

Ulrich Moser

Der IT-Ernstfall – Katastrophenvorsorge

Was Manager wissen müssen!

Business Continuity & Disaster Recovery

- Managementverantwortung
- Disaster-Recovery-Konzepte
- Disaster-Recovery-Services
- Tools & Instrumente
- Riskmanagement
- Kosten/Nutzen
- Praxisbeispiele
- Checklisten
- Trends
- Tipps

Editionspartner

 Telekurs Services

AC 



Ulrich Moser

**Der IT-Ernstfall –
Katastrophenvorsorge
Was Manager wissen müssen!**
Business Continuity &
Disaster Recovery

BPX Best Practice Xperts
Internet www.bpx.ch
E-Mail info@bpx.ch

Moser, Ulrich:
**Der IT-Ernstfall – Katastrophenvorsorge
Was Manager wissen müssen!
Business Continuity & Disaster Recovery**

Rheinfelden/Schweiz, BPX-Edition, 2003/2004
ISBN 3-905413-23-X

© 2002 BPX-Edition Rheinfelden

Alle Rechte, insbesondere die Übersetzung in fremde Sprachen, sind vorbehalten. Kein Teil des Buches darf ohne schriftliche Genehmigung des Verlages fotokopiert oder in irgendeiner anderen Form reproduziert oder in eine von Maschinen verwendbare Form übertragen oder übersetzt werden.

Herstellung: BPX-Edition, Rheinfelden/Schweiz
Druck und Verarbeitung: Druckerei Flawil AG

Inhalt

1	Praxisbeispiele der Editionspartner.....	6
1.1	Telekurs Services AG	6
1.1.1	Biz-Case: Allianz Suisse	6
1.1.2	Unternehmensdaten: Telekurs Services	9
1.2	sunrise AG.....	10
1.2.1	Biz-Case: sunrise gigabit ethernet	10
1.2.2	Unternehmensdaten: sunrise	13
1.3	AC-Service (Schweiz) AG	14
1.3.1	Biz-Case: Sanitas	14
1.3.2	Profil: AC-Service.....	17
2	Einführung und Hintergründe	19
2.1	Was ist ein Disaster?	19
2.1.1	Katastrophe oder Unannehmlichkeit	19
2.1.2	Die zeitliche Komponente	20
2.1.3	Kleine Ursache – grosse Wirkung.....	20
2.1.4	Gefährdungsszenarien.....	20
2.2	Gründe für Business Continuity & Disaster Recovery Planning (BCP).....	23
2.2.1	Rechtliche Rahmenbedingungen	24
2.2.2	Verträge und Haftung.....	24
2.3	Phasen der Planung	25
2.3.1	Schwachstellen- und Risikoanalyse (Health Check)	25
2.3.2	Risikobewertung und Schadenauswirkungsanalyse.....	25
2.3.3	Massnahmen zur Vorbereitung auf Notfälle	31
2.3.4	Notfallpläne	33
2.4	Managementverantwortung auf oberster Ebene	34
2.4.1	ISO/IEC 17799/2000	35
2.4.2	Aufgaben der Geschäftsleitung.....	35
2.4.3	Aufgaben des IT-Managements (CIO)	37

3	Disaster-Recovery-Konzept	38
3.1	Konzept – Zusammenspiel Mensch– Prozesse–Technologie	38
3.2	Bedürfnisse einstufen	39
3.2.1	Recovery Point Objective RPO	40
3.2.2	Recovery Time Objective RTO	42
3.2.3	Maximale akzeptable Ausfallzeit	42
3.3	Faktor Mensch.....	42
3.3.1	Notfallorganisation	42
3.3.2	Erreichbarkeit im Notfall	44
3.3.3	Regelmässige Schulung und Übung von Katastrophenszenarien	45
3.4	Faktor Prozesse	46
3.4.1	Drehbücher für mögliche Katastrophenszenarien	46
3.4.2	Drehbücher für Schulung und Übung.....	49
3.4.3	Notfallprozeduren Eskalationsverfahren	49
3.5	Faktor Technologie.....	50
3.5.1	Ausweichrechenzentrum	51
3.5.2	Physische Sicherheit.....	52
3.5.3	Redundante IT-Systeme	53
3.5.4	Allgemeine Sicherheit	54
3.5.5	Service Level Management	54
3.5.6	Notfall-Arbeitsplätze (intern/extern).....	55
3.5.7	Daten-Kommunikation.....	57
3.5.8	Voice-Kommunikation	60
4	Disaster Recovery Services.....	61
4.1	Cold Service – Datensicherung an Zweitstandort	61
4.2	Warm Service – Betriebsbereite Stand-by-IT-Systeme an Zweitstandort	61
4.3	Hot Service – Paralleler Betrieb der IT-Systeme an zwei Standorten	62
5	Tools und Instrumente	63
5.1	Werkzeuge für Disaster Backup	63
5.2	Evaluationskriterien	65
5.3	Checklisten	66

