MAGISTERARBEIT

Optimierung des Business Continuity Managements von Klein- und Mittelunternehmen mittels ITIL v3

zur Erlangung des akademischen Grades
Magister
(Mag. rer. soc. oec.)

ausgeführt am
Institut für Rechnergestützte Automation
Forschungsgruppe Industrial Software

der Technischen Universität Wien

unter der Anleitung von
Univ.-Prof. Dipl.-Ing. Dr. techn. Thomas Grechenig und
Assistent Dipl.-Ing. (FH) Michael Haselsteiner

durch
Thomas HEINZ
0126467 / 066 926

Ilgplatz 7/16
1020 Wien

Wien, 21. Mai 2008

Eidesstattliche Erklärung

Ich erkläre an Eides statt, daß ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfaßt, andere als die angegebenen Quellen nicht benützt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Wien, am 21. Mai 2008 ----------

Thomas HEINZ

Danksagung

Vielen Dank an meine Eltern für die Unterstützung meiner Studienzeit.

Kurzfassung

Heute wird die Informationstechnologie noch sehr oft als Mittel zum Zweck betrachtet, die strategischen Vorteile durch einen effizienten Einsatz werden oft übersehen. Im Falle eines Ausfalls der Informationstechnologie kommen die fatalen Auswirkungen zum Vorschein, welche durch unzureichende präventive Maßnahmen ausgelöst werden. Im Zentrum der vorliegenden Arbeit steht die vergleichende Untersuchung aktueller präventiver Methoden und deren Potential für die Notfallplanung betreffend die IT von Unternehmen. Dabei werden im Speziellen die Methoden Business Continuity Management und IT-Service Continuity/Disaster Recovery analysiert, wobei der Fokus auf Anforderungen von KMUs liegt. Bei der Methode Business Continuity Management steht der prozessorientierte Ansatz im Vordergrund, wobei Geschäftsabläufe in Unternehmen als sensibel eingestuft werden, welche bei einem Ausfall die schwerwiegendsten Auswirkungen haben. IT-Service Continuity beinhaltet hingegen Maßnahmen für die Sicherstellung einer Beständigkeit bezüglich IT-Services von Unternehmen. Diese Maßnahmen werden mit der Methode Disaster Recovery beschrieben. Im weiteren Verlauf der vorliegenden Arbeit werden Maßnahmen beschrieben, die eine effiziente Verbesserung der IT-Services in Unternehmen ermöglichen. Diese Maßnahmen werden mit Hilfe des aktuellen ITIL-Bandes Continual Service Improvement beschrieben. Als Fallbeispiele werden in dieser Arbeit zwei unterschiedliche Unternehmen und deren Notfallmethoden im Detail dargestellt. In diesem Abschnitt werden entsprechend den Eigenschaften der verschiedenen Unternehmen Maßnahmen vorgeschlagen, wie Notfallplanung eingeführt oder verbessert werden kann. Als Ergebnis der vorliegenden Arbeit konnte gezeigt werden, dass die Möglichkeiten des IT-Service Continuity/Disaster Recovery für kleinere Unternehmen durchaus ausreichend sind, während die Methoden des umfassenderen Business Continuity Management aus Kostengründen eher für größere Unternehmen geeignet sind. Zusätzlich konnte aufgezeigt werden, wie eine Verbesserung der IT-Services durch Methoden des Continual Service Improvements stattfinden kann.

Abstract

Today the importance of Information Technology is often rated in a wrong way. Strategical advantages through efficient use are often not considered. In the case of breakdown of the IT, the company notices the consequences of missing preventive measures. This situation, and in addition to the fact that many companies do not have any preventive measures, was the main motive for this elaboration. This elaboration includes the methods Business Continuity Management and IT-Service Continuity. Business Continuity Management is process-orientated which means, that business-processes with the highest impact in the case of breakdown of the IT are classified as sensitive. IT-Service continuity includes methods for securing continuity of IT-services of a company. These measures are discribed by the method Disaster Recovery. In the following there is a description of possibilites to improve IT-services of a company in an efficient way. These methods are described by the current issue of ITIL v3 Continual Service Improvement. In this elaboration there is a practical experience through the appliance of emergency-methods for two companies. In this chapter there are proposals for measures to establish or to improve emergency-plans. These proposals are made considering the properties of the companies. For the smaller company there is a recommendation for IT-Service Continuity through Disaster Recovery. For the bigger company methods of Business Continuity Management are recommended and described. For bigger companies additionally a description of possibilities to improve the IT-services through methods of Continual Service Improvement is derived.

Inhaltsverzeichnis

Danksagung....3
Kurzfassung....4
Abstract....5
Tabellenverzeichnis....9
Abbildungsverzeichnis....10
Abkürzungsverzeichnis....11
1. Einleitung....13
2. Rechenzentren....15
2.1. Definition....16
2.2. Hardware....16
2.2.1. Mainframes....16
2.2.2. Serversysteme....18
2.2.2.1. IBM System i 515 Express....20
2.2.2.2. IBM System i 520....20
2.3. Möglicher Aufbau eines Rechenzentrums am Beispiel TU Wien....21
2.3.1. Aufbau des Rechenzentrums....21
3. ITIL und moderne IT-Architekturen....24
3.1. Geschichte....25
3.2. Beschreibung Unterschiede ältere Versionen....29
3.3. Serviceorientierte Architekturen....32
3.3.1. Prozessmodellierung mit SOA....33
3.3.2. Auswirkungen von SOA auf IT-Systeme....34
3.4. Hypothese ITIL....34
4. Business Continuity Management....36
4.1.1. Geschäftsprozesse....37
4.1.2. Stabilität....37
4.1.3. Aufgaben....38
4.1.3.1. Aufgaben aus der Sichtweise des Geschäftsbetriebes....38
4.1.3.2. Aufgaben aus der Sichtweise der Software-/Systemlieferanten....39
4.2. Operationale Risiken....41
4.2.1. Äußere Faktoren....41
4.2.2. Prozesse....43
4.2.3. Systeme....43
4.2.4. Personen....44
4.2.5. Kombinierte Risiken....44
4.3. Krisenmanagement....45
4.3.1. Strategie für die Entwicklung von Krisenplänen....45
4.3.2. Informationen in einer Krise....45
4.3.3. Grundlage für einen allgemein gültigen Plan für das Krisenmanagement....47
4.3.4. Überwachung der Krisenbewältigung....49
4.3.5. Kriterien für gute Krisenbewältigungsdokumente....52
4.4. Phasenmodell....53
4.4.1. Untersuchung und Analyse....53
4.4.2. Lösungsarchitektur....56
4.4.3. Implementierung....57
4.4.4. Test und Freigabe....57
4.4.5. Wartung und Überwachung....57
4.5. Continuity-Management Tools....58
4.5.1. CAPT....58
4.5.2. CM....59

4.5.3. RISK....59
4.5.4. XENCOS....60
4.6. Aktuelle Studie....62
5. IT Service Continuity/Disaster Recovery....63
5.1. Definition....63
5.2. Ablauf....64
5.2.1. Vorfall-Enddeckung und Meldung über den Vorfall....64
5.2.2. Bewertung des Vorfalls....65
5.2.3. Eingrenzung des Vorfalls....65
5.2.4. Auslöschung/Bereinigung des Vorfalls....66
5.2.5. Wiederherstellung des Systems....66
5.2.6. Nachfolgeaktionen des Vorfalls (follow up)....70
5.3. CSIRT´s....70
5.4. Notfallplan....70
5.4.1. Bewusstseinsbildung im Unternehmen....71
5.4.2. Vorbereitende Phase....71
5.4.3. Zusammenstellung von wichtigen Daten....73
5.4.4. Analyse des Risikos....76
5.5. Übungen für den Notfall....77
5.6. Verteilung von Kompetenzen....79
5.7. Netzwerk-Architektur....80
5.7.1. Campus Netzwerk....81
5.7.2. Metropolitan Area Network....82
6. Effektives IT-Service Continuity durch Continual Service Improvement....83
6.1. Definition....83
6.2. Verbesserung von Services durch CSI....85
6.2.1. 7-Step Improvement Prozess....86
6.2.2. Service Report....87
6.2.3. Service Messung....88
6.2.4. Return on Investment von CSI....92
6.2.5. Festlegung eines ROI für CSI....92
6.2.5. Messung von erreichten Vorteilen....93
6.3. Beschreibung von sensiblen Prozessen....93
6.3.1. Beispiele für sensible Geschäftsprozesse....94
6.3.2. Verbesserungspotenzial von Prozessen....95
6.3.3. Key Performance Indikatoren....96
6.3.4. Umdenkungsprozess festlegen....97
6.3.5. Zertifizierung BS 15000/ISO 20000....98
7. Konkrete Anwendungen....100
7.1. Kleinunternehmen....104
7.1.1. Maßnahmen Disaster Recovery....104
7.1.1.1. Ablauf bestimmen im Notfall....104
7.1.1.2. Zusammenstellung eines Notfallteams....105
7.1.1.3. Erstellung eines Notfallplans....106
7.1.1.4. Einplanen und Bestimmung von Übungen für den Notfall....106
7.1.1.5. Bestimmung der Kompetenzen....107
7.1.1.6. Wahl eines Disaster-Recovery-Tools....107
7.2. Unternehmen mittlerer Größe....107
7.2.1. Maßnahmen Business Continuity Management....109
7.2.1.1. Festlegung des gewünschten Stabilitätsgrades....109
7.2.1.2. Bestimmung der Aufgaben....109
7.2.1.3. Bestimmung der operationalen Risiken....109

7.2.1.4. Bestimmung der Maßnahmen für ein Krisenmanagement....110
7.2.1.5. Einführung des Phasenmodells....110
7.2.1.6. Wahl eines Business-Continuity-Management-Tools....110
7.2.2. Verbesserungsmöglichkeiten durch ITIL v3 CSI....110
7.2.2.1. 7-Step Improvement Prozess....111
7.2.2.2. Service Report....112
7.2.2.3. Return of Investment von CSI....114
7.2.2.4. Festlegung eines ROI für CSI....114
7.2.2.5. Messung von erreichten Vorteilen....114
7.2.2.6. Evaluierung durch Key-Performance-Indikatoren....115
7.2.2.7. Zertifizierung nach BS 150000/ISO 20000....115
8. Zusammenfassung....115
9. Quellenverzeichnis....117

Tabellenverzeichnis

Tabelle	Name	Seite
1	Vergleich Eigenschaften Systeme Serie i IBM	21
2	Erklärung Begriffe Netzwerk TU Wien	22
3	Aufgaben der Teilgebiete von Service Transition	28
4	Werke ITIL v3	29
5	Aufgaben der Werke ITIL v2	31
6	Unterschiede verschiedene Versionen ITIL	32
7	Aufaben Phasen Prozessgestaltung	34
8	Auswirkungen von äußeren Faktoren	43
9	Wahrscheinlichkeiten Bedrohungen/Vorfälle	55
10	Eigenschaften der einzelnen Phasen Phasenmodell	58
11	Eigenschaften/Nutzen Tools Business Continuity	62
12	Beschreibung der Phasen Disaster-Recovery-Prozess	70
13	Phasen Erstellung Notfallplan	77
14	Häufigkeit und Maßnahmen von Notfalltests	79
15	Methoden für den sicheren Umgang mit Daten	80
16	Aufgaben Management im Katastrophenfall	84
17	Schlüsselaktivitäten und Schlüsselrollen CSI	86
18	Kategorien der Messung Unternehmens-Performance	90
19	Grundprinzipien der Verbesserung von Geschäftsprozessen	96
20	Durchführung Notfalltests Unternehmen	107
21	Ergebnisse Befragung mittelgroßes Unternehmen	108
22	Kategorien Messung Unternehmens-Performance	113

Abbildungsverzeichnis

Abbildung	Name	Seite
1	Mainframe	18
2	Ebenen Rechenzentrum TU Wien	22
3	Einbindung Netzwerk TU Wien	23
4	ITIL V3 Core Framework	26
5	Phasen Prozessgestaltung	33
6	Entwicklungsprozess von Software	40
7	Kommunikationsplan	46
8	Verbindungen Kommunikationsteam	48
9	Checkliste Krise	51
10	Phasenmodell	53
11	Funktionsweise XENCOS	60
12	Phasen Disaster-Recovery-Prozess	64
13	Checkliste für den Schadensfall	69
14	Optimales Kosten-/Nutzenverhältnis	77
15	Campus Netzwerk	81
16	Metropolitan Area Network	82
17	Zusammenspiel zwischen Auswirkungen und Gegenmaßnahmen	84
18	7-Step Improvement Prozess	86
19	Prozess der Service-Messung	90
20	Anteile Ausfallgründe von IT-Systemen	98
21	ISO 20000 Service Management Prozess	100
22	Befragung/Checkliste Unternehmen	101
23	Entscheidung Methode Notfallplanung	102
24	Zusammenstellung Notfallteam	105

Abkürzungsverzeichnis

ASL	Application Services Library
ATM	Asynchronous Transfer Mode
BC	Business Continuity
BCM	Business Continuity Management
BCP	Business Continuity Plan
BNC	Bayonet Neill Concelman, BNC-Steckverbinder
BPEL	Business Process Engineering Language
BS	British Standards
CCTA	Central Computer and Telecommunications Agency
CFIA	Component Failure Impact Analysis
CM	Continuity Management
CMDB	Change Management Database
COBIT	Control Objectives for Information and related Technology
CPU	Central Processing Unit
CRAMM	CCTA Risk Analysis and Management Method
CSI	Continual Service Improvement
CSIP	Continuous Service Improvement Programme
DSL	Definitive Software Library
EDV	Elektronische Datenverarbeitung
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
GITMM	Government Information Technology Infrastructure Management Methodoloy
HP	Hewlett-Packard
IKT	Informations- und Kommunikationstechnologie
ISD	Instructional Systems Design
ISO	International Organization for Standardization
ISPL	Information Services Procurement Library
ITIL	IT Infrastructure Library
J2EE	Java Platform, Enterprise Edition
KMU	Klein- und Mittelunternehmen
KPI	Key Performance Indicator
LAN	Local Area Network
LUW	Logical Unit of Work
MAN	Metropolitan Area Network
NAS	Network Attached Storage
OGC	Office of Government Commerce
OLA	Operational Level Agreement
PR	Public Relations
ROI	Return of Investment

SAN	Storage Area Network
SLA	Service Level Agreement
SOA	Serviceorientierte Architektur
SOAP	Simple Object Access Protocol
TB	Terrabyte
TSM	Tivoli Storage Mangagement
USB	Universal Serial Bus
WAN	Wide Area Network
WDSL	Web Services Description Language
WFMS	Workflow Management-Systeme

1. Einleitung

Diese Ausarbeitung geht von der Problemstellung aus, dass die Informationstechnologie in vielen Unternehmen eine zentrale Rolle spielt, jedoch fehlen oft Maßnahmen um diese Technologie auch entsprechend zu schützen. Der nachfolgende Abschnitt Problemstellung beschreibt die detaillierte Ausgangslage. Die Zielsetzung dieser Arbeit ist es, unterschiedliche aktuelle Methoden der Notfallplanung miteinander zu vergleichen und zu erläutern, um Notfallplanung in einem Unternehmen einzuführen beziehungsweise zu verbessern. Im weiteren Verlauf wird auch beschrieben, wie Prozesse mit ITIL verbessert werden können. Durch konkrete Anwendungen und Beispielen wird der Praxisbezug hergestellt. In diesem Kapitel erfolgt auch die Erklärung des Aufbaus der Arbeit.

1.1. Problemstellung

In jedem Unternehmen wird sie exzessiv eingesetzt – behandelt wird sie jedoch sehr oft wie ein Stiefkind: die Informationstechnologie (IT). Kein Unternehmen kann mehr darauf verzichten, ohne IT würde ein Unternehmen nicht wettbewerbsfähig sein. Die Großzahl der Kommunikation wird über IT abgewickelt, wichtige Informationen werden eingeholt oder sogar die Produkte beziehungsweise Dienstleistungen werden direkt mit der IT vertrieben. Nun stellt sich die Frage, warum ein so wichtiger Bereich eines Betriebes oft so wenig Beachtung findet. Jene Abteilungen, welche direkt dem Absatz/Vertrieb dienen, haben Vorrang beziehungsweise erhalten den Großteil der vorhandenen Ressourcen. Was passiert aber, wenn die IT auf einmal nicht mehr funktioniert – wenn zum Beispiel der Absatz über das Internet für längere Zeit nicht mehr möglich ist. Oder was passiert, wenn Kunden keinen Kontakt mehr zur Service-Hotline des Unternehmens aufnehmen können? Mögliche Resultate sind Umsatzeinbrüche, verärgerte beziehungsweise zukünftig ehemalige Kunden, großer Imageverlust für das Unternehmen und ein Infragestellen der Kompetenz des Unternehmens. Der „worst-case“ für ein Unternehmen ist das komplette Beenden der Geschäftstätigkeit – in Folge eines Ausfalls der IT.

Aufgrund dieser Tatsachen muss sich jedes Unternehmen die Frage stellen, wie man am besten auf unvorhersehbare Ereignisse reagieren kann beziehungsweise diese auf ein Minimum beschränken kann. Solche Ereignisse gibt es in einer großen Anzahl, mögliche Beispiele sind Brände, Überschwemmungen, wie natürlich auch kleinere technische Gebrechen wie Festplattenausfälle am Server oder ähnliche Vorfälle. Auf diese Ereignisse erst im Schadensfall zu reagieren – im Gegensatz dazu solche Ereignisse einzuplanen beziehungsweise überhaupt zu verhindern – bedeutet einen großen Verlust für das Unternehmen. Mit Business Continuity Management ist es möglich, die Auswirkungen von bestimmten Ereignissen einzuschätzen und Personen/Systeme auf solche Szenarien vorzubereiten. Mit IT-Service-Continuity, ein weiteres behandeltes Thema dieser Arbeit, ist es möglich, die angebotenen IT-Services eines Unternehmens auf effiziente Art und Weise zu schützen und im weiteren Verlauf kontinuierlich zu verbessern. Dieser Verbesserungen werden mit dem ITIL-Werk, insbesondere der Band Continual Service Improvement, angestrebt. In dieser Arbeit wird außerdem versucht die Frage zu beantworten, welche

Möglichkeit man mit ITIL hat, wenn man keinen bzw. geringen Einfluss auf ein Service hat. Ein Beispiel für diese Fragestellung wäre die Supply-Chain eines Autoherstellers. Gibt es einen Schadensfall, so wird natürlich der Autohersteller zur Verantwortung gezogen. Dieser Hersteller ist jedoch auf eine große Anzahl von Lieferanten, Vertragspartnern etc. angewiesen und es ist für den Hersteller sehr schwierig herauszufinden, wer tatsächlich für den Schaden verantwortlich ist.

Die Maßnahmen von Business Continuity Management und von ITIL sind Bereiche der IT-Strategie eines Unternehmens. Mit Business Continuity Management wird erreicht, dass gewisse, besonders wichtige Prozesse eines Unternehmens unter allen Umständen funktionieren. Mit den Maßnahmen von ITIL werden Methoden für die Etablierung einer IT-Service-Kontinuität vorgestellt. Darüber hinaus wird mit ITIL auch beschrieben, wie vorhandene Prozesse von Unternehmen kontinuierlich verbessert werden können.

1.2. Zielsetzung

Die wissenschaftliche Relevanz dieses Themas liegt in der Beantwortung der Frage, welche Methode eignet sich am besten für die Absicherung der eingesetzten IT eines Unternehmens. Mit dem Einsatz von ITIL v3 Continual Service Improvement wird definiert, wie eine kontinuierliche Verbesserung von sensiblen Geschäftsprozessen in Verbindung mit IT konkret aussehen kann. Es wird die Frage beantwortet, ob die Maßnahmen für die Absicherung von Geschäftsprozessen monetär als positiv bewertet werden kann. Und ob folglich die Kosten für den Einsatz von Notfallmethoden wirtschaftlich vertretbar im Vergleich zu den möglichen Auswirkungen sind. Es erfolgt also eine Aufstellung der Geschäftsprozesse mit einer Bewertung, ob der Prozess besonders gefährdet ist (Abstufung). Diese Arbeit behandelt sowohl eine serviceorientierte Betrachtung der Notfallplanung in Unternehmen, durch ITIL, als auch eine technikorientierte Betrachtung durch die Maßnahmen des Business Continuity Managements. In dieser Arbeit liegt der Fokus auf Klein- und Mittelunternehmen. Aspekte des Social Engineerings im Bereich der Notfallplanung für Unternehmen werden in dieser Ausarbeitung nicht behandelt.

1.3. Aufbau der Arbeit

Diese Arbeit ist in folgende Kapitel gegliedert: Rechenzentren, Business Continuity Management, IT-Service Continuity, Effektives IT Service Continuity durch Continual Service Improvement und zum Abschluss folgen Fallbeispiele im Kapitel Konkrete Anwendungen. Das erste Kapitel, Rechenzentren, bietet einen Überblick der aktuellen IT-Systeme von Unternehmen. In diesem Kapitel wird durch eine beispielhafte Anwendung eines Rechenzentrums die benötigten Hardware-Komponenten etc. erläutert. Der Fokus dieser Ausarbeitung liegt zwar auf Klein- und Mittelunternehmen, jedoch werden Rechenzentren auch in großen Mittelunternehmen und in Unternehmen mit einem hohen Ressourcenbedarf eingesetzt. Der Abschnitt Business Continuity Management beschreibt Maßnahmen, wie wichtige Abläufe in einem Unternehmen geschützt werden können. Diese Aufrechterhaltung von Abläufen behandelt sowohl Technik- als auch Service-Aspekte. Das Kapitel IT-Service Continuity behandelt Maßnahmen wie IT-Services, im

speziellen durch Disaster Recovery Methoden, geschützt werden können. In diesem Abschnitt und im nächsten Kapitel, Effektives IT-Service Continuity durch Continual Service Improvement, liegt der Fokus auf IT-Services. Mit Hilfe von Continual Service Improvement werden Maßnahmen identifiziert und beschrieben welche helfen, die IT-Services von Unternehmen sicher gegen unvorhersehbare Ereignisse zu etablieren und darüber hinaus diese Services kontinuierlich zu verbessern. Das Kapitel Konkrete Anwendungen beschreibt Vorschläge, wie die Maßnahmen von Disaster Recovery in einem Kleinunternehmen angewendet werden können und wie die Maßnahmen von Business Continuity Management in einem Unternehmen mittlerer Größe eingeführt werden können. Der Abschluss dieser Arbeit bietet eine Zusammenfassung der wichtigsten Ergebnisse und einen Ausblick.

2. Rechenzentren

Die Informationstechnologie ist heute für Unternehmen ein Faktor, welcher von großer Bedeutung ist. Bei einem effizienten Einsatz kann sich ein Unternehmen einen strategischen Vorteil gegenüber Konkurrenten verschaffen, umgekehrt gilt diese „Formel“ ebenfalls. Diese Ausarbeitung beschäftigt sich mit kleinen und mittleren Unternehmen, für diese Unternehmensformen gilt dieser strategische Faktor auch. Diese Unternehmen benötigen eine hohe Rechenleistung, um den Anforderungen der Geschäftsprozesse gewachsen zu sein. In vielen Unternehmen ist es üblich, dass bestimmte Prozesse wie zum Beispiel Bestellungen über das Internet 24 Stunden am Tag und sieben Tage die Woche verfügbar sind. Die ständige Verfügbarkeit stellt besondere Anforderungen an die eingesetzten Systeme, eine besondere Stabilität etc. muss gewährleistet werden. Auch die interne Kommunikation oder Prozess-Abwicklung erfolgt über das IT-System, häufig sehr konzentriert zu bestimmten Zeiten. Diese so genannten Stoßzeiten müssen bei der Konzipierung des Systems berücksichtigt werden, jedoch muss auch auf eine ökonomische Gestaltung des Systems Rücksicht genommen werden. Welche Art von Rechenzentrum in einem Unternehmen eingesetzt wird, hängt sehr stark von der Branche und von der benötigten Kapazität ab. Dieses Kapitel beschreibt zwei sehr häufig eingesetzte Lösungen in Rechenzentren, Mainframes und Serversysteme. Die erst genannte Lösung, Mainframes, wurde schon vor längerer Zeit für Tod erklärt, jedoch weisen gegenwärtige Entwicklungen auf eine längere Lebensdauer hin. Die Begründung, warum Mainframes in dieser Arbeit mit Fokus auf Klein- und Mittelunternehmen behandelt werden ist zu sagen, dass diese Systeme auch für kleinere Unternehmen mit großen benötigten Kapazitäten eingesetzt werden. Bei den Serversystemen erfolgt eine Konzentration auf Server des Unternehmens IBM, da dieses Unternehmen eine Führungsrolle bei den Server-Lösungen besitzt. Es erfolgt dabei eine Beschreibung von zwei Lösungen der „Serie i“, einerseits einer Lösung für kleine Unternehmen und auf der anderen Seite die Beschreibung einer Lösung für mittelgroße Unternehmen. Um sich vorstellen zu können wie die Vernetzung eines Rechenzentrums aussieht, erfolgt in Abschnitt 5.3. eine Beschreibung des „TUNET“ der Technischen Universität Wien.

2.1. Definition

Dieser Abschnitt der Ausarbeitung behandelt die Definition des Begriffes Rechenzentrum. Diese Definition wird getroffen, um ein grundlegendes Verständnis für diese Art von Informationsverarbeitung von Organisationen zu ermöglichen. Ein Rechenzentrum wird auf „IT-Wissen“ folgendermaßen beschrieben: „*Ein Rechenzentrum ist ein Bereich, ein Raum, eine Einrichtung oder ein Standort einer zentralen Datenverarbeitung. Das Rechenzentrum ist ein Dienstleistungsunternehmen oder eine Abteilung eines Unternehmens in dem die Massendatenverarbeitung in Programmläufen und der Betrieb von Mainframes und anderer zentraler Systemkomponenten für netzorientierte Datenverarbeitungssysteme erfolgt. Rechenzentren stellen ihre Rechenleistung der eigenen oder fremden Firmen gegen Entgelt zur Verfügung.*“ (Quelle: [Itwi08g]). Diese Definition unterteilt zwei Arten von Rechenzentren, auf der einen Seite ein externes Dienstleistungsunternehmen und auf der anderen Seite eine unternehmensinterne Abteilung. Welche Art für ein Unternehmen eingesetzt wird, hängt von vielen Faktoren wie zum Beispiel der Größe des Unternehmens, der Branche, dem Anteil von IT-Fachkräften oder dem IT-Budget ab. Diese Ausarbeitung beschäftigt sich mit KMU´s, deswegen erfolgt hier eine Betrachtung der internen Lösung.

2.2. Hardware

Die Hardware von Unternehmen zeichnet sich dadurch aus, dass sie viele Benutzer zugleich verwalten kann, ohne an die Grenzen zu stoßen oder im schlimmsten Fall sogar auszufallen. Dabei ist zu beachten, dass vor allem zu bestimmten Zeiten die Kapazitäten des Systems ausgereizt werden. Mit diesen Spitzenbelastungen muss das System umgehen können, dabei ist aber auch zu beachten, das System so ökonomisch wie möglich zu gestalten. Ökonomisch zu gestalten bedeutet, die Spitzenbelastungen zu kennen und die Kapazität danach auszurichten. Erfolgt keine Ausrichtung, so ist das System sehr wenig ausgelastet und verbraucht unnötigerweise Ressourcen und in weiterer Folge Budget. Es gibt verschiedene Formen von Systemen, welche für den Einsatz in Unternehmen beziehungsweise in Bildungseinrichtungen konzipiert sind. Beispiele für diese Systeme sind Mainframes oder Serversysteme. Welches System in einem Unternehmen am besten eingesetzt wird, hängt von der benötigten Kapazität und von anderen Parametern ab. Die folgenden Abschnitte definieren die beiden angesprochenen Systeme Mainframes und Serversysteme.

2.2.1. Mainframes

Die Blütezeit von Mainframes ist zwar vorbei, jedoch findet diese Art von Großrechnern immer noch großen Einsatz. Eine Studie [Itse07], welche von Attachmate und Corizon in Auftrag gegeben wurde, untersuchte die Bedeutung von Mainframe-Systemen für Unternehmen. Dabei gaben mehr als die Hälfte der Befragten an, dass sie noch Mainframe-Systeme im Unternehmen einsetzen. Diese Studie zeigt auch, dass der Einsatz von Mainframe-Systemen auch in Zukunft eine Rolle spielen wird, 58 % der

Befragten gaben an, diese Systeme auch in Zukunft einsetzen zu wollen. Eine weitere Studie [Info08] im Auftrag von HP kommt zu dem Ergebnis, dass 75 Prozent der Unternehmen mit mehr als 1.000 Mitarbeitern Mainframes im Einsatz haben. Der Einsatz von Mainframes findet in großen Unternehmen und auch in Unternehmen statt, wo sehr große Kapazitäten benötigt werden. Beckmann [Beck08] geht so weit zu behaupten, dass die Zeit von Mainframes bereits nach 1990 vorbei war. Der Grund für diesen Zustand sieht er darin, dass Rechner in einem Netzwerk, und auch die schnelleren CPU´s, die meisten Geschäftsanforderungen erfüllen können. Die Unternehmen gingen auch daran, Desktop-Applikationen anzubieten welche zu den Abteilungs-Datenservern verteilt werden. Die Zeit von großen Rechnerräumen ist ebenfalls vorbei, sehr oft mieten Unternehmen nur einen kleinen Platz in einem kommerziellen Rechnungszentrum für ihr System.

Greis führt in seinem Buch ”Die IBM-Mainframe-Architektur” [Grei05] folgende Gründe an, warum Mainframes auch in Zukunft eine wichtige Rolle in Rechenzentren spielen werden:

- Die ”state-of-the-art-Technik”, welche bezüglich Robustheit, Skalierbarkeit, Sicherheit und Performance große Pluspunkte gegenüber anderen Technologien darstellt.
- Die Unterstützung von standardisierten Technologien wie J2EE zusammen mit WebSphere.
- Die Einsatzmöglichkeiten von Open-Source-Software mit Schwerpunkt auf Linux.

Die folgende Abbildung zeigt eine beispielhafte Konfiguration eines Mainframe-Systems.

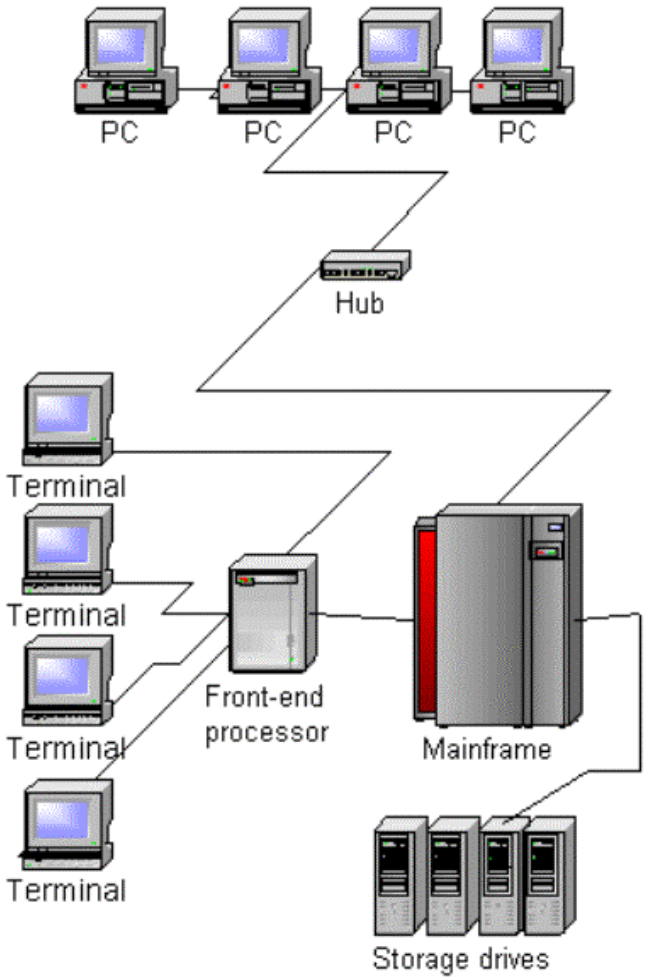

Abbildung 1, Mainframe. Quelle: [Syng08]

Abbildung 1 zeigt, wie ein Mainframe beispielsweise aufgebaut sein kann. Diese beispielhafte Konfiguration unterstützt nicht nur Desktop-Computer, es werden auch Remote-Terminals unterstützt. Diese Terminals sind auf den zentralen Mainframe angewiesen und werden nur für Input/Output benützt. Terminals haben einige Vorteile, sie sind einfach zu verwalten und auf der anderen Seite sind sie sehr preiswert. Ein Vorteil der Mainframe-Architektur ist es, dass diese Systeme zentralisiert arbeiten und deswegen oft eine einfachere Konfiguration als Server-Systeme erlauben. Die einzelnen Arbeitsplätze sind über Hub mit dem Mainframe verbunden, der Mainframe ist wiederum mit den Speichersystemen verbunden.

2.2.2. Serversysteme

Als Serversysteme werden jene Rechner in einer System-Architektur verstanden, welche anderen Rechnern (Clients) Dienste etc. zur Verfügung stellen. Diese Architektur wurde in den letzten Jahren sehr häufig eingesetzt beziehungsweise fast ausschließlich eingesetzt, dieser Trend wird jedoch als beendet betrachtet. Beckmann [Beck08] sieht den Trend zur reinen Aufgabenübertragung zu Server-Client-Architekturen als beendet. Noch vor einigen Jahren war es üblich, Emails über das POP Protokoll auf den eigenen Desktop zu holen.

Heute gehen viele Benutzer wieder zur zentralen Version über, d.h. Emails werden auf einem Server belassen, um überall darauf Zugriff zu haben. Dieser Trend hin zu zentralisierten Servern wird auch dadurch verstärkt, dass viele Unternehmen ihre Dienste online zur Verfügung stellen. Der Anwender muss sich nicht mit hohen Systemanforderungen beschäftigen, die Unternehmen stellen die benötigte Infrastruktur zur Verfügung. Dieser Trend betrifft nicht nur Privatanwender, auch bei Unternehmen ist dieser Trend sichtbar. Dabei erfolgt oft keine Installation beziehungsweise nur noch eine sehr eingeschränkte Installation auf den Rechnern, die benötigten Applikationen laufen auf einem Server eines externen Unternehmens. Die User-Authentifizierung erfolgt über einen Login oder über ähnliche Verfahren. Diese Ausarbeitung beschäftigt sich mit Unternehmen mittlerer Größe, deswegen wird in diesem Abschnitt Server-Systeme vorgestellt, welche für den Einsatz von Unternehmen in kleiner und mittlerer Größe entwickelt wurden. Dieses Server-System behandelt konkret das “System i” des Herstellers IBM. Zur Auswahl dieses Herstellers ist zu sagen, dass laut der Erhebung der Supercomputer-Rangliste 2007 [Tecc08] sechs von zehn Super-Computern von IBM hergestellt wurden und der Einsatz in kleinen und mittleren Unternehmen ebenfalls sehr häufig anzutreffen ist.

Das Unternehmen IDC [IDC08] hat eine Studie durchgeführt, welche den Nutzen für mittelgroßen Unternehmen darstellen soll. IDC, International Data Corporation, ist ein Beratungsunternehmen, welches sich auf den der Bereich der IT-Branche spezialisiert hat. Das Unternehmen hat seinen Hauptsitz in Framingham in den USA und hat international vierzig Niederlassungen. Die Studie “Der betriebswirtschaftliche Nutzen von IBM System i für mittelgroße Unternehmen” [Bozm07] wurde zwar von IBM gesponsert, jedoch ist diese Studie eine gute Quelle für die Eigenschaften der Serie System i von IBM. Diese Studie stützt sich aus Untersuchungen von System i-Anwendungen in den USA, Kanada, Asien und Europa. Die folgende Gliederung bietet einen Überblick über die wichtigsten Ergebnisse der Studie.

- System i von IBM ist bereits seit Ende der 80er Jahre, durch seine Vorgänger, im Einsatz bei mittelgroßen Unternehmen im Einsatz. Es erfolgte eine kontinuierliche Anpassung an die Geschäftsanforderungen und es erfolgt ein Einsatz von neuen Preis-Modellen. Die Performance der Systeme konnte ebenfalls kontinuierlich gesteigert werden.

- Die bestehende Interoperabilität der Systeme ist eine positive Eigenschaft, zum Beispiel ist es möglich, Daten mit x86-Servern mit Windows und Linux auszutauschen.

- Die Konsolidierung von Workloads ist möglich, d.h. es kann eine Unterstützung eines System i-Servers mit mehreren virtualisierten Workloads verschiedener Server stattfinden. Diese Kombination kann zu einer Effizienz-Steigerung von IT-Prozessen führen.

- Mit der System i-Serie erfolgt eine Unterstützung einer Vielzahl von Standard-Geschäftsprozessen, eine Eigenschaft welche für mittelgroße Unternehmen sehr wichtig ist.

- Durch eine Preisreduzierung ist die System i-Serie für mittelgroße Unternehmen erschwinglicher geworden. Das Preis-Leistungsverhältnis hat sich ebenfalls verbessert, verschiedene Kennzahlen wie ROI und TCO konnten ebenfalls verbessert werden.

- Die untersuchten Unternehmen gaben an, dass sich der Einsatz von System i-Systemen in einer Steigerung der Produktivität der IT-Mitarbeiter niedergeschlagen hat. Es erfolgte auch ein Rückgang von Systemausfällen und eine Verminderung der Wartungskosten. Der betriebswirtschaftliche Nutzen von System i-Systemen steigt kontinuierlich.

2.2.2.1. IBM System i 515 Express

Dieses System der i-Serie [IBM08b] ist für kleine Unternehmen mit maximal vierzig Benutzern konzipiert. Auf diesem System kommt ein integriertes Betriebssystem und eine integrierte Dantenbank zur Anwendung. Dieses System beinhaltet auch Tools für die Virenbekämpfung und anderen sicherheitsrelevanten Angelegenheiten. Dieses System bietet auch Backup- und Recovery-Tools an und ein Web-Server ist ebenfalls integriert.

Bei der eingesetzten Hardware kommt ein Power5+-Prozessor zum Einsatz und der Hauptspeicher kann bis zu 16 GB betragen. Dieses System kann mit bis zu acht Plattenlaufwerken ausgestattet werden mit einer Speicherkapazität von bis zu 560 GB. Es gibt bis zu sechs PCI-X-Steckplätze, welche die Installation von zwölf WAN-Verbindungen ermöglichen oder die Installation von bis zu acht LANs. Die Basisausstattung umfasst ein WAN mit zwei Verbindungen.

2.2.2.2. IBM System i 520

Dieses System der i-Serie [IBM08a] ist für Unternehmen mittlerer Größe konzipiert. Viele Unternehmen dieser Art verfügen über funktionierende Systeme, jedoch sind diese Systeme oft sehr kompliziert und umfangreich aufgebaut. Dieses System bietet eine Vereinfachung des IT-Systems an, dadurch kann eine Reduzierung der Serveranzahl und auch des benötigten Personals stattfinden. Bei diesem System werden ebenfalls Power5+-Prozessoren eingesetzt, und es verfügt über eine Multiplattform-Betriebssystemumgebung. Mögliche Betriebssysteme sind i5/OS, Linux oder Microsoft Windows Server.

Bei der Hardware kommen Power5+-Prozessoren zum Einsatz und der Hauptspeicher kann bis zu 32 GB Hauptspeicher betragen. Möglich ist der Einsatz von bis zu 278 Plattenlaufwerken, welche eine Kapazität von 39 TB aufweisen. Dieses System umfasst bis zu 90 PCI-X-Steckplätze, 192 WAN-Leitungen und bis zu 36 LANs. Die Basisausstattung umfasst ein WAN mit zwei Leitungen und es können bis zu 18 Integrated xSeries Server verbunden werden. Die folgende Tabelle vergleicht die Eigenschaften der zwei Systeme.

Merkmal	IBM System i 515 Express	IBM System i 520
Unternehmensgröße	Kleine Unternehmen	Mittlere Größe
Prozessor	Power5+	Power5+
Hauptspeicher max.	16 GB	32 GB
Anzahl Plattenlaufwerke max.	8	278
Kapazität Plattenlaufwerke	560 GB	39 TB
PCI-X-Steckplätze	6	90
WAN-Verbindungen	12	192
LAN-Verbindungen	8	36

Tabelle 1, Vergleich Eigenschaften Systeme Serie i IBM

2.3. Möglicher Aufbau eines Rechenzentrums am Beispiel TU Wien

Rechenzentren sind sehr komplex aufgebaut und schwierig zu verstehen. Dieses Kapitel bietet deshalb ein Beispiel, wie der konkrete Aufbau eines Rechenzentrums aussehen kann. Dieses Beispiel beschreibt die Struktur des Rechenzentrums der Technischen Universität Wien. Dieses Rechenzentrum betreut ungefähr 3.500 Mitarbeiter und ungefähr 19.000 Studenten [Tuwi08]. Die Kapazität ist für die Zielgruppe dieser Arbeit, Klein- und Mittelunternehmen, sehr groß, jedoch kann ein Einsatz bei großen Mittelunternehmen stattfinden.

2.3.1. Aufbau des Rechenzentrums

Das Netz der TU Wien ist hierarchisch konzipiert, d.h. es gibt drei Ebenen. Die höchste Ebene stellt dabei die Verbindung der einzelnen Gebäude dar. Diese Gebäude befinden sich geographisch gesehen sehr konzentriert nebeneinander. Auch weiter entfernte Gebäude werden auf dieser höchsten Ebene miteinander verbunden. In einem Gebäude werden ein oder mehrere Switches verwendet, teilweise gemeinsam mit Routern, für die Verbindung zu den anderen Gebäuden. Die Gebäude sind über das ATM-Backbone entweder mit Ethernet/Fast Ethernet-Verbindungen oder mit Standleitungen der Post verbunden. Innerhalb der Gebäude erfolgt die Verbindung via Gebäudeswitch durch Ethernet/Fast Ethernet/Gigabit Ethernet oder ATM durch Glasfaser oder durch Ethernet-Thickwire. Diese Verbindung stellt die zweite Hierarchie-Ebene dar. Auf der dritten Ebene erfolgt die direkte Anbindung der Benutzer und der Institute. Ausgehend von der zweiten Stufe werden Switches oder Repeater beziehungsweise Hubs angeschlossen. Die Arbeitsplätze werden mit Twisted Pair oder Ehternet-Thinwire erreicht und verbunden. Der Anschlusspunkt an das Netz erfolgt bei den Arbeitsplätzen durch RJ45-Doppeldosen für Twisted Pair oder durch BNC-Steckdosen/Automatik-Dosen für Ethernet-Thinwire mittels Glasfaseranschlüssen. Die folgende Tabelle beschreibt wichtige Komponenten des Rechenzentrums, um ein Verständnis für dieses komplexes Gebilde zu ermöglichen.

