GAI NetConsult GmbH - 13507 Berlin – Am Borsigturm 58 – www.gai-netconsult.de – Tel: 030-417898-0

Erstellung szenariobasierter Notfallkonzepte

Holm Diening

Whitepaper *April 2012*

Die IT-Infrastruktur ist mittlerweile vitaler Bestandteil der Geschäftsprozesse fast jeden Unternehmens. Maßnahmen zur Notfallplanung werden deshalb zunehmend wichtiger und unterstützen die Aufrechterhaltung des Geschäftsbetriebes nach einem Schadensfall. Die Orientierung an Notfallszenarien ist eine praktikable und ressourcenschonende Herangehensweise für die Erstellung von modular erweiterbaren Notfallkonzepten.

Je länger ein Unternehmen besteht und je größer es ist, desto eher wird es sich einer Notfallsituation stellen müssen. Ohne ein durchdachtes und erprobtes Notfallkonzept ist ein koordiniertes und zielführendes Handeln der Beteiligten im Ernstfall erfahrungsgemäß unwahrscheinlich. Eine angemessene Vorbereitung auf Notfallszenarien wird daher auch als essentieller Bestandteil ordnungsgemäßer Corporate Governance angesehen.

Unabhängig davon, dass die Vorbereitung auf Notfälle im eigenen Interesse des Unternehmens liegen sollte, existieren in Deutschland ebenso diverse Verordnungen und Regelungen, die eine Notfallkonzeption im IT-Bereich vorschreiben oder in diese Richtung interpretiert werden. Beispiele hierfür sind:

- § 91 Abs. 2 AktG (Früherkennung von Risiken)
- § 43 Abs. 1 GmbHG (Sorgfaltspflichten)
- Abs. 66 ff. des IDW Prüfungsstandards 330
- Kapitel 9 in den „Mindestanforderungen an das Risikomanagement“

Eine gesetzliche oder durch Verordnung bindende Verpflichtung zur Notfallvorsorge im IT-Bereich würde sich auch dann ergeben, wenn diese Vorschriften allgemein Maßnahmen zur Aufrechterhaltung der Informationssicherheit einfordern, da hier generell auch die Notfallvorsorge einen eigenen Themenkomplex darstellt. Dementsprechend dürfte sich eine Verpflichtung zur Notfallvorsorge auch aus dem neuen §11a des Energiewirtschaftsgesetztes ergeben, der einen „angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die der Netzsteuerung dienen“ fordert.

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. Konkreter, mit Fokus of den IT-Bereich, wird die ISO 27031 „Guidelines for information and communication technology readiness for business continuity“.

Das Bundesamt für Sicherheit in der Informationstechnik hat hierzu ebenfalls einen eigenständigen Standard (BSI-Standard 100-4 „Notfallmanagement“) entwickelt. Zusätzlich enthalten die Grundschutzkataloge hierfür einen eigenen Baustein „B 1.3

Notfallmanagement“, der Gefährdungen und Maßnahmen für die Notfallvorsorge 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“.

Phasen des Business Continuity Management

Dieser Abschnitt beschreibt die einzelnen Phasen des Business Continuity Management, wobei die IT-relevanten Bestandteile im Vordergrund stehen sollen. Die nachstehende Abbildung 1 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, wobei, aus naheliegenden Gründen, diese übergeordnete Sicht auf die Vorgehensweise bei allen Standards vergleichbar ist.

