

Business Continuity Planning

Holm Diening

Whitepaper

April 2008

Die IT-Infrastruktur ist mittlerweile vitaler Bestandteil der Geschäftsprozesse fast jeden Unternehmens. Aus diesem Grunde kann ihr Versagen auch schwerste Schäden sogar bis hin zum Konkurs verursachen. Maßnahmen zur Notfallplanung werden deshalb zunehmend wichtiger und unterstützen die Aufrechterhaltung des Geschäftsbetriebes nach einem Schadensfall.

Dieser Artikel gibt zunächst eine Einführung in die Thematik und beschreibt dann die wesentlichen Phasen des Business Continuity Planning für den IT-Bereich. Dabei geht er auch auf Aspekte der praktischen Umsetzung und den Einsatz von Softwaretools zur Unterstützung ein.

Einführung

„Wenn das passiert, dann können wir hier sowieso einpacken!“ Diese oder eine ähnliche Antwort erhält man nicht selten, wenn in Unternehmen nach der Vorbereitung auf einen eventuellen Großschaden gefragt wird. Dabei klingt immer ein wenig die Einstellung mit, dass man sich auf wirkliche Katastrophen ohnehin nicht ausreichend vorbereiten könne und dass sich so etwas für diese extrem seltenen Fälle auch gar nicht lohne. Die Verantwortung gegenüber den eigenen Mitarbeitern, den Aktionären, aber auch den Kunden, verbietet jedoch hier zu pokern. Je länger ein Unternehmen besteht und je größer es ist, desto eher wird es sich einmal einer solchen Situation stellen müssen. Ohne ein durchdachtes und erprobtes Notfallkonzept ist ein koordiniertes und zielführendes Handeln der Beteiligten im Ernstfall jedoch nicht möglich. Eine angemessene Vorbereitung auf Notfallszenarien wird daher auch als Bestandteil ordnungsgemäßer Corporate Governance angesehen. In Deutschland existiert bisher keine eigene gesetzliche Vorschrift zur Notfallvorsorge. Es werden jedoch einige Gesetze in dieser Richtung interpretiert. Beispiele hierfür sind:

- § 91 Abs. 2 AktG (Früherkennung von Risiken)
- § 43 Abs. 1 GmbHG (Sorgfaltspflichten)

Konkrete Forderungen an eine Notfallvorsorge ergeben sich aber aus einigen branchenspezifischen Bestimmungen und Verordnungen. Als jüngstes Beispiel seien hier die Mindestanforderungen an das Risikomanagement (MaRisk) des Bundesamtes für Finanzdienstleistungsaufsicht genannt. Hier wird in Abschnitt 7.3 explizit ein Notfallkonzept gefordert.¹

Weitere wichtige Impulse für Rechtsgrundlagen könnten sich auch aus dem KRITIS Projekt² des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ergeben. Im Rahmen des „Nationalen Plans zum Schutz kritischer Infrastrukturen“ des Bundesinnenministeriums will das BSI entsprechende Vorgaben für den IT-Bereich entwickeln. Eine konkrete Umsetzung in gesetzliche Anforderungen steht aber noch aus.

¹ http://www.bafin.de/rundschreiben/89_2005/051220.htm

² <http://www.bsi.bund.de/fachthem/kritis/>

Begriffe und Abkürzungen

Nicht ganz einfach ist im Themenkomplex der Notfallplanung die Zuordnung einiger Fachbegriffe. Bei der Auseinandersetzung mit dieser Materie wird man feststellen, dass hier oft noch nicht einmal Einigkeit bei Bezeichnung der eigenen Fachdisziplin herrscht.

Dies betrifft zunächst die Begriffe „Business Continuity Management“ und „Business Continuity Planning“. Meist werden diese beiden Bezeichnungen in der amerikanischen (Planning) und der britischen Literatur (Management) synonym verwandt. In beiden Fällen sind hierbei alle Maßnahmen zur Beibehaltung der Arbeitsfähigkeit einer Organisation während und nach einer unvorhergesehenen Betriebsunterbrechung gemeint. Der British Standard 25999 (mehr zu Standards im nächsten Abschnitt) kennt hingegen durchaus Unterscheidungspotential. Dieses speist sich vor allem aus seiner übergeordneten Betrachtungsweise. Business Continuity Management ist hier ein ganzheitlicher Management Prozess, der a) mögliche Bedrohungen für eine Organisation durch unvorhergesehene Ereignisse identifiziert und b) ein Framework zur Verbesserung der Widerstands- und Reaktionsfähigkeit eines Unternehmens bei solchen Ereignissen zum Schutz der Interessen der Anteilseigner, des Images des Unternehmens und der Wertschöpfungskette bildet. Nach dieser Definition geht der Begriff BCM also weit über die Erhaltung der Geschäftsprozesse bei Katastrophen oder ähnlichen Vorfällen hinaus. Ebenfalls nicht eindeutig ist die Benutzung der Abkürzung „BCP“, die für „Business Continuity Planning“ und auch für den „Business Continuity Plan“, also das Ergebnis des „Planning“, verwendet wird.

