de/service/netze/mailer/imap-push.html. – Stand: 31. August 2008

[Roy08] Royds, James: *The convergence of Business Continuity and Risk Management.* http://www.businesscontinuityexpo.co.uk/page.cfm/link=114. Version: 2008. – Stand: 20. April 2008

[Sch01] *Kapitel* 3. In: Schreider, Tari: *The Legal Issues of Business Continuity Planning.* Auerbach Publishers Inc., 2001 (Business Continuity Planning: Protecting Your Organization's Life). – ISBN 0415204925, S. 15–20

[Sch08] Schmitt, Peter-Philipp: Weltkatastrophenbericht 2008: Mehr Opfer, aber weniger Tote. In: *Onlineausgabe der Frankfurter Allgemeinen Zeitung* (2008). http://www.olev.de/w/wirtsch.htmhttp://www.faz.net/s/RubB08CD9E6B08746679EDCF370F87A4512/Doc~E320E3DBD58C4468491200EE032C525A9~ATpl~Ecommon~Scontent.html. – Stand: 8. September 2008

[Sid05] Sidler, Wolfgang: Disaster Recovery & Notfallvorsorge. In: *Private Homepage zur Information Security Competence* (2005). http://www.sidler.ws/itsicherheit/businesscontinuity/index.html. – Stand: 8. September 2008

[Smi03] Smith, David: Business continuity and crisis management. In: *Management Quarterly* (2003)

[Sne07] Snedaker, Susan: *Business Continuity and Disaster Recovery Planning for IT Professionals.* Syngress Media, 2007. – ISBN 1597491721

[Sue01] Sueddeutsche.de GmbH: *Terror in New York und Washington.* http://www.sueddeutsche.de/ausland/schwerpunkt/893/9884. Version: 2001. – Stand: 20. April 2008

[Sym08] Symantec: *IT Risk Management Report 2 – Myths and Realities: Trends through December 2007*, 2008. http://www.symantec.com/de/de/about/theme.jsp?themeid=itrmr. – Stand: 9. September 2008

[The04] The Gantry Group: The Real Returns of Meeting Sarbanes-Oxley Compliance. In: *DMReview.com* (2004), Dezember. http://www.dmreview.com/news/1015951-1.html. – Stand: 1. April 2008

[The05] The Associated Press: Tyco CEO Kozlowski Found Guilty. In: *MSNBC.com* (2005), Juni. http://www.msnbc.msn.com/id/8261018. – Stand: 14. April 2008

[The06] Theisinger, Felix: Corporate Governance und Procurement. In: *Detecon Consulting Publikationen* (2006), März. http://www.detecon.com/ch/publikationen/studien/studien.html?unique_id=2136. – Stand: 1. April 2008

[U.S02] U.S. Securities and Exchange Commission: *Sarbanes-Oxley Act*, 2002. http://www.sec.gov/about/laws/soa2002.pdf. – Stand: 1. April 2008

[Var05] Varley, Barry: Creating effective business continuity plans. In: *Continuity Central* (2005). http://www.continuitycentral.com/feature0258.htm. – Stand: 12. Mai 2008

[Wag08] Wagner, Wilhelm: *11. März 2004: Terror in Madrid.* http://www.saz-aktuell.com/magdetail~key~636.htm. Version: 2008. – Stand: 20. April 2008

[Wei03] Weiss, Todd: Peregrine Sued by SEC for Fraudulent Financial Reporting. In: *Computerworld.com* (2003), Juli. http://www.computerworld.com/softwaretopics/software/story/0,10801,82674,00.html. – Stand: 14. April 2008

[Wie07] Wiedemann, Jochen: IT-Notfallvorsorge als Komponente des IT-Risikomanagements. In: *Gestaltung von IT-Notfallvorsorge im Kontext des Risikomanagements - Teil1: Eine Analyse des Handlungsbedarfs in der betrieblichen Praxis* (2007)