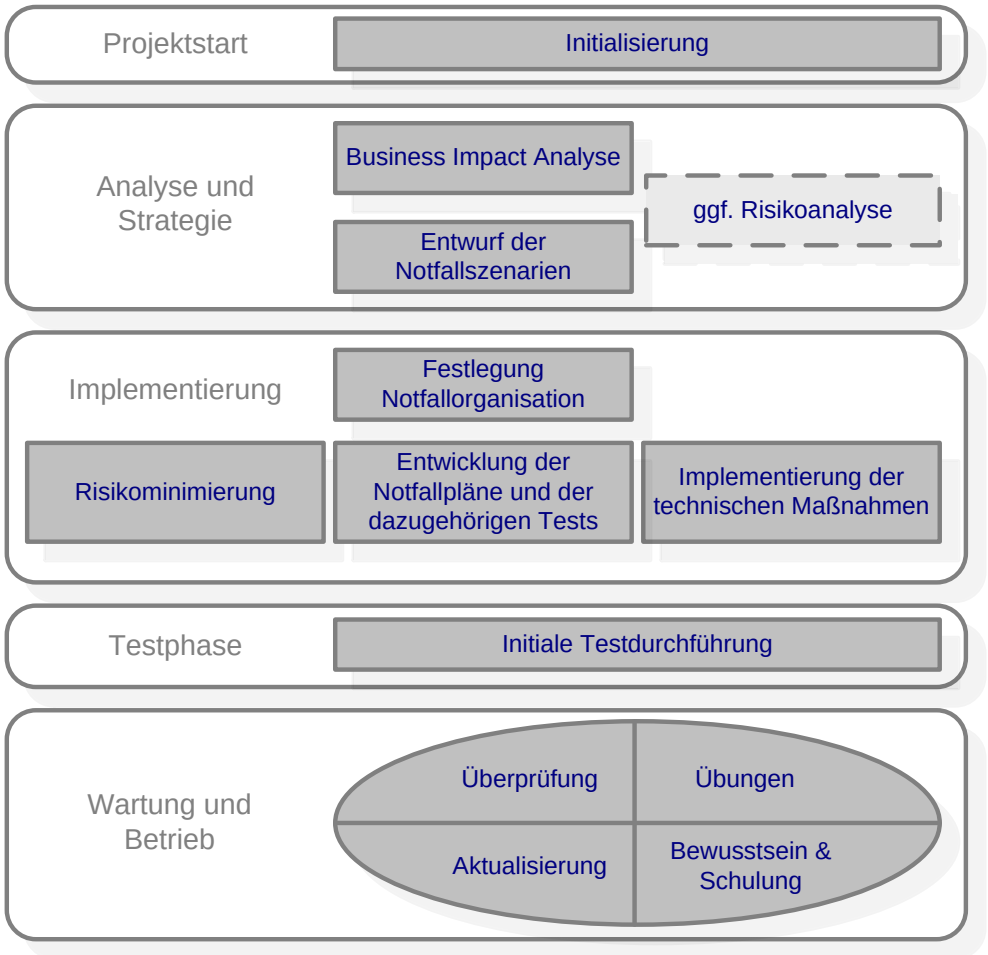

Abbildung 1: Phasenmodell des Business Continuity Management

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 sowohl von der Notwendigkeit des Projektes als auch von der Weiterführung als kontinuierlicher Prozess überzeugt werden. Gerade für die kontinuierliche Weiterführung werden finanzielle und personelle Ressourcen benötigt, die in der ersten Phase der Planung thematisiert werden müssen.

Für ein ressourceneffizientes Notfallkonzept ist es außerdem erforderlich die Anwenderfachbereiche intensiv in die Planung einzubinden. Ohne dieses Vorgehen werden allzu oft die Standard-Wiederherstellungszeiten aus den SLAs oder OLAs als „Recovery Time Objective“, also die Wiederherstellungszeit im Notfall, fehlinterpretiert. Dabei gelten diese Zusagen in den Verträgen fast ausschließlich nur für normale technische Störungen, nicht aber für wirkliche Krisensituationen.

Abgesehen davon, sind diese Wiederherstellungszeiten im wirklichen Notfall meist auch gar nicht notwendig. Bei einer konkreten Analyse der Auswirkungen eines Diensteausfalls auf den Geschäftsbetrieb (Business Impact Analyse [BIA]) stellt sich oft heraus, dass für eine temporäre Überbrückung durchaus Alternativen mit minimaler oder gar keiner IT-Unterstützung bestehen oder die Auswirkungen ohnehin nicht so gravierend sind, wie vom IT-Dienstleister oder vom IT-Fachbereich zunächst angenommen.

Die frühzeitige Einbindung der Anwender in die Bewertung von Notfallszenarien ist daher entscheidend für die Erstellung eines Notfallkonzeptes, das nicht „über das Ziel hinaus schießt“. Dieses Vorgehen dürfte daher auch aus finanziellen Gründen für jede Organisation interessant sein.