Komponente	Definition

Switch	Arbeiten auf der Schicht zwei des OSI-Modells, verteilen Datenpakete intelligent an Ports, welche mit Empfänger verbunden sind [PlWe07]
Router	Für Verkabelung mehrerer Netze zuständig, Arbeiten auf Schicht drei des OSI-Modells, Leiten Pakete entsprechend Zielinformationen weiter [PlWe07]
Backbone	Wird eingesetzt bei mehreren gleichen oder unterschiedlichen Netzwerkstrukturen, Dient als Infrastruktur für den Informationsaustausch zwischen Netzen und Systemen [Itwi08b]
ATM (Asynchronous Transfer Mode)	Ermöglicht durch Zeittransparenz und Skalierbarkeit Realisation von verschiedenen Übertragungsgeschwindigkeiten, Diensten mit verschiedenen Dienstgütern etc. [Itwi08c]
Ethernet	Lokales Netz, welches am häufigsten eingesetzt wird. Spezifikation eines Basisband-LAN´s, welches in den 70er Jahren entwickelt wurde und seitdem kontinuierlich weiterentwickelt wurde. [Itwi08h]
Thickwire	Verkabelungsart im Ethernet
Thinwire	Verkabelungsart im Ethernet
RJ45	Stecker welcher für Datenübertragung in Netzwerken entwickelt wurde, höchste Verbreitung von Datensteckern [Itwi08d]
BNC	Bajonett-Verschluss zum Verbinden von zwei Koaxialkabeln, hohe Übertragungsfrequenzen möglich [Itwi08e]
Repeater	Ursprüngliche Entwicklung für Verstärkung Signalstärke bei langen Kabelwegen, Arbeiten auf Schicht eins des OSI-Modells, sind für darüber liegende Ebenen nicht sichtbar [PlWe07]
Twisted Pair	Symmetrisches Kupferkabel, welches aus zwei Adern besteht, welche gegeneinander verdrillt sind. [Itwi08f]

Tabelle 2, Erklärung Begriffe Netzwerk TU Wien

Die folgende Abbildung zeigt die verschiedenen Ebenen des Rechenzentrums der TU Wien.

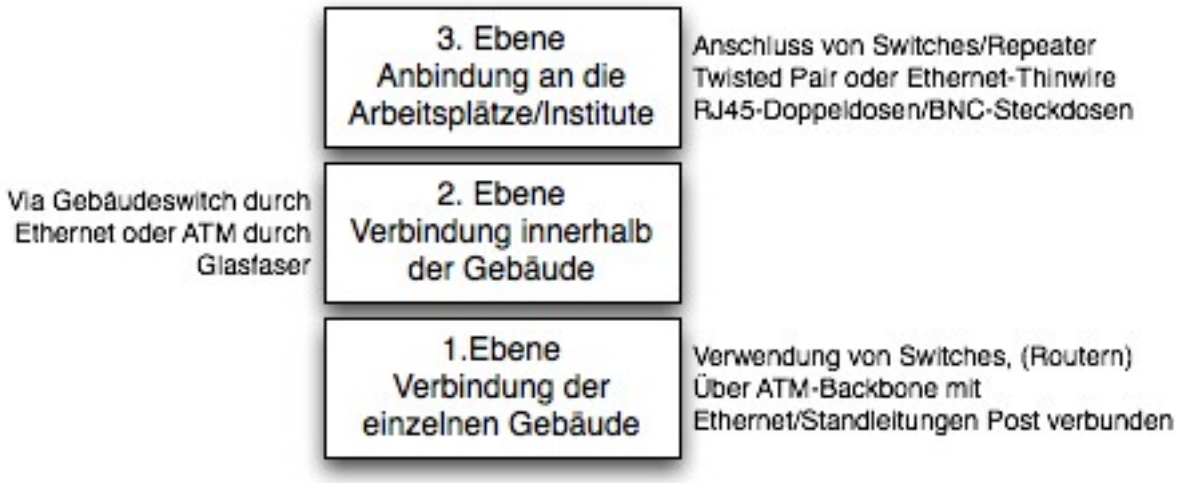

Abbildung 2 Ebenen Rechenzentrum TU Wien.

Abbildung 2 zeigt die Ebenen des Netzwerkes der Technischen Universität Wien. Die erste Ebene stellt die Verbindung zwischen den einzelnen Gebäuden dar, durch die geographische Verstreuung der Gebäude ist diese Ebene notwendig. Für diese Verbindung werden Switches und Router verwendet, welche die verschiedenen Einheiten im Netzwerk identifizieren und in weiterer Folge adressieren. Dieses Netzwerk ist mit einem ATM-Backbone mit Ethernet und Standleitungen mit der Post verbunden, d.h. hier erfolgt die Einbindung in ein übergeordnetes Hochleistungs-Netzwerk. Die nächste Ebene regelt die Verbindung innerhalb der einzelnen Gebäude. Die Verbindung innerhalb der Gebäude wird durch Glasfaser-Leitungen ermöglicht, der Datentransfer wird durch ein Gebäude-Switch durch Ethernet oder durch ATM ermöglicht. Die höchste Ebene regelt die Anbindung an die Arbeitsplätze für die Studenten oder das Personal und auch die Anbindung an die verschiedenen Institute. Diese Anschlüsse werden durch Switches oder Router ermöglicht. Die Verkabelung erfolgt dabei über Twisted Pair oder durch Ethernet-Thinwire. Der Anschluss von Kabeln wird entweder durch RJ45-Doppeldosen oder durch BNC-Steckdosen realisiert. Dieses Netzwerk betreut ungefähr 22.500 Personen. Das Netzwerk der TU Wien ist kein abgeschlossenes System sondern es ist mit anderen Netzwerken verbunden. Um sich diese Verbindung beziehungsweise Einbindung des Netzwerkes der TU Wien vorstellen zu können, zeigt die folgende Abbildung die verschiedenen Verbindungen des TUNET.

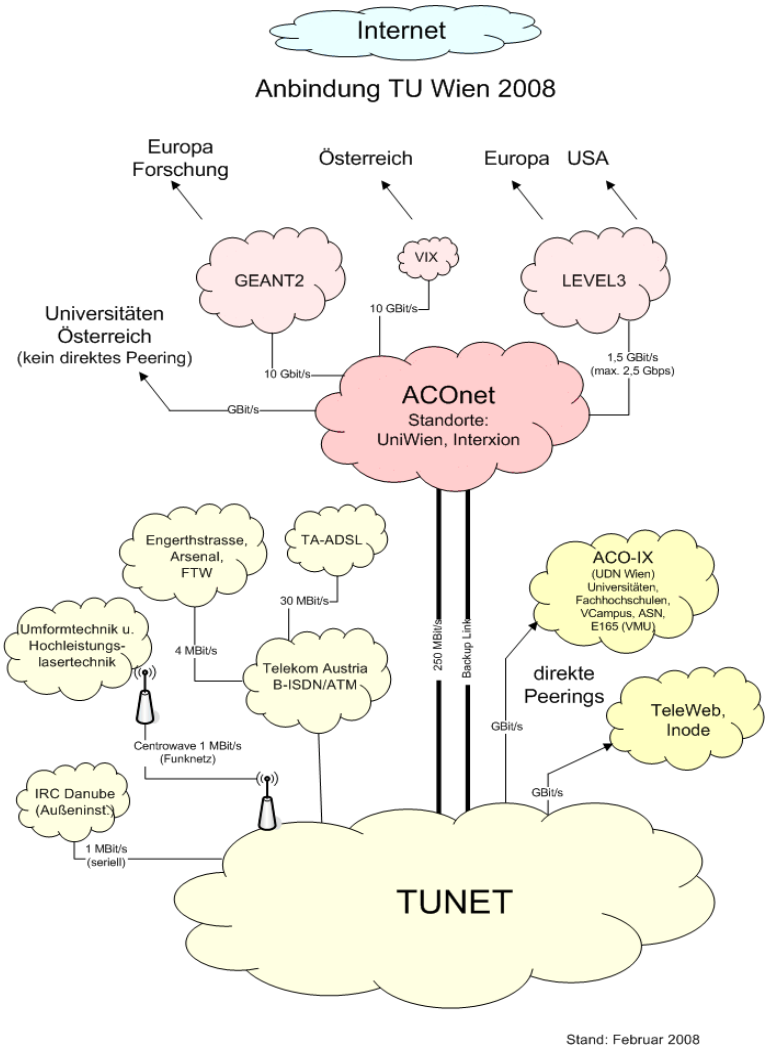

Abbildung 3, Einbindung Netzwerk TU Wien. Quelle: [ZIDT08]

Das Netzwerk der TU Wien umfasst ungefähr 10.500 angeschlossene System, 18 Backbone-Router, ungefähr 810 Repeater/Bridges und Switches, ungefähr 110 Institutsfirewalls und die Länge der Glasfaserkabeln zwischen den Gebäuden beträgt ca. 17 Kilometer. Abbildung 16 zeigt, wie das Netzwerk der TU Wien mit anderen Einrichtungen beziehungsweise mit Providern verbunden ist. Die wichtigste Einbindung erfolgt über ACOnet, welches von der Universität Wien in Kooperation mit anderen Universitäten betrieben wird [Acon08]. ACOnet ist ein leistungsfähiger Internet-Backbone, welcher durch eine internationale Anbindung und durch Peering-Vereinbarungen mit Vienna Internet eXchange einen hohen Datendurchsatz ermöglicht. Teilnehmer an diesem Netzwerk sind neben anderen Universitäten auch zum Beispiel Krankenanstalten, das Bundesrechenzentrum oder die verschiedenen österreichischen Magistrate. Die Vorteile der Anbindung an ACOnet sind ein nahezu unbegrenztere Verkehr von Datenmengen oder auch eine gemeinsame Nutzung einer Backup-Infrastruktur ist in Zukunft möglich. Dieses ACOnet ist wiederum in weitere internationale Netzwerke integriert beziehungsweise gibt es Partnerschaften auf internationaler Basis. Ein Beispiel für diese Zusammenarbeit ist GÉANT2 [Géan08]. GÉANT2 ist ein Wissenschafts- und Forschungsnetz auf europäischer Ebene. Dieses Netz verbindet 34 Länder und umfasst dreißig europäische Wissenschafts-Netzwerke, eines dieser Netzwerke ist ACOnet.

3. ITIL und moderne IT-Architekturen

Es gibt sehr viele Publikationen, welche sich mit der IT-Infrastruktur bzw. der Umsetzung von IT-Services beschäftigen. Diese Publikationen werden oft von kleinen Forschungsgruppen oder Instituten entwickelt, die Qualität der beschriebenen Maßnahmen ist sehr unterschiedlich. Es gibt hervorragende Beispiele für eine gute Umsetzung, leider gibt es im Gegensatz dazu auch „schwarze Schafe“ mit sehr fragwürdigen Empfehlungen. Ein IT-Manager beziehungsweise ein IT-Verantwortlicher steht vor der schwierigen Aufgabe, sich aus der beschriebenen großen Anzahl von Publikationen eine effiziente Methode für den Einsatz von Informationstechnologie zu selektieren. Eine wichtige Quelle für dieses Kapitel ist das Buch „ITIL kompakt und verständlich“ von Alfred Olbrich [Olbr06].

Die Infrastructure Library (ITIL) ist eine Sammlung von Nachschlagewerken welche ermöglicht, das IT-Service Management in einer effizienten Art und Weise umzusetzen.In diesem Werk liegt der Fokus auf Services, d.h. es werden Services behandelt und keine Systeme. Aufgrund der Tatsache, dass ITIL bereits auf ein langes Bestehen zurückblicken kann, und ITIL heute als De-facto Standard gilt kann man davon ausgehen, dass diese Methode sehr gut für den Einsatz in einem Unternehmen geeignet ist. Es gibt auch einige Kritikpunkte an ITIL, jedoch überwiegen die positiven Meinungen bei weitem. ITIL ist nicht die Lösung aller (IT-)Probleme, jedoch ist es eine Sammlung von Best-Practice-Beispielen, welchen jedem IT-Manager eine große Hilfe sein kann. In diesem Kapitel geht es nicht nur um ITIL – es werden auch andere moderne IT-Architekturen vorgestellt. Insbesondere wird

die „Serviceorientierte Architektur (SOA)“ beschrieben und es erfolgen Beispiele aus der Praxis, wie eine konkrete Umsetzung aussehen kann. Diese Architektur versucht die Infrastruktur an den Geschäftsprozessen anzupassen um damit schnell an Änderungen im Geschäftsumfeld reagieren zu können.

3.1. Geschichte

Zum heutigen Zeitpunkt gibt es die ITIL-Bibliothek in der dritten Version. Die ersten Bücher der Sammlung erschienen 1989 und wurden von der britischen Regierung unter Magaret Thatcher in Auftrag gegeben. Das wichtigste Ziel dieses Auftrages war es, auf den rasanten Wachstum der Informationstechnologie zu reagieren und mit einem Nachschlagewerk die notwendigen Maßnahmen zusammenzufassen. Das Herkunftsland ist, wie auch zum heutigen Zeitpunkt, England. Die erste Ausgabe enthielt ungefähr dreißig Einzelbände, welche in weiterer Folge kontinuierlich überarbeitet und auf den neuesten Stand gebracht wurden. In der späteren Entwicklung wurden die einzelnen Bände zu „Kerntexten“ zusammengefasst, die aktuelle Ausgabe enthält dadurch nur noch fünf Bände.

Was wir heute als ITIL V1 bezeichnen, wurde bei der Veröffentlichung unter der Bezeichnung „Government Information Technology Infrastructure Management Methodology“ (GITMM) bekannt. Diese Sammlung war nicht als formale Methode betrachtet worden, sondern als Leitfaden für die Entwicklung einer IT-Strategie. Die Sammlung wurde unter der Leitung der Regierungsbehörde CCTA (Central Computer and Telecommunications Agency) entwickelt. Diese Institution geriet in den späten 80er Jahren unter Beschuss, einerseits von IT-Unternehmen und andererseits von Regierungsabteilungen. Die IT-Unternehmen wollten die zentrale Regierungsberatung übernehmen, welche unter den Aufgaben von CCTA lag. Andere Regierungsbehörden wollten von der Unterdrückung dieser Institution (CCTA) loskommen, d.h. andere Regierungsinstitutionen kämpften für eine Übernahme von zusätzlichen Verantwortlichkeiten. Diese Streitigkeiten führten zu einer Verspätung der Veröffentlichung von ITIL. Obwohl die Entwicklung bereits in den 80er Jahren stattfand, wurde ITIL nicht großartig verändert bis in die mittleren 90er Jahre. Diese Veränderung führte auch zu einer Anzahl von Standards, wie zum Beispiel dem Standard ISO 20000 – welcher später in dieser Kapitel noch näher beschrieben wird. Dieser Standard beinhaltet die IT Service Management Elemente von ITIL. ITIL wird oft verglichen mit anderen Leitfaden für einen effizienten Einsatz von IT wie COBIT (Control Objectives for Information and related Technology) oder ASL (Application Services Library) und ISPL (Information Services Procurement Library). Jede dieser Ausarbeitungen haben Vor- und Nachteile, als De-facto-Standard aktuell jedoch ITIL. Im Dezember 2005 kündigte OGC an, dass die neue Version ITIL V3 in absehbarer Zeit erhältlich sein wird. Diese aktueller Version war schließlich im Mai 2007 erhältlich. ITIL V3 besteht aus folgenden fünf Kerntexten:

- Service Strategy
- Service Design

- Service Transition
- Service Operation
- Continual Service Improvement

Die folgende Abbildung zeigt den Aufbau des ITIL V3 Core Framework.

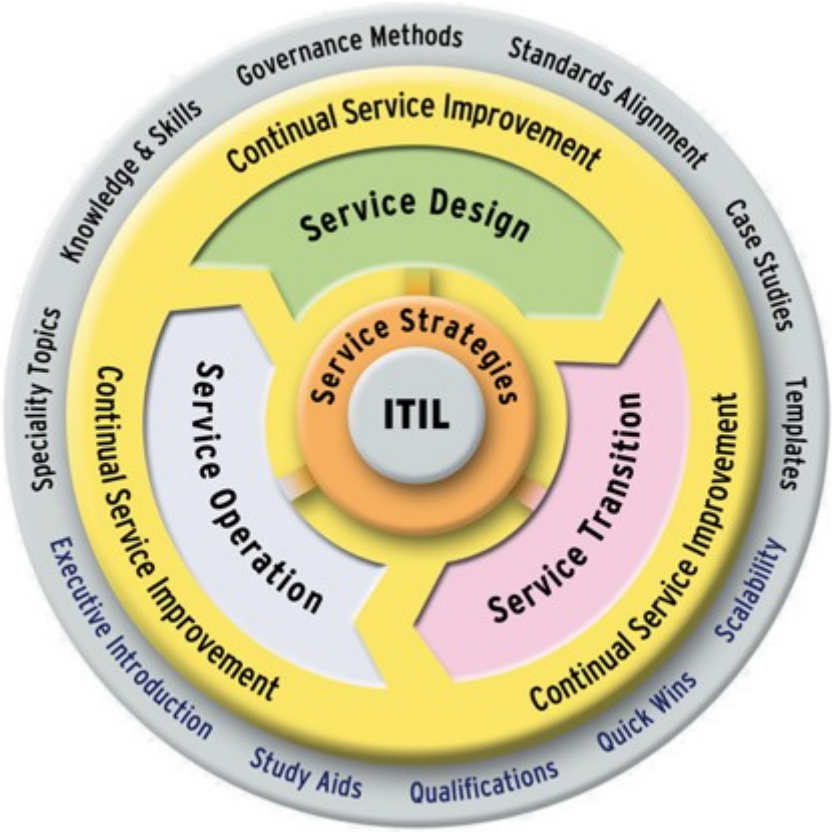

Abbildung 4, ITIL V3 Core Framework. Quelle: [Mana07]

Diese Abbildung zeigt die aktuelle Version von ITIL V3. In der Mitte steht als zentraler Ausgangspunkt das Teilgebiet Service Strategies. Die wichtigste Aufgabe für dieses Teilgebiet ist die Planung und Design von Prozessen und die Erstellung von Strategien für den Aufbau einer IT-Infrastruktur-Lösung, übergreifend im gesamten Unternehmen. Weitere wichtige Aufgaben dieses Teilgebietes ist es, die Koordination aller Aspekte von IT-Design und IT-Planung durchzuführen. Im weiteren ist dieses Teilgebiet für die Bereitstellung von einheitlichen Schnittstellen der IT-Planung zuständig. Eine Quelle für dieses Kapitel ist [Wiki07].

Außen um den Bereich Service Strategies in der Abbildung 17 befinden sich die Teilgebiete Service Design, Service Operation und Service Transition. Service Design beschäftigt sich, wie der Name schon in sich trägt, mit dem Entwurf der Prozesse. Die Prozesse, welche hier definiert werden, werden im späteren Verlauf von Service Operation umgesetzt. Dieses Teilgebiet kann als die Schnittstelle zum Kunden betrachtet werden. Es werden die zu erbringenden Leistungen der IT-Services spezifiziert – diese werden aus

den oft nicht umsetzbaren Zielen der Geschäftsführung definiert. Das heißt, es erfolgt eine Art Übersetzung von utopischen Zielen der Geschäftsführung in realistische, umsetzbare Ziele. Eine wichtige Aufgabe dieses Teilbereichs ist auch die Verwaltung der zur Verfügung stehenden finanziellen Mitteln. Es soll also ein Optimum zwischen Qualität und Kosten erzielt werden. In diesen Bereich fallen auch die vertraglichen Beziehungen von Leistungen. Diese Beziehungen werden mit den Service Level Agreements (SLA´s) festgehalten. [MaNo00] beschreibt die Funktionsweise von SLA´s folgendermaßen: Für einen Nachweis, dass SLA´s erfüllt werden, müssen Eigenschaften von Ressourcen gemessen und mit einem Service direkt verbunden werden können. Eigenschaften von Ressourcen welche nicht gemessen werden können und einem Service beziehungsweise einem Kunden genau zugewiesen werden können, können nicht der Service-Qualität des Service-Attributes in den SLA´s zugewiesen werden. Im weiteren werden auch Absicherungsverträge festgehalten, welche durch Operational Level Agreements (OLA´s) und Underpinning Contracts definiert werden. In dieses Aufgabengebiet fällt auch der so genannte Service Katalog. In diesem Katalog wird definiert, welche Leistungen überhaupt verfügbar sind. Im Gegensatz dazu beschreiben die Service Level Agreements, wie Leistungen erbracht werden müssen.

In diesen Bereich fällt auch das Kapazitätenmanagement, welches aus den Geschäftsanforderungen den Kapazitätsplan erstellt und dessen Einhaltung überwacht. Das Verfügbarkeitsmanagement, ein weiterer Bereich des Service Designs, definiert ein Verfügbarkeitsniveau entsprechend der Services. Ein weiterer Bereich ist das IT Service Continuity Management, auf dieses Teilgebiet wird in dieser Arbeit noch sehr genau eingegangen. Durch die Einschränkung auf fünf Kerntexten in der dritten Ausgabe wurde auch das Information Security Management in dieses Teilgebiet eingegliedert. Das Security Management beschäftigt sich mit der Entwicklung und Einführung eines definierten Sicherheitslevels für die gesamte Informationstechnologie. Das nächste Teilgebiet, oder auch die nächste Publikation, ist Service Transition. In diesem Teilgebiet erfolgt die Umsetzung der geplanten Maßnahmen. Dieses Teilgebiet ist wiederum in folgende Bereiche untergliedert:

- Change Management: Hier werden sämtliche Veränderungen bezüglich der Informationstechnologie geplant beziehungsweise in weiterer Folge umgesetzt. Dazu werden die notwendigen Prozesse im Falle einer notwendigen Änderung behandelt. Die verantwortliche Person ist der Change Manager, welchen die Koordination der notwendigen Schritte und die endgültige Genehmigung oder Ablehnung einer Änderung unterliegt. Es werden auch Pläne für den Notfall erstellt, welche im Bereich Emergency Change zusammengefasst werden.

- Configuration-Management: Hier werden die wichtigsten Informationen für das gesamte IT-Service Management zusammengestellt. Weiters werden die Daten fortlaufend auf ihre Aktualität überprüft.

- Release Management: Das Release Management ist die Entscheidungsstelle für die Freigabe von neuer Hard- und Software. Bei diesem Teilgebiet folgt auch die Entscheidung, wann eine freigegebene Hard- bzw. Software veröffentlicht wird.

- Deployment: Das Deployment wird dann aktiv, wenn neue Hard- bzw. Software vom Release Management freigegeben wurde. Dieser Bereich wird im typischen Fall dann aktiv, wenn Projekte für eine Änderung oder einer Einführung von Systemen bzw. Applikationen stattfinden.

Teilgebiet	Aufgaben
Change-Management	Planung sämtlicher Veränderungen der IT und Umsetzung, Verantwortliche Person ist Change-Manager, Erstellung von Notfall-Plänen
Configuration-Management	Zusammenstellung der wichtigsten Daten für IT-Service-Management, Überprüfung der Daten auf Aktualität
Release-Management	Entscheidungsstelle ob und wann eine Freigabe von neuer Hard- und Software erteilt wird
Deployment	Projekte für Änderung oder Einführung von Systemen verwalten

Tabelle 3, Aufgaben der Teilgebiete von Service Transition

In der Abbildung 4 bildet der nächste äußere Ring das Continual Service Improvement. In dieser Ausarbeitung wird noch sehr detailliert, in Kapitel 7 ITIL v3 Continual Service Improvement, auf dieses Teilgebiet eingegangen, deswegen wird hier nur ein kurzer Überblick geboten. Das Continual Service Improvement lässt sich in folgende Prozesse unterteilen:

- The 7-Step Improvement Process
- Service Reporting
- Measurement
- Business Questions for CSI
- Return of Investment for CSI

Die folgende Tabelle beschreibt die Eigenschaften der fünf Werke des aktuellen ITIL Werkes V3.

Werk	Eigenschaften/Aufgaben
Service Strategy	Planung und Design von Prozessen, Erstellung Strategie IT-Infrastruktur-Lösung, Koordination aller Aspekte von IT-Design und IT-Planung, Bereitstellung einheitlicher Schnittstellen für IT-Planung
Service Design	Entwurf der Prozesse, Schnittstelle zum Kunden, Spezifikation der zu erbringenden Leistungen,

	Übersetzung von Zielen der Geschäftsführung in realistische Ziele, Verwaltung der finanziellen Mittel, Definition SLA´s, OLA´s und Underpinning Contracts, Kapazitätenmanagement, IT Service Continuity Management, Security Management
Service Transition	Umsetzung der geplanten Maßnahmen, Change Management, Configuration Management, Release Management, Deployment
Service Operation	Definition der Maßnahmen um täglichen, reibungslosen Ablauf zu ermöglichen
Continual Service Improvement	Ständige Verbesserung der Services, The 7-Step Improvement Process, Service Reporting, Measurement, Business Questions for CSI, Return of Investment for CSI

Tabelle 4, Werke ITIL v3

3.2. Beschreibung Unterschiede ältere Versionen

Die ursprüngliche Version von ITIL umfasste ungefähr 30 Bände. Die zweite Version (ITIL V2), welche ungefähr 1995 publiziert wurde, enthielt nur noch sieben Bände. Die ITIL V2-Sammlung enthielt folgende Werke:

- Service Support: Service Support konzentriert sich auf die Benutzer von Informations- und Kommunikationsinfrastruktur. Hier soll abgesichert werden, dass die Benutzer Zugang zu den benötigten Services haben, um die Geschäftsfunktionen zu unterstützen. Der Servicedesk ist die einzige Anlaufstelle für Kunden, um Kontakt aufzunehmen und ihre Probleme zu übermitteln. Hier wird versucht, das Problem unmittelbar zu lösen. Ist diese Situation nicht möglich, so wird ein „Incident“ angelegt. „Incidents“ lösen eine Kette von Ereignissen aus. Diese Kette besteht aus folgenden Ereignissen: Incident Management, Problem Management, Change Management, Release Management und Configuration Management.

- Service Delivery: Service Delivery befasst sich primär mit den zukünftigen Services, welche Unternehmen von ihren Informations- und Kommunikationstechnologie-Providern benötigen, um eine entsprechende Unterstützung für die Geschäftskunden bieten zu können. Es fokussiert sich auf die Geschäfte wie auch auf die Kunden von Informations- und Kommunikationstechnologie-Services. Diese Disziplin besteht aus folgenden Teilgebieten: Service Level Management, Capacity Management, IT Service Continuity Management, Availability Management, Financial Managment.

- Security Management: Hier wird beschreiben, wie eine strukturierte Implementation von Informationssicherheit in der Management-Organisation stattfinden kann. ITIL Security Management basiert auf den „code of practice for information security

management“ - welcher auch unter der Norm ISO/IEC 17799 bekannt ist. Die primäre Aufgabe von Security Management ist es, Informationssicherheit zu garantieren. Diese Sicherheit muss gegen viele Risiken geschützt werden.

- Planning to Implement Service Management: Dieses Teilgebiet bietet dem IT-Manager Strategien an, wie man Geschäftsbedürfnisse am besten abdeckt und wie diese am besten vorhergesagt werden können. Die Prozesse und Abläufe in diesem Teilgebiet schlagen eine Entwicklung eines „Continuous Service Improvement Programme (CSIP)“ vor. Folgende Punkte sind in diesem Teilgebiet zu beachten: Schaffung einer Vision, Analyse der Organisation, Ziele setzen, Implementation IT service management.

- ICT Infrastructure Management: Dieses Teilgebiet gibt Vorschläge von Best-Practice-Beispielen für Bedürfnisanalyse, Planung, Design, Entwicklung, kontinuierliches Operations-Management und für die technische Unterstützung einer Informations- und Kommunikationsinfrastruktur. Die Infrastruktur-Management-Prozesse beschreiben diese Prozesse innerhalb ITIL. Diese Prozesse stehen direkt in Verbindung mit der IT-Infrastruktur und Software welche eingesetzt wird, bei der Bereitstellung von IT-Services für Kunden. Folgende Aufgaben werden in diesem Teilgebiet erfüllt: IT Design und Planung, IT Einsatz, IT Operationen und IT Technische Unterstützung.

- Applications Management: In diesem Teilgebiet werden Beispiele für best practice gegeben, um die gesamte Qualität der IT-Software Entwicklung zu gewährleisten. Im weiteren wird auch vorgeschlagen, wie man Geschäftsziele am besten in Verbindung mit dem Lebenszyklus von Software-Entwicklungsprojekten erreichen kann.

- The Business Perspective: Hier ist wieder eine Sammlung von Best-Practice-Beispielen gegeben, welche für das Verständnis und Verbesserung der IT-Service-Bereitstellung notwendig ist – als ein Teil vom gesamten Geschäftsbedürfnisses für hohe IT-Qualitätssicherheit. Diese Aspekte umfassen Business Continuity Management, Surviving Change, Transformation of business practice through radical change und Partnerships and outsourcing.

- Small-Scale Implementation: Bei diesem Teilgebiet werden Vorschläge für kleine Unternehmen beziehungsweise für Unternehmen mit einer kleinen IT-Infrastruktur gemacht. Es werden dieselben Prinzipien wie für „normalen“ Unternehmen angewendet – jedoch werden diese auf die geringere Größe des Unternehmens beziehungsweise der IT-Infrastruktur angepasst.

Werk	Eigenschaften/Aufgaben
Service Support	Sicherstellung des Zugangs der benötigten Services für

	Benutzer, Erstellung eines Servicedesks, Verwaltung von Incidents
Service Delivery	Planung zukünftiger Services, welche von IT-Providern benötigt werden, um Unterstützung für Geschäftskunden bieten zu können, Fokus auf Geschäfte und Kunden von IKT-Services
Security Management	Beschreibung wie strukturierte Einführung von Informationssicherheit in Management-Organisation stattfindet, Verwendung Standard ISO/IEC 17799
Planning to Implement	Entwicklung von Strategien für die optimale Abdeckung von Geschäftsbedürfnissen, Vorhersage Entwicklungen, Schaffung Vision, Analyse Organisation, Zielvereinbarung
ICT Infrastructure Management	Best-Practice-Beispiele für Bedürfnisanalyse, Planung, Design, Entwicklung, kontinuierliches Operations-Management und für technische Unterstützung einer IT-Infrastruktur. Erfüllung der Aufgaben IT-Design und Planung, IT-Einsatz, IT-Operationen, IT-Technische Unterstützung
Applications Management	Vorschläge für die Verbesserung der Qualität der Software-Entwicklung, Koordination Geschäftsziele und Lebenszyklus von Software-Entwicklungsprojekten
The Business Perspective	Verbesserung der IT-Service-Bereitstellung, Bereitstellung hoher IT-Qualitätssicherheit
Small-Scale	Vorschläge für kleine Unternehmen bzw. Unternehmen mit kleiner IT-Infrastruktur, Anpassung an geringe Kapazitäten

Tabelle 5, Aufgaben der Werke ITIL v2

Die folgende Tabelle bietet einen Überblick über die Unterschiede, welche zwischen den verschiedenen Versionen der ITIL-Reihe bestehen [Maxp08].

Merkmal	ITIL V1 (GITMM)	ITIL V2	ITIL V3
Erscheinungsdatum	1989	1995	2007
Anzahl Werke	ca. 30	9	5 Kerntexte
Titel Werke		Service Support, Service Delivery, Security Management, Planning to Implement, ICT Infrastructure Management, Applications Management, The Business Perspective, Small Scale	Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement
Aufbau		Betrachtung der gesamten	Gliederung

		IT-Organisation eines Unternehmens	konzentriert sich stärker auf den Aufbau von IT-Organisationen und Geschäftsprozessen
Zertifizierungsmodelle		Foundation, Practitioner, Manager Certificate in IT Service Management	Foundation Level, Intermediate Level, Advanced Level

Tabelle 6, Unterschiede verschiedene Versionen ITIL

3.3. Serviceorientierte Architekturen

Serviceorientierte Architekturen sind aktuell eine weiterer Trend in der IT – neben dem in dieser Arbeit behandelten Thema ITIL. Der Begriff Serviceorientierte Architekturen wird von Liebhart [Lieb07] folgendermaßen definiert: *„SOA wird als Topologie von Schnittstellen, Schnittstellen-Implementationen und Schnittstellen-Aufrufen gesehen, die wiederum als Ganzes eine Applikation beschreibt. SOA beschreibt das Verhältnis zwischen Services und Service Consumers, beide sind Software-Module, groß genug, um eine komplette Geschäftsfunktion abzubilden [Natis 2003]“*. Diese Definition zeigt, dass SOA sich sehr stark auf die Geschäftsfunktion beziehungsweise auf die einzelnen Geschäftsprozesse bezieht. Für das Verständnis der Geschäftsprozesse ist eine Definition dieser Prozesse notwendig, Masak [Masa07] definiert die Eigenschaften folgendermaßen: Der Geschäftsprozess besteht auf mehreren Aktivitäten, Geschäftsprozesse sind messbar, jeder Prozess enthält Steuer- und Kontrollmechanismen, jeder Geschäftsprozess hat verschiedene soziale und physische Randbedingungen, der Geschäftsprozess hat einen eindeutigen Input und Output und hat im Rahmen eines Unternehmens einen sinnvollen Zweck und der Geschäftsprozess hat eine einen zeitlichen Beginn und ein zeitliches Ende.

Liebhart beschreibt als die beiden wichtigsten Konzepte, welche SOA von anderen vergleichbaren Architekturen unterscheiden, Web-Services und die Modellierung von ablauffähigen Geschäftsprozessen. Für den effizienten Einsatz von Web-Services mittels SOA sind zwei Standards notwendig, Simple Object Access Protocol (SOAP) und Web Services Description Language (WDSL). Für die Modellierung von Geschäftsprozessen werden Workflow Management-Systeme (WFMS) eingesetzt. Diese Systeme ermöglichen die Abbildung von Arbeitsabläufen und werden schon seit vielen Jahren in Unternehmen eingesetzt. Durch den Einsatz von Business Process Engineering Language (BPEL) ist es im weiteren auch möglich, die graphischen Darstellungen in ausführbaren Code zu transferieren. Diese Sprache bietet die Möglichkeit, Prozesse zu beschreiben und graphisch darzustellen. Laut [NiLe07] sind die wichtigsten Aufgaben der BPEL folgende: BPEL ist der de facto-Standard für die Definition von Geschäftsprozessen in einer Web-Services Welt. Die Zusammensetzung von Web-Services kann als ein Fluss zwischen Web-Services-Operationen spezifiziert werden. Für diesen Zweck bietet BPEL mehrere so genannte strukturierte Aktivitäten, welche den Kontroll-Fluss zwischen Interaktions-Aktivitäten - welche andere Interaktionen mit anderen Web-Services modellieren - festlegen. BPEL unterstützt dabei nicht explizit einen Datenfluss, die Daten werden in

globalen Variablen gespeichert. Sie werden referenziert und zusammengesetzt von Interaktions-Aktivitäten und von Daten-Manipulations-Aktivitäten.

3.3.1. Prozessmodellierung mit SOA

Im Rahmen einer SOA ist es erforderlich, eine Modellierung von ausführbaren Prozessen vorzunehmen. Ein grundlegender Unterschied zu anderen Prozessmodellierungen ist, dass die Gestaltung von Abläufen nicht durch Sequenzdiagramme oder Aktivitätsprogramme erfolgen. Die Modellierung von BPEL-Prozessen kann mit Hilfe von Tools abgewickelt werden, jedoch ist es vorher erforderlich, sich über einige Grundfragen Gedanken zu machen. Einige wichtige Fragen sind zum Beispiel was mit einem Prozess überhaupt erreicht werden soll, wie ein Prozess umgesetzt werden soll oder wer konkret die verschiedenen Prozess-Schritte umsetzen soll. Die folgende Abbildung bietet einen Überblick über die verschiedenen Phasen der Prozessgestaltung.

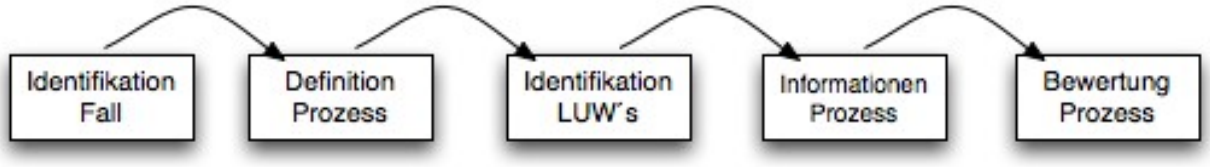

Abbildung 5, Phasen Prozessgestaltung. Quelle [Lieb07], eigene Bearbeitung

Jede der einzelnen Phasen hat verschiedene Aufgaben, die folgende Gliederung zeigt die Aufgaben der verschiedenen Phasen.

- Identifikation des Falles: Ein Fall wird meistens von einem internen oder externen Kunden initiiert, der Fall hat einen Lebenszyklus mit Anfang und Ende, der Fall kann nicht unterteilt werden.

- Definition des Prozesses: Hier werden die Ziele des Prozesses so genau wie möglich definiert, es erfolgt eine Eingrenzung des Prozesses, die Abhängigkeiten werden festgelegt.

- Identifikation der LUW´s (Logical Unit of Work): Hier wird eine genaue Definition durchgeführt, d.h. eine Aufgabe wird von einer Ressource zu einer bestimmten Zeit an einem bestimmten Ort durchgeführt, die Rüstzeiten werden minimiert, die Größe der LUW´s wird entsprechend gestaltet.

- Informationen des Prozesses: Hier werden die wichtigsten Informationen des Prozesses gesammelt wie zum Beispiel der Kommunikationsablauf zwischen den verschiedenen Personen oder Abteilungen.

- Bewertung des Prozesses: Hier werden die Key Performance Indicators (KPI´s) eines Prozesses festgelegt, wie zum Beispiel die Durchlaufzeit eines Prozesses, die Qualität eines Prozesses, die Kosten und die Flexibilität eines Prozesses.

Die folgende Tabelle fasst die wichtigsten Eigenschaften der verschiedenen Phasen zusammen.

Phase	Eigenschaften/Aufgaben
Identifikation des Falles	Beginn durch Kunden, Fall hat eindeutigen Lebenszyklus
Definition des Prozesses	Definition der Ziele, Eingrenzung, Abhängigkeiten
Identifikation der LUW´s	Genaue Definition der Aufgaben der Ressourcen, Minimierung Rüstzeiten
Informationen des Prozesses	Sammlung der wichtigsten Informationen des Prozesses
Bewertung des Prozesses	Festlegung der KPI´s

Tabelle 7, Aufgaben Phasen Prozessgestaltung

3.3.2. Auswirkungen von SOA auf IT-Systeme

Dieser Abschnitt stellt sich der Fragestellung, welche Auswirkungen der Einsatz von serviceorientierten Architektur auf IT-System von Unternehmen hat. Der Einsatz von SOA hat verschiedene Auswirkungen auf die IT-Systeme, welche in Unternehmen eingesetzt werden. Es erfolgt eine Aufteilung der unternehmensweiten IT-Organisation nach technologischen Gesichtspunkten, wie zum Beispiel Web und Betrieb. Diese technologischen Einheiten sind sehr spezialisiert und es erfolgt eine sehr eingeschränkte Kommunikation zwischen den verschiedenen Einheiten. Durch den Aufbau einer SOA in einem Unternehmen gibt es folgende Auswirkungen:

- Vor Beginn des Aufbaus eines neuen Systems müssen die verschiedenen Abteilungen/Einheiten wissen, welche Services die anderen Organisationseinheiten bereits anbieten.

- Die Koordination der Bereitstellung und der Planung der Services müssen vom Projektmanagement und von der Einführungsabteilung mit dem Controlling und den zuständigen Personen der Web- und Betriebsabteilung erfolgen.

- Die einzelnen Entwicklungsteams sind dafür verantwortlich, dass die anderen Abteilungen über die angebotenen Services informiert sind.

3.4. Hypothese ITIL

Dieser Abschnitt befasst sich mit der Fragestellung, welche Möglichkeiten mit ITIL zur Verfügung stehen, wenn man keinen beziehungsweise nur einen geringen Einfluss auf ein Service hat. Ein Beispiel für diese Aufgabenstellung ist die Supply-Chain eines

Autoherstellers. Es gibt folgendes Szenario: Der Kunde hat einen technischen Schadensfall, welcher nicht vom Kunden selbst verantwortet wird. Der Autohersteller wird also zur Verantwortung gezogen. Dieser Hersteller ist jedoch nicht Hersteller jeder einzelner Komponente, sondern erhält die Komponenten von einer großen Anzahl verschiedener Lieferanten, Vertragspartnern etc. Durch dieses Beispiel ist es möglich zu erkennen wie schwierig es ist, die Verantwortung betreffend eines Schadensfall einem bestimmten Unternehmen zuzuordnen. Die Frage welche sich aus diesem Szenario ergibt ist, welche Möglichkeit hat der Autohersteller mit ITIL, um eine Zuordnung zu erreichen und somit dem Kunden eine entsprechende Service-Qualität zu bieten. Dieses Szenario wird jetzt mit den verschiedenen Werken von ITIL v3 durchgenommen, d.h. es werden die Maßnahmen beschrieben, welche zur Lösung des Ansatzes beitragen können. Am Ende dieses Abschnitts steht zusammengefasst die konkrete Empfehlung.

- Service Strategy: Der Prozess, welcher hier im Mittelpunkt liegt, ist der Incident eines Kunden, d.h. Kontaktaufnahme mit dem Unternehmen. Für die Schadensmeldung wird ein zentraler Servicedesk geschaffen, welcher alle Incidents (Anfragen/Schadensmeldungen) von Kunden annimmt. Dieser Servicedesk ist sehr wichtig für das Unternehmen, eine Kontaktaufnahme mit dem Unternehmen ist eine wichtige Reputation. Sehr erfolgreich in der Praxis ist die Schaffung von verschiedenen Desk-Leveln, der „First-Level-Support“ ist nur für die Aufnahme der Meldung und für die Koordination der Weiterleitung zuständig. Für diesen speziellen Fall ist die Schaffung einer zentralen Datenbank für die Aufnahme von Schadensfällen effektiv. Es kann aufgrund gezielter Abfragen in Erfahrung gebracht werden, ob es sich um einen bereits bekannten Fall handelt oder ob es sich um einen neuen Fall handelt. Bei einem neuen Fall erfolgt eine Aufnahme in die Datenbank mit einer Beschreibung der durchgeführten Maßnahmen etc. Für die Kooperation mit den Partnerunternehmen beziehungsweise mit den unternehmensweiten Abteilungen werden einheitliche Schnittstellen zur Verfügung gestellt, um eine Kommunikation/Kooperation der verschiedenen Services zu ermöglichen.

- Service Design: Hier erfolgt der genaue Entwurf des Prozesses. Es wird also festgelegt, wie die Mitarbeiter am Servicedesk bei einer bestimmten Anfrage zu reagieren haben. Für diese Entscheidung werden Diagramme/Checklisten erstellt, wo die verschiedenen möglichen Situationen aufgezeichnet sind. Die Schnittstelle zum Kunden ist der Servicedesk, wo qualifizierte Mitarbeiter eingesetzt werden. In unserem speziellen Fall, Schadensmeldung eines Kunden, ist die zu erbringende Leistung die rasche Reparatur des Schadens. Für den Kunden wird nur der Fakt wichtig sein, wie schnell er wieder sein Auto hat. Hier muss auch beachtet werden, dass für die Geschäftsführung eine Reparatur innerhalb von 24 Stunden wünschenswert ist. Jedoch ist diese Vorstellung nicht realistisch, durch Richtlinien wird zum Beispiel festgehalten, dass ein Schaden innerhalb von vier Werktagen spätestens behoben sein muss. In diesen Bereich fällt auch die Festlegung der SLA

´s, OLA´s und der Underpinning Contracts. Durch eine geschickte Verhandlung dieser Verträge mit Partnerfirmen, Abteilungen kann erreicht werden, dass man direkten Einfluss auf die Supply-Chain hat. Bei einer fehlerhaften Komponente eines Lieferanten wird zum Beispiel festgehalten wie lange es dauern darf, bis ein Austausch/Reparatur stattgefunden hat. Gibt es Abweichungen von den vertraglichen Vereinbarungen, so können hohe Geldstrafen oder andere Konsequenzen vereinbart werden.