6	Kosten: Wie rechnet sich Business Continuity?	68
6.1	Modellrechnungen	68
6.2	Vergleich Insourcing mit Outsourcing von Disaster-Recovery-Lösungen	70
6.3	Kosten-Nutzen-Analyse	71
6.4	Investitionsrechnung gegenüber Versicherungskosten	71
7	Trends und Ausblick	72
8	Referenzen	74
8.1	Bücher	74
8.2	Links	75
9	Glossar	76
10	Autor und BPX	79

1 Praxisbeispiele

1.1 Telekurs Services AG

1.1.1 Biz-Case: Allianz Suisse

Sicherheit ist das zentrale Stichwort für Geschäftsdaten und Arbeitsprozesse. Je stärker eine Unternehmung die IT im Rahmen ihrer Geschäftsprozesse einsetzt, desto wichtiger ist die Gewährleistung eines reibungslosen Ablaufs und klarer Konzepte für das Handling von Notfällen. Zwei Branchen, für welche dies im Besonderen zutrifft, sind Banken und Versicherungen. Am Beispiel der Allianz Suisse wird aufgezeigt, wie Telekurs Services die hohen Sicherheitsanforderungen des Versicherers mit einem Ausweichrechenzentrum und eindeutigen Prozessen für den Notfall realisiert hat.

Ausgangslage und Zielsetzungen

Innerhalb der IT-Strategie der Versicherungsgesellschaft Allianz Suisse wurden die folgenden Statements gemacht:

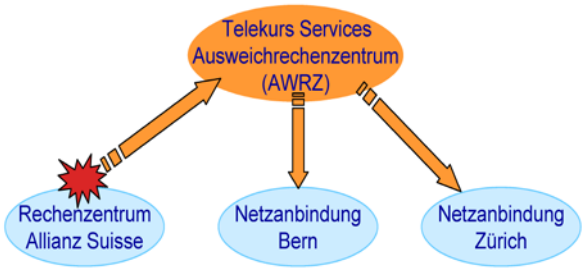
- Bessere Vorbereitung auf Katastrophenszenarien
- Zusätzliche, physisch getrennte Produktionsumgebung

Dabei wurden folgende Zielsetzungen definiert:

- Datenspiegelung zu einem örtlich getrennten Rechenzentrum
- Zugriff auf die Daten bei einem Katastrophenfall
- Aufnahme des normalen Betriebes innerhalb von maximal 48 Stunden

Umsetzung

Für Allianz Suisse war von Anfang an klar, dass diese Zielsetzungen nur mit einem Ausweichrechenzentrum (AWRZ) möglich sind. Aus wirtschaftlichen und zeitlichen Überlegungen entschied man, dieses AWRZ nicht selber zu realisieren.



Für die Ausgangslage hat Allianz Suisse folgende Merkmale definiert:

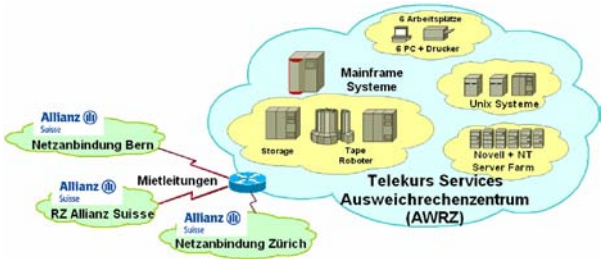
- Örtlich getrenntes Rechenzentrum inklusive Infrastruktur (AWRZ)
- Bereitstellung Mainframe-Rechenleistung für Testzwecke und für den Notfall
- Komplette IT-Systemlandschaft (Server, Storage, Netzwerk)
- Netzanbindung (WAN) zu anderen Standorten
- Notfall-Arbeitsplätze
- Abstimmung und Implementation der Notfall-Prozedur
- Integration in ein System Control Center für Überwachung, Alarmierung und Support

Aufgrund dieser Ausgangslage hat Telekurs Services den Disaster-Recovery-Auftrag mit der Servicevariante «Hot» mit dem folgenden Lösungsumfang erhalten:

- Die zentralen Host-Daten der Allianz Suisse werden zu einem zweiten, örtlich getrennten Ausweichrechenzentrum (AWRZ) gespiegelt.
- Datensicherungen werden mit einem Taperoboter im AWRZ regelmässig durchgeführt.
- Sechs Notfall-Arbeitsplätze im AWRZ für Testzwecke und Systemüberwachungen.
- Mietleitungen stellen die Verbindungen zu den verschiedenen Standorten sicher.
- Zusätzlich stellt Telekurs Services die nötige Mainframe-Rechenleistung (MIPS) der Allianz Suisse für Testzwecke und Notfälle zur Verfügung.

- Jährliche Notfallübung für die Realtime-Umschaltung der IT-Systeme.
- Regelmässige Einübung der Notfallprozeduren für den Ernstfall.