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 nicht-IT Fachbereiche sind in das Vorgehen vollständig integriert.
- 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 deshalb 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 einfachen Scoringverfahrens vorgenommen werden, das die Auswirkungen einer Unterbrechung durch Kennzahlen (zum Beispiel Schulnotensystem) beschreibt. Die Vergabe von Kennzahlen sollte dabei auf der Basis eines festgelegten Beurteilungsschlüssels erfolgen. So können finanzielle Auswirkungen anhand der Vorgaben des unternehmenseigenen Risikomanagements bewertet werden. Auswirkungen auf die Reputation der Organisation lassen sich zum Beispiel von „1“ für „keine Auswirkungen“ bis zu „6“ für „schwerwiegender langfristiger Imageschaden“ beurteilen.

Ein solches Bewertungsschema könnte etwa folgendes Aussehen haben (siehe Tabelle 1):

MCA:	1 Tag		2 Tage		1 Woche		2 Wochen		1 Monat	
	Bemerkungen	Bew.	Bemerkungen	Bew.	Bemerkungen	Bew.	Bemerkungen	Bew.	Bemerkungen	Bew.
Finanzielle Auswirkung										
Verlust von Reputation										
Rechtliche Konsequenzen										
Sicherheit von Personen										
Summe										

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

Wer bereits ein Information Security Management System (ISMS) eingeführt hat, kann und sollte hier Synergien nutzen: Schließlich ist die Business Impact Analyse im Sinne der Notfallplanung nichts anderes als eine „Schutzbedarfsfeststellung“ (Begriff aus der Grundschutzmethodik des BSI) oder ein „Criticality Assessment“ (Begriff aus der Methode FIRM), bei der lediglich die Auswirkungen in Bezug auf den Verlust der Verfügbarkeit (neben „Vertraulichkeit“ und „Integrität“) genauer untersucht werden. Es bietet sich durchaus an, beispielsweise im Rahmen der Schutzbedarfsfeststellung nach Methodik des BSI, bereits eine grobe Vorsortierung durchzuführen. Dabei könnten dann nur die Geschäftsprozesse, die bei Verlust der Verfügbarkeit zu einer Einstufung höher als „normal“ gelangen, in einer detaillierteren BIA betrachtet werden.

Anhand des Ergebnisses der BIA kann dann jeder, der als kritisch eingestuften Geschäftsprozesse nochmals einem der beiden in Abbildung 2 dargestellten Verläufe zugeordnet werden. Je nachdem, ob schwere Schäden unmittelbar nach dem Ausfall oder erst nach einiger Zeit auftreten würden, kann in der Notfallkonzeption verstärkter Fokus auf die Prävention von Notfällen (erster Fall) oder auf eine zeitlich angemessene Notfallreaktion gelegt werden.

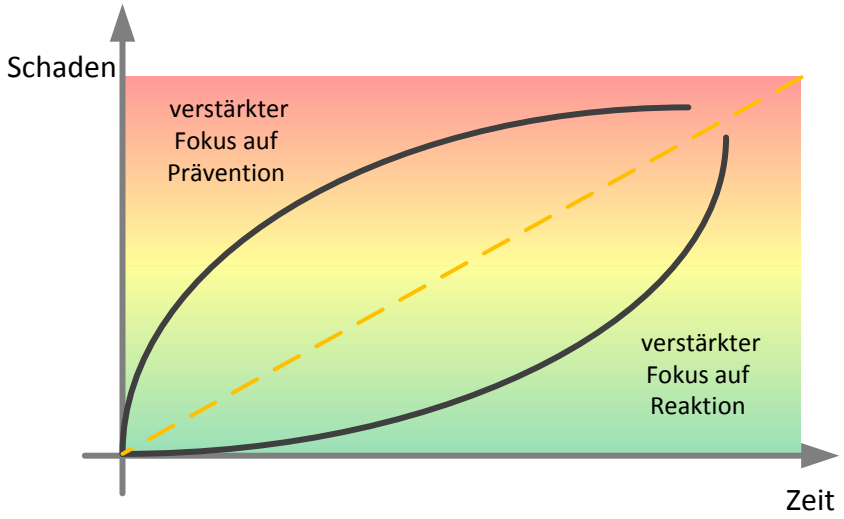

Abbildung 2: Schadensverlauf in Abhängigkeit der Ausfallzeit

Im Bereich der präventiven Maßnahmen muss man dabei nicht immer reflexartig an den Aufbau von Clusterlösungen oder Backup-Rechenzentren denken. Dies wäre nicht nur die mit Abstand teuerste Variante, sondern sie schützt vor allem auch nicht vor Notfällen, die

systematische Ursachen haben. Die praktische Erfahrung zeigt, dass Notfallkonzepte eben oft nur auf schwerwiegende physikalische Schäden oder Hardwareausfälle fokussieren. Leider liegen die Hauptursachen für das Versagen von IT-Diensten eben gerade nicht in der Physik. Vielmehr sind es simple Wartungsfehler, Softwareversagen (gern nach Updates) oder der Verlust der Datenbankintegrität, die sich natürlich auch automatisch in die Ausweichstandorte repliziert; works as designed!