- Service Transition: Hier erfolgt die konkrete Umsetzung der geplanten Maßnahmen. Es werden also Verträge abgeschlossen, ein zentraler Servicedesk installiert, Mitarbeiter des Servicedesks geschult, Checklisten/Entscheidungsbäume erstellt und eine zentrale Datenbank für die Schadensfälle erstellt.

- Service Operation: Hier erfolgt die Definition der Maßnahmen, um einen möglichst problemlosen Einsatz im Alltag zu ermöglichen. Im Falle der Schadensmeldung ist dieser problemlose Einsatz zum Beispiel wie benutzerfreundlich die Checklisten/Entscheidungsbäume für die Mitarbeiter des Servicedesk sind. Eine weiteres Beispiel ist die Art der Kommunikation mit den Partnerunternehmen, funktioniert diese Kommunikation einwandfrei oder kommt es immer wieder zu Problemen. Im nächsten Abschnitt werden die hier gefundenen Probleme verbessert beziehungsweise ausgebessert.

- Continual Service Improvement: Hier erfolgt eine ständige Verbesserung der Services. In unserem Fall können zum Beispiel Befragungen der Kunden nach einem Schadensfall durchgeführt werden. Eine weitere Möglichkeit ist die Methode „The 7-Step Improvement Process“ und Service-Reporting. Es gibt auch KPI´s, welche die Qualität von Services misst und damit Verbesserungsmöglichkeiten offenbart.

Für die Hypothese ist die vorgeschlagene Lösung: Schaffung eines zentralen Servicedesks, Qualifikation der Mitarbeiter, effiziente Verhandlung über SLA´s, Hohe Strafen für Nicht-Einhaltung von Vereinbarungen, Kontinuierliche Verbesserung des Services.

4. Business Continuity Management

Business Continuity Management wird in Unternehmen eingesetzt, um Teile der Geschäftsprozesse oder auch die gesamten Geschäftsprozesse unter allen Umständen verfügbar zu machen. Werden nur Teile der Geschäftsprozesse am höchsten, d.h. als besonders kritisch, eingestuft, so werden diese Prozesse in der Regel die sensiblen Geschäftsprozesse des Unternehmens darstellen. In den folgenden Abschnitten werden Maßnahmen beschrieben, wie Business Continuity Management in einem Unternehmen funktionieren kann, welches sich für die Einführung einer Notfallplanung hinsichtlich der IT

entschlossen hat. Die wichtigste Quelle für diesen Abschnitt ist das Buch Business Continuity von Wieczorek [Wiec02].

4.1.1. Geschäftsprozesse

In diesem Kapitel, Business Continuity Management, werden sehr oft Geschäftsprozesse genannt. Für ein Verständnis dieser Prozesse ist es notwendig, die grundlegenden Eigenschaften zu kennen. Im Buch UML 2.0 projektorientiert [Grba04] werden Geschäftsprozesse folgendermaßen definiert: „*Ein Geschäftsprozess ist eine Zusammenfassung von fachlich zusammenhängenden Geschäftsaktivitäten, die notwendig sind, um einen Geschäftsfall zu bearbeiten. Die einzelnen Geschäftsaktivitäten können organisatorisch verteilt sein, stehen aber gewöhnlich in zeitlichen und logischen Abhängigkeiten zueinander. Geschäftsaktivitäten laufen koordiniert parallel oder nacheinander ab und dienen der Erreichung eines Ziels. Sie können manuell oder IT-unterstützt ausgeführt werden. innerhalb einer betrieblichen Organisationsstruktur mit dem Zweck, ein betriebliches Ziel zu erreichen.*“ (Quelle: [Grba04])

4.1.2. Stabilität

Im Online-Wörterbuch der TU München [Leo07] wird der Begriff „continuity“ mit den deutschen Begriffen Fortbestand, Kontinuität oder auch ununterbrochener Zusammenhang übersetzt. Continuity Management versucht also, den laufenden Geschäftsbetrieb unter allen Umständen am Leben zu erhalten. Durch diese Maßnahmen wird eine Stabilität erreicht, welche sehr wichtig für ein Unternehmen ist. Viele Beispiele aus der nahen Vergangenheit haben gezeigt, dass Stabilität für viele Unternehmen ein Fremdwort war beziehungsweise noch immer ist. Auch wenn die aktuelle Zeit sehr schnelllebig ist, so haben Kunden doch zu den Unternehmen am meisten Vertrauen, welche sich über Jahre durch gute, konstante Leistungen etablieren. Unter Stabilität versteht man bei Unternehmen auch, die Fähigkeit auf unvorhersehbare Ereignisse auf entsprechende Art und Weise reagieren zu können. Diese entsprechende Art und Weise zeichnet sich dadurch aus, dass zumindest der wichtigste Geschäftsbetrieb aufrecht erhalten werden kann. Es gibt einige Möglichkeiten, pro aktiv Strategien für die Reaktion auf solche Ereignisse zu entwickeln. Die folgende Gliederung bildet Maßnahmen ab, welche sich in der Praxis als sehr erfolgreich und effizient herausgestellt haben.

- Installation von Frühwarnsystemen
- Einführung eines Gefahrenbewusstseins im Unternehmen
- Angemessene Fehlertoleranz im Unternehmen
- Flexibilität der Mitarbeiter und breiter Wissensstand der Mitarbeiter
- Ständige Verbesserung der Geschäftsprozesse
- Verbesserung durch technische Neuerungen
- Gezielte Einplanung von Pufferzeiten etc.

Die Komplexität der Systeme, welche heute in Unternehmen eingesetzt werden, führt immer öfter zu unvorhersehbaren Ereignissen beziehungsweise zu Notfällen. Eine Verkettung von unglücklichen Ereignissen kann zu Katastrophen führen – isoliert könnte ein Ereignis keinen großen Schaden anrichten. Es hat sich jedoch nicht nur die Komplexität der Systeme erhöht, sondern auch die zwischenmenschlichen Beziehungen in einem Unternehmen werden immer komplizierter. Die Aufgabenbereiche von Personen sind nicht immer eindeutig definiert oder ein Aufgabenbereich wird auf mehrere Personen aufgeteilt. Diese Situation kann zu Missverständnissen und im weiteren Sinn zur Auslösung eines unvorhersehbaren Ereignisses führen.

4.1.3. Aufgaben

Business Continuity Management bedeutet, dass eine Stabilität beziehungsweise eine Aufrechterhaltung der Geschäftstätigkeit unter allen möglichen Ereignissen erreicht werden soll. Dabei muss festgelegt werden, gegen welche Risiken sich ein Unternehmen überhaupt schützen will beziehungsweise schützen kann. Nur wenn die Risiken bekannt sind ist es möglich, Maßnahmen gegen diese Risiken zu entwickeln und einzusetzen. Ein Unternehmen verfügt nur über sehr begrenzte Ressourcen, deswegen müssen die Maßnahmen sehr effizient eingesetzt werden – eine genaue Beschreibung dieses Problems wird im Kapitel Kosten-/Nutzenanalyse folgen. Die Aufgaben des Business Continuity Management werden in den folgenden Kapiteln aus zwei verschiedenen Sichtweisen dargestellt, zum einem aus der Sichtweise des Geschäftsbetriebes und zum anderen aus der Sichtweise der Software- und Systemlieferanten. Die Interessen und Aufgaben dieser beiden Organisationseinheiten unterscheiden sich deutlich, deswegen werden diese unterschiedlichen Sichtweisen unabhängig voneinander betrachtet.

4.1.3.1. Aufgaben aus der Sichtweise des Geschäftsbetriebes

Welche Aufgaben sind Business-Continuity-Management aus der Sichtweise des Geschäftsbetriebes zuzuschreiben? Der wichtigste Aspekt umfasst die Erhaltung der Stabilität der wichtigsten Prozesse. Diese Stabilität umfasst dabei nicht nur die wichtigsten Geschäftsprozesse, sondern sie umfasst auch die Einhaltung des ethischen Grundsatzes, dass alle Personen vor Gefahren geschützt werden müssen. Dieser Aspekt ist vorrangig zu beachten, durch Gesetze werden Unternehmen zur Einhaltung verpflichtet. Der nächste wichtige Aspekt umfasst die Wiederaufnahme der Geschäftsprozesse nach einem Vorfall beziehungsweise nach einem Notfall. Diese Maßnahme umfasst dabei unter anderen die Mitarbeiter, wichtige Dokumente und die Infrastruktur des Unternehmens. Für einige Unternehmensformen gibt es zusätzliche Vorschriften für Geschäftsprozesse, welche unter allen Umständen funktionieren müssen. Die wichtigsten Aufgaben aus der Sichtweise des Geschäftsbetriebes sind folgende Aufgaben: Fähigkeit zur Krisenbewältigung, Fähigkeit zur Notfallplanung und Schaffung eines Risikobewusstseins. Die folgende Gliederung erläutert diese wichtigen Aufgaben.

- Fähigkeit zur Krisenbewältigung: Die wichtigste Eigenschaft dieser Fähigkeit ist es, dass Unternehmen agieren können, egal was passiert. Unternehmen sollen also in

der Lage sein, in effizienter Art und Weise auf unvorhersehbare Ereignisse reagieren zu können. Unvorhersehbar bedeutet hier, dass die gesamten Auswirkungen beziehungsweise die genauen Eigenschaften eines Ereignisses nie exakt im Vorhinein bestimmt werden können. Wichtig ist es hier, einen Überblick über das Ereignis zu erhalten. Durch diese Maßnahme ist es möglich, alle Personen und Ressourcen zu koordinieren und zu leiten. Ein Aspekt welcher nicht vergessen werden darf ist, dass die Maßnahmen nur dann wirksam sind in einem Notfall, wenn sie bekannt sind und durch Übungen die Einsatzfähigkeit bestimmt wurde. Zu beachten ist auch der Einsatz der Kommunikationsmittel, bei einem Vorfall kommt es häufig zu einem Ausfall der gewohnten Kommunikationsinfrastruktur.

- Fähigkeit zur Notfallplanung: Diese Fähigkeit setzt voraus, dass sich Verantwortliche von Unternehmen mit möglichen zukünftigen Risiken auseinander setzen. Erfolgt dieser Prozess der Schaffung von fiktiven Szenarien, so können Unternehmen Maßnahmen setzen, damit es zu keiner Eskalation bei einem tatsächlichen Eintritt kommt. Mögliche Reaktionen auf Notfälle können zum Beispiel sein: Fortführung des normalen Geschäftsablaufs mit verringerten Kapazitäten, Ausweichen auf andere Produktionsstätten oder Büroräume, Benachrichtigung der Kunden im Falle eines schwerwiegenden Problems, Akquierierung zusätzlichen Personals im Notfall, Umstieg auf manuelle Methoden etc. Auch bei dieser Fähigkeit sind Übungen wichtig.

- Schaffung eines Risikobewusstseins: Hier lautet der Grundsatz: Man kann nur auf mögliche zukünftige Entwicklungen reagieren, wenn man sie kennt. Die Verantwortlichen in einem Unternehmen werden sich intensiv mit den Entwicklungen auseinander setzen, jedoch sind sie auf keinen Fall in der Lage, die gesamten Entwicklungen im Auge zu behalten. Deswegen sind alle Mitarbeiter dazu zu sensibilisieren, Entwicklungen welche einer normalen Ausprägung abweichen, zu melden. Die Verantwortlichen können dann in entsprechender Form darauf reagieren. Diese Reaktion wird von der Bewertung eines Vorfalls abhängen, dazu werden die Vorfälle nach den möglichen Auswirkungen etc. priorisiert. Zusätzlich zu den Meldungen der Mitarbeiter werden auch Frühwarnsysteme installiert , welche bei einer Abweichung der Normalform Alarm schlagen.

4.1.3.2. Aufgaben aus der Sichtweise der Software-/Systemlieferanten

Lieferanten von Software beziehungsweise von Systemen haben eine unterschiedliche Sichtweise auf die Aufgaben im Bezug auf das Business Continuity Management. Hier liegt der Fokus auf die gelieferten Komponenten (und das ganze System) sowie auf die installierten Applikationen. Gibt es öfter Probleme mit Systemen einer bestimmten Firma, so wird sich dieser Zustand negativ auf den Ruf des Unternehmens auswirken. Ein negativer Ruf wird in weiterer Folge zu Umsatzeinbußen und zu einer Verminderung von

Aufträgen führen. Die folgende Abbildung zeigt einen Softwareentwicklungsprozess, bei dem wie in der Praxis bestimmte Restrisiken und Risiken bestehen.

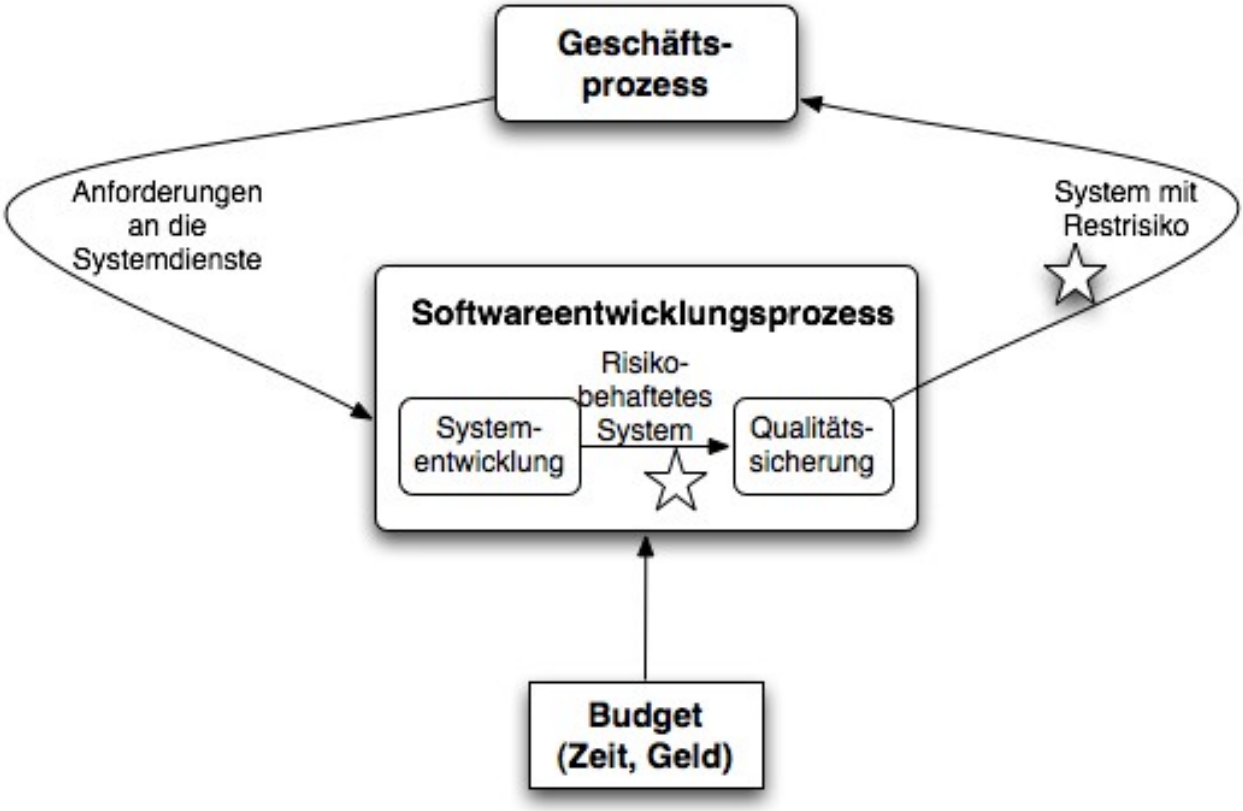

Abbildung 6, Entwicklungsprozess von Software. Quelle: [Wiec02], eigene Darstellung.

Abbildung 6 beschreibt den Ablauf einer Softwareentwicklung für ein bestimmtes Unternehmen. Dieser Ablauf ist auch für die Erstellung eines IT-Systems (bzw. eines Teils eines Systems) ident. Das externe Unternehmen erhält den Auftrag der Erstellung einer bestimmten Software/Systems, welche auf die Geschäftsprozesse des Unternehmens abgestimmt sind. Diese „Anforderungen an die Systemdienste“, linker Pfeil in der Abbildung, bilden den Auftrag für einen Softwareentwicklungsprozess. Der Stern im Bereich des Softwareentwicklungsprozesses in der Abbildung deutet an, dass dieser Vorgang mit Risiko behaftet ist. Das beauftragte Unternehmen steht unter Zeit- und Kostendruck, keine optimalen Voraussetzungen für eine qualitativ-hochwertige Auftragsabwicklung. Ist ein System (vorläufig) fertig gestellt, erfolgt der Prozess der Qualitätssicherung. Hier wird sicher gestellt, dass gewisse Qualitätskriterien eingehalten werden. Durch den Zeit- und Kostendruck wird häufig ein Produkt geliefert, welches nicht komplett ausgereift ist. Dieses Restrisiko, welches bei jeder Software- beziehungsweise Systemlösung besteht, wird durch den zweiten Pfeil bei der Abbildung auf der rechten Seite angedeutet. Am Ende des Kreislaufes erfolgt der Einsatz der Lösung mit den unternehmensspezifischen Geschäftsprozessen.

Die Stabilität von Systemen war früher einfacher zu erhalten, die Benutzer waren Experten und folglich war die Stabilität auf „normale“ Eingaben konzipiert. Heute werden IT-Systeme

von allen Personen benutzt, viele Personen haben das Talent Lücken gnadenlos auszunutzen. Weiters muss auch betrachtet werden, dass sehr viele Services heute im Internet zur Verfügung stehen. Diese Applikationen/Services bieten Angreifern viele Möglichkeiten für schadhafte Aktionen. Für diese Applikationen beziehungsweise Services gibt es eine Vielzahl von Richtlinien, welche einen möglichst sicheren Einsatz ermöglichen. Durch Updates oder Patches ist es auch möglich, auf aktuelle Bedrohungen zu reagieren.

4.2. Operationale Risiken

Die heutige Zeit ist sehr raschen Veränderungen unterworfen. Betrachtet man das Beispiel des Finanzsektors, so wird einem diese Schnelligkeit sehr schnell bewusst. Die Aktienmärkte zum Beispiel reagieren umgehend auf kleine Änderungen in der Nachfrage etc. Kommt es zu einer fehlerhaften Eingabe in ein System, möglicherweise nur durch eine Person, so kann es zu einer Kettenreaktion in einem Ausmaß kommen, welche nur sehr schwer vorstellbar ist. Ein Beispiel für eine Kettenreaktion dieser Art geschah am 15. Mai 2001 an der Londoner Börse, eine unbekannte Person hat eine falsche Eingabe getätigt und aufgrund einer Kettenreaktion kam es zu einem der größten Verluste an der Börse überhaupt. Dieses Beispiel zeigt sehr gut, wie vernetzt und schnelllebig die heutige Zeit ist. Die folgenden Kapitel werden konkret auf mögliche Risiken eingehen, welche berücksichtigt werden müssen, um ein effizientes Business Continuity Management zu betreiben.

4.2.1. Äußere Faktoren

Eine Art von operationalen Risiken sind äußere Faktoren eines Unternehmens. Zu den äußeren Faktoren eines Unternehmens werden jene Geschäftstätigkeiten gesehen, welche mit externen Geschäftspartnern oder mit der Umgebung gemacht werden. Zu diesen externen Geschäftspartnern werden Kunden, Lieferanten und andere Geschäftspartner gezählt. Auf diese externen Geschäftspartner haben Unternehmen oft nur schwer Einfluss, abgesehen von vertraglichen Vereinbarungen oder ähnlichen verpflichtenden Vereinbarungen. Diese äußeren Faktoren haben für ein Unternehmen starke Auswirkungen, bei einem just-in-time-Betrieb wird eine Unterbrechung durch einen äußeren Faktor zu einem Stillstand der Produktion führen. Die folgende Aufzählung bietet einen Überblick über wichtige äußere Faktoren, welche sich bedrohend auf die Geschäftstätigkeit eines Unternehmen auswirken können.

- Materialfluss zwischen Kunden und Lieferanten: Aktuell wird sehr oft die „just-in-time“-Methode eingesetzt. Hält sich der Lieferant nicht an die Vereinbarung, so kann die Produktion nicht stattfinden und in weiterer Folge kann keine Lieferung an den Kunden erfolgen. Eine weitere Möglichkeit für eine Bedrohung durch den Materialfluss zwischen Kunden und Lieferanten ist eine fehlerhafte oder beschädigte Lieferung durch den Lieferanten.

- Dienstleistungen und Lieferungen, welche durch externe Partnerunternehmen erbracht werden: Ein Beispiel für Dienstleistungen welche von externen Partnerunternehmen erbracht werden, ist die Versorgung mit Energie/Strom. Steht für einen längeren Zeitraum keine Energie zur Verfügung, so wird es für ein Unternehmen nahezu unmöglich sein, die normalen Geschäftstätigkeiten aufrecht zu erhalten. Die heutige Informationsgesellschaft ist angewiesen auf sehr aktuelle Daten. Nur mit diesen Informationen kann ein Unternehmen die richtigen Entscheidungen treffen. Die Lieferung von diesen wichtigen Daten erfolgt oft von externen Partnern, ein Ausfall kann ebenfalls verheerende Wirkungen haben. Ein weiteres Beispiel für die Abhängigkeit von externen Partnern kann durch die Verbindung mit Telekommunikations/Internet-Anbietern gegeben werden. Ein Ausfall in diesem Bereich wird zu massiven Verlusten führen.

- Aktivitäten durch Kriminelle mit der Absicht, dem Unternehmen Schaden zuzufügen oder an sensible Daten des Unternehmens zu gelangen: Selbst die besten und aktuellsten Gegenmaßnahmen können dieses Risiko nur minimieren, jedoch nicht ausschließen. Gelangen Kriminelle an sensible Daten des Unternehmens, so kann diese Situation, abgesehen der schlechten Publicity, eine ernsthafte Bedrohung für das Unternehmen darstellen. Vorfälle dieser Art gibt es sehr häufig, Unternehmen versuchen jedoch, diese Vorfälle zu verheimlichen beziehungsweise das Ausmaß eines Angriffs geringer anzugeben.

- Politische Situation in einer Region beziehungsweise in einem Staat: Liegt der Unternehmenssitz beziehungsweise eine Produktionsstätte eines Unternehmens in einer Region oder in einem Land wo die politische Situation als gefährlich eingestuft werden kann, so ist diese Situation als sehr bedrohend für das Unternehmen einzuschätzen. Die Produktionskosten in solchen Ländern sind oft deutlich geringer als in ein „stabilen“ Ländern, jedoch besteht das Risiko einer Eskalation der politischen Situation. Im schlimmsten Fall muss hier wiederum die Aufgabe der Geschäftstätigkeit des Unternehmens betrachtet werden. Die politische Situation eines Landes kann sich schlagartig ändern, eine sichere Vorhersage ist also für kein Land möglich. Jedoch können Schätzungen für die möglichen Gefahren eines Landes getroffen werden, zum Beispiel können EU-Länder als sehr sicher in Hinsicht auf die politische Situation gesehen werden.

- Naturkatastrophen: Naturkatastrophen können nie ausgeschlossen werden. Es gibt jedoch Gebiete, welche überdurchschnittlich gefährdet sind. Die Technik für Vorhersagen wird immer ausgefeilter, jedoch kann eine zu einhundert Prozent sichere Vorhersage nie getroffen werden. Durch Versicherungen und bauliche Absicherungen können Risiken minimiert werden, jedoch kann kein Ausschluss der Katastrophen stattfinden.

Die folgende Tabelle bietet einen Überblick über die verschiedenen äußeren Faktoren und ihren Auswirkungen. Darüber hinaus wird auch festgehalten, welche Gegenmaßnahmen gegen diese Auswirkungen eingesetzt werden können.

Äußere Faktor	Auswirkungen/Gegenmaßnahmen
Materialfluss zwischen Kunden und Lieferanten	"just-in-time-Methode", Produktion kann nicht stattfinden, keine Lieferung an den Kunden, Bedrohung Materialflusses zwischen Kunden und Lieferanten durch fehlerhafte/beschädigte Ware, Risiken durch Einsatz von externen Unternehmen
Dienstleistungen/Lieferungen durch externe Partnerunternehmen	Versorgung mit Energie/Strom, keine Verfügbarkeit von aktuellen Daten, Abhängigkeit von Telekommunikations-/Internetanbieter
Kriminelle Aktivitäten	Gefahr des Verlustes von sensiblen Daten, Planung von Gegenmaßnahmen, Verschlechterung des Rufes, ernsthafte Bedrohung des Unternehmens bei Angriff auf kritische Geschäftsprozesse
Politische Situation Staat/Region	Hohes Risiko jedoch häufig geringere Produktionskosten, Möglichkeit Eskalation der politischen Situation, Einschätzung der Bedrohung
Naturkatastrophen	Gebiete mit überdurchschnittlichem Risiko, Mögliche Vorhersagen, Einsatz von Versicherungen und bauliche Absicherungen

Tabelle 8, Auswirkungen von äußeren Faktoren

4.2.2. Prozesse

In diesen Bereich fallen Abläufe, welche ein Unternehmen abhandeln muss, um einer Geschäftstätigkeit gerecht zu werden. Diese internen Abläufe sind häufig sehr kompliziert, da sie seit mehreren Jahren nicht geändert wurden. Ein mögliche Verbesserung dieser Situation kann durch die Einführung von Standardisierungen erreicht werden. Betrachtet man den Fall von Dokumentation, so gibt es oft sehr zeit intensive Abläufe. Durch eine anerkannte und einsatzerprobte Standardisierung kann eine große Effizienzsteigerung erreicht werden. Die Kosten und der zeitliche Aufwand für eine mögliche Standardisierung dürfen aber nicht unterschätzt werden – der Aufwand wird sich bei guter Einführung aber lohnen.

4.2.3. Systeme

Bei den Systemen kann man zwischen zwei Risiken unterscheiden, zum einen das Potenzial Schaden anzurichten und zum anderen die Wahrscheinlichkeit eines Ausfalls. IT-Systeme sind in einem Unternehmen heute sehr komplex aufgebaut. Diese Komponenten haben oft eine sehr gute „stand-alone“-Qualität, in der vernetzten Version gibt es aber dann oft Probleme beziehungsweise Ausfälle. Der Grund für diese Situation ist, dass die Funktionsweise zwar im alleinigen Betrieb geprüft wurden, eine Überprüfung in der vernetzten Version aber fehlt. Diese Situation ist damit zu erklären, dass es einfach

nicht möglich ist jede Konstellation von verschiedenen Unternehmen durchzugehen und zu testen. Das Potenzial, Schaden anzurichten, hat jede Komponente eines IT-Systems in einem Unternehmen. Jedoch kann dieses Potenzial von Komponente zu Komponente abgestuft werden, d.h. es kann zum Beispiel eine Abstufung von extrem hohen Schadenspotenzial bis hin zu sehr geringen Schadenspotenzial erstellt werden. Komponenten, welche ein sehr hohes Schadenspotenzial haben, sind Teile des Systems welche in Verbindung mit dem Vertrieb/Absatz stehen. Ein Beispiel für ein Teilsystem mit eher geringen Potenzial ist eine Intranet-Applikation, welche auf firmeninterne Veranstaltungen hinweist. Ein Ausfall dieser Applikation ist sehr harmlos im Vergleich zu einem Ausfall eines Teilsystems, welche mit dem Vertrieb in Verbindung steht. Bewertet kann dieser Schaden durch den finanziellen Verlust und durch den zu erwartenden Imageverlust eines Unternehmens. Im Fall des Ausfalls einer Intranet-Applikation sind nur die Mitarbeiter eines Unternehmens betroffen und informiert. Hingegen sind bei einem Ausfall des Vertriebs die Kunden betroffen und diese Situation führt zu einem hohen finanziellen Schaden.

4.2.4. Personen

Der Risikofaktor Mensch ist nicht zu unterschätzen – Menschen machen Fehler. Es werden sehr oft falsche Entscheidungen getroffen, die Wahrscheinlichkeit dafür ist unter bestimmten Situation deutlich höher. Diese Situationen können Zeiten sein, wo ein enormer Druck auf Mitarbeitern lastet. Dieser Druck kann sowohl zeitlich bedingt sein, wie auch zum Beispiel die Auswirkungen einer Entscheidung. Weiters ist es auch immer schwieriger, durch die gegenseitigen Abhängigkeiten von anderen Mitarbeitern beziehungsweise von Systemen einen Überblick über Ursachen eines Problems zu erkennen. Die Fähigkeit Überblick zu bewahren, hängt von den Qualifikationen und der Kenntnisse einer Person ab – und sind damit von Person zu Person unterschiedlich. Auch im Bereich des Risikofaktors Personen werden heute viele Standardisierungen eingeführt. So sind zum Beispiel die Kommunikationswege genau definiert oder es ist genau definiert, wie die Meldung eines Kunden über ein Problem abzuhandeln ist. Diese Form hat nicht nur positive Seiten, negative Folgen können Langeweile, Überroutine oder ein Verlust der Flexibilität durch genaues Abhandeln der Standardisierungs-Regeln sein.

4.2.5. Kombinierte Risiken

Kombinierte Risiken treten auf, wenn mehrere der vorher genannten Risiken zusammenspielen. Aufgrund der Komplexität einerseits von Systemen, andererseits von Befugnissen beziehungsweise Zuständigkeiten von Personen, treten solche kombinierte Risiken heute sehr häufig auf. Sehr oft wird auch die Wirkung des Zufalls unterschätzt, viele bekannte Katastrophen sind aufgetreten, weil zufällig mehrere Faktoren zusammengewirkt haben, welche in isolierter Form keine große Wirkung gezeigt hätten. Beispiele für Kombinierte Risiken stellen jene Katastrophen oder Vorfälle dar, welche durch Fehler in der Kombination Mensch und Maschine entstanden sind. Sehr häufig verlassen sich Personen auf Meldungen von Maschinen, auch wenn diese bei näherer Betrachtung nicht möglich sein können. Steht die Person außerdem unter hohem

Zeitdruck oder arbeitet schon lange an einem Arbeitsplatz (Gewohnheit ist eine häufige Fehlerquelle), so treten oft unerwünschte Vorfälle resultierend aus kombinierten Risiken auf. Diese Risiken können durch immer wieder kehrende Überprüfungen und durch standardisierte Abläufe, wie zum Beispiel Einhaltung einer Abarbeitungsreihenfolge nach genauen Kriterien, sehr stark vermindert werden. Ein weiteres Beispiel für ein Kombiniertes Risiko tritt dann auf, wenn an einem Projekt viele unterschiedliche Unternehmen mit unterschiedlichen Kulturen arbeiten. Auch wenn die Arbeit am Projekt von jedem Unternehmen sehr gut erfüllt wird ist es möglich, dass die Kombination ein Risiko darstellt. Jedes Unternehmen erfüllt seine Aufgaben isoliert, d.h. eine Kommunikation findet nicht oder nicht ausreichend statt.

4.3. Krisenmanagement

Für Unternehmen ist es notwendig zu wissen, wie man mit speziellen Situationen umgehen kann. Im Bereich des Business Continuity Management sind diese angesprochenen Situationen Krisen. Laut Duden wird eine Krise folgendermaßen definiert: „*Krise: griech. Krísis = Entscheidung, entscheidende Wendung, zu krínein. Schwierige Lage, Situation, Zeit [die den Höhe- u. Wendepunkt einer gefährlichen Entwicklung darstellt]; Schwierigkeit, kritische Situation; Zeit der Gefährdung, des Gefährdetseins: eine finanzielle K. steht bevor, droht; die K. Flaut ab; eine schwere, seelische K. Durchmachen, überwinden; in eine K. Geraten; die Wirtschaft, die Partei steckt in einer handfesten K.;*“ Quelle: [Dude07]. Das Krisenmanagement beschäftigt sich mit Situationen, welche die normalen Geschäftsabläufe gefährden können und welche möglicherweise auftreten können. Krisenmanagement weist viele Parallelen und Gemeinsamkeiten mit der Notfallplanung auf, welche im Kapitel 3 behandelt wurde. Deshalb werden in diesen Kapitel nur erweiternde Aspekte angeführt. Das folgende Kapitel behandelt den wichtigen Aspekt, wie Manager überhaupt dazu gebracht werden, Ressourcen für ein Krisenmanagement zur Verfügung zu stellen. Bei dieser Berufsgruppe zählt Zeit zum knappsten und wertvollsten Gut, deswegen ist eine gute Strategie äußerst wichtig.

4.3.1. Strategie für die Entwicklung von Krisenplänen

Für die Einführung von Krisenplänen in einem Unternehmen ist die Überzeugung der Notwendigkeit der Führungsebene Voraussetzung. Diese Überzeugung wird dadurch erreicht werden, wenn die spezifischen Ziele dieser Berufsgruppe mit den Zielen des gesamten Unternehmens übereinstimmen. Zu diesen Zielen werden zum Beispiel die Sicherheit des Arbeitsplatzes, die persönliche Weiterentwicklung der Mitarbeiter insbesondere der Führungsebene oder die Erfüllung von kurzfristigen Zielen zählen.

4.3.2. Informationen in einer Krise

Um am heutigen Markt überhaupt bestehen zu können benötigt man vor allem eins: Informationen. Diese Informationen müssen so aktuell wie möglich sein und sie müssen auch überall verfügbar sein. Dieser grundlegende Aspekt für Manager, wie auch für andere Mitarbeiter eines Unternehmens, kann auch für das Krisenmanagement übernommen werden. Erst wenn die nötigen Informationen verfügbar sind beziehungsweise diese

bekannt sind ist es möglich, sich mit möglichen Lösungen auseinander zu setzen. Im besten Fall werden diese Informationen so verwendet, dass überhaupt keine Krise auftritt und damit ein „pro aktives Krisenmanagement“ betrieben wird. Diese Ideal-Situation ist nicht immer möglich, deswegen müssen sich die verantwortlichen Personen Gedanken darüber machen, wie im tatsächlichen Krisenfall mit Informationen umgegangen wird. Eine große Unterstützung für diese Informationen stellt ein so genannter Kommunikationsplan dar, die folgende Abbildung zeigt eine mögliche Form.

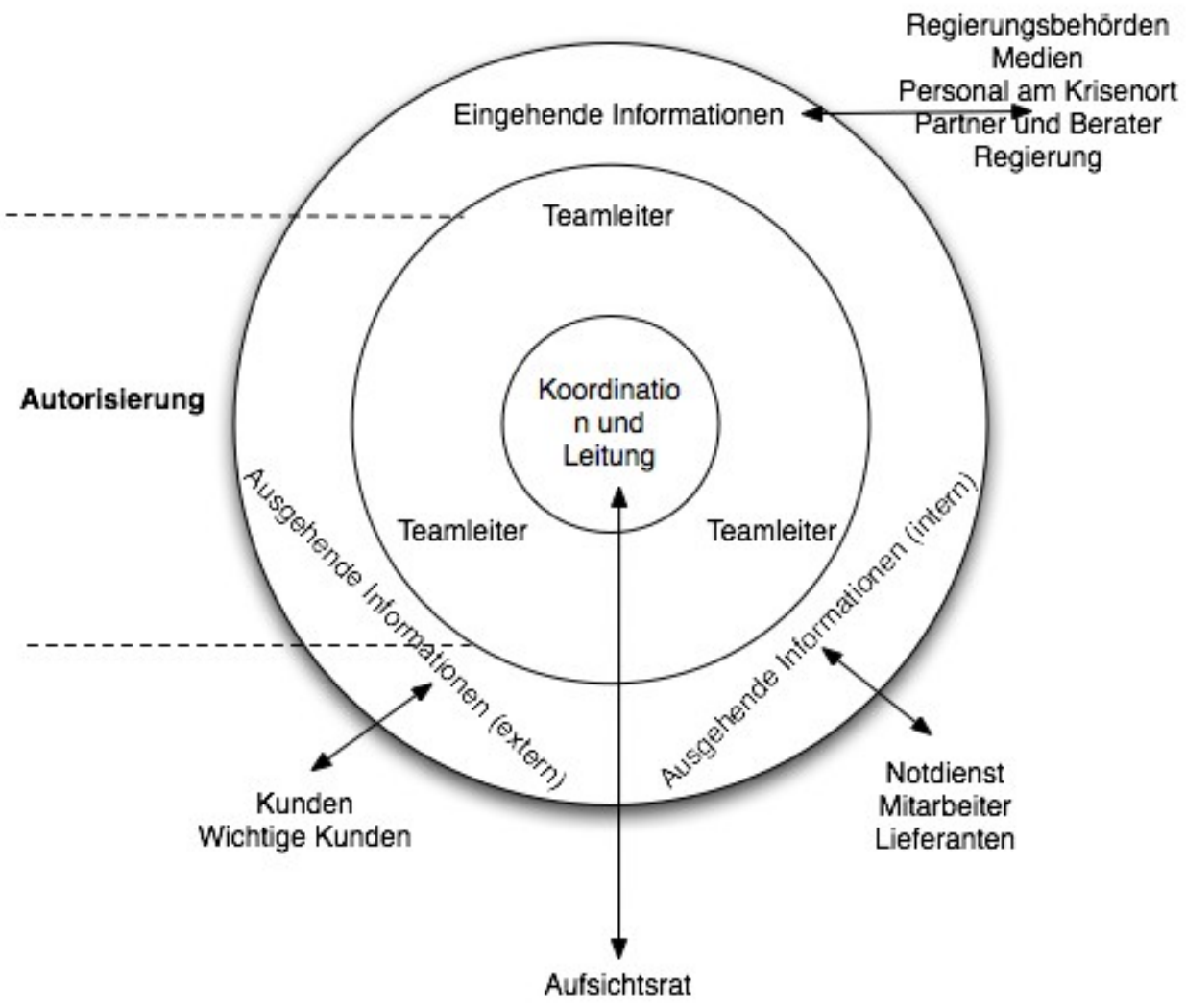

Abbildung 7, Kommunikationsplan. Quelle:[Wiec02] , eigene Darstellung

Bei Abbildung 7 kann man sehen, dass die Informationen von einer zentralen Stelle geleitet werden - Koordination und Leitung. Diese zentrale Stelle muss in mehreren Übungen getestet werden um sicherzustellen, dass sie auch in einem Krisenfall den Anforderungen standhält. Eine Übersicht über die Vorteile einer zentralen Stelle bietet die folgende Aufzählung.

- Diese Stelle ist eine zentrale Anlaufstelle für alle Arten von Fragen. Jeder der Fragen zu den Ereignissen oder zum aktuellen Stand hat, wendet sich an diese Stelle beziehungsweise wird an diese Stelle geleitet.

- Die Zusammenstellung von Informationen und die Interpretation von Informationen erfolgt am besten nach den Erfordernissen der Organisation.

- Diese Stelle inkludiert alle Phasen eines Kommunikationsprozesses, von der Anfrage beziehungsweise Suche bis zu endgültigen Antwort.

- Diese Stelle bereitet einerseits Informationen für interne Zweck auf, andererseits auch für externe Zwecke. Durch diese Situation wird erreicht, dass mögliche Konflikte zwischen diesen beiden Anforderungen vermieden werden.

4.3.3. Grundlage für einen allgemein gültigen Plan für das Krisenmanagement

Auch beim Krisenmanagement gibt es kein allgemein gültigen Aussagen für einen effizienten Plan. Auch hier ist die Komplexität der verschiedenen Unternehmen zu hoch. Jedoch ist es möglich, gewisse Aspekte für die Planung von Krisenmanagementprojekten zu verallgemeinern. Die folgende Abbildung bietet einen Überblick, wie eine Krisenmanagement-Gruppe organisiert sein kann.

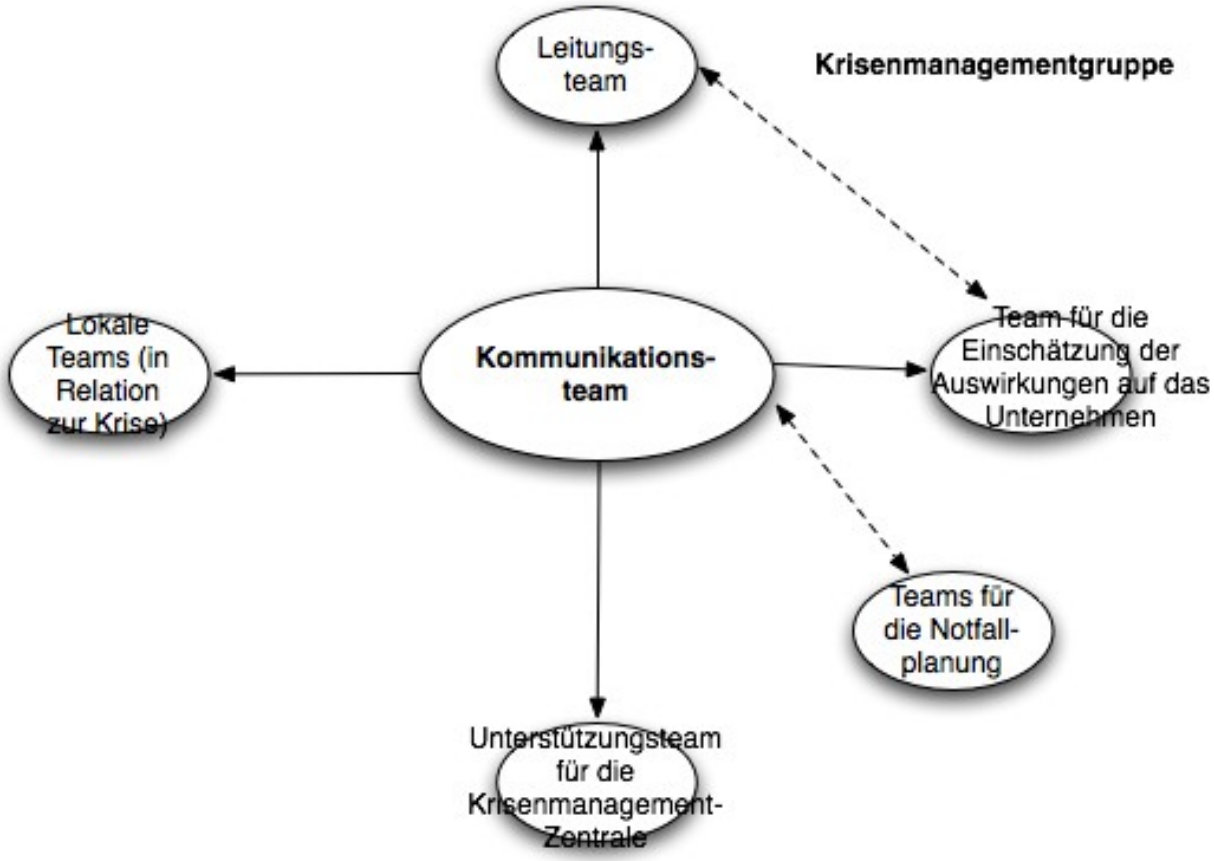

Abbildung 8, Verbindungen Kommunikationsteam. Quelle: [Wiec02], eigene Darstellung.

Diese Abbildung zeigt, wie ein zentrales Kommunikations-Team mit den anderen Teams des Krisenmanagements in Verbindung steht. Die folgende Gliederung beschreibt die Aufgaben der einzelnen Gruppen/Teams.