Lösungsübersicht von Telekurs Services:

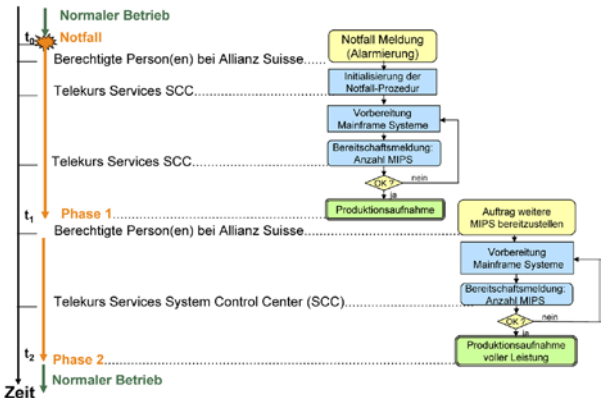


Notfall-Prozedur

Für die Notfall-Prozedur werden die folgenden Schritte eingeleitet:

- IT-Betrieb und -Systeme im Rechenzentrum herunterfahren
- IT-Betrieb zum AWRZ wechseln
- Netzwerk-Anschluss der anderen Standorte in Betrieb nehmen
- IT-Betrieb im AWRZ starten

Schematische Übersicht der Notfall-Prozedur für den Bezug von Mainframe-Rechenleistung:



1.1.2 Unternehmensdaten Telekurs Services



Telekurs Services AG, ein Unternehmensbereich der Telekurs Group, zählt in der Schweiz zu den führenden Anbietern von IT-Dienstleistungen mit hohen Ansprüchen an Sicherheit und Verfügbarkeit. Telekurs Services unterstützt ihre Kunden vor allem in technischen Fragen bezüglich Nutzung, Effektivität und Effizienz von IT-Infrastrukturen und -Applikationen. Telekurs Services beschäftigt über 500 Personen und betreibt zwei der modernsten und leistungsfähigsten Rechenzentren in der Schweiz.

Das Serviceangebot umfasst:

Application Management

Management von Kunden- oder Standard-Applikationen, Helpdesk, Systembetreuung, Hosting.

Disaster Recovery:

Notfall-Arbeitsplätze, Notfallübung des Ernstfalles, Restore und Recovery.

SAP Sourcing:

Pilotinfrastruktur, Hosting von SAP-Komponenten, Business Process Enabling, Business Intelligence (BI, BW, DWH), Customer Relationship Management (CRM).

Weitere:

HP NonStop™-(Tandem-)Kompetenzzentrum, EDI Clearing, File Transfer Service.

Telekurs Services AG

IT Services
Hardturmstrasse 201
CH-8021 Zürich
Tel. +41 1 279 41 11
Fax +41 1 279 41 12
it-services@telekurs.com
www.telekurs-services.com

1.2 sunrise

1.2.1 Biz-Case: sunrise gigabit ethernet – Massgeschneiderte Vernetzung zwischen wichtigen IT-Standorten

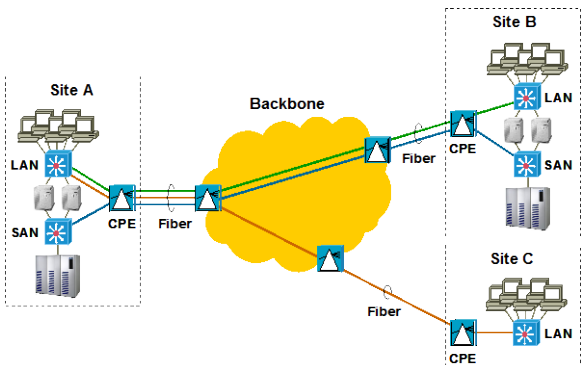
Eine zentrale Management-Herausforderung besteht heute darin, die Sicherheit von Informationen und Transaktionen zu gewährleisten. Die richtige Vernetzung von Rechenzentren spielt dabei eine «matchentscheidende» Rolle.

Die Herausforderung

Hängt Ihre Produktivität und Ihr Erfolg von der Verfügbarkeit von Informationen ab? Ist eine leistungsstarke und zuverlässige Vernetzung Ihrer Rechenzentren überlebenswichtig? Brauchen Sie eine skalierbare Lösung zwischen Ihren Disaster-Recovery-Standorten? Wünschen Sie sich Bandbreite im Gigabit-Bereich, garantierte Sicherheit und vorteilhafte Kosten?

Die Lösung

sunrise gigabit ethernet ist ein optischer Punkt-zu-Punkt-Service im Gigabit-Bereich mit vollem protokolltransparentem Datentransport. Das heisst, Sie haben dedizierte Bandbreite (z.B. 1,062 Gbps für Fibre Channel) für maximalen Datendurchsatz bei maximaler Qualität.



sunrise gigabit ethernet ist in der ganzen Schweiz verfügbar. Die Unternehmensstandorte werden über Glasfaser mit dem sunrise-Backbone-Netzwerk verbunden. Die eingesetzte Technologie macht die Mehrfachnutzung der Glasfaser möglich.