Man sollte sich daher nicht auf dem vorhandenen Backup-Rechenzentrum ausruhen, sondern vielmehr, gerade bei kritischen IT-Diensten, genauer hinsehen. Dieses „genauer Hinsehen“ bedeutet üblicher Weise die Durchführung einer komplexen Risikoanalyse zur Bewertung der potentiellen Ausfallrisiken und der Ableitung entsprechender präventiver Maßnahmen. Diese Risikoanalyse wird meist im technischen Bereich noch unterstützt durch eine „Component Failure Impact Analysis“ (CFIA), bei der die Auswirkungen des Ausfalls einzelner Komponenten auf den gesamten IT-Dienst analysiert werden. Ziel des Ganzen ist die Identifizierung und Eliminierung möglicher „Single Points of Failure“. So wichtig und richtig dieser Vorgang auch ist, so aufwändig ist er auch und erfordert gleichzeitig eine regelmäßige Kontrolle und Überarbeitung. Unser Ziel, möglichst zügig und ressourceneffizient eine Notfallkonzeption zu erstellen und zu pflegen, wird dadurch nicht erreicht.

Wesentlich praktikabler sind hier szenariobasierte Ansätze. Die Grundannahme besteht hierbei darin, dass ein bestimmtes Notfallszenario, zum Beispiel der Ausfall eines essentiellen Dienstes oder die Unbenutzbarkeit der Büroräume wichtiger Abteilungen, irgendwie eintreten wird. Die konkrete Ursache ist dabei zunächst völlig unerheblich. Es spielt also keine Rolle, ob die Büroräume nicht mehr betreten werden können, weil sie von den Behörden gesperrt wurden, weil sie abgebrannt sind oder weil die Stromversorgung ausgefallen ist. Analog könnte dies für den jeweiligen IT-Dienst formuliert werden. Das Wesen des szenariobasierten Ansatzes ist es nun, für dieses Notfallszenario einen akzeptablen Notbetrieb zu entwerfen, der sicher erreichbar ist, nur minimale Ressourcen benötigt und über eine angemessene Zeit aufrecht erhalten werden kann. Sofern dieser Notbetrieb gut geplant ist, muss der Fokus der Notfallplanung weniger stark auf dem eigentlichen Wiederanlauf liegen. In der Realität ist das konkrete Verfahren des Wiederanlaufes stark abhängig von den tatsächlichen Schadensereignissen, die sich erfahrungsgemäß schlecht planen lassen. Kann der Notbetrieb angemessen lange aufrecht erhalten werden, so bleibt für die konkrete Ausgestaltung des Wiederanlaufes in der realen Situation mehr Zeit. Voraussetzung hierfür ist, dass der Notbetrieb und der Wiederanlauf voneinander weitgehend unabhängig sind und möglichst nicht auf gemeinsame Ressourcen zugreifen.