- Leitungsteam: Sorgt für die Leitung der Aktivitäten. Eine wichtige Funktion dieses Teams ist die Verbindung zur Führungsebene und die Verbindung nach „außen“ - zum Beispiel zu den Regulierungsbehörden.

- Lokale Teams: Diese Teams sollen so nah wie möglich am Krisenort bleiben, da sie Informationen an das Kommunikationsteam im Krisenmanagementzentrum weiterleiten. Diese Teams sind auch Anlaufstellen für Medienvertreter oder im Fall von Personenschaden für Angehörige der Opfer.

- Kommunikationsteam: Dieses Team stellt die wichtigsten Informationen zusammen und leitet sie an interne und externe Stellen weiter. Diese Gruppe leitet auch immer aktuelle Informationen an alle Personen, welche bei der Krisenbewältigung beteiligt sind, weiter.

- Team für die Einschätzung der Auswirkungen auf das Unternehmen: Diese Gruppe setzt sich aus den Führungskräften der betroffenen Geschäftsbereiche zusammen. Hier wird versucht festzustellen, welche Auswirkungen eine Krise auf den Geschäftsbetrieb hat. Dieses Team übt auch eine Beratungsfunktion aus, es stellt eine Beratung für das Leitungsteam hinsichtlich Strategien der Wiederherstellung dar.

- Unterstützungsteam für die Krisenmanagementzentrale: Dieses Team stellt die Infrastruktur für die Krisenmanagementzentrale zur Verfügung.

- Team für die Notfallplanung: Dieses Team erhält die wichtigsten Geschäftstätigkeiten aufrecht oder stellt diese wieder her. Eine genaue Beschreibung findet man in Kapitel 3 Disaster Recovery.

4.3.4. Überwachung der Krisenbewältigung

Für die Verantwortlichen von Krisenbewältigungen ist es auch von besonderen Nutzen zu wissen, wie der aktuelle Stand der Krise ist. Bei einem Krisenfall sind schnelle Entscheidungen gefragt, eine mögliche Lösung dafür ist der abermalige Einsatz von Checklisten. Durch diese Checklisten kann festgelegt werden, ob es sich bei einer Krise um einen „Notfall“, einen „Ernsthaften Zwischenfall“ oder einer „Katastrophe“ handelt. Durch diese Festlegung können verschiedene Maßnahmen eingeleitet werden, in genauer Abstimmung auf das Ausmaß einer Krise. Die folgende Aufzählung beinhaltet die Aspekte einer Krise.

- Ausmaß des Vorfalls
- Zeitpunkt des Vorfalls
- Ausmaß der Folgewirkungen
- Situation der Öffentlichkeitsarbeit – Information der Stakeholder
- Ausmaß der externen Auswirkungen
- Verfügbarkeit des Standorts

Werden diese Aspekte, und noch viele weitere Aspekte, in einer Checkliste bewertet, so kann die oben genannte Einschätzung stattfinden. Die folgende Abbildung bietet ein Beispiel für eine Checkliste zur Einschätzung des Zustandes einer Krise.

(a) Beste Situation/Erwartung	Gegenwärtige Erwartung (a)	Zwischen (a) und (b)	(b)	Schlechteste Situation/Erwartung
Ausmaß und Zeitpunkt				
Einzelnes Ereignis				Mehrere Ereignisse
Krisenmanagementgruppe nicht aktiviert				Krisenmanagementgruppe aktiviert
Geschäftsleitung geht ihren normalen Pflichten nach				Die Auferksamkeit der Gruppe wird für
				Mehrere Wochen abgelenkt
Leichte oder keine Verletzungen				Schwere Verletzungen und/oder Todesfälle
Die Auswirkungen werden lediglich für eine kurze Zeit				Die Auswirkungen werden über Monate
Ersichtlich sein				Ersichtlich sein
Eine einzelne Gruppe aus der Organisation kann die				Die Kooperation mehrer Gruppen des gesamten
Lage unter Kontrolle halten				Standorts ist erforderlich
Momentan keine Auswirkungen auf besondere				Auswirkungen auf besondere Tätigkeiten,
Auf die Tätigkeiten des Unternehmens				Die wichtig und dringend sind
Eskalation				
Situation stabil, Eskalation unwahrscheinlich				Eskalation oder Verschlechterung wahrscheinlich
Keine rechtlichen Konsequenzen				Unvermeidbare rechtliche Konsequenzen
Situation der Öffentlichkeitsarbeit				
Kein Interesse der Medien am Ereignis/				Interesse der Medien sicher
Den Auswirkungen				
Keine Beteiligung einer einzelnen Interessengruppe				Beteiligung der einzelnen Interessengruppe sicher
Externe Auswirkungen				
Keine Auswirkungen auf die Kunden				Auswirkungen auf viele und/oder Hauptkunden
Keine Auswirkungen auf den Betrieb des				Schwere Auswirkungen auf den Betrieb des
Unternehmens				Unternehmens
Keine Verschmutzung/Auswirkungen auf die Umwelt				Schwere Auswirkungen auf die Umwelt
Ereignis von lokalen Kommune nicht bemerkt				Schwere Auswirkungen auf die lokale Kommune
Keine Auswirkungen auf den Ruf/				Schwere Auswirkungen auf den Ruf/
Die Wettbewerbsfähigkeit				Die Wettbewerbsfähigkeit
Externe Beteiligung				
Notdienste nicht gerufen				Notdienste gerufen
Keine externen Stellen beteiligt				Externe Stellen müssen benachrichtigt werden
Eine Benachrichtigung über das betroffene Büro				Führungskräfte des Unternehmens müssen
Hinaus ist nicht erforderlich				Sofort benachrichtigt werden
Einsatzverfügbarkeit des Standorts				
Keine Auswirkungen auf den Zugang des Standorts				Zugang des Standorts für eine Woche oder
				Länger nicht möglich
Alle Operationen am Standort können sofort				Vollständige Verlegung des Standorts erforderlich
Weitergehen				
Keine Auswirkungen auf die Aktivitäten des				Probleme für viele Wochen nicht vollständig gelöst
Nächsten Arbeitstages				
Dienstleistungen am Standort innerhalb von				Dienstleistungen am Standort bleiben
Vier Stunden im Normalzustand				Für Wochen unterbrochen
Systeme arbeiten innerhalb von vier Stunden normal				Systeme bleiben für Wochen nicht einsatzbereit
Externe Dienstleistungen/Güter innerhalb von				Externe Dienstleistungen/Güter für
Vier Stunden im Normalzustand				Wochen unterbrochen

Abbildung 9, Checkliste Krise. Quelle: [Wiec02], eigene Darstellung.

Die Bewertung erfolgt in drei Spalten, die erste Spalte stellt dabei die beste Situation beziehungsweise Erwartung für das Unternehmen dar. Das bedeutet, wenn sich viele Bewertungen in dieser Spalte befinden ist ein Vorfall als „Notfall“ einzuschätzen. Das bedeutet, dass die Auswirkungen eines Vorfalls relativ gering sind. Der „Gegenspieler“ dieser Spalte ist die schlechteste Situation beziehungsweise die schlechteste Erwartung für ein Unternehmen. Befinden sich viele Bewertungen in dieser Spalte, so wird der Vorfall als „Katastrophe“ eingestuft werden. Die Auswirkungen in diesem Fall sind schwerwiegend für ein Unternehmen. Die dritte Spalte erlaubt eine neutrale Bewertung, d.h. die Situation befindet sich zwischen den vorher genannten Zuständen beste Erwartung und schlechteste Erwartung für ein Unternehmen.

4.3.5. Kriterien für gute Krisenbewältigungsdokumente

Wenn ein Vorfall auftritt ist es wichtig, rasch die richtigen Dokumente zur Hand zu haben um die richtigen Maßnahmen zu setzen. Diese Dokumente müssen verständlich verfasst werden, um eine schnelle Reaktion zu ermöglichen. Ein wichtiges Kriterium für das Verfassen der Dokumente für eine Krisenbewältigung ist auch der Fakt dass man nicht weiß, wo sich die einzelnen Mitglieder der Krisenmanagementgruppe zum Zeitpunkt des Auftretens eines Notfalls befinden. Es ist auch zu beachten, dass die Mitglieder den Plan für die Krisenbewältigung nicht bei sich haben werden. Die folgende Gliederung bietet eine Übersicht über Maßnahmen, welche zu effizienten Krisenbewältigungsdokumenten führen.

- Die gesamten Dokumente werden in einfacher, leicht verständlicher Form verfasst. Die Dokumente sind leicht und schnell verständlich.

- Die Dokumente werden ohne große Abschweifungen und Hintergrundinformationen verfasst, für diese Informationen bleibt im Notfall keine Zeit.

- In den Dokumenten sind Checklisten für einzelne Personen und Gruppen inkludiert. Diese Checklisten bieten einen sehr guten Überblick.

- Die Dokumente werden alle an einem Ort untergebracht. Querverweise auf andere Dokumente werden so weit wie möglich vermieden.

- Die Dokumente werden in einer ansprechenden Form verfasst, die Farbgestaltung ermöglicht ein schnelles Erkennen von Zusammenhängen etc.

- Die Dokumente werden durch einen Leitfaden ergänzt. Dieser Leitfaden enthält wichtige Informationen wie Kontakte oder zusätzliche Informationen über Maßnahmen, welche in einer Krisensituation sehr schnell abgerufen werden können. Dieser Leitfaden hat im Idealfall eine nur sehr kleine Größe und bietet gerade deswegen die wichtigsten Informationen auf einen Blick.

Das Krisenmanagement-Dokument selbst ist durch verschiedene Maßnahmen wie Farbgebung etc. gegliedert. Die zuständigen Personen erkennen sofort, welches Kapitel für einen bestimmten Vorfall zu kontaktieren ist. Der Plan enthält verschiedene Abschnitte für die verschiedenen Gruppen eines Krisenmanagements (siehe Kapitel 4.5.3. Grundlage für einen allgemein gültigen Plan für das Krisenmanagement).

4.4. Phasenmodell

Ist ein Unternehmen von der Notwendigkeit einer Notfallplanung überzeugt, so will es in effizienter Art und Weise diese in der Unternehmenskultur verankern. Es gibt viele Methoden, wie eine Umsetzung funktionieren kann. Eine Möglichkeit ist es, sich einfach an die Umsetzung zu machen – ohne Zeit für die Planung zu „verschwenden“. Diese Methode ist theoretisch zwar sehr effizient und zeit ersparend, in der Praxis wird diese Methode jedoch nicht funktionieren. Eine andere Möglichkeit ist, trotz der bekannten Risiken nicht auf diese zu reagieren und hoffen, dass die Risiken nicht eintreten. Diese Methode kann ebenfalls sehr kostengünstig sein, im Falle eines Vorfalls ist jedoch mit katastrophalen Auswirkungen für das Unternehmen zu rechnen. Eine bewährte Methode aus der Praxis ist das Phasenmodell. Mit diesem Modell wird in strukturierter Form eine Möglichkeit geboten, alle Aspekte für eine erfolgreiche Notfallplanung im Business-Continuity-Management zu berücksichtigen. Diese Situation wird dadurch ermöglicht, da das Phasenmodell, wie der Name schon verrät, die Notfallplanung in verschiedene Phasen zerlegt und so einen strukturierten Arbeitsablauf ermöglicht. Dieses Modell gliedert sich in sechs Phasen, die erste Phase behandelt dabei den Abschnitt „Untersuchung und Analyse“, die letzte Phase implementiert den Arbeitsvorgang „Wartung und Entwicklung“. Wie man durch die erste und die letzte Phase sehen kann, wird von der erstmaligen Planung bis zur Wartung nach erfolgreicher Implementierung alles eingeplant. Die folgende Abbildung bietet einen Überblick über die einzelnen Phasen des Phasenmodells, eine Beschreibung der Aufgaben jeder einzelnen Phase erfolgt im nächsten Abschnitt.

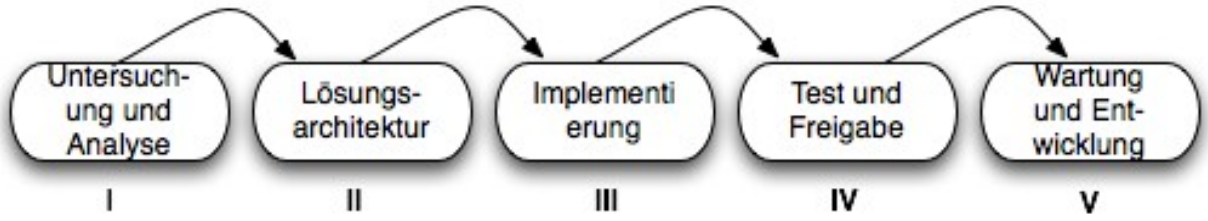

Abbildung 10, Phasenmodell. Quelle: [Wiec02], eigene Darstellung.

4.4.1. Untersuchung und Analyse

Die erste Phase des Phasenmodells behandelt die beiden Maßnahmen Untersuchung und Analyse. Diese Phase kann in zwei Abschnitte gegliedert werden: Zum einen der Abschnitt Einschätzung des möglichen Schadens, zum anderen die Analyse des Risikos. Beim ersten Abschnitt, Schadensabschätzung, wird also versucht, den möglichen Schaden

durch einen Vorfall durch verschiedene Parameter zu beschreiben. Der andere Abschnitt, Risikoanalyse, beschäftigt sich mit der Einschätzung von Wahrscheinlichkeiten für den Eintritt eines bestimmten Risikos.

Die Schadensabschätzung befasst sich mit folgenden Themen:

- Monetäre Auswirkungen eines Ausfalls beziehungsweise eines Vorfalls: Hier wird versucht, den finanziellen Schaden eines Vorfalls in realistischer Form darzustellen. Diese realistische Form wird damit erreicht, da die finanziellen Auswirkungen auf einen durchschnittlichen Geschäftstag berechnet werden. Um auf den gesamten möglichen Schaden zu kommen, müssen drei Parameter berücksichtigt werden: Grenzwert für den „Value-at-Risk“, Liquiditätsrisiko und mögliche Gewinneinbußen. Für den Grenzwert „Value-at-Risk“ wird berechnet, wie hoch der Verlust bei einem eintägigen Stopp der gesamten Handelsaktivitäten für ein Unternehmen ist.

- Schädigung des Image und des Rufes bedingt durch einen Vorfall: Hier wird versucht einzuschätzen, wie schwerwiegend sich ein Vorfall auf das Image eines Unternehmens auswirken kann. Diese Auswirkungen werden von Unternehmen zu Unternehmen und auch von Branche zu Branche unterschiedlich ausfallen. Wenn man zum Beispiel einen Ausfall eines Services eines Unternehmens welches sehr stark in der Öffentlichkeit vertreten ist betrachtet, so kann schon ein sehr kurzer Ausfall zu massiver Rufschädigung führen. Ein anderes Beispiel ist die Website eines Softwareherstellers, ist diese Website für längere Zeit nicht erreichbar, so wird diese peinliche Situation großen Schaden bezüglich des Images des Unternehmens hervor rufen.

- Mögliche gesetzliche Vorschriften, welche auf jeden Fall eingehalten werden müssen: Hier sind Vorschriften zu beachten, welche Bereiche unter allen Umständen – d.h. auch im Falle eines Notfalls – aufrecht erhalten müssen.

- Totaler Verlust über die Kontrolle über das Geschäft: Bei dieser Einschätzung wird versucht voraus zu sagen, welche Auswirkungen der Verlust von Informationen zur Steuerung von Geschäftsabläufen haben kann.

Die Risikoanalyse beschäftigt sich mit folgenden Themen:

- Festlegung eines Wiederhertellungsprofils – Priorisierung von Prozessen: Hier wird bestimmt, wie lange ein Prozess maximal ausfallen darf und welche Prozesse mit bestimmten Mindestkapazitäten unter allen Umständen weiter laufen müssen. Durch diese Maßnahmen erfolgt also eine gewisse Priorisierung von Prozessen, Prozesse welche auf jeden Fall (in voller Kapazität oder auch in verminderter Kapazität) verfügbar sein müssen haben eine höhere Priorisierung als Prozesse, wo ein Ausfall für einen bestimmten Zeitraum in Kauf genommen werden kann. Ein

mögliches Wiederherstellungsprofil für einen Prozess kann lauten, dass ein totaler Ausfall für zwei Tage zulässig ist, danach muss aber mindestens 30 Prozent Kapazität vorhanden sein, die komplette Wiederherstellung muss nach einer Woche abgeschlossen sein – d.h. der Prozess muss nach einer Woche wieder komplett und ohne Einschränkungen einsetzbar sein.

- IT-Verfügbarkeit: Nachdem für die Prozesse Priorisierungen durchgeführt wurden, kann man die Anforderungen für IT-Anwendungen bestimmen. Diese Bestimmung wird sich komplex gestalten, da viele Anwendungen aufeinander aufbauen und deswegen Verflechtungen bestehen.

- Wahrscheinlichkeit einer möglichen Bedrohung: Um die Wahrscheinlichkeit einer Bedrohung möglichst realistisch einzuschätzen, müssen viele Faktoren beachtet werden. Eine einheitliche Bestimmung von Bedrohungen für Unternehmen ist nicht möglich, jedes Unternehmen hat bestimmte Eigenschaften welche unbedingt beachtet werden müssen. Ein Unternehmen in Kalifornien ist zum Beispiel stark erdbebengefährdet, während ein Unternehmen in Tirol möglicherweise von Lawinen bedroht ist. Weiters spielt es auch eine entscheidende Rolle, in welchen Bereich ein Unternehmen tätig ist und welche Produkte/Dienstleistungen angeboten werden.

In der Praxis hat sich der Einsatz einer standardisierten Fünf-Punkte-Skala bewährt, welche für jedes Unternehmen individuell angepasst wird. Diese Skala beschreibt, wie hoch die Wahrscheinlichkeit für einen Eintritt einer Bedrohung beziehungsweise eines Vorfalls ist. Die Skala führt dabei Abstufungen durch, von „Sehr gering“ bis zu „Sehr hoch“. Die folgende Tabelle beschreibt die Kriterien für die einzelnen Abstufungen der Fünf-Punkte-Skala.

Wahrscheinlichkeit	Auftrittshäufigkeit einer Bedrohung/Vorfalls
Sehr gering	Statistisch gesehen weniger als einmal in hundert Jahren
Gering	Mehr als einmal in hundert Jahren, jedoch weniger häufig als einmal in 25 Jahren
Mittel	Mehr als einmal in 25 Jahren
Hoch	Mehr als einmal in 5 Jahren
Sehr hoch	Mehr als einmal in einem Jahr

Tabelle 9, Wahrscheinlichkeiten Bedrohungen/Vorfälle

Szenarien für einen Notfall/Vorfall: Hier werden die Szenarien betrachtet, welche größtmögliche Auswirkungen von Bedrohungen/Vorfällen annehmen können. Es wird also betrachtet, welche „worst-case-Situation“ durch einen Vorfall entstehen kann. Diese Notfall-/Vorfallszenarien sind wieder unterschiedlich, folgende Kriterien werden immer betrachtet:

- Ausfall des Gebäudes und damit verbunden Ausfall des wichtigsten IT-Systems (Dieser Zustand kann auftreten, wenn die Geschäftseinheit und die IT-Infrastruktur im selben Gebäude untergebracht sind)
- Ausfall des Gebäudes
- Ausfall des wichtigsten IT-Systems
- Ausfall von mehreren Gebäuden – inklusive anschließende Nachbargebäude
- Spezielles Notfallszenario für die unterschiedlichen Arten von Räumen, wie zum Beispiel Server-Raum, Produktionsräume etc.
- Außergewöhnliche Szenarien wie zum Beispiel ein möglicher Streik oder eine Maßen-Krankheit

4.4.2. Lösungsarchitektur

In dieser Phase wird bestimmt, wie eine Reaktion auf einen Notfall/Vorfall stattfindet. Durch diese Maßnahme kann bestimmt werden, welche Maßnahmen Vorrang vor anderen Maßnahmen haben und welche essentiell für die Geschäftstätigkeiten eines Unternehmens sind. Hier gibt es drei Stufen für die Wiederherstellung, die erste Phase betrifft den Eintritt eines Vorfalls/Notfalls, die zweite Stufe betrifft die Wiederherstellung und die abschließende Phase behandelt den normalen Geschäftsablauf – d.h. der Vorfall wurde behandelt und abgeschlossen.

- Eintritt des Vorfalls: Es erfolgt eine Meldung, dass ein bestimmter Zustand eingetreten ist. Die Unternehmensführung beziehungsweise das Management hat jetzt die Aufgabe zu entscheiden, welche Maßnahmen aus einem vorgefertigten Maßnahmenkatalog etc. durchzuführen sind.

- Wiederherstellung: Bei der Wiederherstellung wird zwischen verschiedenen Stufen unterschieden, einerseits gibt es jene Maßnahmen, welche sofort eingeleitet werden. Diese sofortige Reaktion auf einen Vorfall bedeutet dass ein Unternehmen versucht, die schwerwiegendsten Auswirkungen in den Griff zu bekommen. Zu diesen Auswirkungen zählen unter anderen Sicherheit der Mitarbeiter, Öffentlichkeitsarbeit und das Aktivieren der Notfallteams. Der Zeitrahmen dieser Phase wird ungefähr zwischen vier und acht Stunden betragen, jedoch ist auch ein größerer Zeitrahmen möglich.

- Die nächste Phase betrifft die sofortige Wiederherstellung. Die wichtigste Tätigkeit hier ist es, die wichtigsten Geschäftstätigkeiten eines Unternehmens innerhalb eines bestimmten Zeitraumes wiederherzustellen – d.h. ein bestimmtes Niveau wird erreicht. Diese Tätigkeiten werden vom Notfallteam durchgeführt, wichtige Elemente der vorigen Phase wie die Sicherheit der Mitarbeiter, Öffentlichkeitsarbeit werden auch in dieser Phase behandelt. In dieser Phase findet auch die weitere Bewertung des Vorfalls statt, um eine vollständige Rückkehr zur „Normalität“ zu ermöglichen. Bei der nächsten Phase, Langfristige Wiederherstellung, wird eine Möglichkeit geboten zu reagieren, wenn die Maßnahmen der sofortigen

Wiederherstellung nicht in einem bestimmten Zeitrahmen zu bewältigen sind. Hier wird bestimmt, wie eine Wiederherstellung in einem längeren Zeitraum aussieht. Hat ein Vorfall/Notfall schwerwiegende Auswirkungen, so wird diese Phase zum Einsatz kommen. Bei einer umfassenden Notfallplanung ist diese Phase zu beachten. Wenn die Aktivitäten der Phasen erfolgreich eingesetzt wurden, so wird zur nächsten Phase, Normaler Geschäftsbetrieb, übergegangen. Bei dieser Phase kann also wieder ohne Einschränkungen wie vor dem Vorfall/Notfall gearbeitet werden.

4.4.3. Implementierung

In dieser Phase werden jene Elemente zur Umsetzung gebracht, welche in den vorigen Phasen vorgeschlagen wurden. Die wichtigsten Funktionen dieser Phase sind folgende Aufgaben:

- Erfassen des Notfallplans
- Erfassen der Informationen über die aktuellen Mitarbeiter
- Festlegung der erforderlichen Soft- und Hardwarekomponenten
- Festlegung des Ablaufs und der Organisation im Falle eines Notfalls/Vorfalls
- Installation der erforderlichen Soft- und Hardwarekomponenten
- Freigabe der Maßnahmen

4.4.4. Test und Freigabe

Die Maßnahmen für einen Notfall/Vorfall müssen getestet werden, um einen effizienten Einsatz im Ernstfall zu ermöglichen. Ohne dieser Tests ist kein effizienter Einsatz möglich. Erst wenn die Tests zur Zufriedenheit der zuständigen Personen/Gruppe verlaufen, werden die Maßnahmen freigegeben.

4.4.5. Wartung und Überwachung

Auch wenn die Maßnahmen bereits erfolgreich eingeführt wurden ist zu beachten, dass es ständig Änderungen im Unternehmen und im Umfeld des Unternehmens gibt. Nur durch eine regelmäßige Aktualisierung kann im Falle eines Notfalls/Vorfall effizient darauf reagiert werden. Weiters werden neue Mitarbeiter mit den Abläufen vertraut gemacht und es werden Schulungen, Trainings etc. abgehalten. Hier ist es auch wichtig, dass Dokumentationen über die Maßnahmen verfasst werden. Durch diese Dokumentationen ist es möglich, den Arbeitsaufwand für ähnliche Aufgaben in der Zukunft einzuschränken. Die folgende Tabelle fasst die wichtigsten Eigenschaften der einzelnen Phasen noch einmal zusammen.

Phase	Eigenschaften
Untersuchung und Analyse	Schadensabschätzung (monetäre Auswirkungen, Schädigung des Image und des Rufes, gesetzliche Vorschriften welche eingehalten werden müssen, totaler

	Verlust über das Geschäft) Risikoanalyse (Festlegung des Wiederherstellungsprofils - Priorisierung von Prozessen, IT-Verfügbarkeit, Wahrscheinlichkeit einer möglichen Bedrohung)
Lösungsarchitektur	Bestimmung, wie auf einen Vorfall/Notfall regiert wird Drei Stufen für die Wiederherstellung: Eintritt des Vorfalls, Wiederherstellung, sofortige Wiederherstellung)
Implementierung	Umsetzung der vorher geplanten Maßnahmen Erfassen des Notfallplans, Informationen über aktuelle Mitarbeiter Festlegung der erforderlichen Soft- und Hardwarekomponenten Festlegung des Ablaufs und der Organisation im Falle eines Notfalls Installation der erforderlichen Soft- und Hardwarekomponenten Freigabe der Maßnahmen
Test und Freigabe	Maßnahmen werden auf Wirksamkeit getestet Freigabe erfolgt erst, wenn Tests erfolgreich verlaufen
Wartung und Entwicklung	Maßnahmen müssen ständig an die aktuellen Umstände angepasst werden Schulung neuer Mitarbeiter Erfassung einer Dokumentation über eingesetzte Maßnahmen

Tabelle 10, Eigenschaften der einzelnen Phasen Phasenmodell

4.5. Continuity-Management Tools

Durch Tools ist es möglich, verschiedene Arbeitsabläufe automatisiert ablaufen zu lassen oder es ist auch möglich, eine strukturierte Durchführung der benötigten Schritte zu ermöglichen. In diesem Kapitel werden vier Tools beschrieben, welche alle von „Heine und Partner“ stammen. Das einzige Tool, welches aktuell noch weiterentwickelt wird ist „XENCOS“, welches als Nachfolge-Tool der anderen Lösungen eingesetzt wird. „XENCOS“ ist also eine Verbindung der drei vorigen Tools, welche durch diese Lösung ersetzt werden.

4.5.1. CAPT

Die Quelle für diesen Abschnitt ist [Hein08a]. Das Tool "CAPT" bietet dem User folgenden Nutzen: Es werden alle Informationen und Daten berücksichtigt, welche im Notfall benötigt werden. Es gibt keine redundante Daten durch den Einsatz einer relationalen Datenbank, d.h. Änderungen müssen jeweils nur an einer Stelle durchgeführt werden. Durch die Erfahrung von den Herstellern erfolgt eine strukturierte und effiziente Erfassung der benötigten Daten. Jene Daten, welche mit einem anderen Tool hauptsächlich genutzt werden, können importiert werden. Aktionspläne können durch eine graphische Bedienfläche einfach erstellt werden. Es ist auch möglich, aus bestehenden Notfallplänen Testpläne zu erstellen. Im weiteren ist es auch möglich, Inhaltsverzeichnisse zur erstellen

und verschiedene Versionen von Notfallhandbüchern zu erstellen. Als Ergebnis des Tools "CAPT" steht dabei ein Notfallhandbuch, welche alle wichtige Daten enthält, welche in einem Notfall benötigt werden. Die Erstellung erfolgt strukturiert, somit ist eine aktuelle, vollständige und korrekte Erfassung der Daten möglich. Ein weiteres Ergebnis des Einsatzes dieses Tools ist, dass die Dokumentation der Inhalte der Notfallpläne durch eine ziel orientierte Struktur der Daten unterstützt wird.

4.5.2. CM

Die Quelle für diesen Abschnitt ist [Hein08b].Mit dem Tool "CM" ist es möglich, entweder "top down" oder "bottom up" zu planen. Um eine effiziente und aktuelle Planung zu gewährleisten, werden Plausibilitäs- und Vollständigkeitskontrollen eingesetzt. Die Prozesse werden dokumentiert und so entsteht eine Voraussetzung für Kontinuität. Mit CM ist es möglich, Handbücher unabhängig der geographischen Lage zu erstellen und zu pflegen. Es erfolgt eine Online-Steuerung im Falle eines Notfalls beziehungsweise bei einer Simulation zu Testzwecken. Durch eine zentrale Informationsdatenbank wird eine einheitliche Struktur für Notfallpläne für alle Abteilungen und Niederlassungen erreicht. Durch diese Struktur ist es auch möglich, dass verschiedene Abteilungen unterschiedliche Pläne beziehungsweise Auszüge aus Plänen erhalten .Durch den Einsatz von CM werden folgende Ergebnisse erzielt: Verschiedene Arten von Handbüchern wie Notfall-, Operator- oder Produktionshandbücher. Die Erstellung kann dabei sowohl auf Papierform als auch online geschehen. Durch die Verwaltung von Verfügbarkeitszielen, Szenarien von Ausfällen und Wiederanlaufstrategien kann eine nachvollziehbare Durchführung und Steuerung des Verfügbarkeitsmanagements erfolgen. Die eingesetzte Online-Begleitung der Plandurchführung im Übungs- beziehungsweise im Ernstfall kann dabei helfen, Schwachstellen oder Lücken rechtzeitig zu finden. Durch eine frei-konfigurierbare Objektverwaltung ist es möglich, dieses Tool nicht nur in der Notfallplanung einzusetzen, sondern auch im Bereich des Business-Continuity-, Availability- und Operations-Management.

4.5.3. RISK

Die Quelle für diesen Abschnitt ist [Hein08c]. Durch "RISK" ist es möglich, eine übersichtliche Darstellung von Ermittlung, Bewertung, Bewältigung und Überwachung von Risiken durchzuführen. Es werden auch die kritischen Geschäftsprozesse eines Unternehmens festgehalten. Diese Ergebnisse werden in regelmäßigen Abständen getestet und wenn nötig neu bewertet. Durch eine freie Anzahl von Risikokatalogen, welche aus einer zentralen Datenbank erstellt werden, kann ein umfassendes Reporting mit unterschiedlichen Kriterien einer Selektion erreicht werden. Auch bei diesem Tool ist eine geographisch-unabhängige Bearbeitung möglich, jeder User mit entsprechender Befugnis kann auf die Dokumente zugreifen. Als Ergebnis bekommt man durch den Einsatz von RISK einen oder mehreren Risikokataloge, welche eine Identifikation und Bewertung der unternehmensspezifischen Risiken beinhalten. Eine Besonderheit hierbei ist, dass auch Präventivmaßnahmen in die Ergebnisse mit einfließen. Durch die

Identifikation und Bewertung findet eine grundlegende Erstellung einer Risikobewältigung des Unternehmens statt.

4.5.4. XENCOS

Die Quelle für diesen Abschnitt ist [Hein08d]. Dieses Tool ist das Nachfolgeprodukt der drei bereits vorgestellten Lösungen. Dieses Tool umfasst alle Funktionen zur Dokumentation und zur Pflege von Daten für Einsatz-Pläne (Aktivitäten und Ressourcen zur Rettung, Evakuierung etc. zur Bekämpfung von Schadensfällen), Krisenmanagementplänen (Beschreibung der Rollen und Aufgaben eines zentralen Krisenmanagements eines Unternehmens), Business-Recovery-Plänen (Wiederherstellung kritischer Geschäftsprozesse), IT-Recovery-Plänen (Maßnahmen für Wiederherstellung der ausgefallenen IT-Services/Komponenten) und für Infrastruktur-Recovery-Pläne (Wiederherstellungsmaßnahmen für Infrastruktur eines Unternehmens). Mit diesem Tool ist es möglich, einzelne Aktivitäten unabhängig von ihrer Verwendung in Aktionsplänen zu bearbeiten. Die Aktionspläne können graphisch aufbereitet werden. Es erfolgt eine automatische Generierung von Handbüchern aus voneinander unabhängig behandelbaren Informationen. Von den benötigten Basisdaten, Personen, IT-Komponenten, Backup-Verfahren etc. können alle Typen von Dokumentationen verwendet werden und es werden ihre gegenseitigen Abhängigkeiten erfasst.

Da XENCOS das Nachfolgeprodukt der drei vorher beschriebenen Tools darstellt ist es möglich, bestehende Kundendaten aus CAPT oder CM-Dateien nach XENCOS zu exportieren. Für diesen Export werden, wie aus der folgenden Abbildung ersichtlich, die Daten aufbereitet, danach in ein XENCOS-fähiges Format umgewandelt und danach nach XENCOS exportiert. Die folgende Abbildung bietet einen Überblick über diese Vorgehensweise.

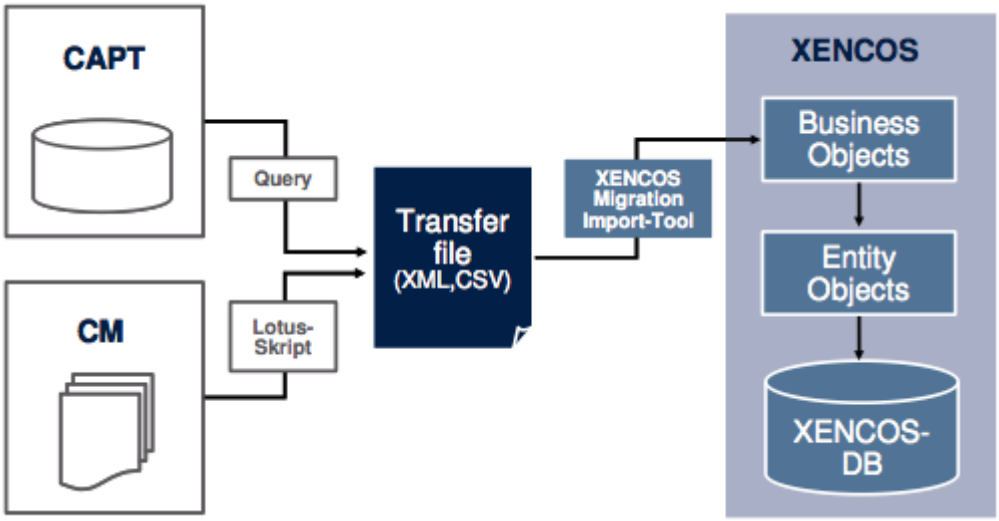

Abbildung 11, Funktionsweise XENCOS. Quelle: [Hein08e]

Für das XENCOS-Tool sind für 2008 zwei wichtige Zusatzfunktionen geplant. Zum einen wird das Modul RIA (Risiko-Analyse) implementiert werden, zum anderen wird das Modul BIA (Business Impact Analyse) in das bestehende Tool eingefügt. Die folgende Gliederung beschreibt die geplanten Eigenschaften der zwei Module.

- Modul RIA: Die Risikoanalyse beschäftigt sich mit den Risiken, welche für ein Unternehmen relevant sind. Anschließend werden diese Daten nach ihrer Eintrittschwahrscheinlichkeit und der möglichen Schadenshöhe bewertet. Dieses Modul soll eine softwaremäßige Darstellung aller Risiken und derer Bewertung erstellen. Für dieses Verfahren stehen definierte Ereigniskataloge bereit, um die möglichen Risiken für ein Unternehmen zu erfassen. Im weiteren Verlauf stehen Bewertungsklassen zur Verfügung, um eine Klassifizierung/Priorisierung vornehmen zu können. Diese Klassen erzeugen einen Handlungsbedarf, welcher den möglichen Auswirkungen eines Risikos entsprechen. Verschiedene Verfahren erlauben es, manuell eine Reihung der Auswertung des Risikokatalogs durchzuführen.

- Modul BIA: Dieses zukünftige Modul wird es erlauben, eine Darstellung der Auswirkungen von Ausfällen oder Unterbrechungen von Geschäftsprozessen in einem Unternehmen zu erstellen. Diese Darstellung umfasst dabei finanzielle wie auch nicht-finanzielle Auswirkungen. Durch diese Darstellung ist es möglich jene Geschäftsprozesse zu identifizieren, welche für den Fortbestand eines Unternehmens essentiell sind. Für diesen Zweck erfolgt eine Erfassung der grundlegenden Variablen eines Unternehmens in einer Datenbank und in weiterer Folge eine Übernahme in XENCOS. Es werden auch Workshops durchgeführt, um Daten für diese Übernahme zu gewinnen. XENCOS erstellt Fragebögen und Tabellen, welche ebenfalls die Grundlage der Erfassung von Daten und in weiterer Folge für den Import darstellen. Auch bei diesem geplanten Modul gibt es wieder die Möglichkeit, die Auswertung nach selbst selektierten Kriterien vorzunehmen.

Die folgende Tabelle bietet einen Überblick über die verschiedenen Eigenschaften und Nutzen der verschiedenen Softwarelösungen.

Tool	Eigenschaften/Nutzen
CAPT	Erstellung Notfallhandbuch inklusive aller benötigten Daten, Dokumentation der Inhalte wird durch ziel orientierte Struktur der Daten unterstützt
CM	Dokumentationen für Prozesse werden erstellt, gepflegt und verwaltet, Stärke durch Flexibilität und Einsatzbreite, Erstellung von Netzplänen für Geschäftsprozesse, Planung und Steuerung des Verfügbarkeitsmanagements wird ermöglicht, Freigabeverfahren für Änderungen an Daten unterstützt Arbeitsqualität nach ISO 9000, Erstellung von Wiederanalaufplänen
RISK	Verfahren zur Identifikation und Bewertung der

	unternehmensrelevanten Risiken, Identifikation von kritischen Prozessen, Schätzung von Eintrittswahrscheinlichkeiten und Schadenshöhen, Miteinbeziehung von präventiven Maßnahmen, Einsatz von Risikobewältigung und Risikominimierung
XENCOS	Erstellung von Einsatzplänen, Krisenmanagementplänen, Business-Revory-Plänen, IT-Recovery-Plänen und Infrastruktur-Recovery-Plänen, Graphische Aufbereitung der Einzelaktivitäten der verschiedene Pläne, Erstellung von Notfallhandbücher/Reporting, Bestimmung und Aufarbeitung der benötigten Basisdaten

Tabelle 11, Eigenschaften/Nutzen Tools Business Continuity

4.6. Aktuelle Studie

Dieses Kapitel beschreibt die Ergebnisse, welche durch eine Umfrage im Jahr 2007 entstanden sind. Der Auftraggeber dieser Umfrage ist das „chartered management institute“ und der Verfasser des Berichts ist Patrick Woodman [Wood07] . Diese Reihe von Umfragen wurde bereits zum achten mal durchgeführt, dabei wurden 10.600 Instituts-Mitglieder befragt und dabei erhielt man 1.257 Antworten. Der geographische Raum, wo sich die befragten Manager befinden, ist Großbritannien. Diese Studie zeigt aktuelle Ausprägungen beziehungsweise Kenntnisse von BCM und stellt deswegen eine gute Erweiterung für diesen Abschnitt dar. Die folgende Gliederung fasst die wichtigsten Ergebnisse zusammen, welche aus der Erhebung beziehungsweise der Befragung gewonnen werden konnten. Die wichtigsten Ergebnisse sind:

- 73 Prozent der Manager geben an, dass BCM wichtig ist in ihrer Organisation, 94 % welche BCM eingesetzt haben stimmen zu, dass BCM Unterbrechungen des Geschäftsablaufs reduziert hat

- Trotz der bekannten Bedeutung und Auswirkungen von Unterbrechungen gaben mehr als die Hälfte der 1257 befragten Manager an, dass sie in Unternehmen tätig sind wo kein spezieller BC-Plan vorhanden ist.

- Ungefähr ein Drittel der Organisationen gaben an, dass sie von Unterbrechungen aufgrund eines Ausfalls der IT-Systeme und dem Verlust von Personen (32 %) im vergangenen Jahr betroffen waren. Jene Unternehmen, welche von extremen Wetter-Bedingungen betroffen waren, erhöhte sich um 9 Prozent auf 28 Prozent.

- Es gibt Anzeichen, dass die Unternehmen ihre Planungsmaßnahmen verbessern: 55 Prozent haben Pläne für ein mögliches Auftreten einer Grippe-Pandemie. Viele Unternehmen sind sich jedoch nicht über die möglichen Ausfallzeiten von Angestellten bewusst.

- Nur die Hälfte der Unternehmen wo Pläne vorhanden sind führen regelmäßige Übungen durch, trotz des Umstandes, dass Übungen eine grundlegende Rolle für den Einsatz der Pläne darstellen. 80 Prozent der Unternehmen wo Übungen durchgeführt wurden, berichteten von Mängeln in den aktuellen Plänen.

- Obwohl 81 Prozent der Manager berichteten dass ihre Organisation eine mögliche Heimarbeit bis zu einem gewissen Ausmaß unterstützen kann, wurde die benötigte IT-/Telekommunikationsinfrastrukturen nicht eingeführt.

5. IT Service Continuity/Disaster Recovery

In jedem Unternehmen wird heute Informations- und Kommunikationstechnologie exzessiv eingesetzt. Diese Technologie ist einer der Schlüsselfaktoren in der heutigen Informationsgesellschaft. Setzt ein Unternehmen diese Technologien nur in einem geringen Ausmaß beziehungsweise nicht in der richtigen Art und Weise ein, so entsteht ein großer Schaden für die Wettbewerbsfähigkeit dieses Unternehmens. Bedrohungen für die Technologie gibt es aktuell in einer großen Anzahl von verschiedenen Formen und Ausprägungen. Diese Bedrohungen gibt es in der Form von Naturkatastrophen, wie zum Beispiel Erdbeben, Überschwemmungen, Lawinenabgänge oder Erdrutsche, oder auch in der Form des direkten Einflusses von Menschen, sowohl in unbeabsichtigter Form oder mit der Absicht einem Unternehmen Schaden zuzufügen. Mögliche Beispiele für unbeabsichtigte Formen sind Fehler in der Konstruktion von Festplatten, Nicht-Einhaltung von Sicherheitsbestimmungen im Umgang mit IT-Systemen oder durch eine unbeabsichtigte Weitergabe von sensiblen Daten. Im Gegensatz dazu gibt es beabsichtigte Formen wie zum Beispiel gezielte Angriffe durch Hacker etc.

Durch die starke Vernetzung, welche durch das Internet heute gegeben ist, kann sich kein Unternehmen erlauben, ein Service oder eine Website für längere Zeit nicht anzubieten. Ist zum Beispiel eine Helpline für längere Zeit nicht erreichbar, so erfolgt sofort eine negative Meldung in einem Forum. Dieses Beispiel führt „nur“ zu einem schlechten Image eines Unternehmens, längerfristig entstehen dadurch Umsatzeinbußen. Kann ein Unternehmen jedoch für längere Zeit nichts verkaufen aufgrund eines Ausfalls der IT, so werden schwerwiegende Auswirkungen die Folge sein. Diese Folgen reichen von Umsatzeinbußen in Millionenhöhe bis zu einer Gesamtauflösung des Unternehmens. Die möglichen Schäden für ein Unternehmen können also finanzieller wie auch nicht-finanzieller Natur sein. Disaster Recovery ist eine Methode, um auf Ereignisse dieser Art zu reagieren beziehungsweise um Ereignisse dieser Art zu vermeiden.