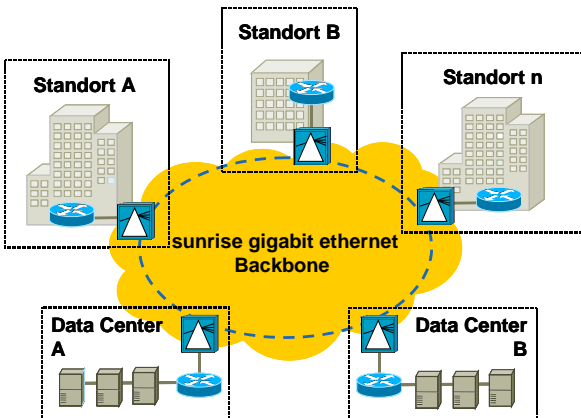
Die skalierbare Plattform, basierend auf Dense Wave Length Division Multiplexing (DWDM), unterstützt folgende Protokolle direkt:

- Gigabit Ethernet (1,25 Gbps)
- Fibre Channel (1,062 Gbps)
- FICON (1,062 Gbps)
- ESCON (200 Mbps)
- weitere IBM-spezifische Protokolle

sunrise stellt den zuverlässigen Betrieb der Services von End-zu-End rund um die Uhr sicher. Der Service wird in verschiedenen Verfügbarkeitsoptionen angeboten. Das kundenspezifische Service Level Agreement garantiert Serviceparameter wie Lieferzeit, Verfügbarkeit und Fehlerbehebung.

Der Nutzen

- Sie verbinden Ihre Disaster-Recovery-Standorte direkt mit dem verwendeten Protokoll und der erforderlichen Performance – regional oder national.
- Sie erschliessen Ihre zur effizienteren Nutzung und zum vereinfachten Betrieb zentralisierten Speicherkapazitäten und Server auf die wichtigsten Standorte.



- Sie nutzen eine entwicklungsfähige, zukunftssichere Lösung, die Ihnen mit Abstand mehr Flexibilität bietet als herkömmliche Lösungen (z.B. SDH- und ATM-Services).

- Sie profitieren vom garantierten Top-Service auf Basis einer individuellen Leistungsvereinbarung (SLA) mit umfassendem 24/7-Monitoring durch das Network Operation Centers (NOC).
- Sie nutzen die Vorteile und die Flexibilität von optischen Services auf Glasfasern – ohne Know-how-Aufbau oder Betrieb eines eigenen Netzes.
- Sie ersparen sich hohe Investitionen und haben kalkulierbare monatliche Fixkosten.
- Sie reduzieren die Komplexität Ihres Netzes zwischen den wichtigsten Standorten.

Die Zielgruppe

sunrise gigabit ethernet ist die Ideallösung für Unternehmen, die

- zwei oder mehrere grosse Niederlassungen haben.
- ihre Data-Center- oder Disaster-Recovery-Standorte effizient verbinden wollen.
- ihr Unternehmensnetz (LAN und SAN) auf die Schweiz ausdehnen wollen.
- neue SAN-Protokolle iSCSI, FCIP und iFCP und Applikationen wie Streaming, Voice over IP nutzen wollen.
- grössten Wert auf Sicherheit und Verfügbarkeit legen.
- mit einer Zentralisierung direkte Einsparungen bei der Infrastruktur und beim Betrieb realisieren wollen.
- generell eine Verbesserung der Netz-Performance erreichen wollen.
- ein gewachsenes Netz mit einem Mix aus traditionellen 2-Mbps-Mietleitungen, SDH- und ATM-Services optimieren wollen.
- die Absicht haben, die Kosten für die interne Kommunikation zu minimieren.

Das Beispiel

sunrise IT, die hausinterne Informationstechnologie-Abteilung, nützt sunrise gigabit ethernet seit über zwei Jahren für die Vernetzung des eigenen Disaster-Recovery-Standortes. Es werden mehr als 20 Gigabit-Services für die Spiegelung des Storage Area Network (SAN) sowie für das LAN eingesetzt. Hierfür kommen

Fibre Channel (FC-100) und Gigabit Ethernet zum Einsatz.

Das Management entschied sich, die zentralen Netzwerkverbindungen für Transaktionen absolut ausfallsicher zu machen. Das Ergebnis: Ein verlustfreies Umschalten ist in weniger als 50 Millisekunden möglich (Protection auf Layer 1). Das heisst, geschäftskritische Applikationen und Daten, z.B. alle für die Rechnungstellung benötigten, sind jederzeit verfügbar.

Die beschriebenen Netzwerk-Services werden durch das sunrise Network Operation Center (NOC) rund um die Uhr überwacht. Sicherheit garantiert.