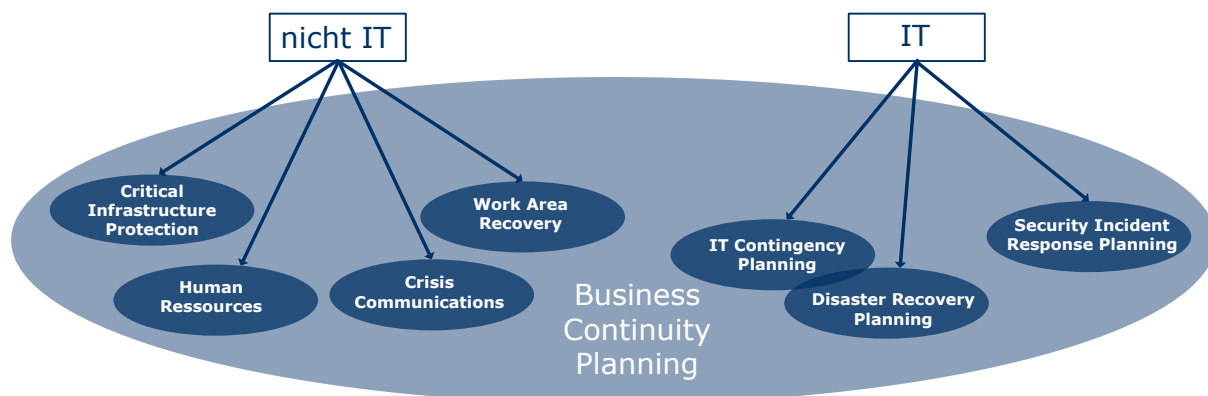


Abbildung 1: Bestandteile des Business Continuity Planning

Der Autor dieses Artikels folgt bei der Unterscheidung zwischen Business Continuity Management und Planning der Darstellung des BS 25999. Da wir uns hier vor allem mit der Planung von Abläufen in konkreten Notfällen beschäftigen wollen, fassen wir alle Maßnahmen mit dieser Zielsetzung nachfolgend unter dem Begriff „Business Continuity Planning“ zusammen.

Business Continuity Planning im IT-Bereich

Die Aufrechterhaltung oder der schnelle Wiederanlauf des Geschäftsbetriebes nach einem Notfall erfordert das koordinierte Handeln in den unterschiedlichsten Ebenen. Der IT-Bereich ist hierin nur eine Facette, deren Bedeutung von der Branche des jeweiligen Unternehmens abhängt. Nicht-IT Aspekte eines BCP wären der präventive Schutz kritischer Infrastrukturen, die Bereitstellung von Produktions- und Büroflächen, die Kommunikation mit den Medien und auch die manuelle Überbrückung wichtiger Geschäftsprozesse im „Offline-Modus“, also ohne die zentrale IT.

Folgende Bestandteile einer Notfall- oder Katastrophenvorsorge sind hingegen für den IT-Bereich relevant (rechts in Abbildung 1):

IT-Contingency Plan (IT-Notfallplan)

Ein IT-Notfallplan wird für die Aufrechterhaltung der Betriebsbereitschaft wesentlicher Applikationen erstellt. Daher existieren in Unternehmen mehrere Notfallpläne für die unterschiedlichen Anwendungen. Oft werden solche Pläne bereits durch externe Systembetreuer oder die Anwendungs- und Systemhersteller mitgeliefert und gewartet. So kann eine IT-Abteilung getrennte Notfallpläne für die Finanzapplikationen, das ERP-System oder den Mailserver haben.

IT-Disaster Recovery Plan

Wie der Name bereits vermuten lässt, handelt es sich hier um die Vorbereitung auf Katastrophen und ähnliche Ereignisse, die einen IT-Betrieb in den bisherigen Räumlichkeiten mittelfristig unmöglich machen. Meistens handelt es sich daher um Pläne, die eine Wiederaufnahme des IT-Betriebes an einem Ausweichstandort zum Gegenstand haben. Es kann hierbei an einigen Stellen zu Überschneidungen mit den IT-Notfallplänen kommen (siehe Abbildung 1), obwohl diese im Allgemeinen keine schwerwiegenden Ereignisse behandeln, die auch eine Verlagerung von IT erforderlich machen.

Cyber Incident Response Plan (CIRP)

Auch der Ausbruch von Computer Viren in einem Netzwerk oder der vorsätzliche Angriff eines Crackers können die Verfügbarkeit von IT-Anwendungen stören. Ein CIRP dient zur frühzeitigen Erkennung solcher Vorfälle, der schnellen und angemessenen Reaktion und der Schadensbegrenzung.

Backlog Processing

Aufarbeitung des Arbeitsrückstandes

BCM (Business Continuity Management)

Ganzheitlicher Ansatz zur Aufrechterhaltung des Geschäftsbetriebes bei unvorhergesehenen Ereignissen

Business Continuity Planning

Planung von Maßnahmen zur Aufrechterhaltung oder Wiederherstellung des Betriebes in Notfällen. **Hinweis:** Die Abkürzung BCP bedeutet auch den „Business Continuity Plan“, also das Produkt des Business Continuity Plannings.

BIA (Business Impact Analyses)

Analyse der Auswirkungen von unvorhergesehenen Ereignissen auf wichtige Geschäftsprozesse

IT-CP (Contingency Plan)

Plan zur Aufrechterhaltung wichtiger IT-Dienste bei größeren Störfällen

IT-DRP (Disaster Recovery Plan)

Plan zur Wiederherstellung des IT-Betriebes nach einer Katastrophe

MCA (Mission Critical Activity)

Ein Kernprozess, der für den Geschäftsbetrieb unabdingbar ist

RTO Recovery Time Objective

Zeitrahmen, innerhalb dessen ein Prozess wieder hergestellt sein muss

RPO Recovery Point Objective

Maximaler Datenverlust. Meist das Mindestintervall zwischen zwei Datensicherungen

Abbildung 2: Begriffe und Abkürzungen (alphabetisch)

Wichtige Standards und Best Practices

Die Thematik der Notfallplanung findet sich im Fokus diverser Standards und Best Practices. Je nach Herkunft sind diese eher IT-orientiert oder beschreiben Notfallplanung aus der Sicht der Geschäftsprozesse.