5.1. Definition

Bei der Definition von Disaster Recovery wird festgelegt, was genau unter diesem Begriff zu verstehen ist. Wichtig ist auch zu definieren, für welche Bereiche Disaster Recovery geeignet ist. Eine wichtige Quelle für diesen Abschnitt ist das Buch „Backup und Disaster Recovery“ von Egbert Wald ([Wald02]). IT-Wissen beschreibt Disaster Recovery folgendermaßen: „*Desaster-Recovery (DR) umfasst alle Maßnahmen zur Wiederherstellung der Datenbestände nach einem Katastrophenfall und zur kurzfristigen Wiederaufnahme der Geschäftstätigkeit. Da für die Wiederaufnahme der Geschäftstätigkeit nicht alle unternehmensbezogenen Datenbestände zwingend erforderlich sind, befasst sich das Desaster-Recovery auch mit Strategien in denen die Unternehmensdaten und Applikationen nach ihrer Wichtigkeit kategorisiert werden. Diese Strategien richten sich nach den Geschäftsanforderungen und können u.a. die Verfügbarkeit oder die Kosten optimieren. Bestimmte Datenbestände haben dabei höhere Prioritäten als andere. So müssen bestimmte Daten für Online-Transaktionen unmittelbar nach dem Recovery wieder verfügbar sein.*“ (Quelle:[Itwi08i])

Disaster Recovery kommt zum Einsatz, wenn unvorhersehbare Ereignisse, ein Unternehmen treffen. Die Maßnahmen dieser Methode kommen sowohl im Hardware- als auch im Softwarebereich zum Einsatz. Im Bereich der Hardware wird zum Beispiel geplant, wie ein Ausfall eines Rechenzentrums kompensiert werden kann. Auf der Software-Seite wird versucht, durch spezielle Tools den Verlust von Daten auf ein Minimum zu reduzieren bzw. zu verhindern. Diese Maßnahmen sind sehr schwierig in ein Unternehmen einzuführen. Die Geschäftsleitung wird erst dann von einem sinnvollen Einsatz überzeugt sein, wenn die möglichen Kosten durch einen Notfall präsentiert werden. Ansonsten verlässt man sich häufig auf das laufende System, andere Entscheidungen welche direkt den Geschäftserfolg betreffen, haben Vorrang. Im weiteren Verlauf müssen die Mitarbeiter über die Notwendigkeit überzeugt werden. Hier gibt es oft das selbe Problem wie bei der Führungsebene, so lange ein System funktioniert wird nicht über Absicherungsmaßnahmen nachgedacht. Die Festlegung der Notwendigkeit dieser Methodik in den Köpfen von Mitarbeitern wird unter dem Namen Bewusstseinsbildung zusammengefasst.

5.2. Ablauf

In diesem Abschnitt wird beschrieben, wie die Einführung von Disaster Recovery Maßnahmen in einem Unternehmen funktioniert, besonderer Stellenwert wird auf die chronologische Reihenfolge der Maßnahmen gelegt. Es werden jene Maßnahmen definiert, welche für eine erfolgreiche Abhandlung eines unvorhersehbaren Ereignisses durchzuführen sind. Die wichtigsten Maßnahmen beziehungsweise Teilgebiete sind: Vorfall-Enddeckung und Meldung über den Vorfall, Bewertung des Vorfalls, Eingrenzung, Auslöschung, Wiederherstellung und die Folgemaßnahmen. Die folgende Abbildung zeigt diese chronologische Abhandlung eines Schadensfalls, die genaue Definition der einzelnen Teilgebiete folgt im Anschluss der Abbildung. Eine wichtige Quelle für dieses Kapitel stellt die Ausarbeitung „Responding to a costumers security incidents – part 2: Executing a policy.“ [Masu03] dar.

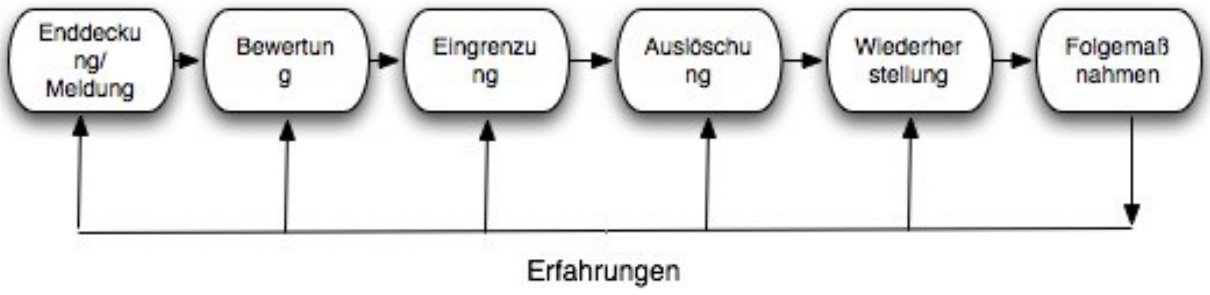

Abbildung 12, Phasen Disaster-Recovery-Prozess. Quelle: : [Masu03], eigene Darstellung.

5.2.1. Vorfall-Enddeckung und Meldung über den Vorfall

Diese Phase behandelt den Zeitraum zwischen der Enddeckung eines Vorfalls und der dazugehörigen Meldung. Wird ein Vorfall entdeckt, so muss dieser Vorfall sofort an die zuständige Stelle gemeldet werden. Diese Meldung kann von jedem Mitarbeiter ausgehen,

die zuständige Stelle sollte jeden Mitarbeiter im Unternehmen bekannt sein beziehungsweise sollten die Mitarbeiter wissen, wo die zuständigen Personen zu finden sind. Diese Situation kann durch einen Zuständigkeitsplan erreicht werden. Eine effiziente Möglichkeit für die Vorfallmeldung sind Formulare im firmeninteren Intranet, mit diesen Formularen wird eine strukturierte Bearbeitung der zuständigen Person erfolgen. Diese Formulare werden jedoch nicht eingesetzt, wenn der Vorfall nach einer schnellen Reaktion verlangt. Für diese Form ist die zuständige Person direkt zu kontaktieren, zum Beispiel persönlich oder über Telefon etc.

5.2.2. Bewertung des Vorfalls

Diese Phase beschreibt die Einschätzung der Auswirkungen eines Vorfalls durch eine zuständige Person/Stelle. Nachdem die Meldung die verantwortliche Stelle erreicht hat, kann diese Person oder Gruppe eine Bewertung des Vorfalls durchführen. Dabei kann grob eingeschätzt werden, welche mögliche Auswirkungen der Vorfall für das Unternehmen hat. Dem Verantwortlichen stehen dabei verschiedene Methoden zur Verfügung, wie zum Beispiel die eigene Erfahrung in diesem Gebiet, eine Datenbank über vergangene Vorfälle, Fachliteratur etc. Mit dieser Bewertung kann auch eine Priorisierung für die Abhandlung des Vorfalls stattfinden. Sehr bedrohliche Vorfälle werden also höher bewertet als wenig- beziehungsweise nicht-bedrohliche Vorfälle. Es wird auch immer wieder „falsche Alarme“ geben. Diese Alarme werden durch die Kenntnisse des Verantwortlichen schnell identifiziert werden, eine weitere Quelle für die schnelle Identifizierung sind Listen mit typischen Symptomen von falschen Alarmen. Bei der Bewertung des Vorfalls wird es auch eine Rolle spielen, wer die Meldung eingebracht hat. Einige Quellen werden als sehr kompetent betrachtet werden, Meldungen von anderen Quellen werden intensiver geprüft werden. Mitarbeiter müssen natürlich dazu ermutigt werden Meldungen zu verfassen, wenn sie eine bedrohliche Situation entdecken. Das bedeutet, dass Mitarbeiter auf dieses Thema sensibilisiert werden.

5.2.3. Eingrenzung des Vorfalls

In dieser Phase, Eingrenzung des Vorfalls, wird diagnostiziert, welche Bereiche eines Systems betroffen sind. Nachdem die Bewertung des Vorfalls stattgefunden hat ist zu bestimmen, welches System beziehungsweise welche Teile eines Systems betroffen sind. Erst eine genaue Eingrenzung stellt klar, wo sich das Problem konkret befindet. Erfolgte eine Einstufung eines Vorfalls als sehr kritisch, so kann eine Abschaltung eines betroffenen Systems beziehungsweise eines Teiles des Systems eine Lösung darstellen. Für die Identifikation dieses Teilsystems ist eine genaue Eingrenzung erforderlich. Der normale Betrieb muss so weit wie möglich erhalten werden und es darf keine negativen Auswirkungen auf die gesamte Systemleistung haben. Mit verschiedenen Tools, siehe Kapitel 3.8. Disaster Recovery Tools, ist eine sehr gute Wiederaufnahme ohne Beeinflussung der restlichen Prozesse möglich.

Sehr wichtig ist auch die Fragestellung, welche Absicht steckt hinter einem Vorfall beziehungsweise hinter einem vermeintlichen Angriff. Wird ein Vorfall als Angriff

eingestuft/identifiziert, so wird dieser Vorfall mit einer höheren Priorität behandelt. Diese höhere Priorität bedeutet, dass dieser Vorfall sehr schnell behandelt wird und es werden außerdem größere Ressourcen für die Beseitigung des Vorfalls eingesetzt. Die angesprochenen Ressourcen können dabei zum Beispiel eingesetzte Mitarbeiter sein oder auch der Einsatz von finanziellen Ressourcen. Bei einer Einstufung eines Vorfalls als Angriff, werden auch störende Maßnahmen für die Geschäftsabwicklung wie Abschaltung von einem (Teil-)System vermehrt stattfinden. Wenn diese Frage geklärt ist, können die notwendigen Maßnahmen eingeleitet werden. Diese Maßnahmen umfassen dabei nicht nur das direkt betroffene (Teil-)System, sondern das gesamte Unternehmen. Wenn der Zusammenhang abgeklärt ist kann beurteilt werden, ob Beispiel ein Angriff auf die Lahmlegung eines gesamten Unternehmens abzielte oder ob versucht wurde, unternehmenskritische Daten auszulesen. Je nach Zusammenhang werden unterschiedliche Maßnahmen gesetzt. Diese Absicht wird durch unterschiedliche Fragestellungen geklärt.

5.2.4. Auslöschung/Bereinigung des Vorfalls

Diese Phase behandelt die Wiederherstellung des ursprünglichen Zustands eines Systems – d.h. vor Eintritt eines Vorfalls. Es werden also alle notwendigen Maßnahmen gesetzt, um die Systeme komplett vom Schadensfall zu befreien und den ursprünglichen Zustand wieder herstellen. Für diese Herstellung des ursprünglichen Zustands stehen verschiedene Tools zur Verfügung, welche auch präventiv eingesetzt werden können.

Auch im Falle eines bereits vorhandenen Schadensfalls gibt es unterschiedliche Software-Lösungen, welche eine effiziente Abhandlung ermöglichen. Die Verantwortlichen müssen sich pro aktiv mit den Lösungen auseinander setzen. Welche Software eingesetzt wird, lässt sich nur von Fall zu Fall beantworten – auch die Kenntnisse der Verantwortlichen spielen eine große Rolle.

5.2.5. Wiederherstellung des Systems

Nachdem das System vom Vorfall bereinigt worden ist, erfolgt die Wiederherstellung des Systems. Es werden alle Komponenten nach aktuellen Richtlinien wiederhergestellt und somit wird das System optimiert. Das System wird zumindest wieder auf Normalzustand (Zustand vor einem Schadensfall) gebracht. Um eine schnelle und effiziente Wiederherstellung zu ermöglichen, werden vorgefertigte Checklisten verwendet. Mit diesen Checklisten hat der Verantwortliche schnell einen Überblick, welche Maßnahmen einzuleiten sind. Ist ein kritischer Vorfall gegeben, so sind die Entscheidungen innerhalb von Minuten notwendig. Durch diese schnelle Vorgehensweise wird verhindert, dass sich der Schaden weiter ausbreitet und damit noch mehr Schaden anrichten kann.

Diese Checklisten werden auf verschiedene Vorfälle optimiert beziehungsweise vorgefertigt und ermöglichen dadurch schnelle und gute Entscheidungen bezogen auf den jeweiligen Schadensfall. Diese Checklisten werden akribisch vorbereitet und ständig aktualisiert. Möglich. Weiters ist es wichtig, dass zuständige Mitarbeiter wissen, wo sich

diese Checklisten befinden. Die folgende Abbildung zeigt eine beispielhafte Anwendung einer Checkliste.

Schadensfall Antwort und Festlegung Checkliste

Status
Seite unter Angriff

Kontaktinformationen
Name: Titel:
Organisation:
Telephon: Email:
Kontaktname: Telefon:
Ort/Seiten involviert:
Straße
Stadt: Provinz: Land:

Welche Form hat der Notfall (alle ankreuzen welche zutreffen)
Denial of service attack he Bewachung
Netzwerk Einbruch
Schadhafter Code (Virus, Trojaner, Wurm)
Website Defacement
Anderes (bitte erklären):

Datum: Zeit:

Dauer des Angriffs:

Wirkung des Angriffs
Verlust oder Gefährdung von Geschäftsdaten?
Ja

System Down-Zeit:
Schaden der Systeme:
Finanzieller Verlust (geschätzter Verlust):
Schaden an Integrität oder Lieferbarkeit von kritischen Gütern, Services, oder Information
Andere betroffene Organisationssysteme:

Ausmaß/Stärke des Angriffs (inkl. Finanzieller Verlust): klein

Hat der Angreifer Root-, Administrator- oder System-Zugriff?

Wie wurde der Vorfall bemerkt?

Intrusion Detection System oder Audit logs
Externe Beschwerde
User Report
Anderes:

Was sind die bekannten Symptome:

Welche Geschäftsbereiche sind betroffen: (so viel Information wie möglich über Systeme, inkl. verdächtigte Systeme, Plattformen, Applikationen, IP-Adressen, betroffene oder verdächtige User-ID´s, vor kurzen durchgeführte Änderungen)

Sind die Systeme immer noch am firmeninternen Netzwerk angeschlossen?
Ja

Sind die Systeme immer noch am Internet angeschlossen? (Abschließen wenn möglich)
Ja

Sind die Backups von den betroffenen Systemen verfügbar? (Alle Informationen bezüglich online, onsite oder offsite backups)
Ja, Informationen:
Nein

Sind die betroffenen Systeme immer noch risikoanfällig oder angriffsbedroht? (Mögliches Abschließen der Systeme oder Sicherung der Konten wenn möglich)
Ja

Wird das System möglicherweise eine forensische Untersuchung benötigen? (Abschalten und Sicherung des Systems für forensische Bestandsaufnahme).
Ja

Abbildung 13, Checkliste für den Schadensfall. Quelle: [Masu03], eigene Darstellung.

Abbildung 13 zeigt eine beispielhafte Checkliste für einen Schadensfall. Mit dieser Checkliste kann die zuständige Person jene Eigenschaften auswählen, welche auf einen aktuellen Angriff zutreffen. Mit einer einer Auswertung kann sehr schnell identifiziert werden, welche Maßnahmen zur Behandlung des Schadensfalls am besten geeignet sind. Die Auswertung wird schnell erfolgen, um weiteren Schaden zu verhindern und um eine rasche Reaktion zu ermöglichen.

5.2.6. Nachfolgeaktionen des Vorfalls (follow up)

Auch wenn alle Maßnahmen zur Bereinigung bereits getätigt wurden, ist der Prozess noch nicht abgeschlossen. Durch eine Dokumentation kann zum Beispiel festgelegt werden wie zu reagieren ist, sollte ein gleicher beziehungsweise ein ähnlicher Vorfall noch einmal auftreten. Diese Dokumentation kann in eine zentrale Datenbank gespeichert werden und bei einem Vorfall wird darauf zugegriffen.

Diese sechs Maßnahmen sind nötig, um möglichst schnell und effizient auf einen Schadensfall reagieren zu können. Die Geschäftsprozesse werden dadurch minimal belastet. Jeder Schadensfall ist einzigartig, jedoch können die Erkenntnisse eines Schadensfalls auf andere Fälle angewendet werden. Eine gute Dokumentation über die Behandlung eines Falles ist dabei sehr wichtig. Die folgende Tabelle bietet einen Überblick der Eigenschaften der verschiedenen Phasen.

Phase	Aufgaben/Eigenschaften
Enddeckung/Meldung	Meldung an die zuständige Stelle, Zuständigkeiten müssen bekannt sein
Bewertung	Verantwortlichen führen Bewertung des Vorfalles durch, Priorisierung von Vorfällen,
Eingrenzung	genaue Festlegung des Schadens, Definition der Absicht
Auslöschung	Maßnahmen zur Bereinigung des Vorfalls werden eingeleitet, Einsatz von Tools
Wiederherstellung	System wird wieder auf Normalzustand gebracht oder verbessert, Einsatz von Checklisten zur schnellen Abhandlung
Folgemaßnahmen	Erstellung einer Dokumentation über den Schadensfall, Festlegung von Kriterien für eine effiziente Abhandlung

Tabelle 12, Beschreibung der Phasen Disaster-Recovery-Prozess.

5.3. CSIRT´s

Ein Notfall Team (CSIRT = computer security incident response team) ist damit beauftragt, Meldungen über Schadensfälle zu erhalten und dann entsprechend darauf zu reagieren. Dieses Team ist für einen bestimmten Teil eines IT-Systems oder für die gesamte IT-Organisation eines Unternehmens zuständig. Dieses Team kann formell oder informell bestehen – informell bedeutet, dass die Mitglieder eines Teams im Schadensfall kontaktiert werden und dann die Zusammenarbeit beginne. Dieses Team besteht also nicht ständig, es wird nur im konkreten Schadensfall eingesetzt.

5.4. Notfallplan

Tritt ein unerwartetes Ereignis in einem Unternehmen auf welche die IT-Systeme betreffen, ist es zu spät, sich mit solchen Ereignissen zu beschäftigen. Diese Planung muss in Zeiten passieren, wo es keine Probleme mit den Systemen gibt und wo ein normaler Arbeitsablauf stattfindet. Wenn das System normal arbeitet ist es jedoch sehr schwierig,

Mitarbeiter für die Planung von Notfällen zu motivieren. Erst wenn eine Bewusstseinsbildung im Unternehmen eingeführt wurde, werden sich Mitarbeiter kooperativ verhalten. Diese Bewusstseinsbildung wird zusammen mit den entsprechenden Anweisungen der Führungsebene eine Etablierung von Notfallplänen ermöglichen. Es gibt keinen Notfallplan, welcher in allen Unternehmen eingesetzt werden kann. Für eine einheitliche Umsetzung sind die aktuellen IT-Systeme und Applikationen zu komplex. Es ist notwendig, die einzelnen Mitarbeiter in den Gestaltungsprozess eines Notfallplans mit einzubeziehen. Die Arbeitsweise von Mitarbeitern unterscheidet sich oft gravierend zwischen Unternehmen beziehungsweise zwischen verschiedenen Abteilungen innerhalb eines Unternehmens. Ein wichtige Quelle für dieses Kapitel ist das Buch „Backup und Disaster Recovery“ von Egbert Wald [Wald02].

Bei der erstmaligen Erstellung eines Notfallplans können typischerweise folgende Phasen unterschieden werden:

- Bewusstseinsbildung im Unternehmen: Die Mitarbeiter werden von der Wichtigkeit überzeugt und zur Mitarbeit „gezwungen“, die Notfallplanung wird zur Chefsache erklärt.

- Vorbereitende Phase: In dieser Phase wird ein Projektteam zusammengestellt, verschiedene Meetings werden abgehalten, die wichtigsten Rollen werden definiert.

- Zusammenstellung von wichtigen Daten: In dieser Phase ist es vor allem wichtig, Richtlinien für die Dokumentation der wichtigen Daten festzulegen.

- Analyse des Risikos: In dieser Phase wird eingeschätzt, wie hoch ein eventueller Schaden ausfallen kann, Priorisierung von Aufgaben.

5.4.1. Bewusstseinsbildung im Unternehmen

Diese Bewusstseinsbildung im Unternehmen ist vor allem wichtig um Mitarbeiter im Unternehmen zu überzeugen, wie wichtig die Maßnahmen des Disaster-Recory´s sind. Diese Überzeugungsarbeit muss bei allen Mitarbeitern geleistet werden, angefangen von der Führungsebene bis zur Reinigungskraft eines Unternehmens. Erst wenn alle Mitarbeiter eines Unternehmens von der Notwendigkeit der Maßnahmen überzeugt sind, wird einer Etablierung dieser Methode nichts im Wege stehen.

5.4.2. Vorbereitende Phase

In dieser Phase werden alle Planungsmaßnahmen für eine erfolgreiche Umsetzung eines effizienten Disaster-Recovery´s getroffen. Ein Notfallplan ist von Unternehmen zu Unternehmen verschieden, es gibt jedoch Gemeinsamkeiten der unterschiedlichen Pläne. Folgende Gemeinsamkeiten werden in fast allen Notfallplänen zu finden sein:

- Auftrag zur Schaffung eines Notfallplans
- Informationsbeschaffung zu den verschiedenen Geschäftsprozessen im Unternehmen
- Bestandsaufnahme der aktuell vorhandenen Infrastruktur im Unternehmen
- Analyse der gewonnen Informationen
- Durchführung einer Risikoanlyse aufgrund der Informationen
- Planung von Strategien zur Reaktion auf unvorhersehbare Ereignisse
- Planung von Vorbeugemaßnahmen
- Planung eines unternehmensweiten Backup-Systems
- Bestimmung von Notfallübungen
- Tests der Notfallübungen
- Planung der Aktualisierungen der Tests

In der vorbereitenden Phase ist auch die Zusammenstellung eines Projektteams vorgesehen. Dieses Projektteam ist erforderlich, um die vorher definierten Ziele zu erreichen, das Projektteam besteht auf folgenden Mitgliedern :

- Projektmanager: Diese Person ist zuständig für die Gesamtleitung des Projektes. Zu den Aufgaben dieser Rolle fallen die Zeitplanung, die Koordination mit der Führungsebene und die Kontrolle über die korrekte und zeitgerechte Umsetzung des Projektes.

- Netzwerkadministrator: Diese Person muss ausgezeichnete Kenntnisse über das Netzwerk haben, welches im Unternehmen eingesetzt wird.

- Datenbankadministrator: Diese Rolle muss umfassende Informationen über die eingesetzten Datenbanksysteme haben. Diese Rolle ist sehr wichtig für die Planung eines effizienten Backup-Systems.

- Benutzerservices-Leiter: Diese Person/Rolle muss gut über die Abläufe im Benutzerservice informiert sein. Hier ist vor allem wichtig, dass die Bedürfnisse der Anwender bekannt sind.

- Consultant: Diese Personen werden eingesetzt, da sie in der Regel bereits viel Erfahrung bei anderen, ähnlichen Projekten sammeln konnten.

Ein wichtiger Erfolgsfaktor für das Gelingen eines Projektes der Einführung eines Notfallplans ist die Unterstützung durch die Führungsebene. Diese Personen werden im positiven Fall die erforderlichen Ressourcen, finanzieller als auch humaner Art, zur Verfügung stellen. Ein weiterer wichtiger Faktor ist die Priorität der Umsetzung für die Teammitglieder. Nur wenn dieses Projekt eine hohe Priorität besitzt, wird eine erfolgreiche Umsetzung möglich sein. Wichtig ist es auch, dass eine offene Kommunikation zwischen

den Teammitgliedern besteht. Behalten einzelne Personen wichtige Informationen für sich, ist ein Scheitern vorprogrammiert. Ein weiterer Erfolgsfaktor ist auch die Einbeziehung der zukünftigen Benutzer. Durch diese Maßnahme ist es möglich, viele Vorbehalte gegenüber Änderungen zu eliminieren.

Nachdem die einzelnen Personen für das Projektteam bestimmt sind, kann ein Meeting zur genauen Klärung der einzelnen Zuständigkeiten/Aufgaben abgehalten werden. In diesem Meeting werden die wichtigsten Eckdaten des Projektes bestimmt. Unter diesen Eckdaten fallen unter anderen die Schwerpunkte des Projektes, die Aufgaben des Teams, die konkreten Aufgabenbereiche der einzelnen Personen und vor allem ein festgelegter Zeitplan. Die Leiter des Projektes setzen auch gerne Tools für die Umsetzung von Notfallplänen ein, die Möglichkeiten beziehungsweise die Einschränkungen werden im Kapitel 3.8. Disaster Recovery Tools definiert. Die folgende Gliederung fasst die wichtigsten Aufgaben dieser Phase zusammen.

- Entwicklung eines durchdachten und umfassenden Projektplans
- Festlegung der wichtigsten zu erreichenden Abschnitte als so genannte Meilensteine
- Zusammenstellung eines funktionierenden Teams
- Management steht hinter dem Projekt und unterstützt die Vorhaben
- Erstes Meeting nach der Zusammenstellung

5.4.3. Zusammenstellung von wichtigen Daten

Für die Erstellung eines Notfallplans ist eine Zusammenstellung von wichtigen Daten notwendig. Diese Zusammenstellung der wichtigen, d.h. jene Daten welche für eine Umsetzung notwendig sind, kann durch folgende Richtlinien erfolgen.

- Dokumentation sollte kurz, klar und verständlich gestaltet werden
- Dokumentation sollte in einfacher Sprache abgefasst werden, auch Nicht-Experten sollten sie ohne Probleme verstehen können
- Verwendete Abkürzungen sollen in einem Abkürzungsverzeichnis zusammengefasst werden
- Die Dokumentation sollte in verschiedenen Bereiche unterteilt sein
- Richtlinien für die Verfassung der wichtigen Informationen
- Unmittelbare Erfassung von Änderungen in der Dokumentation

Werden diese Richtlinien eingehalten, so ist eine Reaktion auf einen Vorfall möglich. Eine unstrukturierte, unregelmäßige Dokumentation führt genau zum Gegenteil. In großen Unternehmen gibt es viele verschiedene Abteilungen. Wenn eine Notfallplanung durchgeführt wird, so benötigt man die Informationen aller Abteilungen. Diese Informationen kann man ebenfalls durch vorgefertigte Formulare erhalten. Es gibt jedoch das Problem, dass bei vielen Abteilungen nur wenig beziehungsweise kein technisches

Know-How besteht. Die Mitglieder der Abteilungen wissen zwar wie die einzelnen Geschäftsprozesse ablaufen und wie man dafür das IT-System verwendet, sie wissen jedoch nicht welche Technik genau hinter den Abläufen steckt. Um diesen Mangel an technischen Know-How auszugleichen, sollte für die Erfassung der wichtigen Geschäftsabläufe ein Mitarbeiter der IT-Abteilung eingesetzt werden. Dieser Mitarbeiter wird Angaben der Mitarbeiter der verschiedenen Abteilungen in technische Sprache „übersetzen“. Diese Fragebögen, welche für die Erfassung sämtlicher mit IT-Technologien im Zusammenhang stehende Komponenten werden für jeden Teilbereich anders aussehen, es gibt jedoch folgende Gemeinsamkeiten:

- Überschrift „Notfallplanung“
- Datum der Erfassung
- Person welche die Angaben macht, zum Beispiel Abteilungsleiter etc.
- Name der Abteilung und Telefonnummer der Abteilung
- Genaue Anschrift der Abteilung
- Feld für die Bestätigung durch den Abteilungsleiter - wenn nicht Abteilungsleiter selbst die Angaben macht
- Beschreibung der genauen Aufgabe, zum Beispiel detaillierte Beschreibung der Arbeitsabläufe
- Anschrift und Telefonnummer des Teams der Notfallplanung und Projektmanagers
- Feld für die aktuelle Versionsnummer

Mit diesen Bestandteilen ist eine Erfassung von Informationen der verschiedenen Abteilungen und im speziellen den Aufgaben dieser Abteilungen möglich. Für ein umfassendes Erfassen der im Zusammenhang stehenden Komponenten eines IT-Systems werden unter anderen folgende Aufgabenstellungen für die Abteilungsleiter beziehungsweise für die befähigten Personen auf den Fragebögen auszufüllen sein:

- Genaue Darstellung/Beschreibung der Geschäftsprozesse. Hier wird von den zuständigen Personen verlangt, dass sie Angaben über die benötigten Ressourcen anführen. Unter diese Ressourcen fällt unter anderen die Vernetzung zu anderen Abteilungen. Weiters sollen bereits vorhandene Dokumentationen wie Arbeitsabläufe, Handbücher etc. dem Projektteam zur Verfügung gestellt werden.

- Ausstattung des Arbeitsplatzes. Hier sollen alle Komponenten angeführt werden, welche zur Erledigung der anfallenden Aufgaben in einer Abteilung am Arbeitsplatz benötigt werden. Diese Komponenten können Computer, Telefone oder auch Drucker sein. Weiters ist es auch erforderlich, Informationen über vorhandene Datenträger zu erhalten – zum Beispiel welche Datenträger werden verwendet und wo werden diese Datenträger aufbewahrt.

- Bewertung von Ausfällen. Dieser Teil ist sehr wichtig für die Notfallplanung, die Einschätzung gestaltet sich in der Regel sehr schwierig. Hier wird von den

zuständigen Personen verlangt, Kosten im Falle eines möglichen Ausfalls eines (Teil-)Systems zu einzuschätzen. Es werden jedoch nicht nur die direkten finanziellen Schäden betrachtet, sondern auch die Schäden welche indirekt finanziellen Schaden für das Unternehmen anrichten. Zu diesen indirekten Schäden kann man zum Beispiel Imageverlust, Serviceausfall oder im schlimmsten Fall Aufgabe der Geschäftstätigkeit zählen. Bei diesem Fragebogen wird in abgestufter Form erfasst, welchen Schaden ein Ausfall eines Systems auf die Abteilung hat. Diese Abstufungen werden in „kein Schaden“, „geringer Schaden“ oder „hoher Schaden“ eingestuft.

- Bereits vorhandene Notfallpläne. Hier werden die Abteilungen befragt, welche Notfallpläne bereits existieren. Es werden Angaben über die Art der Datensicherung (automatische Prozeduren etc.) und über den Ort der Aufbewahrung der Datensicherungen verlangt. Ein weiterer Abschnitt behandelt die gesetzlichen Vorschriften für die Aufbewahrung der Daten. In vielen Fällen gibt es explizite Vorschriften, wie gewissen Daten aufzubewahren sind - zum Beispiel Aufbewahrung außerhalb der Arbeitsräume. Weiters wird auch die Frage gestellt, welche Sicherheitseinrichtungen wie zum Beispiel Feuerlöscher etc. in einer Abteilung vorhanden sind. Weitere Angaben sind zu der Versicherungsart im Schadensfall zu treffen. Außerdem werden auch die Maßnahmenpläne für einen Notfall in einer Abteilung abgefragt.

Es gibt noch eine große Anzahl von möglichen Fragebögen, welche von Unternehmen zu Unternehmen verschieden gestaltet werden. Die Auswertung wird, zumindest in größeren Unternehmen, durch Datenbanken erfolgen. Durch die Gestaltung einer Datenbank mit diesen wichtigen Informationen können in einfacher Art und Weise Abfragen für die Bestimmung wichtiger Zusammenhänge etc. gestaltet werden. Die folgende Gliederung zeigt noch einmal, welche Daten für diese Phase notwendig sind.

- Ausgefüllte Fragebögen
- Zusätzliche Information durch Gespräche von IT-Mitarbeitern mit Abteilungsleiter bzw. mit beauftragten Personen
- Darstellung der Geschäftsprozesse
- Auflistung der bereits vorhandenen Notfallpläne
- Mögliche Meldungswege im Falle eines Notfalls
- Auflistung der vorhandenen Infrastruktur im Hardware- und im Softwarebereich
- Auflistung der aktuellen Mitarbeiter

Im weiteren Verlauf muss geprüft werden, ob die getroffenen Angaben der Wahrheit entsprechen. Durch stichprobenartige Überprüfung kann zumindest der Fehleranteil verringert werden.

5.4.4. Analyse des Risikos

Bei der Analyse des Risikos geht es um die schwierige Aufgabe, Bedrohungen richtig einzuschätzen und den möglicherweise resultierenden Schaden zu identifizieren. Dieser Schaden kann wieder finanzieller oder nicht-finanzieller Natur sein. Bei der Analyse des Risikos geht man von folgenden Risiken aus:

- Fehler bei der Hardware
- Fehler bei der Software
- Zusammenbrechen der Infrastruktur
- Schaden durch Feuer
- Schaden durch Wasser
- Schaden durch Sturm
- Schaden durch Sabotage/Terror
- Schaden durch Unfälle verschiedenster Art

Die möglichen Risiken müssen in einer realitätsnahen Art und Weise eingeschätzt werden. Übertriebene Annahmen sowie Unterschätzung von Risiken werden vermieden, bei einer guten Zusammensetzung des Notfallteams wird eine realistische Einschätzung möglich sein. Bei den möglichen Schadensfällen kann zwischen zwei Arten unterschieden werden: Totalausfall eines Systems und teilweiser Ausfall eines Systems. Bei einem Totalausfall sind sämtliche Komponenten eines Systems auszutauschen, bei einem Teilausfall können die fehlerhaften Teile repariert werden. Bei einem Totalausfall kann man bei den zu erwartenden Schaden nicht davon ausgehen, dass die Summierung der Wiederherstellungskosten den Schaden beziffert. Man muss beachten, dass bei einem Totalausfall keine Geschäftsprozesse mehr stattfinden können und somit kein Umsatz erzielt werden kann. Bei einem Teilausfall reicht es ebenfalls nicht aus, nur die Kosten für die Reparatur zu betrachten. Viele Geschäftsabläufe sind untereinander stark vernetzt, so kann zum Beispiel eine Abteilung erst dann arbeiten, wenn sie einen Input von einer anderen Abteilung erhält.

Es gibt einige Unternehmensformen, wo Ausfälle besonders kritisch sind. Solche Unternehmen sind zum Beispiel Betriebe, wo häufig „just in time“-produziert wird. Bei der Einschätzung von Schadensfällen kann man nicht auf die dokumentierten Schadensfälle von früher zurückgreifen, Unternehmen gehen mit Schadensfällen nicht gerne an die Öffentlichkeit. Deswegen ist es um so wichtiger, erfahrene Mitarbeiter zu befragen oder externe Consultants einzusetzen. Es muss ein ausgeglichenes Verhältnis zwischen den Kosten für Schutzmaßnahmen und für das Sicherheitsmaß gefunden werden. Sind die Kosten für Schutzmaßnahmen zu hoch, so wird sich das Management gegen diese Maßnahmen entscheiden. Ist das Maß an Sicherheit sehr gering, so sind hohe Verluste zu erwarten. Die folgende Graphik visualisiert das optimale Kosten-/Nutzenverhältnis.

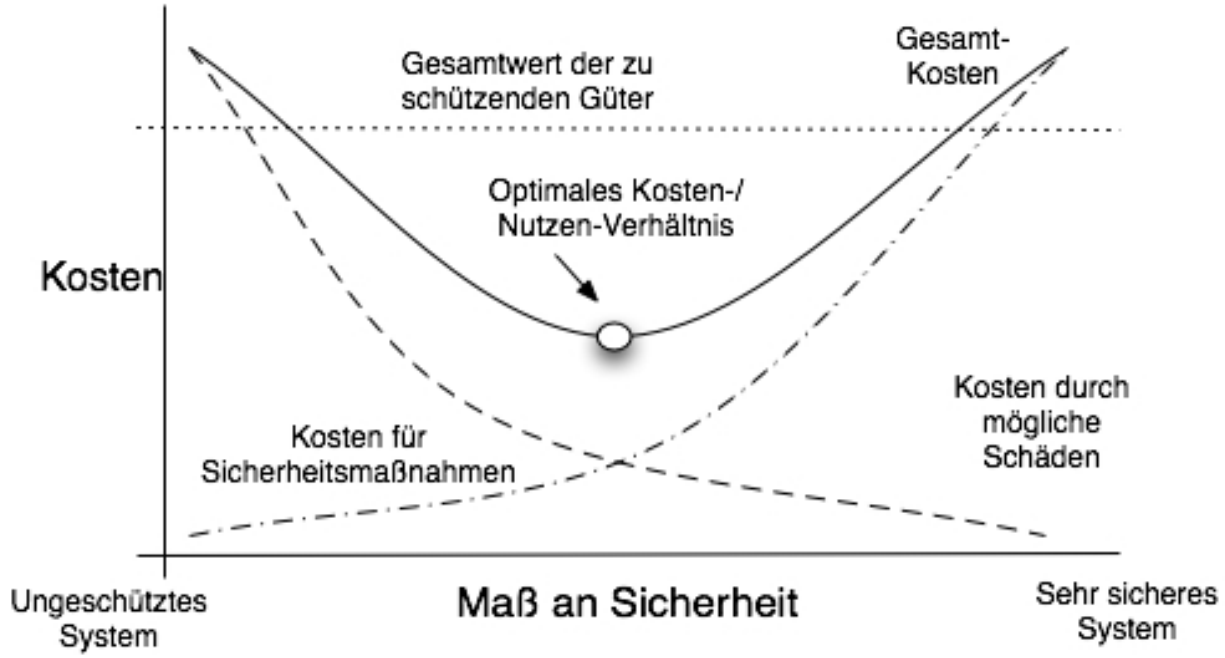

Abbildung 14, Optimales Kosten-/Nutzenverhältnis . Quelle: [Wald02], eigene Darstellung.

Die folgende Tabelle bietet eine Zusammenfassung der wichtigsten Eigenschaften der einzelnen Phasen für die Erstellung eines Notfallplans.

Phase	Aufgaben
Bewusstseinsbildung	Überzeugungsarbeit bei den Mitarbeitern und in der Führungsebene, Mögliche Weisungen der Führungsebene
Vorbereitende Phase	Zusammenstellung Projektteam, Alle notwendigen Informationen über das Unternehmen werden eingeholt, Entwicklung Projektplan, Festlegung von Meilensteinen
Zusammenstellung der wichtigsten Daten	Erstellung von Formularen für die Aufstellung der wichtigsten Informationen, Ausfüllen der Formulare durch befugte Personen der einzelnen Abteilungen, Stichprobenartige Überprüfung der Richtigkeit der Angaben
Analyse Risiko	Einschätzung des Risikos, Identifikation des möglichen Schaden, Einsatz von Kosten-/Nutzenverfahrens um optimale Ausprägung zu finden

Tabelle 13, Phasen Erstellung Notfallplan

5.5. Übungen für den Notfall

Auch die beste Notfallplanung hat keinen Nutzen für ein Unternehmen, wenn die Notfallpläne nicht trainiert werden beziehungsweise an die veränderten Eigenschaften eines Unternehmens angepasst werden. Zu möglichen veränderten Eigenschaften zählen Veränderungen in der IT-Infrastruktur oder der veränderte Einsatz von Anwendungsapplikationen. Die Übungen für den Notfall müssen nach einem Zeitplan stattfinden, um Aktualität zu gewährleisten. Weiters muss auch berücksichtigt werden,

dass immer wieder neue Mitarbeiter im Unternehmen beschäftigt werden. Die folgende Gliederung beschreibt notwendige Maßnahmen für Notfallübungen.

- Programm für die Übungen: Um ein Programm für die Übung von Notfallplänen zu erstellen, gibt es zwei Möglichkeiten. Eine Möglichkeit ist dass jene Personen das Programm zusammenstellen, welche auch für die Erstellung des Notfallhandbuches verantwortlich waren. Eine andere Möglichkeit ist der Einsatz von externen Beratern, welche für die Planung eines Programms eingesetzt werden. Beide Varianten haben Vor- und Nachteile, für die interne Lösung spricht das bereits vorhandene Wissen über das System im Unternehmen. Für externe Berater spricht eine höhere Objektivität und die höhere Erfahrung in diesem konkreten Einsatzgebiet. Zu Beginn des Projektes der Erstellung eines Programms für Übungen im Notfall wird die Erstellung eines Trainingsplans stehen. Mit diesem Plan werden nicht nur die zu trainierenden Abläufe beschrieben, sondern es wird auch beschrieben wie die Übermittlung des Lehrstoffes stattfindet. In der praktischen Anwendung wird sehr oft das Modell „Instructional Systems Design“ (ISD) eingesetzt.

- Häufigkeit von Notfallübungen: Hier stellt sich die Frage, wie oft es nötig ist, einen Notfall zu planen beziehungsweise eine Simulation von Notfällen durchzuführen. Gibt es zu wenige Übungen, so sind die Pläne nicht mehr auf dem aktuellen Stand und damit nicht wirkungsvoll. Diese Notfallübungen werden nicht zu häufig durchgeführt, die Kosten der Übungen durch entgangene Arbeitszeit etc. spricht gegen eine häufige Durchführung. In der Praxis hat sich vor allem eine Methode durchgesetzt. Diese Methode beinhaltet den Leitsatz, dass bei einer Ersterstellung eines Notfallplans sieben Tests innerhalb von drei Jahren durchgeführt werden sollen. Im konkreten Fall soll diese Methode wie folgt durchgeführt werden:Im ersten Jahr müssen 3 Einzeltests durchgeführt werden, diese Einzeltests umfassen dabei das Rechenzentrum, die Infrastruktur des Netzwerkes und die unternehmenskritischen Geschäftsprozesse. Durch diese Tests wird eine Verbesserung der Notfallpläne gewährleistet. Das zweite Jahr umfasst zwei Tests, der erste Test stellt eine komprimierte Wiederholung der Tests aus dem ersten Jahr dar. Hier wird getestet, ob die vorgeschlagenen Änderungen tatsächlich Verbesserungen darstellen. Der zweite Test zielt auf die Backup-Prozesse eines Unternehmens ab. Es wird auf Testrechnern ausprobiert, wie lange eine Wiederherstellung von Applikationen dauert. Das dritte Jahr beinhaltet wieder zwei Tests, der erste Test umfasst einen unternehmenskritschen Prozess, welcher unter einer extremen Belastungssituation getestet wird. Unter einer extremen Belastungssituation versteht man hier, dass die Netzwerke überdurchschnittlich stark ausgelastet werden - wie zum Beispiel bei einem Jahresabschluss. Der zweite Test umfasst eine ganzheitliche Simulation eines Katastrophenfalls. Es werden sämtliche Recovery-Szenarien durchgespielt, dadurch ist dieser Test sehr

ressourcenaufwändig. Die folgende Tabelle beschreibt die Anzahl und die Maßnahmen der Tests.

Zeit	Anzahl Tests	Maßnahmen
1. Jahr	3	Überprüfung Rechenzentrum, Netzwerkinfrastruktur und unternehmenskritische Geschäftsprozesse
2. Jahr	2	Wiederholung des Tests aus dem 1. Jahr Überprüfung Backup-Prozesse
3. Jahr	2	Überprüfung eines unternehmenskritischen Geschäftsprozess unter Extrembedingung Ganzheitliche Simulation eines Katastrophenfalls

Tabelle 14, Häufigkeit und Maßnahmen von Notfalltests

- Zeitliche Planung der Tests: Die Tests werden durchgeführt, um gewisse Ziele zu erreichen. Nur mit genau definierten Zielen ist es möglich festzustellen, ob die Tests ein Erfolg waren oder nicht. Die Zielvorgaben werden unterschiedlich gestaltet werden, so kann zum Beispiel eine Recovery-Aktion an einem Wochentag vor mittags viel kürzer zeitlich eingeplant werden, als wenn die Recovery-Aktion abends am Wochenende stattfindet. Da die Tests zeitaufwändig sind ist es wichtig, dass die Tests eine möglichst geringe Störung der üblichen Geschäftstätigkeit hervorrufen.