1.2.2 Unternehmensdaten: sunrise



sunrise ist der Markenname von TDC Switzerland AG. Die Beteiligungsverhältnisse an der TDC Switzerland AG setzen sich zusammen aus der Tele Danmark mit 79 Prozent, der Holding 17 Prozent, SBB 2 Prozent und UBS 2 Prozent. Gegenwärtig beschäftigt sunrise rund 2200 Mitarbeiter.

sunrise bietet seinen Kunden Telekommunikationsdienstleistungen nach dem neuesten Stand der Technik in den Bereichen Festnetz, Internet und Mobilfunk.

sunrise verfügt über ein breites Service-Portfolio, basierend auf einem qualitativ hochwertigen Hochleistungs-Glasfasernetz, das sich mit einer Gesamtlänge von 7000 Kilometern über die gesamte Schweiz erstreckt.

sunrise
Business Solutions
Thurgauerstrasse 60
8050 Zürich
Tel. 0800 111 555
Fax 0800 111 556

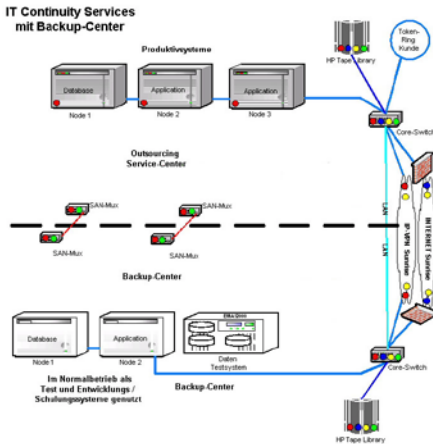
business@sunrise.net
business.sunrise.ch

1.3 AC-Service (Schweiz) AG

1.3.1 Biz-Case: Sanitas

Ohne IT Service Continuity keine Business Continuity: Wie die IT der Sanitas auch bei Nichtverfügbarkeit des Service-Centers weiterläuft.

Rund 430 000 Versicherungsnehmer (1969: 12 000), über 6% der gesamten Bevölkerung der Schweiz, sind bei der Sanitas Krankenversicherung versichert. Eine Basis für die erfolgreiche Geschäftspolitik von Sanitas ist die umfangreiche IT des Krankenversicherers. Sie wird seit Jahren im Outsourcing-Service-Center der AC-Service (Schweiz) AG, Wettingen, betrieben und betreut. Servicequalität, Kontinuität und Erfahrung von AC-Service sind rückblickend die Gründe, die Sanitas zu AC-Service geführt haben. So ist der Outsourcing-Dienstleister in der Schweiz, aber auch in Deutschland, Österreich und Benelux seit über 40 Jahren am Markt.



Auch bei längerer Nichtverfügbarkeit des Service-Centers – kein Datenverlust und nur kurzzeitige Unterbrechungen.

Der Systembetrieb für Sanitas im Outsourcing-Service-Center von AC-Service in Wettingen ist auf täglich 12 Stunden und 5 Tage die Woche ausgelegt. Der 7x24-Stunden-Betrieb ist mit dem Einsatz der eBusiness-Suite von Partnergate geplant. Etwa 500 Bildschirmarbeitsplätze nutzen diesen Service. Die Hoch-

verfügbarkeit der Anwendungssoftware Sirius wird durch hochwertiges Systemmanagement auf Basis von HP-Unix-Systemen und durch umfangreiche, gespiegelte Speichernetzwerke erzielt. So weit die Regel. Besondere Vorbereitungen aber erfordern Notfälle, in denen die IT aus dem Service-Center einmal längere Zeit nicht zur Verfügung stehen könnte, denn auch dann muss der Geschäftsbetrieb von Sanitas trotzdem weiterlaufen. Dazu haben Sanitas und AC-Service ein neues, umfassendes Service-Continuity-Konzept realisiert. Beim Ausfall des Sanitas-Hauptsystems treten nur geringfügige Unterbrechungen im Bereich weniger Minuten auf, die sich in der Praxis (Eskalationsprozess, Krisenstab, Entscheidungen, Kommunikation usw.) auf max. 1 bis 2 Stunden Prozessverlust addieren dürften. Dann übernimmt das Backup-Center von AC-Service den Betrieb der Sanitas-Lösung. Der entscheidende Vorteil derartiger Service-Continuity-Lösungen: Es kommt praktisch zu 0% Datenverlust, denn ein solches Backup-Center wie das von AC-Service ist viel mehr als nur ein Ausweichrechenzentrum. Denn anstatt im Ernstfall erst zeitaufwändig ausweichen zu müssen, ist der Kunde des Backup-Centers immer längst bereits dort.