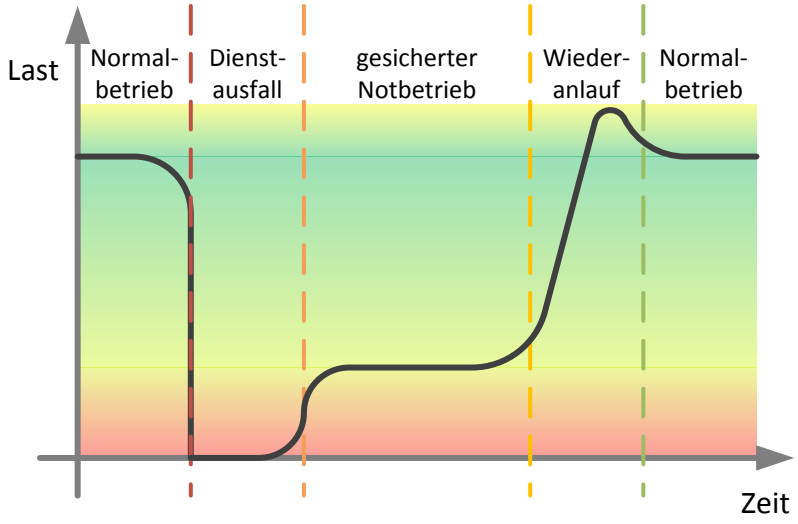

Abbildung 3: Idealer Zeitverlauf einer Notfallbewältigung

Die Grafik in Abbildung 3 verdeutlicht dieses Konzept: Direkt nach dem Eintreten des Notfallszenarios sinkt die Arbeitsfähigkeit auf null. Zu diesem Zeitpunkt wird der Notfall festgestellt und das Konzept zur Erreichung des Notbetriebes aktiviert. Der Notbetrieb stellt über einen möglichst langen Zeitraum die absolut wichtigsten Abläufe des Unternehmens sicher und dient vor allem dazu weiteren Schaden abzuwenden. In dieser Zeit kann, in Abhängigkeit des tatsächlichen Vorfalls, der Wiederanlauf durchgeführt werden. Dabei kommt es auch zu einer kurzfristigen Überhöhung der Arbeitslast durch die Abarbeitung des entstandenen Rückstandes. Anschließend ist der Normalbetrieb wiederhergestellt.

Die wichtigsten Rahmenbedingungen für einen eingeschränkten Betrieb zur Überbrückung der Zeit bis zum Wiederanlauf können dabei, wie folgt zusammengefasst werden:

- Schadensbegrenzung geht vor
- Benötigte technische Ressourcen sollten möglichst unabhängig von der eigenen Infrastruktur funktionieren:
    - Mobiltelefone (oder Satellitentelefone -> bei Stromausfall auch kein Mobilfunknetz!) ersetzen die TK-Anlage
    - Notebooks mit den wichtigsten Daten offline ersetzen den PC
    - UMTS/LTE Verbindungen ersetzen den lokalen Internetzugang
    - Bleistift und Papier
- Es sollten nur Mitarbeiter tätig sein, die innerhalb des Notfallkonzeptes für die Geschäftsfortführung vorgesehen sind.

Natürlich gibt es gegen die Methode der szenariobasierten Notfallplanung auch Einwände, die prinzipiell berechtigt sind. Sie sollen hier entsprechenden Gegenargumenten gegenübergestellt werden:

- Die Konzeption dieser Offline-Version des Geschäftsbetriebes wird nicht immer möglich sein.

  Meistens lassen sich aber adäquate Lösung im Dialog mit den Anwenderfachbereichen deutlich häufiger finden, als von den IT-Abteilungen angenommen.
- Es werden nur Notfälle betrachtet, für die vorher ein Szenario entworfen wurde.

  Das ist richtig. Erfahrungsgemäß sind dies aber auch die relevantesten Szenarien. Es geht bei dieser Methodik, wie bereits benannt, um eine vereinfachte und schnell zum Ziel führende Vorgehensweise. Unabhängig davon können beliebig neue Szenarien hinzugefügt werden.
- Der Notbetrieb könnte in vielen Notfallsituationen unangemessen spartanisch sein, weil das Ausmaß der Notsituation einen geringeren Umfang hat als angenommen.

  Dafür muss aber nur für ein abstraktes Szenario geplant werden und der Notbetrieb ist sicher und verlässlich erreichbar. In der Praxis würde die geringere Tragweite der tatsächlichen Notsituation ohnehin schnell adaptiert werden.
- Der Notbetrieb erfordert zusätzlichen Aufwand und Ressourcen, die bei klassischen Wiederanlaufplänen nicht erforderlich wären.

  Zu beachten ist aber auch, dass der Aufwand für das Pflegen und Testen der differenzierteren Wiederanlaufpläne deutlich erhöht ist, während in diesem Konzept nur wenige Notfallverfahren gepflegt werden müssen und diese meist auch unabhängig von der produktiven Infrastruktur getestet werden können.

Phase 3: Implementierung

Die Implementierung eines Notfallkonzeptes erfolgt in drei Stufen: Der Festlegung einer geeigneten Notfallorganisation und der Alarmierungsketten, der Erarbeitung von

Ablaufplänen mit der Implementierung der technischen Grundlagen des Notbetriebes sowie abschließend die 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 Vorfalls wird eine andere Stelle die Alarmkette auslösen, die jedoch am Ende immer die Alarmierung aller für den jeweiligen Notfall relevanten Teams zur Folge hat.