- Dokumentation der Notfallübungen: Bei der Dokumentation der Übungen hat es sich wieder als effizient herausgestellt, vorgefertigte Formulare zu verwenden. Zu Beginn soll auf einem Formular die Ziele festgehalten werden. Auf einem weiteren Formular sollen die einzelnen Ziele genau beschrieben werden. Eine Checkliste für die Vorbereitung eines Tests kann einige Zeit einsparen. Ein weiteres Formular wird für die Testbeobachtung benötigt, hier werden die gestellten Ziele und die Ergebnisse miteinander verglichen. Ein weiteres Formular wird für die Verfassung eines Abschlussberichtes benötigt. Dieses Dokument ist äußerst wichtig und wird dem Management vorgelegt. Eine gute Erweiterung des Abschlussberichtes ist das Formular der Testergebnisse, hier werden die Ergebnisse mit Empfehlungen versehen.

5.6. Verteilung von Kompetenzen

Für die Behandlung von Notfällen ist es notwendig, Zugang zu sensiblen Daten eines Unternehmens an bestimmte Personen zu erlauben. Diese sensible Daten, welche in den falschen Händen großen Schaden anrichten können, dürfen nur an autorisierte Personen verteilt werden. Bei einer möglichen Systemwiederherstellung gibt es das selbe Problem, sehr oft werden damit externe Unternehmen beauftragt. Diese Unternehmen werden auch Einsicht auf sensible Daten haben, hier ist eine rechtliche Absicherung erforderlich. Es gibt verschiedene Möglichkeiten, auf diese Situation zu reagieren. Im Normalbetrieb gibt es ebenfalls Einschränkungen, wer auf welche Daten zugreifen darf. Bei einem Notfall ist

jedoch eine gesonderte Zugangsregelung zu treffen. Zwei mögliche Methoden werden jetzt im konkreten Zusammenhang vorgestellt.

- Prinzip des letzten Privilegs: Alles was nicht ausdrücklich erlaubt ist, ist verboten. Zum Beispiel wird die Firewall so konfiguriert, dass nur die benötigten Services laufen. Weiters gibt es auch die physikalische Sicherheit, wie zum Beispiel bei der Verteilung von Schlüsseln zu Räumen in einem Betrieb.

- Abschottung von Information: Informationen sollten aufgrund der „need-to-know-Basis“ erreichbar sein und werden auch so verteilt. Diese Maßnahme bedeutet zum Beispiel, dass Mitglieder des Sicherheitsteams Informationen über die Sicherheitsprodukte eines Unternehmens erhalten. Das Sicherheitsteam benötigt diese Informationen, um die Arbeiten erledigen zu können. Die Mitglieder des Sicherheitsteams brauchen jedoch keine Informationen über persönliche Daten von Angestellten. Das bedeutet, dass Personen beziehungsweise Teams immer nur die Informationen erhalten, die sie unbedingt zur Erledigung der Arbeit benötigen. Andere Daten, welche nicht unmittelbar mit einer Arbeit verbunden sind werden nicht zur Verfügung gestellt. Durch diese Vorgehensweise wird ein möglichst sicherer Umgang mit Daten gewährleistet. Ein möglicher Datenmissbrauch wird stark eingegrenzt da es möglich ist einzusehen, wer zu welchen Daten Zugang hat und warum. Es können auch verschiedene Rechte vergeben werden, d.h. eine Person darf nur in gewisse Daten einsehen, während eine andere Person diese Daten auch bearbeiten darf.

Die folgende Tabelle fasst die Eigenschaften der beiden Methoden für den sicheren Umgang mit Daten im Unternehmen zusammen.

Methode	Eigenschaften
Prinzip des letzten Privilegs	Alles was nicht ausdrücklich erlaubt ist, ist verboten Festlegung physikalische Sicherheit
Abschottung von Information	Einsatz „need-to-know-Basis“ Vergabe von verschiedenen Rechten bei der Bearbeitung von Daten Nur wenn Daten benötigt werden, werden sie zur Verfügung gestellt

Tabelle 15, Methoden für den sicheren Umgang mit Daten

5.7. Netzwerk-Architektur

Die Technologien in einem Unternehmen für die Information und die Kommunikation sind stark untereinander vernetzt. Es gibt nur noch selten Technologieeinheiten, welche isoliert von anderen Einheiten arbeiten und nur selbst die Ressourcen nutzen. Es gibt natürlich auch eine negative Seite dieser Vernetzung – vor allem wird für die Sicherheit ein außerordentlich hoher Aufwand geleistet. Dieser Aufwand richtet sich gegen den drohenden Schaden, wenn ein Netzwerk durch einen Ausfall beziehungsweise durch

einen teilweisen Ausfall betroffen ist. Ein weiterer Angriffspunkt auf ein Netzwerk ist die zentralisierte Speicherung von kritischen Geschäftsdaten. Gelingt es einem Angreifer auf diese Daten zuzugreifen, kann ein großer Schaden für das Unternehmen entstehen. Werden zum Beispiel kritische Kundendaten (wie Kreditkartennummern, Adressen etc.) ausgelesen, so ermöglichen diese Daten dem Angreifer lukrative kriminelle Handlungen. Dieser Abschnitt beschäftigt sich mit den aktuell am häufigsten eingesetzten Netzwerk-Architekturen in Unternehmen.

5.7.1. Campus Netzwerk

Eine Netzwerk-Art, welche sehr häufig in Unternehmen und anderen Organisationen eingesetzt wird ist das Campus Netzwerk. IT-Wissen beschreibt ein Campus Netzwerk folgendermaßen: „*Mit Campus-Netzwerken bezeichnet man Netzwerke, die sich auf einen bestimmten geografischen Bereich, wie ein Gebäude, einen Unternehmens-Campus oder einen Industriepark beziehen. Solche Netzwerke benutzen nicht den öffentlich-rechtlichen Fernmeldebereich und sind in ihrer Ausdehnung auf kürzere Entfernungen begrenzt.*“ Quelle:[Itwi07a]. Abbildung fünf zeigt eine beispielhafte Anwendung eines Campus-Netzwerkes.

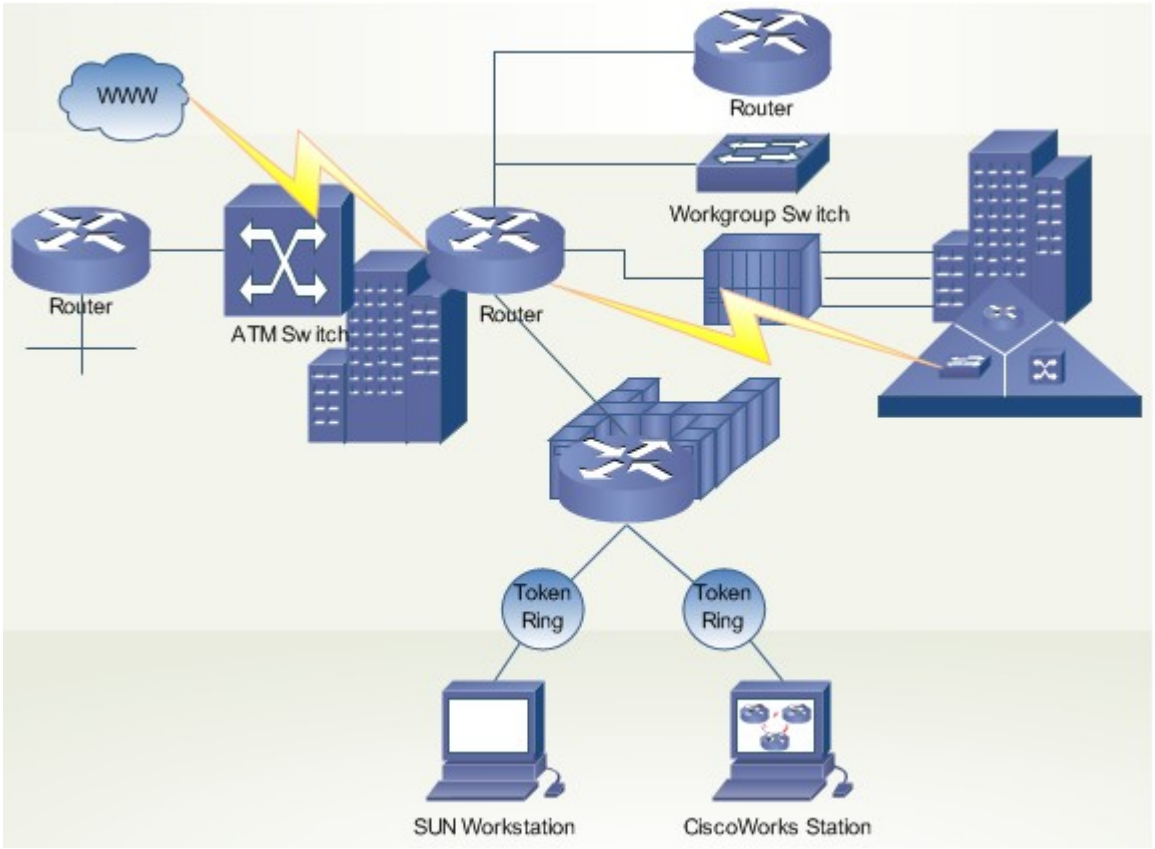

Abbildung 15, Campus Netzwerk. Quelle: [Edra07]

Ein Campus-Netzwerk ist ein Gebilde oder eine Gruppe von Gebilden welche alle in einem Unternehmens-Netzwerk verbunden sind. Dieses Netzwerk besteht aus vielen einzelnen local-area-Netzwerken (LAN´s). Ein Campus ist normalerweise ein Teil eines

Unternehmens, oder auch das gesamte Unternehmen, welcher auf eine bestimmte geographische Lage eingeschränkt ist. Die wichtigste Eigenschaft eines Campus-Netzwerkes ist es, dass jenes Unternehmen welches den Campus betreibt auch die physikalische Verkabelung im Campus besitzt. Die Technologie des Campus-Netzwerkes ist primär LAN-Technologie, welche alle End-Systeme innerhalb eines Gebäudes verbindet. Campus-Netzwerke verwenden normalerweise LAN-Technologien wie Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), Fast Ethernet und Asynchronous Transfer Mode (ATM). Eine ausführliche Beschreibung dieser Netzwerk-Art findet in Kapitel 5 Rechenzentren statt.

5.7.2. Metropolitan Area Network

Diese Art von Netzwerken, Metropolitan Area Network, wird sehr häufig für die Vernetzung von wichtigen Bürozentren einer Stadt eingesetzt. Bullhost beschreibt die Eigenschaften dieses Netzwerkes folgendermaßen: „*Bei der EDV Abkürzung MAN handelt es sich um ein Hochgeschwindigkeitsnetz, dessen äußere Knoten bis zu 50 Kilometer auseinander liegen dürfen um als MAN bezeichnet zu werden. Die Übertragungsgeschwindigkeit solcher Stadtbereichsnetze oder kurz MAN liegt bei ca. 200 MBit/s. Dieses Netzwerk eignet sich neben der Übertragung von Datenbeständen ebenso für die Übertragung von Videokonferenzen. Die MAN-Netzwerke sind durch die Standards IEEE 802.6 ANSI X3T9.5 genormt. Als Basis für ein MAN dient die DQDB Technologie.*“ (Quelle: [Bull07]). Abbildung sechs zeigt eine beispielhafte Anwendung eines Metropolitan Area Netzwerkes.

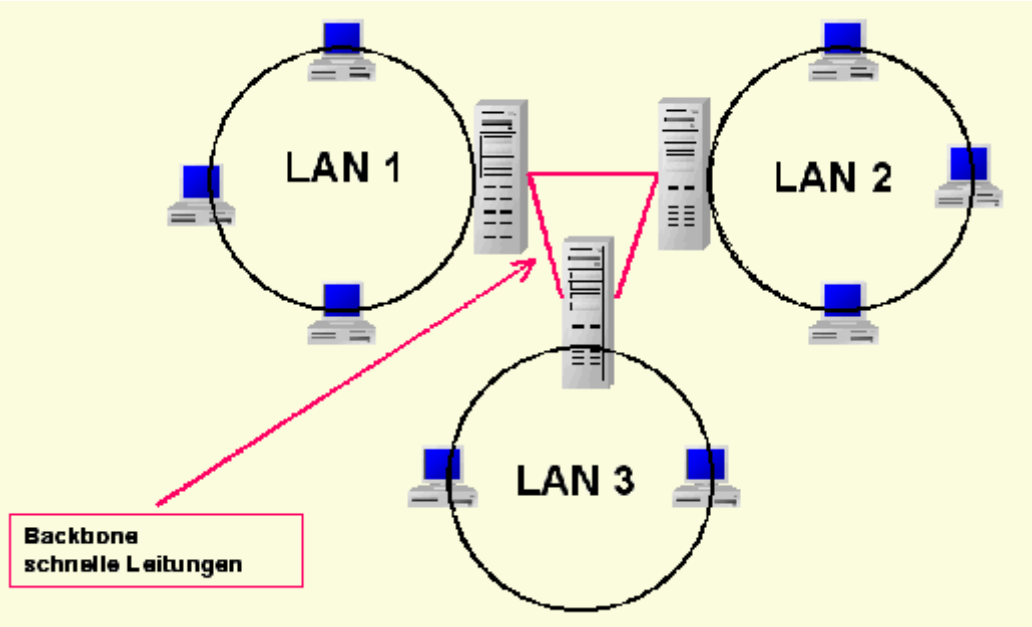

Abbildung 16: Metropolitan Area Network. Quelle: [Lehr07]

Diese Art von Netzwerken wird normalerweise mit Glasfasertechnologie umgesetzt. Die Ausdehnung dieser Form von Netzwerken beträgt maximal 100 Kilometer und verbindet oft die wichtigsten Bürozentren einer Stadt. Die Metropolitan Area Networks (MAN´s) werden häufig in Wide Area Networks (WAN´s) eingegliedert.

6. Effektives IT-Service Continuity durch Continual Service Improvement

Dieses Kapitel beschreibt Auszüge aus dem Buch Continual Service Improvement des ITIL-Werkes der dritten Version [OGC07]. Das Hauptaugenmerk dieses Abschnittes liegt dabei auf den Verbesserungsmöglichkeiten für sensible Prozesse.

6.1. Definition

Die Aufgaben des Business-Continuity-Managements wurden bereits im Kapitel 4 beschrieben. In diesem Kapitel wird erläutert, welche Unterschiede und Erweiterungen durch das Standardwerk „ITIL“ möglich sind. Insbesondere behandelt dieses Kapitel die neueste Ausgabe, ITILv3, und dafür die Ausarbeitung „Continual Service Improvement“. ITIL ist eine Sammlung von Best-Practice-Beispielen, es stellt somit keine Vorschrift oder ähnliches für einen effizienten Einsatz von IT in Unternehmen dar. ITIL ist jedoch ein bewährtes und häufig eingesetztes Werk und kann somit als eine „state-of-the-art“ Methode gesehen werden. Es gibt sehr viele Gemeinsamkeiten mit Methoden von Business-Continuity-Management, welche in Kapitel 4 bereits behandelt wurden. Deswegen werden hier nur die Erweiterungen beziehungsweise Unterschiede definiert. Die folgende Gliederung bietet einen Überblick über die Hauptaufgaben des Continual Service Improvement.

- Fortbestand eines Unternehmens nach einem Katastrophenfall zu gewährleisten
- Durch ständige Überprüfungen, Tests, Analysen Risiken, Schwachstellen und Bedrohungen zu erkennen und in weiterer Folge zu vermindern beziehungsweise zu eliminieren
- Einsatz eines Planes für die Kontinuität nach einem Katastrophenfalls für die kontrollierte Wiederherstellung der IT-Services nach einem Katastrophenfall, nach verschiedenen Qualitätsgesichtspunkten

In der ITIL-Reihe hat das Continual Service Improvement enge Schnittstellen mit den ITIL-Prozessen Incident Management, Change Management, Configuration Management, Service Level Management, Availability Management, Capacity Management und Finance Management. Wie man hier erkennen kann, sind die ITIL-Prozesse untereinander stark verbunden. Die folgende Tabelle zeigt die Aufgaben des Rollenmodells im Continual Service Improvement wo festgelegt wird, wer welche Aufgaben in einer bestimmten Situation, Normalbetrieb oder Katastrophenfall, zu erfüllen hat.

	Normalbetrieb	Katastrophenfall
Geschäftsführung	Start der IT-Service Kontinuität Rollen und Zuständigkeiten festlegen Erteilen von Entscheidungskompetenzen	Krisenmanagement Treffen der wichtigsten Entscheidungen Koordination

Oberes Management	Sicherstellung der Service-Kontinuität Problembewusstsein fördern Erteilen von Genehmigungen	Koordination Erteilen von Anweisungen Freigabe und Autorisierung von Ressourcen
Mittleres Management	Durchführung Service-Kontinuität KPI´s festlegen Abschluss von Verträgen Koordination von Tests und anderen Qualitätsmaßnahmen	Teamführung Standort-Management Berichterstattung
Unteres Management/Mitarbeiter	Durchführung der Tests Verhandlungen über Services Entwicklung von Prozessen	Durchführung von Aufgaben und Anweisungen Berichterstattung

Tabelle 16, Aufgaben Management im Katastrophenfall.

Wie auch beim „normalen“ Business Continuity Management, gibt es bei ITIL Methoden, um Risiken einzuschätzen und zu bewerten. Im ITIL-Werk werden vor allem CFIA (Component Failure Impact Analysis) und CRAMM (CCTA Risk Analysis and Management Method) eingesetzt. Diese Methoden unterscheiden sich zwar deutlich voneinander, jedoch ist das gemeinsame Ziel, Bedrohungen und damit assoziierten Risiken und Schwachstellen zu identifizieren. Nach der Identifikation werden die möglichen Auswirkungen auf die Geschäftsprozesse und Vermögenswerte festgelegt. Die folgende Abbildung bietet einen Überblick über die Gemeinsamkeiten der verschiedenen eingesetzten Methoden.

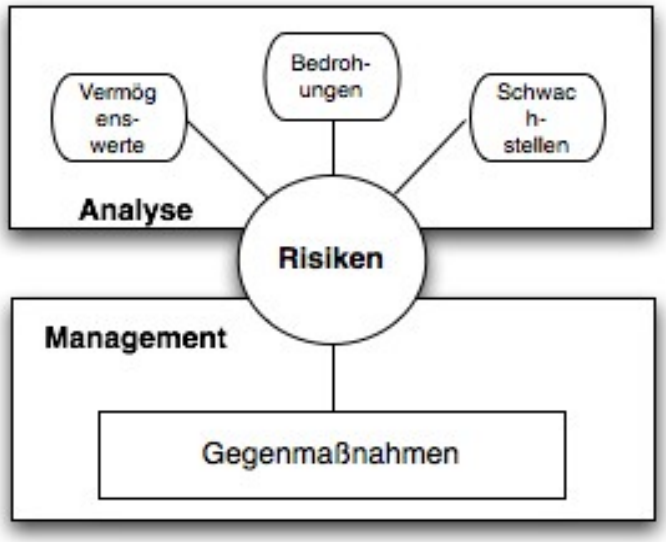

Abbildung 17,Zusammenspiel zwischen Auswirkungen und Gegenmaßnahmen. Quelle: [Olbr06], eigene Bearbeitung.

Abbildung 17 zeigt die Verknüpfung der möglichen Risiken mit der Analyse und dem Management. Bei der Analyse wird festgestellt, welche Vermögenswerte von den auftretenden Risiken betroffen sind. Im weiteren wird auch festgestellt, welche Bedrohungen durch die identifizierten Risiken auftreten können. Es wird auch analysiert, welche Schwachstellen die Risiken betreffen. Auf der Seite des Managements wird festgelegt, welche Gegenmaßnahmen ein Unternehmen gegen die identifizierten und analysierten Risiken treffen kann. Diese Gegenmaßnahmen entsprechen dem Grundsatz des effizienten Einsatzes von Ressourcen.

Die wichtigsten Anforderungen aus der Praxis an diesem ITIL-Abschnitt sind die folgenden Aufgaben:

- Definition von Schnittstellen zu CMDB, DSL und anderen Prozessinformationen
- Erzeugen und Umsetzen von Standardvorlagen
- Sicherheitsrelevante Daten an die betroffenen Standorte hinterlegen
- Durchführung von Risikoanalysen
- Effiziente Simulation und Erprobung von Katastrophen-Szenarien und der Gegenmaßnahmen.

6.2. Verbesserung von Services durch CSI

Das Continual Service Improvement (CSI) ist ein Buch der Reihe ITIL v3. In diesem Buch werden Methoden beschrieben, wie bestehende Prozesse verbessert werden können oder wie eine Einführung von neuen Prozessen in effizienter Art und Weise funktionieren kann. Diese Beschreibungen sind Best-Practice-Lösungen und stellen damit einen Leitfaden dar, sie sind jedoch keine Vorschriften. Durch eine Vielzahl von Publikationen und Studien ist die positive Wirkung von ITIL sicher gestellt, außerdem bietet die Zertifizierung nach BS 15000 oder ISO 20000 einen Nachweis der positiven Wirkung. Die folgende Tabelle beschreibt Schlüsselaktivitäten des CSI von ITIL, auf der rechten Seite werden die zugehörigen Schlüsselrollen definiert.

Schlüsselaktivitäten	Schlüsselrollen
Daten sammeln und Trends analysieren verglichen mit Baselines, Ziele, SLA´s und Benchmarks. Beinhaltet den Output von Services und Servicemanagement-Prozessen	CSI Manager, Service Manager, Service Owner, IT Prozess Owner
Ziele festlegen für Verbesserung in Effizienz und Kosten-Effizienz durch den ganzen Service-Lebenszyklus	CSI Manager, Service Manager
Ziele festlegen für Verbesserungen in Service-Qualität und Ressourcen-Verwendung	CSI Manager, Service Manager, Service Owner, Business Process Owner

Betrachten neuer Geschäfts- und Sicherheitsanforderungen	CSI Manager, Service Manager, Geschäftsprozess Owner
Betrachten von neuen externen Verpflichtungen wie regulatorische Vorschriften	CSI Manager, Service Manager, Geschäftsprozess Owner
Festlegung eines Plans und Implementierung der Verbesserungen	CSI Manager, Service Manager, Service Owner, Prozess Owner
Anbieten eines Hilfsmittel für Angestellte um Verbesserungsmöglichkeiten vorzuschlagen	CSI Manager, Service Manager
Messungen, Reports der Service Verbesserungsinitiativen, kommunizieren der Initiativen	CSI Manager, Service Manager
Überarbeitung Policen, Prozesse, Prozeduren und Erstellung von Plänen wo notwendig	CSI Manager, Service Manager
Versichern dass alle vorgeschlagene Aktionen vollständig durchgeführt werden und dass sie die gewünschten Resultate erzielen	CSI Manager, Service Manager, Business Manager, IT-Prozess Owner, Geschäftsprozess Owner

Tabelle 17, Schlüsselaktivitäten und Schlüsselrollen CSI.

6.2.1. 7-Step Improvement Prozess

Dieser Prozess beschreibt den Weg, wie ein Service verbessert werden kann [OGC07]. Dieser Weg beinhaltet sieben Phasen, welche inkrementell ein Service zuerst analysieren und zum Schluss wird das verbesserte Service implementiert. Die folgende Abbildung bietet einen Überblick über die verschiedenen Phasen.

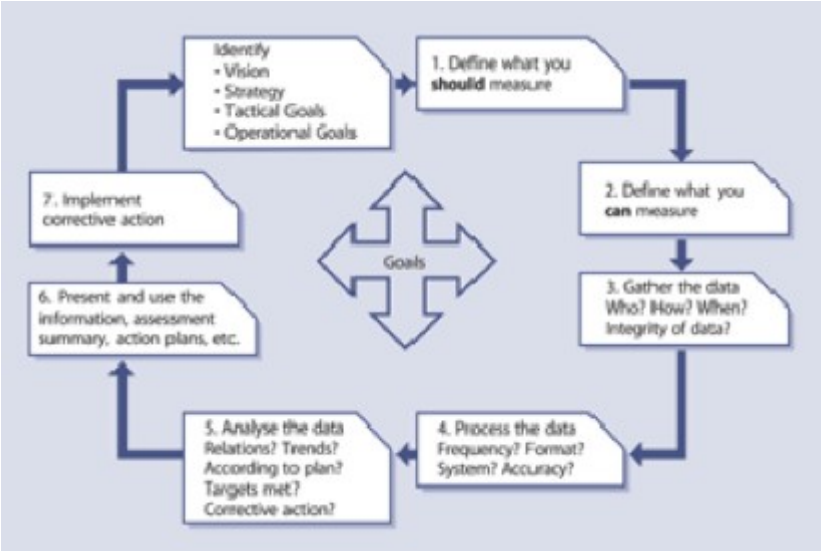

Abbildung 18, 7-Step Improvement Prozess. Quelle: [OGC07]

Abbildung 18 zeigt den Ablauf des 7-Step Improvement Prozesses. Die folgende Gliederung definiert die Aufgaben der einzelnen Phasen.

- Festlegung was gemessen werden soll: Hier wird definiert, wo das Unternehmen gerade steht, es wird die ideale Situation identifiziert dabei der Geschäftsbereich und die IT betrachtet. Inputs sind hier unter anderen Service Level Requirements und Ziele, Service-Kataloge, Balanced Scoreboard und gesetzliche Bestimmungen.

- Festlegung was gemessen werden kann: Hier wird festgelegt, wo das Unternehmen sein will. Hier kann eine Gap-Analyse eingesetzt werden, um die Verbesserungsmöglichkeiten festzulegen und außerdem die Frage zu beantworten, wie ein Unternehmen an seine Ziele kommt. Input-Möglichkeiten sind hier zum Beispiel Messlisten, Prozessabläufe, Arbeitsanweisungen oder existierende Reports.

- Sammlung der Daten: Alle notwendigen Informationen werden dieser Phase gesammelt. Diese Informationen werden in dieser Phase jedoch nicht analysiert. Input-Möglichkeiten sind hier neue Geschäftsanforderungen, existierende SLA´s, Verfügbarkeits- und Kapazitäten-Pläne, Service-Verbesserungspläne, Listen was gemessen werden soll oder kann und Kundenzufriedenheits-Umfragen.

- Bearbeitung der Daten: In dieser Phase werden die gesammelten Daten nach verschiedenen Gesichtspunkten wie zum Beispiel den KPI´s bearbeitet. Hier werden Zeitpläne erstellt, Daten in ein bestimmtes Format gebracht etc. Ziel dieser Phase ist es, die Daten analysierbar zu machen. Input-Möglichkeiten sind hier Daten welche durch Beobachtung gewonnen wurden, SLA´s, OLA´s, Service-Kataloge oder die Report-Frequenz.

- Analyse der Daten: Hier erfolgt die Umwandlung von Daten in Information. Diese Umwandlung ist notwendig, damit auch alle Nicht-Experten die Ergebnisse verstehen können.

- Präsentieren und Verwendung der Informationen: In diesem Abschnitt wird die Fragestellung beantwortet, ob die Zielsetzung erreicht wurde.

- Implementierung verbessertes Service: Hier werden die geplanten Aktivitäten im Unternehmen tatsächlich umgesetzt. Diese Umsetzung erfolgt mit gesammelten Informationen, um die betrachteten Services zu optimieren, zu verbessern und zu korrigieren.

6.2.2. Service Report

Der Service-Report hat die Aufgabe festzulegen, welche Informationen für wen interessant sind. Es werden in der routinemäßigen Überwachung der IT-Systeme ein hohe Anzahl von Informationen ermittelt, welche aber nur zu einem Bruchteil für das Management für ein Unternehmen interessant sind. Ein, laut ITIL [OGC07], guter Ansatz für eine Zielgruppen-

genaue Abstimmung der Informationen setzt sich aus folgenden Eigenschaften zusammen:

- Vereinbarung was gemessen wird und über was der Report handelt
- Vereinbarte Definitionen aller Begriffe und Grenzen
- Erläuterungen zu allen Berechnungen
- Zeitplanung der Report-Erstellung
- Zugang zu Reports und Medium welches benutzt wird
- Vereinbarung von Treffen um Diskussion um Reviews von Reports durchzuführen

Wichtig ist es beim Service Report zu wissen, wer das Publikum ist. Wenn das Publikum bekannt ist, kann der Inhalt eines Reports genau auf das Publikum zugeschnitten werden. Zum Beispiel hat eine Verkaufsabteilung andere Interessen betreffend das IT-System eines Unternehmens als die Produktionsabteilung. Alle verschiedenen Reports und Policen sollen in einem einheitlichen Framework zur Verfügung gestellt werden. Durch automatisierte Abläufe können die verschiedenen Abteilungen die wichtigen Informationen für sich filtern und in weiterer Folge ausgeben lassen. Wichtig ist auch, dass die Sprache des Publikums gesprochen wird und keine eigene IT-Sprache eingesetzt wird.

6.2.3. Service Messung

Aufgrund der Bedeutung der IT in Unternehmen ist es nicht mehr möglich, diese Technologie getrennt von den anderen Geschäftszweigen zu betrachten. Eine Trennung ist außerdem nicht möglich, da viele Unternehmen erst mit Hilfe der IT in der Lage sind Geschäfte abzuwickeln. Durch diese Tatsache ist es notwendig festzulegen, welche Ansprüche betreffend der Verfügbarkeit, der Verlässlichkeit und der Stabilität gestellt werden und wie diese Faktoren in weiterer Folge gemessen werden können. Wichtig ist vor allem eine ganzheitliche Betrachtung des Systems. Erfolgt eine Betrachtung einzelner Komponenten so kann nicht sicher gestellt werden, ob das ganze System funktioniert oder nicht. Eine Messung der Performance einzelner Komponenten wird beispielsweise auch nicht die Kundenzufriedenheit mit dem gesamten System widerspiegeln. Dieser Abschnitt beschreibt Möglichkeiten, welche Maßnahmen für eine ganzheitliche Messung durchgeführt werden können.

- Entwicklung eines Service-Messungs-Frameworks: Diese Entwicklung ist sehr schwierig in Unternehmen einzuführen und führt sehr häufig erst nach einigen Versuchen zu Erfolgen. Zu Beginn ist es notwendig ein Verständnis über die verschiedenen Geschäftsprozesse aufzubauen und in weiterer Folge die kritischsten Prozesse zu identifizieren. Wichtig ist hier sicherzustellen, dass die Ziele der IT auch die Ziele des gesamten Unternehmen behandeln. Durch diese Maßnahme kann sicher gestellt werden, dass kein Wert gemessen wird, welcher keinen Nutzen für den Kunden oder andere Stakeholder generiert. Konkret bedeutet die Einführung eines Service-Messungs-Frameworks zu entscheiden, welche der Einheiten Services, Komponenten, Service-Management-Prozess, Aktivitäten und

Outputs gemessen werden. Es wird auch entschieden, wie eine gelungene Messung aussieht. Dabei ist zu beachten, welche Messung durchgeführt wird um benötigte Informationen für strategische, taktische und operationale Entscheidungen treffen zu können. Es ist auch notwendig, Ziele für die Messungen festzulegen. Diese Zielsetzung kann durch SLA´s oder Service-Level-Ziele, welche intern in der IT festgelegt wurden, erfolgen. Bei der Entwicklung werden auch die Prozesse und Policen definiert, welche für die Erreichung der Ziele notwendig sind. Diese umfassen zum Beispiel die Rollen und Verantwortlichkeiten für die Service-Messung.

- Verschiedene Levels von Messung und Reports: Für die Erstellung eines Frameworks ist es notwendig, verschiedene Messungen und verschiedene Maße zu integrieren. Diese Integration findet durch verschiedene Komponenten-Messungen statt. In weiterer Folge werden Service-Scoreboards und Service-Dashboards erstellt, welche wiederum in eine ganzheitliche Balanced Scorecard eingehen. Im Detail sehen die verschiedenen Stufen bei der Messung folgendermaßen aus: Messung der einzelnen Komponenten (Verfügbarkeit, Verlässlichkeit und Performance). Hier wird zum Beispiel bestimmt, ob die Server innerhalb festgelegter Richtlinien arbeiten. Diese Messungen fließen in weiterer Folge in eine ganzheitliches end-to-end-Service-Messung ein. Diese Service-Messung wird mit den festgelegten KPI´s verglichen und daraus werden die Service-Scorecard und das Service-Dashboard erstellt. Die höchste Ebene bildet die IT-Scorecard oder die Balanced Scorecard. Service-Scorecards bilden dabei einen Schnappschuss eines gewissen Service, es wird also der Zustand zu einem gewissen Zeitpunkt festgehalten. Das Service-Dashboard stellt eine Echtzeit-Messung der Services dar, welche zum Beispiel das Intranet durchgeführt werden können. Die Balanced-Scorecard bietet einen umfassenden Blick auf die gemessenen Aspekte des Services. Die folgende Abbildung zeigt den beschriebenen Ablauf der Messungen.

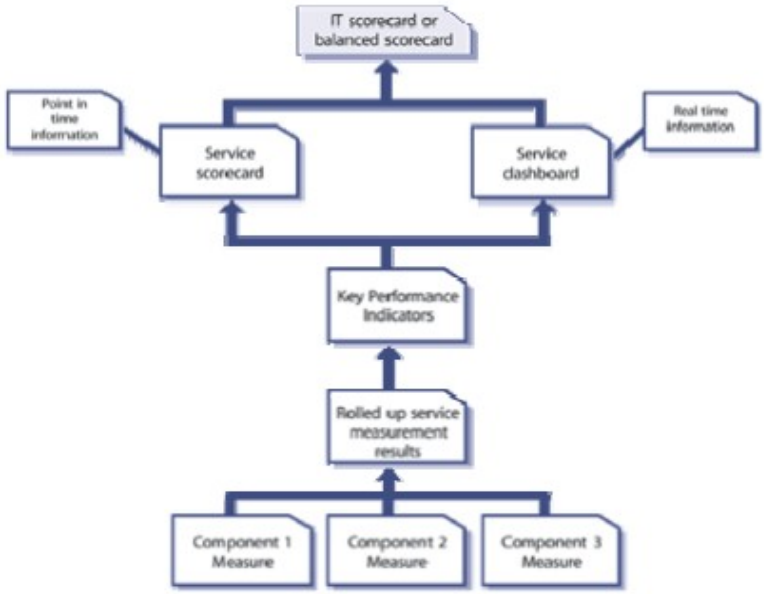

Abbildung 19, Prozess der Service-Messung. Quelle: [OGC07]

- Definition des Inhalts der Messung: In vielen Unternehmen wird die Performance der IT zu ausführlich gemessen was zur Folge hat, dass die Messungen keinen erkennbaren Nutzen auf Services haben. Die folgende Tabelle bietet einen Überblick über Kategorien, welche für die Geschäfts-Performance der IT wichtig sind.

Kategorie	Definition
Produktivität	Produktivität von Kunden und IT-Ressourcen
Kundenzufriedenheit	Kundenzufriedenheit und erhaltenen Wert von IT-Services
Value Chain	Auswirkung der IT auf funktionale Ziele
Ganzheitliche Performance	Vergleich mit mit internen und externen Resultaten in Bezug auf Geschäftsmessungen und Infrastruktur-Komponenten
Geschäftsausrichtung	Kritik der Unternehmensservices, Systeme und Portfolio von Applikationen und Geschäftsstrategie
Investitionsauswirkungen	Auswirkungen von IT-Investition auf Kostenstruktur des Unternehmens
Management-Vision	Verständnis der Geschäftsführung des strategischen Wertes der IT und Fähigkeit der Vorgabe der Richtung für zukünftige Aktionen

Tabelle 18, Kategorien der Messung Unternehmens-Performance

Eine weitere Kategorie stellt das Service-Level dar, welches sich unter anderen aus dem Service, der Komponentenverfügbarkeit, der Transaktions- und Antwortzeit, der rechtzeitigen und kostengerechten Lieferung von Services und Applikationen zusammen setzt.

- Festlegung von Zielen: Wichtig bei der Festlegung von Zielen ist zu wissen, welche Möglichkeiten ein System hat. Erst wenn diese grundlegenden Informationen bekannt sind ist es möglich, sinnvolle Ziele festzulegen. Diese Ziele sollen folgende Eigenschaften aufweisen: sie sind spezifisch, sie sind messbar, die Ziele sind erreichbar, sie sind relevant und zeitgerecht. Die Festlegung von Zielen darf nicht auf ein Ziel fokussiert sein, sondern es ist das Service ganzheitlich zu behandeln. Ein Beispiel für diese umfassende Behandlung ist die Messung des Services eines Call-Centers. Wird bei diesem Call-Center nur die Menge von behandelten Personen pro Zeiteinheit betrachtet, nicht jedoch die Kundenzufriedenheit, so wird diese Messung zu keiner Verbesserung der Qualität des Services führen.

- Service-Management Prozess-Messung: Diese Messung behandelt die Wartung eines IT-Systems. Viele Ausfallzeiten resümieren aus fehlerbehafteter Wartung des zuständigen Personals. Diese Messung umfasst auch die Anzahl von dringenden

Änderungen, die Anzahl von nicht-geschafften dringenden Änderungen und die unautorisierten Änderungen. Typische KPI´s für diese Messung sind: Verbesserung der Verfügbarkeit durch Services/Systeme/Applikationen, Reduzierung der „mean time to repair“ und die Reduzierung des Anteils von dringenden Änderungen und von Notfall-Änderungen.

- Interpretieren und Verwendung von Messzahlen: Hier wird sicher gestellt, dass die Ergebnisse überhaupt realistisch sind. Anstatt die Ergebnisse frühzeitig zu präsentieren, kann eine Aufklärung der zweifelhaften Ergebnisse durch folgende Fragen beantwortet werden: Wie wurden die Daten zusammen gestellt, wer stellte die Daten zusammen, wer bearbeitete die Daten etc. Bei der Auswertung von „sinnvollen“ Daten ist zu beachten, dass viele Faktoren bei der Betrachtung der Ergebnisse eine Rolle spielen. Ein Faktor kann zum Beispiel sein, dass an einem Service Änderungen vorgenommen wurden und deswegen es zu einer Veränderung gegenüber des Vormonats gekommen ist. Die Verwendung von Messzahlen kann zu folgenden Zwecken benützt werden: Bewertung, Rechtfertigung von Zielen, Intervention. Häufig sind auch Vergleiche sinnvoll, folgende Vergleich sind für Unternehmen sehr hilfreich: Vergleiche ob ein Ziel erreicht wurde, Vergleich mit anderen Unternehmen, Vergleiche mit Zeiteinheiten wie zum Beispiel ein anderer Tag/Woche, Vergleich zwischen verschiedenen Geschäftseinheiten oder verschiedenen Services.

- Anlegen von Scorecards und Reports: Messungen werden für verschiedene Zwecke und für verschiedene Zielgruppen durchgeführt. Deswegen ist es wichtig Daten aus den Untersuchungen speziell der Zielgruppe anzupassen. Die Zielgruppen können eingeteilt werden in die Geschäftsführung, das IT-Management und den IT-Verantwortlichen für die operative und technische Planung. Die Balanced Scorccard ist eine Möglichkeit, alle Zielgruppen und Ziele miteinander zu verbinden. Bei dieser Methode werden zum Beispiel die finanzielle Perspektive, die Kunden-Perspektive und die interne Perspektive verwendet. Die verschiedenen Zielsetzungen werden von den einzelnen Zielgruppen unterschiedlich priorisiert werden. Bei der Erstellung von Reports ist es sinnvoll vor der Ausführung ein Konzept zu erstellen, was unter anderen folgende Fragestellungen beantwortet: Wer ist das Zielpublikum vom Report, für was wird der Report verwendet, wer ist für die Erstellung des Reports zuständig, wie wird der Report erstellt, wie oft wird der Report erstellt.

- Erstellung von CSI-Policen: Im Continual Service Improvement-Werk von ITIL ist die Verwendung von CSI-Policen ein Schlüsselprinzip, welches in der IT-Organisation definiert und kommuniziert wird. Beispiele für solche Policen sind: Überwachungsanforderungen werden definiert und implementiert, Daten müssen auf einer konstanten Basis gesammelt und analysiert werden, interne und externe Service-Reviews müssen auf einer konsistenten Basis komplettiert werden,

Service-Management-Prozesse müssen kritische Erfolgsfaktoren und Schlüssel-Performance-Indikatoren haben um festzulegen, ob es eine Lücke zwischen dem erwarteten Ergebnis und dem tatsächlichen Ergebnis gibt.

6.2.4. Return on Investment von CSI

Für eine Messung der Auswirkungen einer Investition werden sehr häufig Kennzahlen eingesetzt. Eine der am häufigsten eingesetzten Kennzahlen ist der Return of Investment – ROI. Nur sehr wenige Unternehmen werden dazu bereit sein CSI zu unterstützen, wenn nicht messbare Ergebnisse von Kosten und Nachweise von positiven Auswirkungen gegeben sind. Die folgenden Beispiele zeigen, welche Herausforderungen laut ITIL [OGC07] zu lösen sind.

- Es gibt kein richtiges Verständnis der aktuellen IT-Fähigkeiten oder Kosten
- Es gibt nur ein geringes Verständnis von wichtigen Faktoren des Geschäftes und ihrer Verbindung zur IT
- Sehr häufig gibt es ein geringes Wissen über die Kosten einer IT-Downtime für die Geschäftsabwicklung und für die IT
- Es gibt eine geringe Erfahrung bei der Festlegung von Messungs-Frameworks neben einfachen Komponenten-/System-Messungen
- Es gibt wenig Verständnis für den Unterschied zwischen Benefits und ROI

6.2.5. Festlegung eines ROI für CSI

Der ROI von CSI ist sehr umfassend, auf der einen Seite stehen die Investment-Kosten und auf der anderen Seite die erhaltenen Vorteile. Die Kosten setzen sich zusammen aus internen Ressourcen-Kosten, Tool-Kosten, Consulting-Kosten etc. Die erhaltenen Vorteile sind sehr schwierig zu definieren, für eine Definition laut ITIL [OGC07] ist es notwendig, die Antworten auf folgende Fragestellungen zu kennen:

- Was sind die Kosten einer Downtime? Diese Kosten umfassen dabei die verlorene Produktivität der Kunden und den Verlust von Einnahmen.
- Was sind die Kosten von Nacharbeiten?
- Was sind die Kosten von redundanter Arbeit? In vielen Organisationen ohne klaren Prozessen und guter Kommunikation findet redundante Arbeit statt.
- Was sind die Kosten von nicht-gewinnbringenden Projekten?
- Was sind die Kosten von einer verspäteten Lieferungen einer Applikation?
- Was sind die Kosten von Vorfällen welche im „third level-support“ und „second-level-support“ gelöst werden anstatt bereits im „first-level-support“ gelöst werden?
- Was sind die Gesamtkosten einer Arbeitsstunde für verschiedene Angestellten-Levels?

Es gibt verschiedene Ansätze um die Verfügbarkeit zu messen und aufzubereiten. Mögliche messbare Auswirkungen sind die Auswirkungen von Downtime-Minuten, hier erfolgt eine Kalkulation der Downtime-Dauer mit der Anzahl von betroffenen Kunden. Eine

weitere Möglichkeit ist die Auswirkung von Geschäftstransaktionen, diese Berechnung basiert auf der Anzahl von Geschäftsprozessen welche während der Downtime nicht stattfinden können. Eine weitere Möglichkeit sind auch die bereits vereinbarten Kosten der Downtime. Für Unternehmen ist es sehr hilfreich, die wahren Kosten einer Downtime zu kennen. Sind diese Kosten bekannt, so kann eine Berechnung der Auswirkungen der unterschiedlichen Servicetypen erfolgen. Diese Servicetypen sind Kategorien/Abstufungen wie geschäftskritische Services, kritische Services oder nicht-kritische Services.