Backup-Center: Daten und Datenverarbeitung redundant

Fachleute bezeichnen dieses Konzept als «warmen Backup». Im Mittelpunkt steht hier eine Zweitsystemlandschaft. Sie ist systemtechnisch ähnlich ausgestattet wie das eigentliche Hauptsystem, wird aber im Backup-Center von AC-Service betrieben. Besonders ausfallsichere Hochleistungsmehrfachverbindungen (Glasfaserverbindungen mit Multiplexing) sorgen für den Link zwischen dem Standort des Outsourcing-Service-

Centers in Wettingen und dem Backup-Center. Das Backup-System ist permanent «warm», d.h. laufend in Betrieb. Im Normalfall wird es für Tests, Demo, Entwicklung und Ausbildung genutzt. Im Ernstfall geht deshalb alles ganz schnell. Dazu sind bereits alle Teilnehmer, rund 500 Sanitas-User verteilt auf 17 Standorte, nicht nur mit dem Outsourcing-Service-Center, sondern auch mit dem Backup-Center von AC-Service per Netzwerk verbunden. Hauptstandort und Backup-Standort des Outsourcing-Centers verfügen über separate Taperoboter und Speichernetzwerke, die Sanitas-Daten werden permanent und transaktionsgenau gespiegelt. So muss das Backup-System im Ernstfall nicht neu installiert werden, was in der Praxis viel kostbare Zeit verschlingt. Vielmehr genügt ein einfacher «reboot». Dabei werden lediglich die gespiegelten Daten des Hauptsystems zugeschaltet, die Netzwerk-Umschaltung der Sanitas-User auf das Backup-Center geschieht automatisch. Bis vor kurzem nutzte Sanitas noch einen «kalten» Backup im Ausweichrechenzentrum, der im Ernstfall zu Prozessverlusten von bis zu 2 Tagen sowie Datenverlusten bis zu 1 Tag geführt hätte. Dies war nach einer neuen Beurteilung nicht mehr genügend.

IT Service Continuity – von Sanitas lernen

Nicht nur für Sanitas ist die Verfügbarkeit der IT von zentraler Bedeutung. Zwar verfügen auch die meisten anderen Unternehmen über bewährte Prozeduren für die regelmässige Sicherung ihrer Daten. Kommt es zu einem Ausfall der IT, genügt dies aber oft nicht. Die Geschäftsabläufe, die zwischen der letzten Sicherung und dem Ausfall liegen, können nicht mehr nachgebildet werden. Kunden und Geschäftspartner sind direkt betroffen, der Schaden entsprechend gross. Daher empfehlen Berater für die geschäftskritischen Systeme zunehmend IT-Service-Continuity-Konzepte mit «warmem» Backup. Prozessverluste können auf diese Weise wirkungsvoll reduziert, Datenverluste sogar nahezu ganz vermieden werden. Genaue Analysen sind als Basis von IT-Service-Continuity-Konzepten unerlässlich:

- **Welcher Prozessverlust kann akzeptiert werden?**
Ausfälle von Entwicklungs- und Demo-Systemen richten meist nur geringe Schäden an, der Stillstand geschäftskritischer Anwendungen kann dagegen die Existenz des Unternehmens gefährden. Ein Tag IT-Unterbruch für einen PC-Distributor kann schon das «Ende» bedeuten. Für ein Handelssystem einer

Bank müssen sich «Schaltzeiten» gar im Bereich von wenigen Minuten bewegen.

■ **Welcher Datenverlust kann akzeptiert werden?**

Diese Frage wiegt in der Praxis meist höher als der eigentliche Prozessverlust. Genügt es, auf der letzten Datensicherung, die oft nur ein- bis zweimal pro Tag erfolgt, aufzusetzen? Kann der Datenverlust zwischen letzter Sicherung und Wiederanlauf überhaupt nachgestellt werden?

Teure und im Betrieb sehr anspruchsvolle Backup-Ressourcen aus dem Backup-Center nutzen

Viele Fragen stehen am Anfang eines IT-Service-Continuity-Konzepts. Je nachdem, wie eng das Zeitfenster für Umschalten und Wiederaufnahme bemessen werden kann, unterscheiden sich auch die technischen Konzepte der Service-Pakete. Sie reichen vom «Tape Restore» mit ausgelagerten IT-Systemen, die im Normalbetrieb anderweitig genutzt werden, zum Beispiel als Qualitätssicherungssystem, bis hin zu exklusiven und komplett redundant vorgehaltenen Systemen, die mit gespiegelten Daten arbeiten.

AC-Service bietet für alle Anforderungen wirtschaftliche Lösungen aus dem Outsourcing-Service-Center. Sie werden auf unterschiedlichen Technologieplattformen sowie unter Einbezug eines eigenen Backup-Centers realisiert, welches etwa 15 km vom Hauptstandort entfernt liegt. Die teuren und im Betrieb sehr anspruchsvollen Backup-Ressourcen aus dem Service-Center zu nutzen statt selber zu kaufen und zu betreiben, ist dabei meist die wirtschaftlichste und praktikabelste Variante.