Die ISO 27002 „Code of practice for information security management“ beschreibt auf fünf Seiten die Einbindung der Information Security in das BCM (Kapitel 14: „Business Continuity Management“). Dabei wird allerdings die Existenz eines übergeordneten Business Continuity Management Prozesses im Unternehmen bereits vorausgesetzt. Das Bundesamt für Sicherheit in der Informationstechnik entwickelt hierzu einen eigenständigen Standard (BSI-Standard 100-4 „Notfallmanagement“), der sich zurzeit noch im Entwurfsstadium befindet. Zusätzlich enthalten die Grundschutzkataloge hierfür einen eigenen Baustein: „B 1.3 Notfallvorsorge-Konzept“ der Gefährdungen und Maßnahmen für die Notfallvorsorge im IT-Bereich zusammenfasst. Das Subset „Service Delivery“ der IT Infrastructure Library (ITIL) befasst sich im Abschnitt „IT Service Continuity Management“ über knapp 50 Seiten mit dem gesamten Prozess der IT-Notfallplanung, den Teststrategien, der Sensibilisierung und den Verantwortlichkeiten. Zielsetzung ist hier die Aufrechterhaltung von IT-Prozessen aus Sicht der Erbringung eines IT-Services. Ähnlich strukturiert, aber noch ausführlicher, ist die amerikanische NIST Special Publication 800-34 „Contingency Planning Guide for Information Technology Systems“.

Alle diese Standards haben ausschließlich die IT-Notfallplanung und deren Beitrag zur Aufrechterhaltung der Geschäftsprozesse zum Gegenstand. Weiter gefasst und ohne speziellen Fokus auf die IT ist der BS 25999. Der Standard unterteilt sich dabei nach der bei Management Standards üblichen Gliederung in BS 25999-1:2006 „Code of practice for business continuity management“ und BS 25999-2:2007 „Specification for business continuity management“. Eine Adaption der Standards durch die ISO war angestrebt. Letztendlich wurde im November 2007 der Standard ISO 22399 „Societal security - Guideline for incident preparedness and operational continuity management“ („Societal security“ dt.: „Sicherheit und Schutz des Gemeinwesens“) veröffentlicht, der in starkem Maße vom BS 25999 beeinflusst wurde, aber auch auf anderen nationalen Best Practices basiert.

Phasen des Business Continuity Planning

Dieser Abschnitt beschreibt die einzelnen Phasen des Business Continuity Planning, wobei die IT-relevanten Bestandteile im Vordergrund stehen sollen. Die nachstehende Abbildung 3 gibt einen Überblick über ein aus fünf getrennten Abschnitten bestehendes Modell. Es ist angelehnt an das Vorgehensmodell für IT Service Continuity Management aus dem ITIL Service Delivery Handbuch.

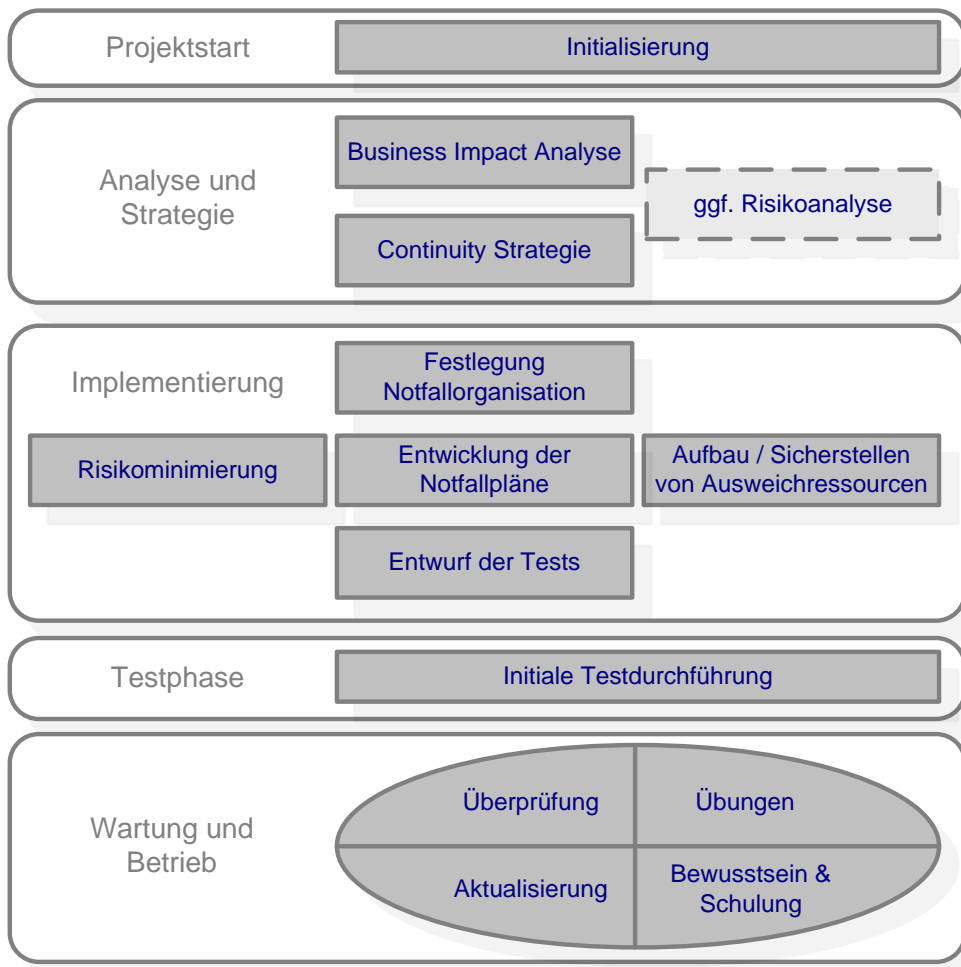


Abbildung 3: Phasenmodell in Anlehnung an ITIL IT Service Continuity Management

Phase 1: Initialisierung

Die erste Phase ist, langfristig gesehen, zugleich die wichtigste. Hier gilt es, die genauen Ziele zu definieren, sowie den Umfang und die Vorgehensweise zu bestimmen. Gleichzeitig muss bereits hier das Management von der Notwendigkeit des Projektes und auch der Weiterführung als nachfolgender Prozess überzeugt werden. Gerade für den Prozess werden finanzielle und personelle Ressourcen benötigt, die in der ersten Phase der Planung thematisiert werden müssen. Folgende Punkte sind wichtige Ergebnisse der ersten Phase:

- Zu erwartende Kosten, benötigte Ressourcen, geplante Dauer sind bekannt.
- Die Projektorganisation (Teamzusammensetzung, Rollen, Befugnisse, Reporting) ist abgestimmt.
- Ein Projektplan mit Meilensteinen existiert.
- Die BC-Policy mit Zielen und Scope wurde vom Management unterschrieben.
- Die Weiterführung des Prozesses nach Ende des Projektes ist sichergestellt.

Phase 2: Analyse und Strategie

In der zweiten Phase schafft man die Grundlagen für die eigentliche Planung. In einer Business Impact Analyse werden zunächst wichtige Geschäftsprozesse identifiziert und die Auswirkungen möglicher Unterbrechungen analysiert. Die Auswirkungen sind dabei nicht nur monetärer Art und müssen in verschiedener Hinsicht bewertet werden. Wichtig ist dabei auch die Darstellung der Auswirkungen in Abhängigkeit der Dauer der Unterbrechung. Die

Bewertung einer MCA (Mission Critical Activity) kann anhand eines Scoringverfahrens vorgenommen werden, das die Auswirkungen einer Unterbrechung durch Kennzahlen (zum Beispiel Schulnotensystem) beschreibt und anschließend die einzelnen Bewertungskriterien mit einem vorher festgelegten Schema gewichtet. Die Vergabe von Kennzahlen sollte dabei auf der Basis eines festgelegten Beurteilungsschlüssels erfolgen. So können finanzielle Auswirkungen in ihrer Höhe mit dem zu erwartenden Jahresgewinn verglichen werden. Auswirkungen auf die Reputation bewertet man zum Beispiel von „1“ für „keine Auswirkungen“ bis zu „6“ für „schwerwiegender langfristiger Imageschaden“.

Ein solches Bewertungsschema könnte etwa folgendes Aussehen haben:

MCA:	1 Tag			2 Tage			1 Woche			2 Wochen			1 Monat		
	Note	Gew.	Bew.	Note	Gew.	Bew.	Note	Gew.	Bew.	Note	Gew.	Bew.	Note	Gew.	Bew.
Finanzielle Auswirkung															
Verlust von Reputation															
Rechtliche Konsequenzen															
Sicherheit von Personen															
Verlust von Konkurrenzvorteilen															
Auswirkungen auf den Marktanteil															
Aufwand für das Backlog Processing															
Summe															

Tabelle 1: Scorecard für Bewertung der Auswirkungen einer Unterbrechung einer MCA

Anhand dieser Auswertung und anderer Kenntnisse über den jeweiligen Geschäftsprozess ergeben sich dann auch die RTO und RPO (siehe Abbildung 2). Die Mindestanforderungen an einen eingeschränkten Betrieb zur kurzfristigen Überbrückung von Notfällen (zum Beispiel mit weniger Personal oder unter Verzicht auf bestimmte Applikationen) müssen ebenfalls bekannt sein.

Nachdem die wichtigsten Geschäftsprozesse und deren Kritikalität bestimmt sind, können nun Bedrohungen identifiziert und bewertet werden, die möglicherweise zu einer Unterbrechung führen. Gegebenenfalls, wenn der Prozess als besonders kritisch für das Unternehmen eingeschätzt wird, sollte man eine klassische Risikoanalyse hierfür bemühen.

Das Ergebnis dieses Schrittes für den IT-Bereich ist eine priorisierte Liste von wichtigen Geschäftsprozessen, die von der IT abhängig sind und daher nach einer Unterbrechung im Bereich der IT nicht mehr oder nur eingeschränkt ablaufen können.

In Abhängigkeit der Ergebnisse der BIA und der organisatorisch/technischen Möglichkeiten erfolgt nun die Festlegung der Strategie zur Aufrechterhaltung der jeweiligen Geschäftsprozesse. Sämtliche Optionen im IT-Bereich lassen sich in drei Kategorien unterteilen:

- Risikominimierung
- Notfallplanung zur Wiederherstellung
- Ausweichlösungen

Die Maßnahmen im Bereich der Risikominimierung zielen darauf ab, einen Ausfall von kritischen IT-Anwendungen von vorn herein zu vermeiden. Dazu zählen zum Beispiel die Vermeidung von „Single Points of Failure“ in der eingesetzten Hardware, der physikalische Schutz der IT-Infrastruktur oder die Nutzung von zwei verschiedenen Internet Providern.

Notfallpläne sollen im Bedarfsfall (wie: Serverausfall, Netzwerkunterbrechungen, Softwarefehler nach Versionswechsel) eine rasche Wiederherstellung der wichtigsten Applikationen an Ort und Stelle erleichtern.

Die Nutzung von Ausweichlösungen ist die Option für die Bewältigung der schwerwiegendsten Störfälle. Hier ist eine Verlagerung des IT-Bereiches an einen anderen Standort erforderlich. In wie weit dieser neue Standort schon auf die Übernahme des RZ-Betriebes vorbereitet ist, hängt von der zulässigen Wiederherstellungsfrist (RTO) ab. Ausweichrechenzentren können ausgeführt sein als:

Hot-Site

- Betriebsbereites RZ mit vollständig duplizierter Hardware und aktueller Software, Daten können sofort eingespielt werden oder sind bereits vorhanden (Mirrored Site)

Warm-Site

- Zentrale IT steht bereit. Es fehlen noch Peripherie, Software und Daten.