6.2.5. Messung von erreichten Vorteilen

Eine Frage, welche immer wieder von Verantwortlichen in Unternehmen gestellt wird, ist die Frage nach erreichten Vorteilen einer getätigten Maßnahme. Durch die Messung von erreichten Vorteilen kann genau diese Fragestellung beantwortet werden. Die Vorteile von Aktionen werden im Verlauf der Einführung geschätzt, die tatsächliche Bestimmung und Messung erfolgt in dieser Phase. Diese Phase legt fest, ob:

- Die anvisierten Verbesserungen realisiert wurden.
- Die Benefits durch die Verbesserungen erreicht wurden.
- Der Ziel-ROI erreicht wurde.
- Der VOI (Indended value-added) erreicht wurde.
- Genug Zeit vergangen ist bevor die Benefits gemessen wurden. Einige Benefits werden erst später Wirkung zeigen.

6.3. Beschreibung von sensiblen Prozessen

Nahezu alle Geschäftsprozesse werden heute mit Hilfe von IT-Systemen durchgeführt. Diese Geschäftsprozesse haben sehr unterschiedliche Ausprägungen, einige dienen nur zur internen Information, mit anderen Prozessen hingegen werden die Verkäufe eines Unternehmens durchgeführt. Es gibt sowohl interne Prozesse als auch externe Prozesse. Zu den internen Prozessen zählen zum Beispiel Intranet, Formulare für das Ansuchen von Urlaub, Informationen über die Mitarbeiter usw. Zu den externen Prozessen zählen alle Interaktionen, welche mit Kunden oder Lieferanten des Unternehmens abgewickelt werden. Beispiele für externe Prozesse sind der Verkauf über das Internet-Portal eines Unternehmens, der Kontakt mit einem Kunden/Anwender über die Service-Hotline oder die Bestellung bei einem Lieferanten.

Die verschiedenen Geschäftsprozesse haben sehr unterschiedliche Auswirkungen bei einem eventuell auftretenden Ausfall. Es ist für ein Unternehmen zwar lästig, wenn das Intranet für ein paar Stunden nicht verfügbar ist. Jedoch hat diese Situation keine schwerwiegenden Auswirkungen auf den gesamten Geschäftsbetrieb eines Unternehmens. Wenn aber kurz vor Weihnachten der Online-Shop eines großen Versandhandels für einige Zeit nicht funktioniert, dann wird das sehr wohl schwerwiegende Auswirkungen auf den Geschäftsbetrieb eines Unternehmens haben. Diese zweite Form, Geschäftsprozesse mit schwerwiegenden Auswirkungen, werden als sensible

Geschäftsprozesse eingestuft. Ein weitere Form von sensiblen Geschäftsprozessen sind jene Prozesse, welche gesetzlich vorgeschrieben unbedingt geschützt werden müssen.

6.3.1. Beispiele für sensible Geschäftsprozesse

Dieser Abschnitt beschreibt Beispiele für sensible Geschäftsprozesse. Unter diesen Prozessen werden jene Abläufe verstanden, welche bei einem Ausfall besonders schwere Auswirkungen haben. Mühleck [DiSc06] beschreibt die folgenden Kerngeschäftsprozesse im Unternehmen VW, welche durch die IT getragen werden:

- Strategische Steuerungs- und unterstützende Prozesse: Zu diesen Prozessen zählen unter anderen die Unternehmenssteuerung, die Personalverrechnung, das Finanzwesen oder das Qualitätsmanagement. Die Aufgaben der IT in diesen Prozessen sind eine umfassende Unternehmenssteuerung der Finanzen des gesamten Konzerns mit Bereitstellung von Kennzahlensystemen, eine Steigerung der Effizienz des Controllings und Reportings durch den Einsatz einheitlicher Mechanismen, Steigerung der Effizienz der einzelnen Fachbereiche und der IT durch die Verwendung von einheitlichen IK-Tools wie Portale, Dokumenten-Management etc.

- Produktprozess: Dieser Prozess beinhaltet die gesamte Lebensdauer einer Produkts. Die wichtigsten Aufgaben dieses Prozesses sind unter anderen die Verkürzung des Produktprozesses im Unternehmen, Erweiterung des digitalen Einsatzes in der Fabrik und die Einbindung von finanziellen Vorgaben im Produktprozess.

- Kundenauftragsprozess: Dieser Prozess beinhaltet die Verfolgung des Auftrages des Kunden bis hin zur Übergabe, in diesem Fall, des Fahrzeuges. Einige wichtige Aufgaben dieses Prozesses sind die Reduzierung der Komplexität, Kommunikation von Best-Practice-Lösungen über alle Produkte, die Auswahl der Lieferanten und die Verkürzung der Durchlaufzeiten der Kundenaufträge.

- Serviceprozess des Kunden: Dieser Prozess umfasst die das gesamte Kundenbeziehungsmanagement in verschiedenen Bereichen wie die Lieferung von Originalteilen und auch Dienstleistungen im Finanzbereich. Hier sind die wichtigsten Aufgaben unter anderen die Erhöhung der Kundenzufriedenheit, Reduzierung der Komplexität oder die Steigerung der Kompetenzen hinsichtlich Verkauf.

- IT-Services: Dieser Prozess betrifft die Verfügbarkeit des gesamten IT-Systems. Wichtige Aufgaben sind hier zum Beispiel die Einführung von unternehmensweiten einheitlichen Dienstleistungen und eine vorausblickende Unterstützung des Geschäftsbetriebes, die Sicherstellung der wichtigsten Kompetenzen durch qualifiziertes Personal und eine Senkung der Kosten der Services durch Optimierungsmaßnahmen.

Reisig [ReSc05] gibt noch ein anderes Beispiel für eine typische Verkettung von verschiedenen Geschäftsprozessen in der Praxis: Vermietung eines Autos. Hier sind mehrere Services beziehungsweise Geschäftsprozesse untereinander verknüpft und es erfolgt eine Kommunikation zwischen der verschiedenen Partnern. Der Autoverleiher kommuniziert mit Kunden, Händlern von Fahrzeugen etc. Auf der Gegenseite hat auch der Kunde eine bestimmten Ablauf von zusammenhängenden Geschäftsabläufen: er stellt mit dem Führerschein seine Lenkerberechtigung unter Beweis, er wählt eine Versicherungsart beziehungsweise den Umfang der Versicherung aus etc.

6.3.2. Verbesserungspotenzial von Prozessen

Geschäftsprozesse stellen eine zentrale Bedeutung in der Unternehmensführung von Unternehmen dar. Diese Prozesse werden bei jeder Interaktion mit Kunden oder anderen Personengruppen angewendet, häufig gibt es bei diesen Prozessen ein hohes Potenzial an Verbesserungsmöglichkeiten. Durch den hohen Einsatz der Prozesse, führt bereits eine geringe Veränderung zu großen positiven Auswirkungen für das Unternehmen. Dieser Abschnitt beschreibt allgemein eine Auswahl von Möglichkeiten für Unternehmen, eine Verbesserung der Geschäftsprozesse zu erreichen.

Günter Schuh [Schu06] stellt einige Prinzipien vor, welche bei der Neugestaltung von Prozessen beachtet werden sollen, um eine Basis für Verbesserungen hinsichtlich Effizienz etc. im täglichen Geschäftsablauf zu schaffen. Diese Neugestaltung von Prozessen umfasst hier sowohl die Prozessoptimierung, die Gestaltung allgemeiner Problemfelder sowie auch die Neugestaltung von Prozessen. Die folgende Tabelle bietet einen Überblick über wichtige Grundprinzipien.

Prinzip	Maßnahmen
Eliminieren	Alle Tätigkeiten, welche nicht direkt einen „spürbaren“ Wert für den Kunden erzeugen, müssen eliminiert werden. Die Entscheidung ob eine Tätigkeit einen Wert erzeugt oder nicht, ist vom jeweiligen Kontext abhängig.
Standardisieren	Durch die Gestaltung von Routinefällen verschiedener Tätigkeiten wird die Fehleranfälligkeit vermindert und die Effizienz gesteigert.
Verbesserung des Mitteleinsatzes	Durch effiziente Ressourcennutzung und durch Verwendung von hochwertigen Produzenten, d.h. kritische Betrachtung der Leistungen der Lieferanten.
Reduktion der Varianz	Die Elemente eines Prozessen weisen normalerweise immer Varianzen auf, durch Reduktion einerseits der zeitlichen Varianz und andererseits durch Reduktion der ergebnisbezogenen Varianz erfolgt eine Steigerung der Stabilität sowie eine Steigerung der Prozessqualität.
Substituieren	Durch den Einsatz von neuen Produktionsmöglichkeiten können einzelne Elemente eines Prozesses oder eine ganze Prozesskette substituiert werden.

Integrieren	Durch Zusammenfassen von Aufgaben einen Geschäftsprozess effizienter gestalten, diese Maßnahme ist jedoch durch die gewohnten Arbeitsabläufe der Bearbeiter sehr schwierig einzuführen. Beinhaltet jedoch ein großes Verbesserungspotenzial.
Parallelisieren	Auch bei dieser Methode ist ein großes Verbesserungspotenzial möglich, durch zeitliche Einsparung kann ein Ablauf deutlich effizienter gestaltet werden.
Verlagern	Bei dieser Methode sind zwei Ausführungen möglich: Einerseits das Auslagern aus einem Prozess, andererseits das Integrieren in einen Prozess. Hier können auch externe Unternehmen in den Arbeitsablauf integriert werden (oder im Gegenteil das eigene Unternehmen übernimmt Tätigkeiten).
Vermeidung von Interaktionen	Viele Strukturen in Unternehmen wachsen über einige Jahre hinweg. Diese Strukturen werden jedoch häufig nicht an die aktuellen Zustände/Bedürfnisse angepasst, eine Neubetrachtung bietet Möglichkeiten für eine Einsparung.
Kooperation	Hier ist eine bessere Nutzung von Ressourcen möglich. Es ist auch möglich, dass durch die frühe Abstimmung von Anforderungen bessere Ergebnisse erzielt werden.

Tabelle 19, Grundprinzipien der Verbesserung von Geschäftsprozessen

6.3.3. Key Performance Indikatoren

Unter den Key Performance Indikatoren (KPI´s) versteht man den prozentualen Abdeckungsgrad der vorher definierten Risiken bei Geschäftsprozessen. Im weiteren Sinn versteht man unter den KPI´s auch jene Verfahren, welche den Geschäftsprozessen zugrunde liegen. Der Abdeckungsgrad richtet sich nach den Maßnahmen, welche bereits getestet wurden oder welche geplant sind. Dabei kann weiters unterschieden werden, ob die Geschäftsprozesse wieder komplett und uneingeschränkt zur Verfügung stehen müssen/sollen, oder ob ein verminderter Einsatz ebenfalls seinen Zweck erfüllt.

Folgende Kennzahlen werden sehr häufig in Unternehmen eingesetzt:

- Abdeckungsgrad aller gefundenen Risiken
- Anzahl der durchgeführten Notfallübungen
- Kosten der Business-Continuity-Maßnahmen
- Änderungen an den Continuity-Plänen (Update nach Tests etc.)
- Ausbessern von schwerwiegenden Störungen am System
- Abgeschlossene Kooperationsverträge im Falle von Störungen
- Anzahl der durchgeführten Audits
- Anzahl (nicht) erreichter Continuity-Anforderungen
- Anzahl der vertraglich vereinbarten Rahmenbedingungen, welche nicht durch den IT Continuity-Plan abgedeckt werden
- Anzahl der Ausfälle von IT-Services in der Folge von mangelhaften Sicherheitsmaßnahmen im Notfall
- Anzahl der durchgeführten Notfallübungen

Jener KPI mit der stärksten Aussagekraft ist die Ausbesserung von schwerwiegenden Störungen am System, welcher durch die Maßnahmen des Continuity-Managements erreicht wurden. Die Anzahl der abgeschlossenen Kooperationsverträge, welche mit externen Partnerunternehmen durchgeführt werden, sind ein deutliches Zeichen dafür, dass Business-Continuity in einem Unternehmen ernst genommen wird. Martin Kütz [Kütz03] hält in seinem Buch folgende Kennzahlen im Bereich des Continuity-Management für sehr wichtig:

- Risikoabdeckungsgrad
- Identifizierte Fehler/Mängel der Prozesse
- Anzahl von erfolgreichen Tests für den Wiederanlauf im Katastrophenfall

6.3.4. Umdenkungsprozess festlegen

Dieser Abschnitt beschreibt Methoden, wie ein Umdenkungsprozess bei den Mitarbeitern eines Unternehmens eingeleitet werden kann. Für die Geschäftsführung zählen vor allem der Gewinn/Absatz etc. und nicht Maßnahmen, wie mögliche Verluste verhindert werden können. Jedoch wird auch jene Geschäftsführung mit den härtesten Zweiflern zum Einsatz der Maßnahmen bereit sein, wenn die möglichen negativen Auswirkungen präsentiert werden. Die folgende Gliederung bietet einen Überblick über jene Systemkomponenten, welche für die häufigsten Ausfälle und somit für negative Auswirkungen verantwortlich sind.

- Fehler am Betriebssystem
- Ausfall des Datenbankservers
- Fehler bei Server-Client-Architekturen
- Fehler bei der Middleware
- Fehler an Netzwerkkomponenten wie Switches und Router

Die folgende Abbildung bietet einen Überblick, über die prozentuale Verteilung der Ausfallgründe der IT-Systeme in der Praxis. Man sieht, dass ein sehr großer Teil, 37 Prozent, der Fehler durch Probleme in den Applikationen verursacht werden. Die nächsten Gründe mit der ungefähr selben Auftrittswahrscheinlichkeit sind Hardware-Fehler am Hauptserver, Fehler in der Datenbank, Netzwerkfehler und Fehler durch die menschliche Anwendung. Zu dieser menschlichen Komponente zählen zum Beispiel Administrations- oder Bedienungsfehler. Zu den menschlichen Fehlern zählen auch unter anderen Unwissenheit, Unfälle oder bewusste Maßnahmen wie Sabotage. Die nächste Gruppe, welche zwischen drei und vier Prozent der Ausfälle verantwortlich sind, sind Umwelteinflüsse oder geplante Ausfälle bei der Administration etc. Zu den Umwelteinflüssen können dabei zum Beispiel Erdbeben, Stromausfälle, Brände oder auch die mangelnde Kühlung der Hardwarekomponenten zählen.

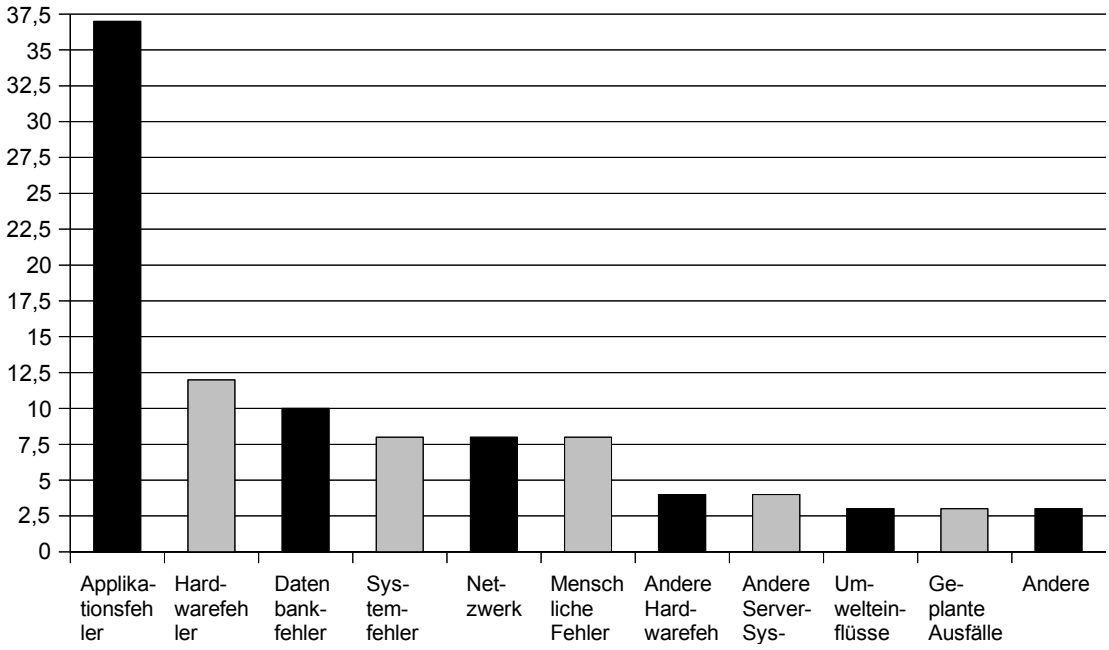

Abbildung 20, Anteile Ausfallgründe von IT-Systemen. Quelle: [Wood07], eigene Bearbeitung

6.3.5. Zertifizierung BS 15000/ISO 20000

Aktuell versuchen viele Unternehmen, ihre IT-Systeme nach ITIL aufzubauen. Es stellt sich dabei die Frage, wie ein Erreichen der angestrebten Ziele messbar ist. Für den Nachweis der Erfüllung kann BS 15000 eingesetzt werden, mit dieser Methode ist eine objektive Beantwortung der Fragestellung nach der Erreichung der Ziele möglich. Der Standard BS 15000 wird folgendermaßen definiert: „*BS 15000 ist der erste weltweite Standard, der sich speziell auf das IT Service Management bezieht. Dieser Standard beschreibt einen integrierten Satz von Management-Prozessen für die Lieferung von Dienstleistungen.*“ Quelle: [ISO08]. In einem Unternehmen, welches Prozessverbesserungen anstrebt, kann mit Hilfe von Assessments die Fähigkeiten der Prozesse und die aktuelle Reife der Prozesse ermittelt werden. Durch diese Vorgehensweise werden Risiken offen gelegt und der individuelle Handlungsbedarf wird ermittelt. Im konkreten Fall entstehen für Unternehmen Wettbewerbsvorteile, da BS 15000 sicherstellt, dass auf aktuelle Gegebenheiten und Veränderungen entsprechend reagiert werden kann. Das Unternehmen bekommt mit dieser Standardisierung bestätigt, dass es die Flexibilität auf mögliche Veränderungen besitzt und dass es über eine hohe Verfügbarkeit der IT-Services vertrauen kann. Diese Bestätigung wird durch eine externe Stelle offiziell besiegelt.

Der Standard BS 15000 besteht aus folgenden Bestandteilen:

- BS 15000 Part 1: Specification for Service Management, dieser Teil kümmert sich um die Qualität der IT-Services, welches ein Unternehmen bereitstellen muss, um eine vordefinierte Qualitätsstufe zu erreichen. Hier wird keine Unterscheidung getroffen, ob es sich um einen internen oder einen externen Kunden handelt.

- BS 15000 Part 2: Code of Practice for Service Management, bei diesem Abschnitt wird der erste Teil durch Empfehlungen und Anleitungen für die Festlegung eines IT-Service-Managements ergänzt.

- PD 0005: IT Service Management - A Managers Guide, dieser Abschnitt ist eine Beschreibung für das Management für die Zielsetzung der Inhalte von IT Service Management auf der Basis von ITIL.

- PD 0015: IT Service Management Self-Assessment Workbook, mit dieser Vorgabe kann eine Bewertung der bestehenden Prozesse in einem Unternehmen durchgeführt werden. Hier werden Best-Practice-Vorgaben des BS 15000 angegeben.

Der Standard ISO 20000 ist der Nachfolgestandard des BS 15000. Mit diesem Standard wird ebenfalls erreicht, dass ein Unternehmen, welches diesen Standard erfüllt, mit seinen IT-Services Mindestanforderungen an Qualitätsmerkmalen erfüllt. Ein Unternehmen kann also ISO 20000 zertifiziert sein, es kann jedoch nicht ITIL zertifiziert sein. Eine ITIL-Zertifizierung ist nur für Einzelpersonen möglich. Die folgende Gliederung beschreibt die Bestandteile des Standards ISO 20000 [Iso08].

- ISO 20000 Part 1 - Service Management Specification, hier werden jene Kriterien festgehalten welches ein Unternehmen erfüllen muss, um den Standard zu erreichen.

- ISO 20000 Part 2 - Service Management: Code of Practice, hier erfolgt wiederum (vergleichbar mit BS 15000) eine Ergänzung der Kriterien mit Leitlinien und Empfehlungen.

Die folgende Abbildung zeigt den ISO 2000 Service Management Prozess, im Kern befinden sich die zentralen Prozesse mit dem Konfigurations- und Change-Management.

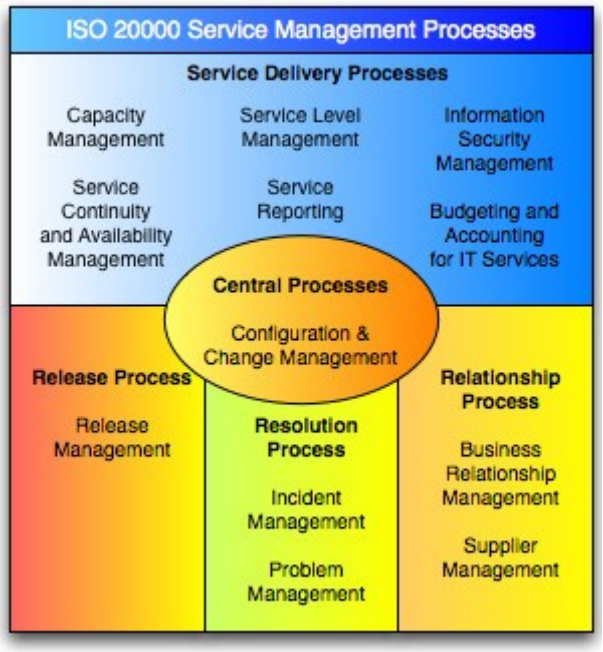

Abbildung 21, ISO 20000 Service Management Prozess . Quelle: [Live08]

7. Konkrete Anwendungen

Ziel dieses Kapitels ist es, die bereits in dieser Ausarbeitung beschriebenen Methoden – Disaster Recovery, Business Continuity Management und ITIL – konkret auf verschiedene Unternehmen anzuwenden. Diese konkrete Umsetzung beinhaltet als erste Maßnahme zu entscheiden, welche der beiden erstgenannten Methoden sich am besten für ein spezifisches Unternehmen eignet. Die Unterscheidung der Unternehmen wird sich nach mehreren Kriterien richten, einerseits nach der Unternehmensgröße (Anzahl der Mitarbeiter und Höhe des Umsatzes) andererseits nach dem Beschäftigungsfeld (zum Beispiel Finanzbereich, Telekommunikationsbranche etc.). Für die Entscheidung welche Methode, Disaster Recovery oder Business Continuity Management, am besten eingesetzt wird, wird eine selbst entwickelte Checkliste angewendet. Durch die Auswertung dieser Checkliste ist es möglich zu entscheiden, welche Methode sich bezüglich eines effizienten, jedoch ökonomischen Einsatz, am besten eignet.

Die folgende Abbildung zeigt den Fragebogen, welcher an verschiedene Unternehmen gesendet wurde. Eine Zusammenarbeit konnte mit zwei Unternehmen erreicht werden, die anderen Unternehmen waren nicht zu einer Kooperation bereit. Die zwei Unternehmen welche den Fragebogen ausfüllten, decken jedoch sehr gut das betrachtete Spektrum an Unternehmen dieser Ausarbeitung: Kleinunternehmen und Unternehmen mittlerer Größe. Der Fragebogen in Abbildung 22 wurde leicht modifiziert an diese beiden Unternehmen gesendet, nachdem sie einer Kooperation zugestimmt hatten.

Befragung

Mitarbeiter

Wie viele Mitarbeiter beschäftigt Ihr Unternehmen?
Wie viele Mitarbeiter haben einen Arbeitsplatz mit Internet?
Wie viele Mitarbeiter brauchen für die Erledigung Ihrer Aufgaben unbedingt Internet?
Durch eine Grippe-Pandemie fallen mehr als die Hälfte Ihrer Mitarbeiter für eine Woche aus.
Wie kritisch betrachten Sie die Auswirkungen für Ihr Unternehmen?

Nicht kritisch	Kritisch	Sehr kritisch

Umsatz

Wie hoch war der Umsatz des letzten Geschäftsjahres?
Wie hoch ist der Anteil bzw. wie hoch schätzen Sie den Anteil des Absatzes über das Internet am Gesamt-Umsatz?

0-30 %	30-60%	60-100 %

Geschäftsprozesse/Geschäftsablauf

Gibt es für Ihr Unternehmen gesetzliche Bestimmungen für bestimmte Geschäftsprozesse?

Ja	Nein

Schätzen Sie den Anteil von kritischen Geschäftsprozessen an der gesamten Anzahl von Geschäftsprozessen:

0-30 %	30-60%	60-100 %

Absatz

Wie kritisch schätzen Sie einen Ausfall des Absatz-Kanals für eine Stunde ein?

Nicht kritisch	Kritisch	Sehr kritisch

Wie kritisch schätzen Sie einen Ausfall des Absatz-Kanals für zehn Stunden ein?

Nicht kritisch	Kritisch	Sehr kritisch

Wie kritisch schätzen Sie einen Ausfall des Absatz-Kanals für einen Tag ein?

Nicht kritisch	Kritisch	Sehr kritisch

Wie kritisch schätzen Sie einen Ausfall des Absatz-Kanals für mehrere Tage ein?

Nicht kritisch	Kritisch	Sehr kritisch

Unterscheiden sich einzelne Geschäftsprozesse hinsichtlich Bedeutung, Wichtigkeit, Auswirkungen bei einem möglichen Ausfall deutlich von anderen Geschäftsprozessen?

Ja	Nein

Welche Geschäftsprozesse sind bei einem Gesamtausfall der IT am stärksten betroffen, d.h. welche Prozesse halten Sie für besonderes wichtig?

Allgemein Unternehmen

Setzen Sie bereits Maßnahmen gegen mögliche Katastrophen/Notfälle in Ihrem Unternehmen ein?

Ja	Nein

Wenn ja, welche:

Welche Unternehmensform hat Ihr Unternehmen? (GmbH, AG, KG etc.)
Ist Ihr Unternehmen stark in der Öffentlichkeit vertreten? (Webpräsenz, Marketing-Maßnahmen etc.)

Ja	Nein

Wie stark ist das Kriterium Sicherheit in Ihrer Unternehmens-Philosophie vertreten?

Nicht stark	Stark	Sehr stark

Gibt es die Möglichkeit manuell die Arbeit fortzusetzen, wenn das IT-System komplett ausfällt?

Ja	Nein

(Ein Beispiel ist die manuelle Verrechnung beim Verkauf von Waren/Schikarten etc.)
Wie schwerwiegend schätzen Sie einen Ausfall des IT-Systems auf die gesamte Geschäftsabwicklung Ihres Unternehmens?

Leicht	Mittel	Schwer

Abbildung 22, Befragung/Checkliste Unternehmen.

Die folgende Abbildung bietet einen Überblick wie Unternehmen entscheiden können, welche Methode für einen Einsatz von Notfall-Strategien am besten geeignet ist. Für diese Entscheidung wird vorausgesetzt, dass Unternehmen Maßnahmen für eine Notfallplanung setzen möchten. Die Entscheidung welche Methode am besten geeignet ist, hängt von ökonomischen und organisatorischen Gesichtspunkten ab. Der ökonomische Gesichtspunkt soll sicherstellen, das die Kosten der eingesetzten Maßnahmen den erhaltenen Nutzen rechtfertigen. Der organisatorische Gesichtspunkt beschäftigt sich mit den verschiedenen Eigenschaften von Unternehmen wie zum Beispiel der Größe des Unternehmens oder der Unternehmensbranche. Ein Unternehmen mit vielen Angestellten braucht zum Beispiel aufgrund der Größe und der Vielzahl von sensiblen Geschäftsprozessen eine unterschiedliche Lösung als ein kleines Architekturbüro. Für das letztgenannte Unternehmen, Architekturbüro, ist ein Verlust von vergangenen und aktuellen Arbeiten ein möglicherweise verhängnisvoller Verlust, jedoch hat dieses Unternehmen keine hohe Anzahl von sensiblen Geschäftsprozessen.

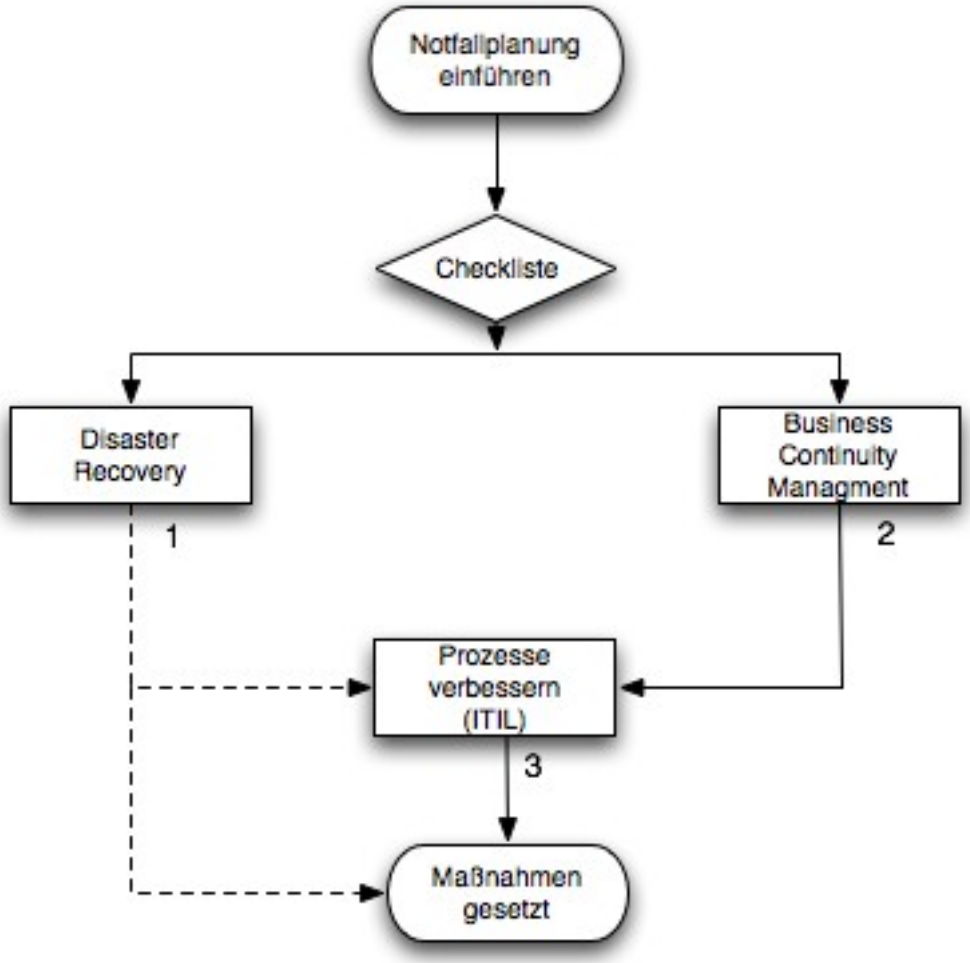

Abbildung 23, Entscheidung Methode Notfallplanung.

Abbildung 23 zeigt den Entscheidungsweg, welche Methode am besten eingesetzt wird. Zu Beginn gibt es ein Unternehmen welches den Beschluss gefasst hat, sich mit Methoden der Notfallplanung beziehungsweise mit der Auseinandersetzung mit kritischen Geschäftsprozessen zu beschäftigen. Nach diesem Entschluss eines Unternehmens solche Maßnahmen einzusetzen erfolgt die Entscheidung, welche Methode eingesetzt wird. Diese Entscheidung erfolgt durch eine Checkliste, welche die entscheidenden Fragen über die Charakteristika eines Unternehmens enthält. Wenn diese Checkliste korrekt und im vollen Umfang ausgefüllt wird, so kann eine Entscheidung getroffen werden, welchen Umfang die Maßnahmen haben müssen. Bei kleineren Unternehmen sowie bei Unternehmen mit wenigen kritischen Geschäftsprozessen wird die Entscheidung zu Disaster Recovery tendieren, während bei größeren Unternehmen beziehungsweise bei Unternehmen mit einer hohen Anzahl von kritischen Geschäftsprozessen die Entscheidung auf Business Continuity Management fallen wird. Im nächsten Schritt werden die identifizierten kritischen Geschäftsprozesse verbessert. Der gestrichelte Pfeil in der Abbildung von Disaster Recovery deutet an, dass diese Verbesserung eine mögliche Option darstellt, jedoch nicht obligatorisch ist. Nach dieser Verbesserung der (kritischen) Prozesse ist ein Unternehmen auf mögliche Notfall-Szenarien vorbereitet. Die Zahlen in der Abbildung (eins bis drei) werden in der folgenden Gliederung erläutert, sie umfassen die jeweiligen Maßnahmen, welche von der spezifischen Methode eingesetzt werden.

Disaster Recovery (1):

- Ablauf bestimmen im Notfall
- Zusammenstellung eines Notfallteams
- Erstellung eines Notfallplans
- Einplanen und Bestimmung von Übungen für den Notfall
- Bestimmung der Kompetenzen
- Wahl eines Disaster-Recovery-Tools

Business Continuity Management (2):

- Festlegung des gewünschten Stabilitätsgrades
- Bestimmung der Aufgaben
- Durchführung einer Kosten-Nutzen-Analyse
- Bestimmung der operationalen Risiken
- Bestimmung der Maßnahmen für ein Krisenmanagement
- Einführung des Phasenmodells
- Wahl eines Continuity-Management-Tools
- (Bestimmung der aktuellen Bedrohungen)

Prozesse verbessern (ITIL) (3):

- Beschreibung/Definition der sensiblen Prozesse
- Identifikation der Verbesserungsmöglichkeiten der einzelnen Prozesse
- Evaluierung durch Key-Performance-Indicators
- Umdenkungsprozess im Unternehmen festlegen
- Zertifizierung nach BS 150000/ISO 20000

7.1. Kleinunternehmen

Für die konkrete Anwendung eines Kleinunternehmens/Mittelbetriebes wurde ein Unternehmen gewählt, welches zwar nur einen geringen Anteil des Erlöses über Internet - Webservices, Verkauf etc. - erzielt, welches jedoch stark in der Öffentlichkeit vertreten ist. Das Unternehmen setzt also stark auf seine positive Darstellung in der Öffentlichkeit und ein Ausfall des IT-Systems würde zu einer schlechten Reputation des Unternehmens führen. Ein Ausfall des IT-Systems zu einer bestimmten Zeit würde auch zu massiven Umsatzverlusten und ebenfalls zu einer schlechten Reputation führen. Aufgrund der Ergebnisse der Checkliste ist für dieses Unternehmen die Methode Disaster Recovery am besten geeignet. Die folgende Gliederung fasst die wichtigsten Fakten zusammen, welche zu einer Entscheidung für Disaster Recovery geführt haben.

- Unternehmen ist stark in der Öffentlichkeit vertreten
- Absatz über Internet macht nur einen sehr geringen Anteil aus
- Ausfall des IT-Systems ist nur zu einer gewissen Zeit sehr kritisch
- Arbeit kann zu einem großen Ausmaß manuell fortgeführt werden
- Es gibt keine gesetzlichen Regelungen für den Schutz bestimmter Geschäftsprozesse

7.1.1. Maßnahmen Disaster Recovery

Der folgende Abschnitt zeigt mögliche Maßnahmen, wie Disaster Recovery in diesem Unternehmen erfolgreich eingeführt wird. Die Beschreibung der einzelnen Maßnahmen befindet sich in Kapitel 3, Disaster Recovery, dieser Ausarbeitung.

7.1.1.1. Ablauf bestimmen im Notfall

Der Ablauf wird in diesem Unternehmen nach folgenden Phasen unterschieden: Enddeckung/Meldung, Bewertung, Eingrenzung, Auslöschung, Wiederherstellung und den Folgemaßnahmen. Für die Phase „Enddeckung/Meldung“ werden die Mitarbeiter zuerst auf das Thema sensibilisiert, d.h. sie wissen über die Form etc. von möglichen Gefahren bescheid und wissen außerdem, wie sie im weiteren Verlauf handeln sollen. Für dieses Unternehmen ist es am besten, wenn ein Formular im Intranet zur Verfügung gestellt wird, welches im Meldungsfall an den Leiter der EDV gesendet wird. Diese Person wird dann auch die nachfolgende Aktion, Bewertung des Vorfalls, durchführen. Der Leiter der EDV entscheidet also, ob es sich bei der Meldung um eine ernsthafte Bedrohung handelt oder nicht. Für diese Bewertung stehen sehr viele Ressourcen zur Verfügung, sehr viele Websites bieten hier kostenlos aktuelle Informationen. Aufgrund der überschaulichen Größe des Unternehmens beziehungsweise des IT-Systems, wird diese Person auch die

Eingrenzung des Vorfalls vornehmen. Hier gilt es zu definieren, welche Bereiche des IT-Systems betroffen sind. Durch den Einsatz eines geeigneten Disaster Recovery Tools wird die Arbeit sehr erleichtert und hilft dabei, dass der „normale“ Ablauf des Unternehmens nicht gestört wird. Es wird auch ermittelt, welche Absicht hinter dem Angriff etc. steckt. Die nächsten Schritte, Bereinigung des Vorfalls und Wiederherstellung, beziehen sich auf die vollständige Wiederherstellung des Systems. Es werden außerdem Maßnahmen getroffen, welche einen zukünftigen Angriff/Vorfall dieser Art nicht mehr erlauben. Bei der nächsten Phase, Folgemaßnahmen, wird eine genaue Dokumentation des Vorfalls angelegt. Diese Dokumentation wird in einer Datenbank gespeichert, um bei einen gleichen oder ähnlichen Fall schnell Zugriff auf diese Ressource zu haben. In diesem Unternehmen werden alle diese Aufgaben vom Leiter der EDV-Abteilung erledigt.

7.1.1.2. Zusammenstellung eines Notfallteams

Das Notfallteam wird bei diesem Unternehmen aus folgenden Personen gebildet: Leiter des PR und des Marketings als Vertreter der Geschäftsführung, Mitarbeiter Controlling, Leiter EDV und ein Mitarbeiter des PR. Begründung: Durch einen Vertreter der Geschäftsführung wird gesichert, dass sich die anderen Mitarbeiter für das Projekt engagieren. Außerdem will die übrige Geschäftsführung über den Verlauf des Projekts aus vertrauenswürdiger Quelle informiert sein. Der Mitarbeiter des Controllings ist sehr gut über die verschiedenen Geschäftsprozesse informiert und kann somit sein Wissen gut in das Projekt einbringen. Der Leiter der EDV kennt das IT-System sehr gut, deswegen ist diese Person sehr wichtig für die Einführung eines funktionierenden Disaster Recoverys. Der Mitarbeiter der PR-Abteilung ist mit den möglichen negativen Auswirkungen im Falle eines Ausfalls des IT-Systems vertraut. Diese negativen Auswirkungen betreffen hier vor allem die negative Reputation des Unternehmens. Im positiven Sinn, nach dem erfolgreichen Einführen der Maßnahmen, kann diese Person auch die positiven Auswirkungen an die verschiedenen Stakeholder kommunizieren. Die folgende Abbildung bietet eine Übersicht über die beteiligten Personen.

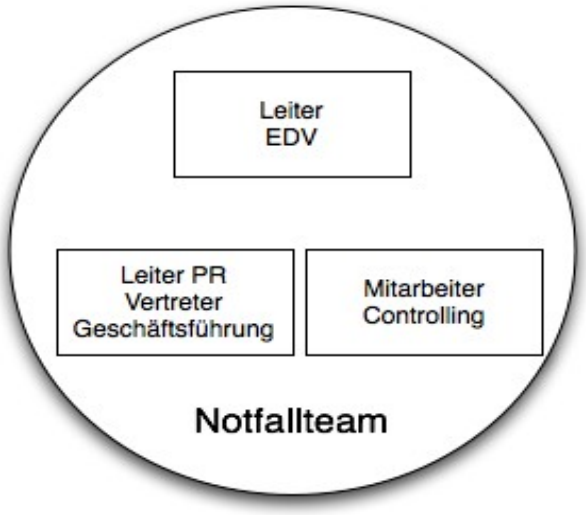

Abbildung 24, Zusammenstellung Notfallteam.

7.1.1.3. Erstellung eines Notfallplans

Für die Erstellung eines Notfallplans sind mehrere Maßnahmen notwendig. Zu Beginn muss im Unternehmen eine Bewusstseinsbildung eingeführt werden, um alle Mitarbeiter von der Notwendigkeit zu überzeugen. In diesem Unternehmen haben sehr viele Mitarbeiter Zugang zum IT-System, deshalb ist diese Maßnahme als sehr wichtig zu betrachten. Diese Bewusstseinsbildung kann in diesem Unternehmen durch unterschiedliche Wege betrieben werden, zum Beispiel durch Präsentationen bei Mitarbeiterversammlungen oder durch den Versand von Informations-Emails. In der vorbereitenden Phase werden die ersten Treffen mit dem Notfall-Team durchgeführt. Diese Treffen dienen zur Festlegung der Ziele und eines Zeitplans. Dieser Zeitplan umfasst auch die wichtigsten Meilensteine auf dem Weg der Einführung. Hier kann auch schon bestimmt werden, welches Disaster Recovery Tool am besten eingesetzt werden kann. Für dieses Unternehmen ist „Acronis True Image 9.1 Enterprise Server“ am besten geeignet, die Begründung für diese Wahl erfolgt später in diesem Kapitel. Nach dem ersten Treffen kann mit der Zusammenstellung der wichtigsten Daten begonnen werden. Diese Daten umfassen dabei die Ausstattung des Arbeitsplatzes und die Bewertung von Ausfällen. Diese Bewertung kann durch einen speziell angepassten Fragebogen erreicht werden.

Bei diesem Unternehmen gibt es noch keinen vorhandenen Notfallplan, ansonsten werden diese Notfallpläne in die Informationsgewinnung miteinbezogen. Die Informationsgewinnung kann in vielen Wegen geschehen, bei diesem Unternehmen werden folgende Maßnahmen den größten Erfolg bringen: Fragebögen, Darstellung Geschäftsprozesse, Auflistung der aktuellen Mitarbeiter. Nach der Zusammenstellung der wichtigsten Daten kann mit der Analyse der bestehenden Risiken begonnen werden. In diesem Unternehmen sind folgende Risiken am wahrscheinlichsten: Fehler bei der Hardware/Software, Schaden durch Feuer, Schaden durch Sturm, Schaden durch Unfälle verschiedenster Art.

7.1.1.4. Einplanen und Bestimmung von Übungen für den Notfall

Für dieses Unternehmen wird ein spezielles Notfall-Handbuch angefertigt. Diese Anfertigung entsteht durch die Zusammenarbeit mit dem Notfall-Team, diese Personen haben alle wichtigen Informationen welche für die Erstellung nötig sind. In diesem Unternehmen wird ein Notfallplan zum ersten Mal eingeführt, deswegen sind sieben Übungen in den ersten drei Jahren notwendig. Diese Anzahl ist zwar aufgrund der Größe des Unternehmens nicht unbedingt erforderlich, jedoch gibt es in diesem Unternehmen eine hohe Mitarbeiter-Fluktuation und es ist die erste Einführung eines Notfallplans. Die folgende Tabelle zeigt die Übungen für die ersten drei Jahre.