1.3.2 Profil: AC-Service



AC-Service ist fokussiert auf IT-Outsourcing- und -Beratungsdienstleistungen auf der Basis von SAP und anderen Systemen. Der Outsourcing-Dienstleister ist bereits seit über 40 Jahren am Markt und zählt in punkto

- Kontinuität (Unternehmen, Management, Mitarbeiter, Angebot)
- Erfahrung (Branchen, Applikation/Geschäftsprozesse, Technologie)
- Substanz (Bilanz, finanzieller Background)

- Verlässlichkeit (Aussagen, Geschäftsgebaren)
- Dynamik (gezielte Erweiterung des bestehenden Dienstleistungsportfolios)
- Transparenz (Informationspolitik, Finanzberichterstattung)

zu den besten der Branche. AC-Service ist strategisch gut ausgerichtet. Der Fokus auf hochwertige IT-Outsourcing- und -Beratungsleistungen sowie ein ausgeprägtes Wissen um die Kerngeschäftsprozesse und Anforderungen der Kunden dienen AC-Service als Basis für langjährige Kundenbeziehungen. AC-Service notiert im Prime Standard der Frankfurter Wertpapierbörse und weist eine gesunde Geschäftsentwicklung auf. Die Bilanz ist gesund, der Anteil Eigenkapital an der Bilanzsumme beträgt über 60%, das Unternehmen wird nach hohen ethischen Grundsätzen wie Glaubwürdigkeit, Zuverlässigkeit, Kontinuität und Durchsetzungskraft geführt.

Kontakt: AC-Service (Schweiz) AG

Beat Finkbeiner
Hardstrasse 73
5430 Wettingen 1
Tel. 056 4374 111
beat.finkbeiner@ch.ac-service.com
www.ac-service.com

Kontakt: InfoService

AC-Service AG
Postfach 80 01 80
D-70501 Stuttgart
Tel. +49 711 78 80 7-260
info@de.ac-service.com
www.ac-service.com

2 Einführung und Hintergründe

2.1 Was ist ein Disaster?

“... a disaster is defined as an interruption of mission-critical information services for an unacceptable period of time.”

Jon W. Toigo

Diese Definition¹ ist eine starke Einschränkung des Begriffs Disaster oder, wie man im deutschsprachigen Raum eher sagen würde, Katastrophe, da man beim Wort Katastrophe doch eher an grosse Naturkatastrophen oder grosse Unfälle denkt, bei denen Menschen zu Schaden kommen und grössere Sachschäden entstehen. Da es in diesem Booklet aber um Business Continuity und Disaster Recovery geht und heute der ordentliche Geschäftsbetrieb für fast jeden Betrieb stark von der Verfügbarkeit der eingesetzten Informations- und Kommunikationstechnologie abhängig ist, scheint mir diese Definition für die folgenden Betrachtungen sinnvoll. Trotzdem soll nicht verschwiegen werden, dass Katastrophen im Bereich der Informations- und Kommunikationstechnologie auch katastrophale Auswirkungen im breiteren Sinn haben können. Man denke nur daran, wie abhängig heutige Grossflugzeuge oder Kernkraftwerke vom Funktionieren der Informationstechnologie sind.



2.1.1 Katastrophe oder Unannehmlichkeit

Jetzt stellt sich allerdings die Frage, was unter dieser Prämisse eine Katastrophe ist. Diese Frage muss man leider mit der rhetorischen Formel «alles ist relativ» beantworten. Denn was für ein Unternehmen ein echtes Disaster sein kann, ist für ein anderes lediglich eine tolerable Unannehmlichkeit. Dies möchte ich an einem kleinen Beispiel verdeutlichen.

Für eine Bank kann ein Ausfall der Telefonleitungen zur Geschäftszeit bereits nach wenigen Minuten eine Katastrophe darstellen, da dann z.B. die Händler ihrer Aufgabe nicht mehr nachkommen können und dadurch erhebliche Verluste und Regressansprüche entstehen

¹ Toigo, Jon W., Disaster Recovery Planning, siehe Referenzen

können. Dagegen kann es für eine Versicherung mit starker Aussendienstorientierung eine Unannehmlichkeit sein, aber sie beeinträchtigt nicht notwendigerweise die Geschäftstätigkeit in einer Weise, dass grössere Schäden entstehen oder geschäftskritische Anwendungen nicht verfügbar wären.

2.1.2 Die zeitliche Komponente

Das Beispiel liefert aber noch ein weiteres Charakteristikum. Was zu einer Zeit ein Disaster sein kann, kann sich zu einer anderen Zeit unbemerkt ereignen und ist dann völlig unbedeutend. Stellen Sie sich in unserem Beispiel einfach vor, dass der Ausfall während der Nachtstunden auftritt und zu dieser Zeit nur die Tagesendverarbeitung läuft.

2.1.3 Kleine Ursache – grosse Wirkung

Was die Definition von Toigo auch zeigt, ist die Tatsache, dass es nicht immer den Totalausfall eines Betriebsgebäudes einschliesslich der darin befindlichen Infrastruktur z.B. durch Brand oder Überflutung braucht, damit ein Notfall desaströse Ausmasse annehmen kann. Wenn z.B. bei einem Online-Broker die Netzkapazität der Internet-Anbindung so stark beeinträchtigt wird, dass Kundenanfragen in Timeout-Zustände laufen, dann kann dies je nach Dauer durchaus ernsthafte Folgen für die Geschäftstätigkeit zur Folge haben.