Cold-Site

- Ein leeres RZ ohne jede Hardware. Stromversorgung, Klimatisierung und andere Infrastruktur sind jedoch vorhanden.

MVRZ

- Mobiles Vorsorge-Rechenzentrum. Es ist meist ähnlich ausgestattet wie eine Warm-Site, kann aber direkt vor Ort gebracht werden. Je nachdem, wie schwer bspw. das Firmengebäude betroffen ist, kann die RZ-Umgebung an Ort und Stelle oder auch an einer Ausweichlokation aufgebaut werden.

Die Ergebnisse dieser Phase sind die Richtschnur für die eigentliche IT-Notfallplanung. Sie geben Auskunft über die Prioritäten bei der Wiederherstellung der einzelnen Business Applikationen und die Fristen, nach denen diese wieder bereit stehen müssen.

Phase 3: Implementierung

Die Implementierung eines Notfallkonzeptes erfolgt in drei Stufen: Der Festlegung einer geeigneten Notfallorganisation, der Erarbeitung von Alarmierungsketten und Ablaufplänen und sowie der Planung und Durchführung von Tests.

Die Notfallorganisation einer IT Abteilung sollte sich von der Organisationsstruktur im Tagesgeschäft kaum unterscheiden. Schließlich werden die Notfallpläne auch von den Fachbereichen entwickelt und betreut, die sie auch im Ernstfall ausführen sollen. Es müssen jedoch einige Punkte beim Aufbau der Notfallteams beachtet werden, die im Tagesgeschäft weniger relevant sind:

- Leitende Funktionen in Notfallteams sollten durch zwei Stellvertreter abgesichert sein.
- Die Anfahrtswege der Mitarbeiter von zu Hause sollten in der Teambildung berücksichtigt werden.
- Einige Mitarbeiter sind als Ersthelfer ausgebildet und haben im Notfall andere Verpflichtungen. Sie stehen für die Notfallteams ggf. nicht zur Verfügung.
- Je nach Eskalation (Störung, Notfall, Krise) wird der Fachbereichs- oder Abteilungsleiter in einem übergeordneten Krisenstab des Unternehmens mitarbeiten und ist daher für interne Aufgaben nicht abkömmlich.
- Die Führungsqualitäten in Krisensituationen sollten bei der Teambildung mit berücksichtigt werden.

Ein weiterer organisatorischer Aspekt sind die Rahmenbedingungen für die zeitlich befristete Erweiterung von Befugnissen. Dies betrifft zum Beispiel die kurzfristige Beschaffung von Ersatzhardware durch die IT ohne den Umweg über den Einkauf, oder auch die Anordnung von Sonderschichten, Wochenendarbeit und Urlaubssperren ohne die Zustimmung des Personalbereiches.

Aus der Festlegung der Notfallorganisation erschließt sich im Wesentlichen auch die Definition von Alarmketten. Je nach Art des Vorfalles wird eine andere Stelle die Alarmkette auslösen, die jedoch am Ende immer die Alarmierung aller für den jeweiligen Notfall relevanten Teams zur Folge hat.

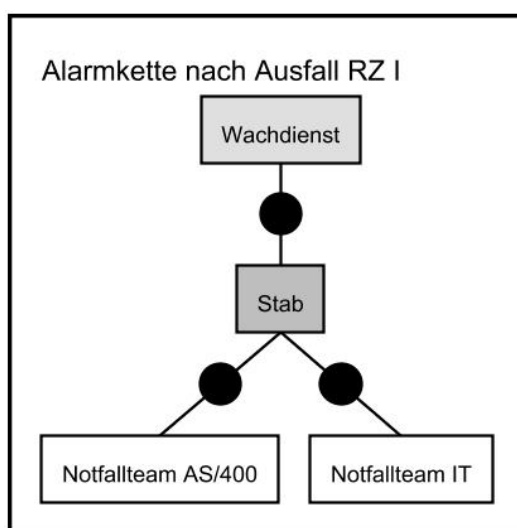


Abbildung 4: grafische Darstellung einer einfachen Alarmkette

Die Planung der eigentlichen Handlungsabläufe in einem Notfall enthält zunächst Pläne für übergeordnete Aspekte wie:

- Sofortmaßnahmen bei Unglücksfällen
- Bestandsaufnahme
- Umgang mit Medien
- Rettung von Backupbändern, Festplatten und anderen Datenträgern

Die nächste Ebene der Notfallpläne orientiert sich dann an den Aufgaben zur Erreichung eines eingeschränkten Betriebs zur einstweiligen Überbrückung der Notsituation (nach Festlegung aus Phase 2) und anschließend zur Wiederherstellung der vollständigen Betriebsbereitschaft. Hierfür ist zunächst ein genauer Überblick über die IT-Infrastruktur und deren Beitrag zu den abzusichernden Geschäftsprozessen notwendig. Das klassische Vorgehen nach der Top-Down Methode beginnt dabei mit der Ermittlung der kritischen Geschäftsprozesse, bestimmt dann die dafür benötigten Applikationen und schließlich die zugrunde liegenden IT-Systeme. Ergänzend hierzu empfiehlt es sich, im IT-Bereich einen eigenständigen Bottom-Up Ansatz zu verfolgen. Dieser beginnt mit der Strukturierung der Anwendungssysteme und des Datenbestandes und nimmt anschließend die Zuordnung zu den Geschäftsprozessen vor. Dies hat den Vorteil, dass die betreffenden BCP-Projektmitarbeiter zunächst ihr eigenes Metier von der Basis her untersuchen können und dadurch wichtige Bindeglieder wie zum Beispiel Systeme zur Anpassung von Datenformaten oder Schnittstellenrechner nicht übersehen. Das Vorgehen hierfür lässt sich folgendermaßen zusammenfassen:

- Systematische Erfassung aller Anwendungssysteme und dort verarbeiteter Datenbestände
- Strukturierung und Zuordnung zu wichtigen Geschäftsabläufen
- Bestimmung gegenseitiger Abhängigkeiten von Anwendungen / Daten / IT-Systemen und Geschäftsabläufen
 - o Bestimmung funktionaler Abhängigkeiten (welche Daten und welche Systeme werden für welche Anwendung benötigt)
 - o Bestimmung zeitlicher Abhängigkeiten (in welcher Reihenfolge müssen welche Daten und Anwendungen zur Verfügung stehen)

Bei der anschließenden Erstellung der Notfallpläne für die ermittelte Systeminfrastruktur ist auf ein möglichst hohes Abstraktionsniveau zu achten. Einem Plan zur Wiederherstellung eines Datenbankservers sollte es egal sein, warum diese Wiederherstellung notwendig wird oder wo diese stattfindet. Ursache und Wirkung müssen hier getrennt bleiben. Nur so können Planungsbestandteile modular in anderen Blöcken und Abläufen, wie zum Beispiel der Wiederherstellung des gesamten RZ an einem Ausweichstandort, eingesetzt werden. Abgesehen davon reduziert sich hierbei auch der Pflegeaufwand.

Die Gesamtheit der Notfallpläne sollte sowohl spezifische Wiederherstellungsverfahren (Server, Netzwerkknoten, MVRZ) umfassen, als auch solche, die auf bestimmte Schadensereignisse, wie Hochwasser oder die Abtrennung von Gebäudeteilen, ausgerichtet sind.

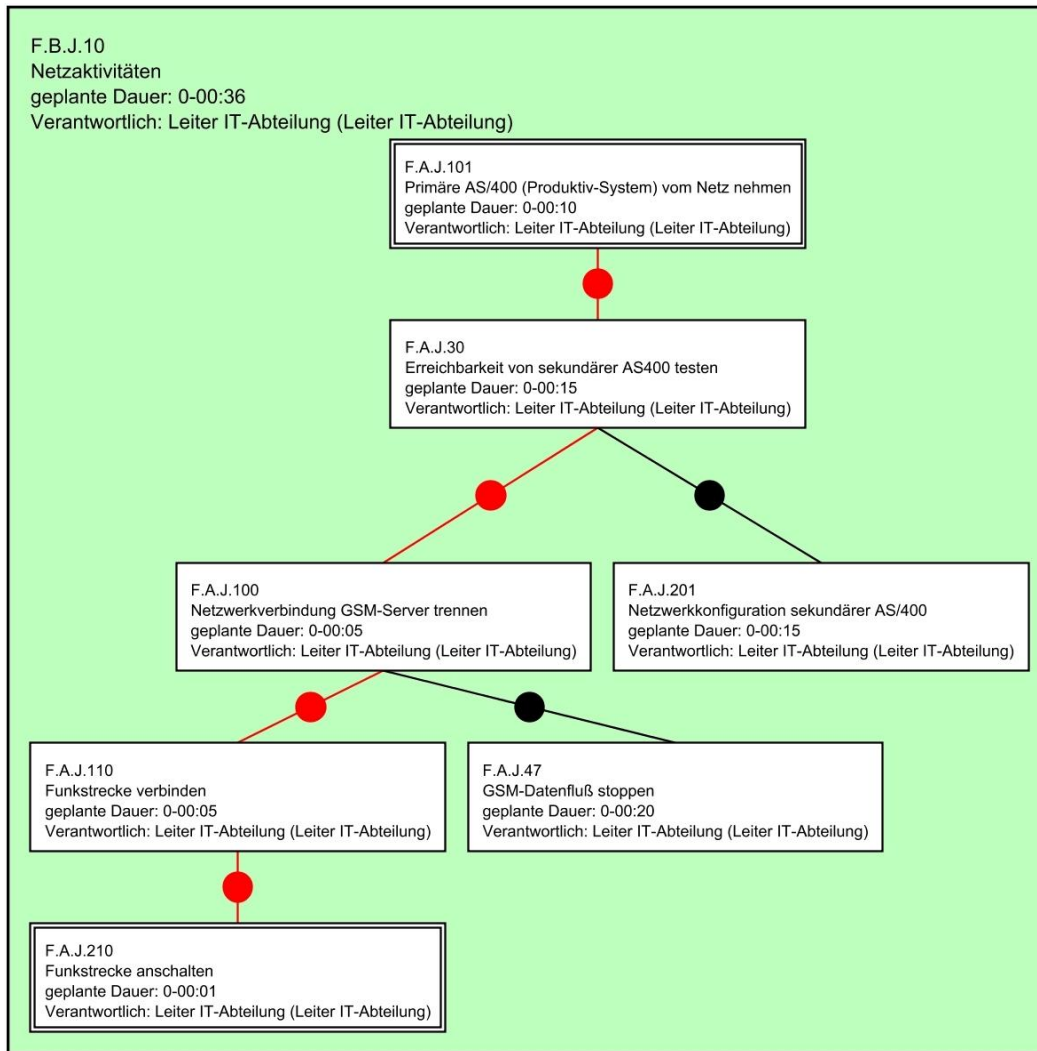


Abbildung 5: grafische Darstellung eines modularen Planungsblocks

Ist die Planung abgeschlossen, werden alle gewonnenen Informationen in einem Notfallhandbuch zusammengeführt. Folgende Angaben sollten dort in jedem Fall enthalten sein:

- Kurze Einleitung mit Zweck und den Aufbau des Dokumentes
- Darstellung der Notfallorganisation
- Krisenstäbe und Rollen der Mitarbeiter in den Krisenstäben
- Rufnummern- und Adresslisten von Mitarbeitern und Servicepartnern
- Übersichtliche Raum- und Gebäudepläne, Netzwerkstruktur, Adressräume usw.
- kurze System- und Anwendungsbeschreibungen
- Grafische Darstellung von Systemabhängigkeiten
- Auflistung der definierten Notfälle
- Alarmierungsketten und Ablaufpläne

Teststrategien

Haben Sie in Ihrem Büro einen Feuerlöscher? Natürlich! Aber haben Sie jemals in Ihrem Leben schon mal einen bedient? Wissen Sie zum Beispiel, wie lange ein normaler Pulverlöscher funktioniert, bevor er leer ist? Im Ernstfall gibt es eben doch manchmal böse Überraschungen!