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

- Sofortmaßnahmen bei Unglücksfällen
- Schadensbegrenzung (Notabschaltungen, u.ä.)
- Bestandsaufnahme
- Kommunikation mit den Medien

Die nächste Ebene der Notfallpläne orientiert sich dann an den Aufgaben zur Erreichung des vorher definierten Notbetriebes zur stabilen Überbrückung der Notsituation (nach Festlegung der Notfallszenarien aus Phase 2) und, nachgeordnet, der Wiederanlauf zum Normalbetrieb.

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
- Beschreibung der definierten Notfallszenarien
- Alarmierungsketten und Ablaufpläne
- Rufnummern- und Adresslisten von Mitarbeitern und Servicepartnern
- Andere wichtige Informationen im Anhang (Raumpläne, Umzugslisten, etc.)

Dabei hat das Kapitel „Beschreibung der definierten Notfallszenarien“ eine ganz wesentliche Rolle: Es soll für jedes Notfallszenario grob auf maximal einer Seite skizzieren, wie das jeweilige Notfallszenario charakterisiert ist (dazu gehört auch die Abgrenzung von normalen technischen Störungen), was die erwarteten Auswirkungen auf den Geschäftsbetrieb wären und wie das Notfallverfahren aussehen soll. Diese Beschreibung ist natürlich nur als Vorspann zur eigentlichen Ablaufplanung zu verstehen, gibt dem Leser aber einen, in Notfällen so wichtigen, ersten Überblick. Als Beispiel soll hier das im Rahmen von Schulungen verwendete Notfallszenario („Ausfall des Onlineshops“) eines fiktiven kleinen Versandhandels dienen:

1 Beschreibung des Szenarios

Das Szenario „Gesamtausfall des Onlineshops“ tritt ein, wenn z.B. aufgrund einer technischen Störung die Bestellung über das Onlineshop-System nicht mehr möglich ist und die Störung vermutlich länger als 4 Stunden anhalten wird. Der Ausfall des Onlineshops kann verschiedene Ursachen haben:

- Ausfall des Webservers
- Ausfall des Payment-Gateways
- Ausfall des Datenbank-Backends
- Gesamtausfall des IT-Systems
- Softwarefehler

2 Einschätzung der Auswirkungen auf den Geschäftsbetrieb

Der Komplettausfall des Onlineshops für länger als 4 Stunden ist als Notfall definiert. Da 90% des Umsatzes über den Onlineshop generiert werden, bedeutet auch ein kurzfristiger Ausfall bereits höhere Umsatzeinbußen. Längerfristige Ausfälle können ebenso mit einem Vertrauensverlust der Stammkundschaft einhergehen. Aus diesem Grund wurde für dieses Szenario ein Notfallverfahren festgelegt.

3 Notfallverfahren

Unabhängig von der Ursache und dem tatsächlichen Umfang der betroffenen IT-Systeme gilt folgendes Notfallverfahren:

- Es ist zunächst ein Notverfahren für das Bestellwesen zu etablieren. Dieses besteht aus der Aktivierung einer statischen Bestellseite bei unserem Provider und der manuellen Entgegennahme der Bestellungen per Telefon oder Fax (bzw. eMail wenn funktionsfähig)
- Die Abrechnung der Lieferung erfolgt bei Kreditkartenzahlungen über das Mailorderverfahren. Lieferungen per Rechnung oder Lastschrift sind nur möglich, wenn das System zur Bonitätsprüfung noch bereit steht, anderen Falls werden diese Bestellungen gesammelt.
- Rechnungen sind aus der Excel-Vorlage zu erstellen und lokal zu speichern.

Parallel zum Notbetrieb erfolgt der Wiederanlauf der produktiven IT-Umgebung. Nach deren Übergabe in den Normalbetrieb sind folgende Nacharbeiten erforderlich:

- Manuelles Verbuchen der Bestellungen in die Buchhaltung
- Abarbeiten aller Bestellungen auf Basis von Rechnung oder Lastschrift sobald das System zur Bonitätsprüfung wieder online ist

Die Abwicklung des Notfalls erfolgt im Detail sowie im Notfallablauf „Gesamtausfall des Onlineshops“ (siehe Kapitel „Ablaufpläne“) beschrieben.