Jahr	Anzahl	Maßnahmen	Ergebnisse
1	3	Überprüfung der Netzwerkinfrastruktur, Definition unternehmenskritische Geschäftsprozesse	Kassen-System ist sehr kritisch, Verbesserungsmöglichkeiten Infrastruktur
2	2	Wiederholung der Übungen aus dem 1.	Einsatz neuer Tools,

		Jahr, Überprüfung Backup-Prozesse	Aktualisierung/Schulung neuer Mitarbeiter
3	2	Aktualisierung/Überprüfung unternehmenskritische Geschäftsprozesse unter Extrembedingungen	Aktualisierung der Ergebnisse aus dem 1. Jahr in der am stärksten frequentierten Zeit (Extrembedingung)

Tabelle 20, Durchführung Notfalltests Unternehmen

7.1.1.5. Bestimmung der Kompetenzen

In diesem Unternehmen wird nach dem „need-to-know“-Prinzip vorgegangen. Es werden also nur jene Daten zur Verfügung gestellt, welche unbedingt für den effizienten Einsatz von Disaster Recovery benötigt werden. Alle anderen Daten werden explizit nicht zur Verfügung gestellt. Welche Daten benötigt werden, wird bei den einzelnen Treffen vereinbart und durch die verschiedenen Mitglieder des Projekt-Teams überprüft.

7.1.1.6. Wahl eines Disaster-Recovery-Tools

Bei der Auswahl des am besten geeigneten Disaster Recovery Tools ist das Unternehmen mit „Acronis True Image 9.1 Enterprise Server“ am besten beraten. Aufgrund der Testergebnisse und der relativ geringen Kosten empfiehlt sich dieses Produkt. Die umfangreichen Möglichkeiten dieses Tools bieten eine große Hilfe beziehungsweise in weiterer Folge auch einen großen Schutz für das Unternehmen. Dieses Unternehmen beschäftigt viele Mitarbeiter, welche zu einem sehr hohen Anteil Internet für die Erledigung ihrer Aufgaben benötigen. Die Frage nach einem Ausfall eines großen Anteils der Mitarbeiter aufgrund einer Grippe-Pandemie wird als sehr kritisch eingestuft.

7.2. Unternehmen mittlerer Größe

Bei den ermittelten Daten des Unternehmens mittlerer Größe und durch die Auswertung der Checkliste fiel die Entscheidung eindeutig auf einen Einsatz von Business Continuity Management. Dieses Unternehmen ist sehr stark in der Öffentlichkeit vertreten und setzt in der Unternehmensphilosophie sehr stark auf das Kriterium Sicherheit. Im Falle eines publik werdenden Vorfalls ist die negative Reputation aufgrund der Bedeutung von Sicherheit in diesem Unternehmen schwerwiegend. Dieses Unternehmen hat auch einen hohen Anteil von unternehmenskritischen Geschäftsprozessen. Das bedeutet, ein Ausfall des IT-Systems hat schwerwiegende Auswirkungen auf den Geschäftsablauf des Unternehmens. Bei der Frage nach den Auswirkungen eines Ausfalls für eine bestimmte Zeit des Absatz-Kanals wurden die längerfristigen Zeiträume als sehr kritisch eingestuft. Es gibt zwar keine gesetzlichen Vorschriften für den Schutz einzelner Geschäftsprozesse des Unternehmens, jedoch wurde ein Ausfall des IT-Systems für die gesamte Geschäftsabwicklung als kritisch eingestuft. Die folgende Gliederung bietet eine Übersicht über die wichtigsten Fakten, welche zu einer Entscheidung für Business Continuity Management geführt haben. Die folgende Tabelle fasst die Antworten des Unternehmens zusammen.

Frage	Antwort
Mitarbeiter im Unternehmen	2100
Davon benötigen Internet	2.100
Einstufung eines Ausfalls mehr als die Hälfte der Mitarbeiter	Kritisch
Umsatz letztes Geschäftsjahr	1.500.000.000
Anteil Absatz über das Internet	0-30 %
Gesetzliche Bestimmungen für bestimmte Geschäftsprozesse	Ja
Einschätzung Absatz-Kanal für eine Stunde	Nicht kritisch
Einschätzung Absatz-Kanal für zehn Stunden	Kritisch
Einschätzung Absatz-Kanal für einen Tag	Kritisch
Einschätzung Absatz-Kanal für mehrere Tage	Sehr kritisch
Unterschied einzelnen Geschäftsprozesse hinsichtlich Bedeutung von anderen	Ja
Geschäftsprozesse, welche bei einem Gesamtausfall der IT am stärksten betroffen sind	Billing, Provisioning, Verkauf
Bereits vorhandene Maßnahmen gegen mögliche Katastrophen/Notfälle	Krisenmanagement; Katastrophenvorsorgepläne, Wiederanlaufpläne, Evaluierung der Bedrohungsszenarien, Desastertolerante Lösungen inkl. Regelmäßige Tests, verteilte Rechenzentren
Unternehmensform	AG
Stark in der Öffentlichkeit vertreten	Ja
Sicherheit wichtiges Kriterium in der Unternehmens-Philosophie	Sehr stark
Manuelle Fortsetzung der Arbeit möglich	Ja
Auswirkungen auf die gesamte Geschäftsabwicklung des Unternehmens	Mittel

Tabelle 21, Ergebnisse Befragung mittelgroßes Unternehmen

Kurz zusammengefasst hat dieses Unternehmen folgende wichtige Charakteristika hinsichtlich einer Business-Continuity-Planung: Sehr starkes Augenmerk auf Sicherheit, das Unternehmen ist stark in der Öffentlichkeit vertreten, ein Ausfall eines großen Anteils der Mitarbeiter wird als sehr kritisch eingestuft, es gibt einige geschäftskritische Prozesse, alle Mitarbeiter benötigen für die Erledigung ihrer Aufgaben Internet, ein Ausfall des IT-Systems hat mittelschwere Auswirkungen auf die gesamte Geschäftsabwicklung des Unternehmens.

7.2.1. Maßnahmen Business Continuity Management

Der folgende Abschnitt zeigt mögliche Maßnahmen, wie Business Continuity Management in diesem Unternehmen eingeführt werden kann. Die Beschreibung der einzelnen Maßnahmen befindet sich in Kapitel 4, Business Continuity Management, dieser Ausarbeitung.

7.2.1.1. Festlegung des gewünschten Stabilitätsgrades

Für dieses Unternehmen ist es wichtig, dass Stabilität hinsichtlich des IT-Systems besteht. Dieses Unternehmen ist ein Dienstleistungsunternehmen und die Sicherheit spielt eine große Rolle in der Unternehmens-Philosophie. Deswegen werden auch schon sehr sicherheitsspezifische Maßnahmen im Unternehmen eingesetzt. Der gewünschte Stabilitätsgrad ist also sehr hoch einzustufen.

7.2.1.2. Bestimmung der Aufgaben

Für dieses Unternehmen werden die Aufgaben nach zwei verschiedenen Sichtweisen bestimmt, auf der einen Seite aus der Sichtweise des Geschäftsbetriebes und auf der anderen Seite aus der Sichtweise der Softwarehersteller. Aus der Sichtweise des Geschäftsbetriebes sind die wichtigsten Geschäftsprozesse des Unternehmens Provisioning, Billing und Verkauf. Diese Geschäftsprozesse werden mit der höchsten Priorität behandelt. Im Falle eines Notfalls steht die Sicherheit der Mitarbeiter an vorderster Stelle, deswegen muss bei den eingesetzten Übungen eine besondere Beachtung dieses Kriteriums eingeplant werden. Für das Unternehmen ist es auch sehr wichtig, die Fähigkeit zur Krisenbewältigung zu erreichen. Für eine effiziente Bewältigung einer Krise ist es nötig, pro aktiv auf die möglichen Auswirkungen einer Problemsituation zu planen. Eine weitere Aufgabe ist die Fähigkeit zur Notfallplanung. Das Unternehmen besitzt bereits einen Plan, welcher die wichtigsten Kriterien für eine unterbrechungsfreie Abwicklung eines Notfalls beinhaltet. Eine weitere, wichtige Aufgabe ist die Schaffung eines Risikobewusstseins unter allen Mitarbeitern. Einzig durch die Affinität auf die mögliche Reaktion in einer bestimmten Situation kann eine effektive Notfallplanung funktionieren. Aus der Sichtweise der Softwareherstellers ist die Sicherheit/Funktionsweise der eingesetzten externen Software zu beachten. Durch die Erfahrungswerte, zum Beispiel Ausfallzeiten, Fehleranfälligkeit etc., werden bestimmte Lieferanten anderen Lieferanten vorgezogen. Ein bestimmtes Restrisiko kann nie ausgeschlossen werden.

7.2.1.3. Bestimmung der operationalen Risiken

In diesem Abschnitt werden die operationalen Risiken festgelegt, welche das Unternehmen betreffen. Zu diesen Risiken zählen die äußere Faktoren, welche das Unternehmen betreffen: Leistungsfluss zwischen Kunden und Lieferanten, Dienstleistungen durch externe Lieferanten/Partner, kriminelle Aktivitäten innerhalb des Unternehmens und von außerhalb und die politische Situation in der Region. Weiters müssen auch die möglichen Naturkatastrophen in den Regionen, wo das Unternehmen tätig ist, beachtet werden.

7.2.1.4. Bestimmung der Maßnahmen für ein Krisenmanagement

Um die Führungsebene für den Einsatz von Krisenmanagement-Maßnahmen zu überzeugen, empfehlen sich für das Unternehmen beziehungsweise für die Führungsebene folgende Anreize: Sicherheit des Arbeitsplatzes, Anerkennung durch Vorgesetzte und Mitarbeiter oder durch die finanzielle Belohnung. Für das Unternehmen ist es effizient, wenn Pläne für eine zentrale Informationsstelle in einem Krisenfall erstellt werden. Diese Pläne umfassen dabei unter anderen die Namen der Personen, welche im Krisenfall bestimmte Aufgaben zu erfüllen haben.

7.2.1.5. Einführung des Phasenmodells

Für die Etablierung eines funktionieren Business Continuity Managements ist das Phasenmodell eine große Hilfestellung. Für dieses Unternehmen umfasst das Phasenmodell folgende Phasen: Untersuchung und Analyse, Lösungsarchitektur, Implementierung, Test und Freigabe und Wartung und Entwicklung. Die erste Phase, Untersuchung und Analyse, teilt sich auf zwei Abschnitte auf: Schadensabschätzung und Risikoanalyse. Bei der Schadensabschätzung werden für das Unternehmen die Auswirkungen von möglichen Notfällen/Krisen festgelegt. Für dieses Unternehmen ist ein Ausfall des IT-Systems ein großer Schaden in Hinsicht auf das Image des Unternehmens. Bei der Risikoanalyse werden jene Prozesse am höchsten priorisiert, welche den größten Schaden anrichten können. Für dieses Unternehmen sind die Prozesse mit der höchsten Priorisierung Billing, Provisioning und Absatz. Hier werden auch die Wahrscheinlichkeiten der möglichen Bedrohungen festgehalten. Die Lösungsarchitektur legt fest, auf welche Art und Weise auf einen bestimmten Vorfall reagiert wird. Tritt ein Vorfall ein, wird die Führungsebene im Unternehmen informiert und entscheidet über die Handlungsweise. Die Führungsebene entscheidet auch, welche Teile/Prozesse sofort wiederhergestellt werden und welche erst später. Die Implementierung umfasst den konkreten Einsatz der Maßnahmen, welche in den vorigen Phasen geplant wurden. Zu den Aufgaben der Implementierung zählt zum Beispiel das Erfassen eines Notfallplans oder das Erfassen der Informationen über die aktuellen Mitarbeiter. Die Phase Test und Freigabe gibt bei der erfolgreicher Überprüfung der Maßnahmen frei – damit erfolgt der tatsächliche Einsatz im Unternehmen. Die abschließende Phase, Wartung und Entwicklung, zielt auf die ständige Aktualisierung der Maßnahmen ab.

7.2.1.6. Wahl eines Business-Continuity-Management-Tools

Für das Unternehmen ist, unter Berücksichtigung der in der Arbeit beschriebenen Tools, der Einsatz von „XENCOS“ empfehlenswert. Durch dieses Tool ist ein umfassendes Business-Continuity-Management mit nur einem Tool möglich.

7.2.2. Verbesserungsmöglichkeiten durch ITIL v3 CSI

Dieser Abschnitt beschreibt die Möglichkeiten der Prozessverbesserung mit dem ITIL v3 Continual Service Improvement-Framework. Die Maßnahmen, welche in Kapitel 7 beschrieben werden, werden vor allem auf die beiden kritischen Prozesse „Billing“ und „Provisioning“ des Unternehmens angewendet. Dieser Abschnitt beinhaltet die Kategorien

7-Step Improvement, Service Report, Messung des Services, ROI für CSI und die Festlegung eines ROI für CSI. Der 7-Step Improvement Prozess beschreibt den Weg, wie ein Service verbessert werden kann. Der Service-Report beschreibt die Aufbereitung von wichtigen Daten für die verschiedenen Zielgruppen. Die Messung des Services beschreibt die Möglichkeit der ganzheitlichen Überprüfung eines Unternehmens-Services. Der ROI für CSI beschreibt die Möglichkeit, den Nutzen von CSI-Maßnahmen in Zahlen auszudrücken. Die Festlegung eines ROI für CSI beschreibt den Vergleich von Kosten von Verbesserungsmaßnahmen verglichen mit dem erhaltenen Nutzen.

7.2.2.1. 7-Step Improvement Prozess

- Festlegung was gemessen werden soll

Für das Unternehmen wird wird eine Analyse des gesamten Geschäftsbereichs und der IT durchgeführt um zu sehen, wo das Unternehmen gerade steht.

- Festlegung was gemessen werden kann

Hier kommt eine Gap-Analyse zum Einsatz um zu sehen, wo sich Lücken zwischen der gewünschten Situation und der tatsächlichen Situation ergeben.

- Sammlung der Daten

In dieser Phase werden die Daten gesammelt um sie in weiterer Folge bearbeiten zu können. Input-Möglichkeiten des Unternehmens sind beispielsweise Kundenzufriedenheits-Umfragen oder Kapazitäten-Pläne.

- Bearbeitung der Daten

In dieser Phase werden die Input-Daten in analysierbare Daten umgewandelt.

- Analyse der Daten

Die Analyse der Daten kann als Übersetzung gesehen werden, es werden Fachbegriffe der IT in für das Management verständliche Begriffe transformiert. Für diese Aufgabe ist eine Person am besten geeignet, welche über Wissen von beiden Berufsgruppen verfügt.

- Präsentieren und Verwendung der Informationen

Das Unternehmen legt fest, ob die Zielvorgaben erreicht wurden oder nicht.

- Implementierung verbessertes Service

In dieser Phase werden die zuvor geplanten Verbesserung in der Praxis umgesetzt.

7.2.2.2. Service Report

- Entwicklung eines Service-Messungs-Frameworks

Zu Beginn bei der Erstellung eines Service-Messungs-Frameworks ist eine Identifikation der kritischsten Prozesse durchzuführen. Durch die Befragung des Unternehmens wurden diese beiden Prozesse als sehr kritisch eingestuft: Provisioning und Billing. Für diese kritischen Prozesse soll ein Verständnis aufgebaut werden, um Verbesserungspotenziale zu identifizieren. Bei der Erstellung eines Frameworks ist darauf zu achten, dass messbare Ergebnisse für Kunden entstehen. Beim Prozess „Billing“ ist beispielsweise der messbare Erfolg für Kunden, dass die erhaltenen Rechnung zu 99,5 Prozent die wahren Kosten berechnet. Diese Kennzahl ist ein für einen Teil der Stakeholder ein Vorteil, für einen anderen Teil wie zum Beispiel der Aktionäre ist eine Einsparung der Kosten durch Kundenanfragen betreffend der Rechnungsstellungen ein Vorteil. Für einen weiteren Teil der Stakeholder, die Lieferanten, ist eine Einhaltung der vereinbarten SLA´s und damit verbundene vereinbarte Prämien ein Vorteil.

- Verschiedene Levels von Messung und Reports

Für die Erstellung eines umfassenden Frameworks ist eine ganzheitliche Betrachtung aller Teile eines Systems notwendig. Beim Beispiel-Prozess „Billing“ kann dabei der eingesetzte Server als unterste Ebene betrachtet werden. Hier kann eine Messung der Performance des Servers durchgeführt werden, die Messungen werden innerhalb definierter Toleranz-Grenzen durchgeführt. Zusammen mit anderen Komponenten-Messungen wird ein Vergleich mit wichtigen KPI´s durchgeführt, um Stärken/Schwächen zu identifizieren. Aus den Ergebnissen der Vergleiche werden Service-Scorecards und Service-Dashboards erstellt. Diese Ergebnisse fließen wiederum in eine IT-Scorecard oder Balanced Scorecard ein. Das Ergebnis dieses Ablaufs sind umfassende Informationen über das betrachtete Service wie zum Beispiel „Billing“.

- Definition des Inhalts der Messung

Die folgende Tabelle bietet einen Überblick über Kategorien, welche für den Prozess „Billing“ für den Kunden eine Steigerung der Qualität des Services bedeuten.

Kategorie	Definition
Produktivität	Wie schnell kann ein Kunde zum Beispiel seine Rechnung im Internet abrufen, wie sieht dabei die Performance der IT aus
Kundenzufriedenheit	Durchführung einer Umfrage bezüglich der Zufriedenheit
Value Chain	Hier kann zum Beispiel die mittelfristige Kundenbindung als Indiz für positive Performance ausgelegt werden

Ganzheitliche Performance	Hier kann ein Vergleich mit anderen Services des Unternehmens oder mit Services anderer Unternehmen gemacht werden
Geschäftsausrichtung	Anpassung des Services an der gesamten Geschäftsstrategie
Investitionsauswirkungen	Finanzielle Betrachtung von IT-Investitionen für die Verbesserung des Services
Management-Vision	Kommunikation der Auswirkungen der Verbesserung des Services

Tabelle 22, Kategorien Messung Unternehmens-Performance

- Festlegung von Zielen

Für die konkrete Festlegung von Zielen ist es notwendig für das Unternehmen, die Kapazitäten zu kennen. Die Zielsetzung ist umfassend zu gestalten und nicht auf einzelne Teilbereiche anzuwenden. Für den Prozess „Billing“ ist die Kundenzufriedenheit mit diesem Service eine umfassende Zielgestaltung. Im Gegensatz dazu ist die Betrachtung der Anzahl von Reklamationen zu diesem Service zu spezifisch und führt nicht zu einer Verbesserung des gesamten Services.

- Service-Management Prozess-Messung

Hier erfolgt eine interne Betrachtung des Prozesses. Es wird beobachtet, wie viele Ausfallzeiten oder andere Probleme durch fehlerhafte Behandlung des IT-Systems resümieren und es werden, bei negativen Ergebnissen, Konsequenzen daraus gezogen.

- Interpretation und Verwendung von Messzahlen

In diesem Abschnitt wird beobachtet, ob die erhaltenen Ergebnisse der Messung realistische Werte ergeben. Ob es sich um ein realistisches Ergebnis der Messung des Prozesses „Billing“ handelt kann durch einen Vergleich von beispielsweise Werten des Vorjahres festgestellt werden. Für diese Feststellung wird jedoch vorausgesetzt, dass sich keine gravierenden Änderungen des Services innerhalb des betrachteten Zeitraums ergaben.

- Anlegen von Scorecards und Reports

Bei der Erstellung von Scorecards und Reports wird speziell auf die verschiedenen Unternehmensbereiche des Unternehmens eingegangen. Das bedeutet, es gibt verschiedene Reports zum Beispiel für die Geschäftsführung und für die IT-Abteilung. Bei der Balanced-Scorecard werden alle unterschiedlichen Geschäftsbereiche und auch die verschiedenen Perspektiven der verschiedenen Bereiche in einer Ausarbeitung zusammengefasst.

- Erstellung von CSI-Policen

Hier erfolgt eine Erstellung von Policen, welche verschiedene Ausprägungen haben. Für den Prozess „Billing“ ist zum Beispiel eine Überwachungspolice sinnvoll. Bei der Sammlung von Daten für die Erstellung dieser Police ist darauf zu achten, dass diese Daten eine konstante Basis aufweisen und damit analysierbar sind. Die Erstellung von Schlüssel-Performance-Indikatoren ist ebenfalls für die Verbesserung des Services sinnvoll. Ein Vergleich der tatsächlichen Situation mit den Indikatoren zeigt Verbesserungspotenziale an.

7.2.2.3. Return of Investment von CSI

Für eine Unterstützung der CSI-Maßnahmen ist es erforderlich das Management über die Sinnhaftigkeit zu überzeugen. Diese Überzeugungsarbeit kann dadurch erreicht werden, wenn folgende Schritte unternommen werden:

- Aufbau eines Verständnisses für die aktuelle IT-Situation inklusive Kosten
- Aufbau eines Verständnisses für die wichtigsten Bereiche eines Geschäftes inklusive Verbindung zur IT
- Definition der gesamten Kosten einer IT-Downtime

7.2.2.4. Festlegung eines ROI für CSI

Der ROI für CSI ist sehr komplex und deswegen sehr schwierig zu ermitteln. Für das Unternehmen ist es erforderlich, die Antworten auf folgende Fragestellungen zu ermitteln:

- Kosten einer Downtime
- Kosten von Nacharbeiten
- Kosten redundanter Arbeit
- Kosten von nicht-gewinnbringenden Projekten
- Kosten von verspäteten Lieferung einer Applikation
- Kosten third/second/first-level-Support

7.2.2.5. Messung von erreichten Vorteilen

In dieser Phase wird überprüft, ob eine tatsächliche Verbesserung des betrachteten Services stattgefunden hat oder nicht. Folgende Punkte helfen bei der Entscheidung, ob die Vorgänge erfolgreich waren:

- Tatsächliche Realisierung der anvisierten Ziele
- Erreichung der Benefits durch die durchgeführten Verbesserungen
- Erreichung des Ziel-ROI
- Erreichung des VOI

7.2.2.6. Evaluierung durch Key-Performance-Indikatoren

Es werden sehr häufig KPI´s für eine Messung der Qualität eines Services eingesetzt werden. Folgende KPI´s werden für das Unternehmen vorgeschlagen:

- Abdeckungsgrad aller gefundenen Risiken
- Anzahl der durchgeführten Notfallübungen
- Kosten der Business-Continuity-Maßnahmen
- Änderungen an den Continuity-Plänen (Update nach Tests etc.)
- Ausräumen von schwerwiegenden Störungen am System
- Abgeschlossene Kooperationsverträge im Falle von Störungen
- Anzahl der durchgeführten Audits
- Anzahl (nicht) erreichter Continuity-Anforderungen
- Anzahl der vertraglich vereinbarten Rahmenbedingungen, welche nicht durch den IT Continuity-Plan abgedeckt werden
- Anzahl der Ausfälle von IT-Services in der Folge von nicht-ausreichenden Sicherheitsmaßnahmen im Notfall
- Anzahl der durchgeführten Notfallübungen

7.2.2.7. Zertifizierung nach BS 150000/ISO 20000

Für das Unternehmen wird die Zertifizierung nach dem Standard ISO 20000 vorgeschlagen. Diese Zertifizierung bringt den Nachweis, dass die Maßnahmen nach dem ITIL-Framework Wirkung zeigen. Eine erfolgreiche Zertifizierung kann auch als Nachweis für die Qualität der einzelnen Services bei der Kommunikation mit Stakeholdern verwendet werden.

8. Zusammenfassung

Die vorliegende Arbeit beschäftigt sich mit dem aktuellen Thema der Notfallplanung in der IT. Darüber hinaus wird eine Möglichkeit definiert, wie sich die Qualität von Geschäftsprozessen von Unternehmen mit eingeführter Notfallplanung weiter kontinuierlich steigern lässt. Die Methoden für die Notfallplanung umfassen dabei Business Continuity Management und IT-Service Continuity. Die Möglichkeit für die weitere kontinuierliche Verbesserung von Geschäftsprozessen wird mit ITIL v3 Continual Service Improvement erreicht. Continual Service Improvement ist ein Teil des aktuellen ITIL-Werkes der dritten Version.

Zu Beginn der Arbeit erfolgt eine Beschreibung von Rechenzentren. Der Abschnitt Rechenzentren beschäftigt sich mit der eingesetzten Hardware von Unternehmen. Da der Aufbau von solchen IT-Systemen sehr komplex ist, wurde anhand eines konkreten Beispiels erklärt, welche Komponenten benötigt werden und wie die organisatorischen Rahmenbedingungen dazu aussehen. Dieses Beispiel behandelt das Rechenzentrum der Technischen Universität Wien und eignet sich deshalb für die Zielgruppe dieser Ausarbeitung, Unternehmen mittlerer und kleiner Größe, sehr gut.

Der nächste Abschnitt, ITIL und moderne IT-Architekturen, beschäftigt sich mit aktuellen Themen der IT-Strategie: Das ITIL-Werk und Serviceorientierte Architekturen. Zu Beginn

des Kapitels wird die Geschichte des ITIL-Werkes beschrieben und danach erfolgt ein Vergleich der verschiedenen Versionen. Der Abschnitt Serviceorientierte Architekturen definiert Möglichkeiten und Auswirkungen des Einsatzes dieses IT-Ansatzes. Dieser Ansatz verfolgt das Ziel, Dienste von Unternehmen zu strukturieren und damit effizienter nutzbar zu machen. Zusammen mit dem ITIL-Werk bieten diese beiden Methoden große Chancen für Unternehmen in der aktuellen Geschäftswelt. In diesem Abschnitt wird die Hypothese aufgestellt was man mittels ITIL machen kann, wenn man in einer Supply-Chain keinen direkten Einfluss auf die Leistungserstellung eines Produktionsablaufs oder einer Dienstleistungs-Erstellung hat. Eine Antwort auf diese Fragestellung ist die effiziente Verhandlung von SLA´s mit Hilfe von rechtlicher Absicherung durch Verträge.
Im nächsten Abschnitt der Ausarbeitung wird Business Continuity Management behandelt. Bei dieser Methode steht, im Gegensatz zu IT-Service Continuity, die Aufrechterhaltung bestimmter Prozesse im Vordergrund. Diese Methode ist stark prozessorientiert was bedeutet, dass bestimmte Abläufe in einem Unternehmen aufgrund ihrer Eigenschaften als besonders kritisch eingestuft werden und deswegen speziell behandelt werden. Bei dieser Methode ist eine Strategie für die Einführung von Notfallplanung notwendig, die einzelnen Schritte umfassen dabei die Definition der wichtigsten Geschäftsprozesse, die Beschreibung der gewünschten Stabilität der Prozesse, die Aufgaben von Business Continuity, eine Definition der operationalen Risiken, Maßnahmen für ein Krisenmanagement und möglicherweise das Phasenmodell – welches einen Leitfaden für die Einführung von Business Continuity Management bereitstellt.
IT-Service Continuity umfasst Maßnahmen, welche nach beziehungsweise während einem mehr oder weniger unvorhersehbaren Ereignis betreffend die IT eines Unternehmens durchgeführt werden können. Solche Ereignisse sind verschiedenster Natur, mögliche Ereignisse sind Naturkatastrophen, Feuer oder eine Krankheit vieler Mitarbeiter zur selben Zeit. Mit IT-Service Continuity ist eine umfassende, pro aktive Planung der möglichen Szenarien möglich. Um Disaster Recovery-Maßnahmen in einem Unternehmen einzuführen, ist eine umfassende Strategie notwendig. In der Ausarbeitung werden jene Maßnahmen beschrieben welche notwendig sind, um eine wirksame Notfallplanung in einem Unternehmen zu etablieren.
Der Abschnitt Effektives IT-Service Continuity durch Continual Service Improvement beschreibt konkret jene Maßnahmen welche Unternehmen einsetzen können, um ein Service kontinuierlich zu verbessern. Dabei sind folgende Schritte notwendig: Der 7-Step-Improvement Prozess, der Service Report, die Service Messung, die Festlegung eines Return of Investment für Continual Service Improvement sowie die Messung von erreichten Vorteilen. In diesem Abschnitt werden die Methoden des neuesten ITIL-Werkes für eine kontinuierliche Verbesserung von Prozessen/Services vorgestellt.
Das Kapitel Konkrete Anwendungen beschreibt die beispielhafte Anwendung der vorher definierten Methoden IT-Service Continuity, Business Continuity Management und effektives IT-Service Continuity durch ITIL v3 Continual Service Improvement. Dabei werden zwei Unternehmen behandelt, welche über ihre Strategie hinsichtlich Notfallplanung mittels eines Fragebogens befragt wurden. Diese Unternehmen haben unterschiedliche Eigenschaften, wie zum Beispiel Größe und Anzahl von sensiblen

Geschäftsprozessen. Diese und weitere Eigenschaften führen zur Anwendung einer entwickelten Checkliste welche vorschlägt, welche Methode (IT-Service Continuity oder Business Continuity Management) für ein Unternehmen hinsichtlich ökonomischer Faktoren etc. besser geeignet ist. Konkret angewendet auf die beiden behandelten Unternehmen werden IT-Service Continuity-Maßnahmen für das kleinere Unternehmen und Business Continuity-Maßnahmen für das größere Unternehmen vorgeschlagen. Diese Vorschläge wurden auf das jeweilige Unternehmen angewendet und sollen die Möglichkeiten der jeweiligen Methode beleuchten. Für das größere Unternehmen wurde außerdem vorgeschlagen, wie die kritischen Geschäftsprozesse mit den Methoden des ITIL v3 Continual Service Improvement verbessert werden können.
Die Ausarbeitung der Arbeit erfolgte zu Beginn durch eine umfassende Recherche zu diesem noch verhältnismäßig wenig bearbeiteten Thema. Das Kapitel Konkrete Anwendungen enthält Vorschläge für eine Notfallplanung für zwei kooperierende Unternehmen. Dieser Teilbereich der IT-Strategie, Notfallplanung, wird auch in Zukunft einen großen Stellenwert einnehmen beziehungsweise wird sich zu einem wichtigen Bereich entwickeln. Viele Studien bestätigen, dass unvorhersehbare Ereignisse jeglicher Natur immer häufiger auftreten. Die Bedeutung der IT wird ebenfalls in der absehbaren Zukunft nicht abnehmen sondern noch weiter zunehmen. Eine wichtige Aufgabe in der Zukunft wird es sein, einen Umdenkungsprozess bei allen Mitarbeitern eines Unternehmens einzuführen. Durch eine Sensibilisierung der Mitarbeiter können viele Ereignisse im Vorhinein abgewendet werden. Für die automatisierte Unterstützung erfolgt auf jeden Fall eine Weiterentwicklung der bereits vorhandenen Tools, sodaß in einigen Jahren eine noch ausgeprägtere Hilfestellung/Automatisierung gegeben sein wird. Der Einsatz von Maßnahmen für die Notfallplanung wird zunehmen, da sich die Verantwortlichen über mögliche Auswirkungen bewusst werden beziehungsweise da es noch zusätzliche gesetzliche Bestimmungen für Notfall-Maßnahmen geben wird. So lange wie die gesetzlichen Bestimmungen noch weitgehend fehlen, werden viele Unternehmen durch fehlende Notfall-Strategien die Geschäftstätigkeit aufgeben müssen.

9. Quellenverzeichnis

[Acon08] ACOnet: Organisation. http://www.aco.net/organisation.html?&L=0&F= (19.04.2008), 2008.

[Acro07] Acronis: Compute with Confidence. http://www.acronis.de/enterprise/products/ATIES/, (04.12.2007), 2007.

[Beck08] P. Beckman, C. Bash, C. Patel, M. Beitelmal: Clusters, Servers, Thin Clients, and On-line Communities. http://www.springerlink.com/content/20bfelt4ruu1nyfe/fulltext.pdf (09.04.2008), 2008.

[Bozm07] J. Bozman: Der betriebswirtschaftliche Nutzen von IBM System i für mittelgroße Unternehmen.

http://www.03.ibm.com/systems/i/advantages/pdf/ISL03007DEDE.PDF (10.04.2008), 2008.

[Bull07] Bullhost: EDV Definition bzw. Erklärung: MAN – Metropolitan Area Network. http://www.bullhost.de/m/man.html (10.12.2007), 2007.

[Disc06] L. Dietrich, W. Schirra: Innovationen durch IT : Erfolgsbeispiele aus der Praxis ; Produkte, Prozesse, Geschäftsmodelle. Addison-Wesley; 2. Auflage, 1998.

[DiSc06] L. Dietrich, W. Schirra: Innovationen durch IT, Erfolgsbeispiele aus der Praxis Produkte-Prozesse-Geschäftsmodelle. http://www.springerlink.com/content/n2l71158336258wg/fulltext.pdf (22.02.2008), 2006.

[Dude07] Duden, Deutsches Universalwörterbuch: Das umfassende Bedeutungswörterbuch der deutschen Gegenwartssprache. Dudenverlag; 6. Auflage, 2007.

[Edra07] EdrawSoft: Vector-Based Graphic Design. http://www.edrawsoft.com/Campus-Network.php, (04.12.2007), 2007.

[Géan08] GÉAN: GÉAN. http://www.geant2.net/ (19.04.2008), 2008.

[Glen06] Glenfis: BS 15000 – ITIL, Der neue IT Service Management Standard Framework. http://www.bs15000certification.com/news.asp?NewsID=16 (04.02.2008), 2006.

[Grba04] P. Grässle, H. Baumann, P. Baumann: UML 2.0 projektorientiert. Galileo Computing; 3. Auflage, 2004.

[Grei05] W. Greis: Die IBM-Mainframe-Architektur. Open Source Press; 1. Auflage, 2005.

[Hein08a] Heine und Partner: CAPT. http://www.heine-partner.de/uploads/media/Produktblatt_CAPT.pdf, (13.01.2008), 2008.

[Hein08b] Heine und Partner: CM http://www.heine-partner.de/uploads/media/Produktblatt_CM_01.pdf, (13.01.2008), 2008.

[Hein08c] Heine und Partner: RISK http://www.heine-partner.de/uploads/media/Produktblatt_RISK.pdf, (14.01.2008), 2008.

[Hein08d] Heine und Partner: Xencos http://www.heine-partner.de/uploads/media/Xencos_Factsheet.pdf, (14.01.2008), 2008.

[Hein08e] Heine und Partner. http://www.heine-partner.de/uploads/media/XENCOS-Fact_Sheet_V02.1.pdf, (15.01.2008), 2008.

[IBM08a] IBM: IBM System i 520. http://www.ibm.com/common/ssi/fcgi-bin/ssialias?infotype=PM&subtype=SP&htmlfid=ISD00001USEN&attachment=ISD00001USEN.PDF&appname=STG_IS_USEN_SP (14.04.2008), 2008.

[IBM08b] IBM: IBM System i 515 Express http://www.ibm.com/common/ssi/fcgi-bin/ssialias?infotype=PM&subtype=SP&htmlfid=ISD03001DEDE&attachment=ISD03001DEDE.PDF&appname=STG_IS_DEDE_SP (14.04.2008), 2008.

[IDC08] IDC: Analyze the Future. http://www.idc.com/ (10.04.2008), 2008.

[Info08] HP hilft bei der Mainframe-Ablösung. http://www.infoweek.ch/news/NW_single.cfm?news_ID=17974&sid=0 (14.04.2008), 2008.

[ISO08] ISO 20000: Standard for IT Service Management. http://www.iso20000.ch/, (04.02.2008), 2008.

[Iso08] ISO 20000: IT Process Wiki. http://wiki.de.it-processmaps.com/index.php/ISO_20000, (19.01.2008), 2008.

[Itse07] I-SecCity: Aktuelle Studie bestätigt die noch immer weite Verbreitung von Legacy-Systemen. http://www.itseccity.de/?url=/content/markt/studien/070315_mar_stu_attachmate.html (14.04.2008), 2008.

[Itwi07a] IT Wissen: Das große Online-Lexikon für Info. http://www.itwissen.info/definition/lexikon/_cancan_cancampus%20area%20networkcan_cancampus-netzwerk.html, (04.12.2007), 2007.

[Itwi08b] Das große Online-Lexikon für Informationstechnologie: Backbone. http://www.itwissen.info/definition/lexikon/Backbone-BB-backbone.html (07.04.2008), 2008.

[Itwi08c] Das große Online-Lexikon für Informationstechnologie: ATM (Asynchroner Übertragungsmodus).

http://www.itwissen.info/definition/lexikon/asynchronous-transfer-mode-ATM-Asynchroner-Uebertragungsmodus.html (07.04.2008), 2008.

[Itwi08d] Das große Online-Lexikon für Informationstechnologie: RJ-45-Stecker. http://www.itwissen.info/definition/lexikon/RJ-45-Stecker-RJ-45-male-connector.html (07.04.2008), 2008.

[Itwi08e] Das große Online-Lexikon für Informationstechnologie: BNC (BNC-Stecker). http://www.itwissen.info/definition/lexikon/bayonet-Neil-Concelmann-BNC-BNC-Stecker.html (07.04.2008), 2008.

[Itwi08f] Das große Online-Lexikon für Informationstechnologie: Twisted Pair. http://www.itwissen.info/definition/lexikon/twisted-pair-TP-TP-Kabel.html (07.04.2008), 2008.

[Itwi08g] IT-Wissen: Rechenzentrum. http://www.itwissen.info/definition/lexikon//_RZ_computer%20centre_Rechenzentrum.html (08.04.2008), 2008.

[Itwi08h] IT-Wissen: Ethernet. http://www.itwissen.info/definition/lexikon/Ethernet-Ethernet.html (14.05.2008), 2008.

[Itwi08gi] IT-Wissen: Disaster Recovery. http://www.itwissen.info/definition/lexikon/Desaster-Recovery-DR-disasterrecovery.html (14.05.2008), 2008.

[Köhl07] P. Köhler: Das IT-Servicemanagement Framework. http://www.springerlink.com/content/m524t13841552q3u/fulltext.pdf (29.01.2008), 2007.

[Kütz03] M. Kütz: Kennzahlen in der IT. Dpunkt Verlag; 1. Auflage, 2003.

[Lehr07] Lehrer Uni Karlsruhe: Informatik in der Oberstufe. http://www.lehrer.uni-karlsruhe.de/~za714/informatik/infkurs/uebertrag1.html, (06.12.2007), 2007.

[Leo07] LEO: Ein Online-Servie der LEO GmbH. http://dict.leo.org/, (18.12.2007), 2007.

[Lieb07] D. Liebhart: SOA goes real. Hanser; 1. Auflage, 2007.

[Live08] Livetime: Empower, Transform, Protect. http://www.livetime.com/webservicedesk/ServiceCompliance.html, (04.02.2008), 2008.

[Mana07] managIT: tecnogias e modelos de governacao de IT. managit.files.wordpress.com/2007/02/itilv3.jpg, (23.12.2007), 2007.

[MaNo00] C. Mayerl, Z. Nochta, M. Müller, M. Schauer, A. Uremovic, S. Abeck: Specification of a Service Management Architecture to Run Distributed and Networked Systems. http://citeseer.ist.psu.edu/mayerl00specification.html (04.03.2008), 2000.

[Masa07] D. Masak: SOA? Serviceorientierung in Business und Software. http://www.springerlink.com/content/g5124j7068321262/?p=8a4c6db49bce4bda8368aeabe40e3f4b&pi=5 (21.02.2008), 2007.

[Masu03] V. Masurkar: Responding to a costumers security incidents – part 2: Executing a policy. www.sun.com/solutions/blueprints/0403/817- 1796.pdf (02.11.2007), 2003.

[Maxp08] Maxpert AG: ITIL V3: Unterschiede zwischen ITIL V2 und ITIL V3. http://www.maxpert.de/main/kompetenzen/itil_v3/itil_v3_unterschiede.html, (13.01.2008), 2008.

[NiLe07] J. Nitzsche, T. Lessen, D. Karastoyanova, F. Leymann: BPEL for Semantic Web Services (BPEL4SWS). http://www.springerlink.com/content/b320801276747w00/?p=3de61cafa7074f5c84a2c7f39a21d2dd&pi=0 (21.02.2008), 2007.

[OGC07] Office of Government Commerce: ITIL Version 3, Continual Service Improvement . Stationery Office Books; 1. Auflage, 2007.

[Olbr06] A. Olbrich: ITIL kompakt und verständlich, effizientes IT-Service-Management - den Standard für IT-Prozesse kennenlernen, verstehen und erfolgreich in der Praxis umsetzen . Vieweg; 3. Auflage, 2006.

[PlWe07] J. Plötner, S. Wendzel: Praxisbuch Netzwerk-Sicherheit. Galileo Press; 1. Auflage, 2007.

[Pros07] Prosoft: We open Windows. http://www.prosoft.de/produkte/backup/index.html, (08.12.2007), 2007.

[Quir03] G. Quirchmayr: Invited Keynote Address, Survivability and Business Continuity Mangement. crpit.com/confpapers/CRPITV32Quirchmayr.pdf (01.11.2007), 2003.

[ReSc05] W. Reisig, K. Schmidt, C. Stahl: Kommunizierende Workflow-Services modellieren und analysieren. http://www.springerlink.com/content/7567g7635n367k75/fulltext.pdf (25.02.2008), 2005.

[Schu06] G. Schuh: Change management – Prozesse strategiekonform gestalten.Springer Berlin Heidelberg. http://www.springerlink.com/content/r11362734l141tpn/fulltext.pdf (25.02.2008), 2006.

[Scsc06] H. Schiefer, E. Schitterer: Prozesse optimieren mit ITIL. Vieweg; 1. Auflage, 2006.

[Syng08] Benefits of the Mainframe Model. http://www.syngress.com/book_catalog/111_citrix/chapter_01.htm (14.04.2008), 2008.

[Syng08] Syngress: Mainframe. http://www.syngress.com/book_catalog/111_citrix/chapter_01_files/image002.gif; (25.02.2008), 2008

[Tecc08] N. Eikner: Top 500: Die neue Supercomputer-Rangliste 2007. http://www.tecchannel.de/server/extra/482660/index2.html (10.04.2008), 2008.

[Tuwi08] TU Wien: Die TU in Zahlen. http://www.tuwien.ac.at/wir_ueber_uns/zahlen_und_fakten/daten/DE/#c2650 (09.04.2008), 2008.

[Wald02] E. Wald: Backup & Disaster Recovery. mitp-Verlag; 1. Auflage, 2002.

[Wiec03] M. Wieczorek: Business Continuity. Springer; 1. Auflage, 2003.

[Wiki07] Wikipedia: Die freie Enzyklopädie. http://de.wikipedia.org/wiki/ITIL_V3_Service_Strategy, (13.01.2008), 2008.

[Wood07] P. Woodman: Business Continuity Management. http://www.managers.org.uk/client_files/user_files/Woodman_31/Research%20files/Business%20Continuity%20Management%20report%202007.pdf (13.01.2008), 2007.

[ZIDT08] Zentraler Informatik Dienst TU Wien: Einbindung. http://www.zid.tuwien.ac.at/fileadmin/files_kom/images/einbindung.gif; (14.03.2008), 2008

[ZuWu08] M. Zuo, B. Wu: SOA Oriented Web Services Operational Mechanism. http://www.springerlink.com/content/73845432807p845q/?p=376560c14cd8496cb177a44ad749bb9d&pi=9 (20.02.2008), 2008.