Ebenso verhält es sich mit Notfallhandbüchern. Prinzipiell ist immer alles klar, die Ablaufpläne theoretisch narrensicher. Beim initialen Test eines Notfallplanes zeigen sich

jedoch (nach unserer Erfahrung) ausnahmslos immer noch kleine Unwägbarkeiten, die vorher nicht eingeplant wurden. Daher gilt ein Notfallplan auch nie als einsatzbereit, solange er nicht getestet wurde.

Für ein Notfallkonzept ist parallel daher auch immer ein Testkonzept zu entwickeln. Dabei werden, angepasst an die Art der Notfallpläne und die Wichtigkeit der dadurch abgesicherten Geschäftsprozesse, verschiedene Testabläufe festgelegt. Diese reichen vom einfachen „geistigen Durchgehen“ der Pläne bis hin zu einer realistischen Notfallübung mit einer tatsächlichen Unterbrechung des Produktivbetriebes. Dabei ist es offensichtlich, dass bei Tests der ersten Kategorie der Aufwand sehr gering ist und diese relativ häufig durchgeführt werden können, während ein wirklicher „Full Interruption Test“ wahrscheinlich nur sehr selten oder, realistisch gesehen, nie durchgeführt wird. Die Teststrategie zur Notfallplanung legt nun fest, wie häufig welche Tests mit welchen Beteiligten durchzuführen sind. Dadurch werden sowohl die Pläne auf ihre Gültigkeit hin geprüft, als auch die Beteiligten geschult. Die Ergebnisse solcher Tests fließen wiederum in die Korrektur der Notfallplanung ein. Die nachstehende Tabelle gibt einen Überblick über verschiedene Testmethoden und ihren Aufwand.

BEZEICHNUNG	INHALT	BETEILIGTE	FREQUENZ	AUFWAND
Checklist Test	Der BCP verantwortliche jeder Abteilung geht für sich den Plan durch und überprüft ihn auf eventuelle Fehler oder Unzulänglichkeiten.	BCP verantwortlicher oder sein Team	oft	gering
Structured Walk-Through Test	Alle Pläne werden gemeinsam an einem Tisch durchgearbeitet um eventuelle Fehler in der Zusammenarbeit der Abteilungen aufzudecken (z.B. doppelte Verwendung von Ressourcen). Zusätzlich wird die Kommunikation zwischen den Teams getestet.	Alle BCP Teams zusammen		
Simulation Test	Es werden alle Schritte von allen Beteiligten ausgeführt, wie sie im tatsächlichen Notfall geplant sind. Ausnahmen: Es werden keine Ersatzkomponenten geliefert (aber die Bestellung geprobt), es werden keine produktiven IT-Systeme modifiziert, es findet kein Umzug in einen Ausweichstandort statt. Es stehen nur die Ressourcen zu Verfügung, die im Notfall auch vorhanden wären.	Alle Mitarbeiter, die operationelle Aufgaben im BCP haben.		
Parallel Test	Einrichtung des IT-Systems in einem Ersatzstandort. Dies kann eine MVRZ Übung oder die Verlagerung in ein Recovery Center	Alle Mitarbeiter, die operationelle Aufgaben im BCP haben sowie externe Dienstleister		
Full Interruption Test	Das Produktivsystem wird tatsächlich abgeschaltet und der Notfallplan durchgeführt	Alle Mitarbeiter, sowie externe Dienstleister	selten	hoch

Tabelle 2: Teststrategien in Bezug auf Häufigkeit und Aufwand (nach BS 25999-1:2006)

Die Durchführung von Tests ist dabei nicht nur in starren zeitlichen Intervallen vorzusehen. Die Wirksamkeit von Notfallplänen lässt sich am besten durch unangekündigte Übungen überprüfen. Zusätzlich sollte ein außerplanmäßiger Test eingeschoben werden, wenn:

- neue Pläne erstellt wurden
- wesentliche Bestandteile der Planung geändert wurden
- neue Mitarbeiter den Notfallplan noch nicht kennen
- neue externe Dienstleister eingebunden werden
- Änderungen an Hard- und Software vorgenommen wurden
- eine neue Risikosituation Gewissheit über die Gültigkeit der Pläne erforderlich macht

Phase 4: Wartung und Betrieb

Wir sind am Ende des BCP „Projektes“ angekommen. Ab jetzt muss sich zeigen, ob die Vorbereitung in Phase 1 und die Kommunikation mit dem Management während des Projektes ausreichend waren, um die Notfallplanung mit den nun notwendigen Ressourcen als Prozess weiter zu führen.