Die tatsächliche Planung, inklusive der notwendigen Referenzen auf Rufnummern, Servicekennwörter und dergleichen, ist in der eigentlichen Ablaufplanung enthalten. Zu beachten ist auch, dass bereits in diesem simplen Schulungsbeispiel die Notfallverfahren

angemessen vorbereitet sein müssen, hier nämlich durch die Hinterlegung (und Pflege) einer statischen Bestellseite. Gleichzeitig wird aber auch der Vorteil dieser Herangehensweise deutlich: Anstelle einer deutlich komplexeren Notfallkonzeption für allerlei technische Störungen, die zudem auch einen entsprechend hohen Pflegeaufwand nach sich zieht, kann hier mit einem einfachen Verfahren, welches sich ebenso leicht testen lässt, zunächst Schadensbegrenzung betrieben und Zeit für den situationsspezifischen Wiederanlauf gewinnen.

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!

BEZEICHNUNG	INHALT	BETEILIGTE	FREQUENZ	AUFWAND
Desktop Test	Der BCM Verantwortliche sowie alle anderen Beteiligten gehen den Plan „am Schreibtisch“ durch und identifizieren mögliche Abweichungen	BCM Verantwortlicher und sein Team	oft ↓ selten	niedrig ↑ hoch
Structured Walk Through Test	Die Notfallkonzeption wird gemeinsam durchgearbeitet, um eventuelle Fehler in der Zusammenarbeit der Beteiligten aufzudecken (z.B. die doppelte Verwendung von Ressourcen). Zusätzlich wird die Kommunikation zwischen den Teams getestet.	Alle BCM Teams gemeinsam		
Simulation Test	Es werden alle Schritte von allen Beteiligten ausgeführt, wie sie im tatsächlichen Notfall geplant sind. Ausnahmen: Es werden keine Ersatzkomponenten geliefert und es werden keine produktiven IT-Systeme modifiziert.	Alle Mitarbeiter, die operative Aufgaben in der Notfallplanung haben		
Parallel Test	Es wird ein Simulation Test durchgeführt, der aber zusätzlich auch die Inbetriebnahme von Ausweichressourcen umfasst.	Alle Mitarbeiter, die operative Aufgaben in der Notfallplanung haben sowie externe Dienstleister		
Full Interruption Test	Die Durchführung eines Notfalltests durch die tatsächliche Betriebsunterbrechung der produktiven Systeme	Alle Mitarbeiter, die operative Aufgaben in der Notfallplanung haben sowie externe Dienstleister		

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

Ebenso verhält es sich mit Notfallhandbüchern. Prinzipiell ist immer alles klar, die Ablaufpläne theoretisch narrensicher. Beim initialen Test eines Notfallplanes zeigen sich jedoch (auch 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 eine wirkliche Unterbrechung des Produktivbetriebes 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 Tabelle 2 gibt einen Überblick über verschiedene Testmethoden und ihren Aufwand.

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 oder
- eine neue Risikosituation Gewissheit über die Gültigkeit der Pläne erforderlich macht

Phase 4: Wartung und Betrieb

Wir sind am Ende des BCM „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

Notfallhandbücher mit allen wichtigen Informationen, Tabellen und Plänen zur Bewältigung von größeren Störfällen ist das wichtigste Ergebnis des Business Continuity Management. 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 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 BCM-Verantwortlichen verbleiben.

Fazit

Darüber, dass die angemessene Vorbereitung auf Notsituationen eine zwingende Notwendigkeit ist, besteht heutzutage in den meisten Organisationen weitgehend Einigkeit. Entsprechende Gesetze und Verordnungen tun ihr Übriges. Für eine praktikable Umsetzung fehlen aber vielfältig noch die Kochrezepte, denn ein stringentes Durchexerzieren der einschlägigen Standards würde oftmals zu unangemessen hohen Aufwänden führen. Eine vereinfachte Notfallplanung auf Basis eingeschränkter Notfallszenarien ist eine Methode, die sowohl rasch zu vorzeigbaren Ergebnissen führt, als auch kontinuierlich zu einer vollständigen Notfallkonzeption erweiterbar ist. Der Einsatz entsprechend spezialisierter Tools kann dabei die Erstellung der Dokumentation und den Nachweis regelmäßiger Tests und Übungen gegenüber der Revision erleichtern.

Holm Diening *ist als IT-Security Consultant bei der GAI NetConsult GmbH in den Bereichen „Sicherheitsmanagement“ und „Notfallplanung“ tätig.*

*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“.*