Regelmäßig wiederkehrende Tests und Reviews stellen die fortlaufende Aktualität und Anwendbarkeit der Notfallpläne sicher. Kennzeichnend für diese Phase ist auch die enge Integration in andere IT-Prozesse. Das Change Management ist hierbei am stärksten hervorzuheben. Das Notfallkonzept muss in den Change Management Prozess derart eingebunden werden, dass erfolgte Änderungen an der Systemumgebung umgehend in das Notfallkonzept eingearbeitet werden. Aber auch die Ergebnisse der BIA, ganz am Anfang des Projektes, sind nicht statisch. So werden sich ändernde Prämissen in den Geschäftsprozessen oder eine neue Risikosituation auch auf die dazugehörige Notfallplanung auswirken. Last but not least sind Schulungs- und Sensibilisierungsmaßnahmen der Mitarbeiter für ein lebendiges Notfallkonzept unabdingbar. In einem Notfall hat niemand die Zeit, zunächst ein dickes Handbuch zu studieren, dass er oder sie vorher nie gesehen hat.

Einsatz von Tools

Das Notfallhandbuch mit allen wichtigen Informationen, Tabellen und Plänen zur Bewältigung von größeren Störfällen ist das wichtigste Ergebnis des Business Continuity Planning. Die Erstellung und Verwaltung von Notfallhandbüchern auf der Basis von reinen Office-Dokumenten ist jedoch aufgrund ihres großen Umfangs und der Komplexität sehr mühsam. Dass die gesamte Wartung und Pflege einer Notfallplanung oft unerledigt liegen bleibt, ist zum Teil auch durch hohen Aufwand begründet, den die ständige Aktualisierung der Dokumentation mit sich bringt. An dieser, aber auch an anderen Stellen, spielen die am Markt befindlichen Notfallplanungstools ihre Stärken aus. Folgende Aspekte sprechen für die Nutzung einer spezialisierten Software bei der Notfallplanung:

- Alle für den professionellen Einsatz relevanten Tools kennzeichnet die Nutzung einer internen Datenbank. Dadurch wird redundante Datenhaltung vermieden. Änderungen müssen nur an einer Stelle vorgenommen werden.
- In vielen Situationen wird es sinnvoll sein zu wissen, wo überall und in welchen Handbüchern eine bestimmte Adresse oder ein bestimmter Ablauf verwendet werden. Entsprechende Software erspart Ihnen hier die mühselige Volltextsuche in allen Dokumenten.
- Die Rückverfolgbarkeit von Änderungen wird wesentlich erleichtert.
- Die Vergabe von Zugriffsrechten kann bis auf die Ebene einzelner Datensätze eingeschränkt werden, während bei der Version mit Office-Dokumenten nur ein Zugriffsschutz auf Dateiebene möglich ist.

- Oft werden mehrere Personen gleichzeitig am Notfallhandbuch arbeiten wollen. Ein Handbuch, das aus Office-Dokumenten besteht, ermöglicht das nicht.
- Bestehende Daten, zum Beispiel das Inventar von IT-Systemen, können bei den meisten Systemen problemlos importiert werden.
- Eine ansprechende grafische Präsentation der Ablaufpläne wird automatisch erstellt und muss nicht gezeichnet werden.
- Einige Tools bieten auch die Begleitung und Protokollierung von Tests, so dass deren Ergebnisse sofort in die Planung aufgenommen werden können.

Ein Tool, das auf Knopfdruck Notfallhandbücher schreibt, gibt es hingegen nicht. Auch die Verantwortung für eine vorausschauende Planung wird immer bei den BCP-Verantwortlichen verbleiben.

Es wird derzeit eine Reihe von Tools in diesem Segment am Markt angeboten. Wichtige Beispiele sind das Produkt LDRPS von Strohl Systems, ROGS/DMS von ROG, CAPT/CM von Heine & Partner sowie „alive-IT“ von Controll-IT. Die Screenshots in diesem Artikel stammen aus letzterem Tool.

Fazit

Die Maßnahmen zur Notfallvorsorge, vor allem im IT-Bereich, haben lange Zeit ein eher stiefmütterliches Dasein gefristet. Teilweise wurde der Beitrag der IT zu den Geschäftsprozessen eines Unternehmens unterschätzt oder aber die vollständige Abhängigkeit von ihr ohne Sicherungsseil in Kauf genommen. Das ständig latente Risiko einer größeren Betriebsunterbrechung konnte den fehlenden gesetzlichen Zugzwang und die Sorge vor den Kosten eines Notfallkonzeptes nicht ausgleichen. In den letzten Jahren holt hier das Bewusstsein der Unternehmer langsam auf. Auch der Gesetzgeber und die Branchenverbände legen nach und fordern in immer mehr Verordnungen eine angemessene Vorbereitung auf solche Ereignisse. Das wachsende KnowHow auf dem Gebiet der Notfallplanung, die steigende Zahl von Anbietern mobiler oder stationärer Ausweichstandorte und auch die fortschreitende Standardisierung erleichtern zunehmend die Umsetzung eines wirksamen und effektiven Notfallkonzeptes.

***Holm Diening** ist als IT-Security Consultant bei der GAI NetConsult GmbH für die Bereiche "IT-Sicherheitsmanagement" und „Notfallplanung“ zuständig.*

*Die **GAI NetConsult GmbH** ist ein bundesweit tätiges unabhängiges Software- und Consulting-Unternehmen mit besonderer Expertise in den Bereichen IT-Sicherheit, Software-Entwicklung und Integration. Das Angebot umfasst dabei die qualifizierte Beratung, sowie die Konzeption und Realisierung individueller Aufgabenstellungen bis zur Einführung und Betreuung im laufenden Betrieb. Zum Kundenstamm der GAI NetConsult gehören vorwiegend Unternehmen aus den Branchen Energieversorgung, Finanzdienstleistung, Chemie/Pharma sowie Öffentliche Verwaltungen und Bundesinstitute. Nachgewiesenes fachliches Know-how, weithin beachtete Publikationen sowie eine Vielzahl von Beiträgen auf exponierten Fachkongressen und nicht zuletzt exzellente Kundenreferenzen unterstreichen die Positionierung des Unternehmens als einen der führenden Dienstleister für „Sichere eBusiness-Lösungen“.*