2.1.4 Gefährdungsszenarien

Um Reaktionsmöglichkeiten abgestuft planen zu können, unterscheidet man Katastrophen häufig als

- lokale Katastrophen, die nur das betrachtete Unternehmen betreffen
- regionale Katastrophen, die sich in der unmittelbaren Umgebung ereignen, aber direkte Auswirkungen auf die eigene Geschäftstätigkeit haben
- überregionale Katastrophen, die ein grossflächigeres Gebiet, z.B. einen gesamten Kanton oder das gesamte Land, betreffen oder darüber hinaus Auswirkungen haben

Lokale Katastrophen

Als lokale Ereignisse gelten in der Regel Schäden wie Feuer- oder Wasserschäden im Gebäude. Aber auch Angriffe auf elektronischem Weg (Cyber-Kriminalität),

die zu Beschädigung der Daten führen, können lokaler Art sein.

Regionale Katastrophen

Klassisch werden Notfälle wie Hochwasser, Murenabgänge, Verschneigungen oder starke Behinderungen des Verkehrs durch Windbruch als regional eingestuft. Daneben gibt es aber auch weniger offensichtliche Ereignisse, die auch für Schweizer Unternehmen zu einer realistischen regionalen Katastrophe werden können. Ein Beispiel dazu ereignete sich im Sommer 2002 in einer deutschen Stadt. An mehreren Stellen des städtischen Versorgungssystems kam es gleichzeitig zu Kabelbränden in den unterirdischen Kabelkanälen. Durch die starke Rauchentwicklung wurden die Löscharbeiten derart erschwert, dass die betroffenen Strassenzüge mehrere Tage gesperrt werden mussten, bis endgültig klar war, dass alle Brandherde und etwaige Schwelbrände gelöscht waren. Dadurch waren viele Unternehmen während der gesamten Sperrung weder für die Mitarbeiter noch für die Kunden erreichbar.

Ein anderes Beispiel lieferte uns vor einigen Jahren der Sturm Lothar, der in vielen Gegenden Europas – so auch in der Schweiz – schwere Schäden anrichtete, in vielen Bereichen Unterbrüche in der Stromversorgung verursachte und viele Verkehrswege unpassierbar machte. Daneben gibt es auch wiederkehrende Notstände, die kleinere Regionen, einzelne Städte oder Stadtteile treffen, wie z.B. Hochwasser an der Aare, das zu Überschwemmungen in Bern führt.

Überregionale Katastrophen

Überregionale Gefährdungen sind sicher Viren-Attacken und Trojanische Pferde, die sich unkontrolliert global verbreiten und je nach Implementierung dann auch Schäden auslösen können. Eine überregionale Gefährdung liegt aber auch vor bei einem Flugzeugabsturz auf ein Kernkraftwerk, sei es durch Unfall oder in Form eines terroristischen Anschlags. Dabei muss berücksichtigt werden, dass nach aktuellen Einschätzungen, auch aufgrund der geografischen Verhältnisse, einige der höchstgefährdeten Städte in der Schweiz liegen.

- Nach dem Afghanistan-Konflikt wurde Genf, das aufgrund der vielen dort ansässigen Organisationen ohnehin schon als stark gefährdet galt, nochmals in der Terrorgefährdung hochgestuft.

- Basel ist durch Unfälle in den elsässischen Kernkraftwerken gefährdet und liegt zudem auf einer tektonischen Bruchlinie.
- In Zürich sollte sich jede Unternehmung im Stadtbereich auf einen möglichen Bruch des Sihlдамms und der daraus folgenden Probleme, die weit über eine Überflutung hinausgehen können, vorbereiten.

Weitere Charakterisierungen von Katastrophenszenarien

Neben dieser Unterscheidung aufgrund des betroffenen Umkreises gibt es eine zweite Klassifizierung nach der Art, in der solche Katastrophen auftreten. Diese ist in der folgenden Tabelle zusammengestellt.

Vorhersehbare Katastrophe	<p>Katastrophen, deren Herannahen sich ankündigt, die in dieser Form regelmässig auftreten, z.B.</p> <ul style="list-style-type: none">■ Unwetter (Stürme, Sturzregen)■ Überschwemmungen <p>Daneben auch geplante Störungen des ordnungsgemässen Betriebs wie geplante Stromunterbrechungen</p>
Nicht vorhersehbare Katastrophen	<p>Ereignisse, deren Möglichkeit zwar in Betracht gezogen wird, deren Auftreten sich jedoch nicht in irgendeiner Weise ankündigt, z.B.</p> <ul style="list-style-type: none">■ Feuer■ Umweltunfall (siehe Basel 1986)
Rollende Katastrophe	<p>Ereignisse, die sich rollend oder schneeballartig ausbreiten, z.B.</p> <ul style="list-style-type: none">■ Malware (Trojaner, Viren, Würmer)■ Applikationsfehler■ Ausfälle in Teilnetzen, die zu einer sich ausbreitenden Überlast führen
Unbekannte oder unerwartete Katastrophen	<p>Katastrophen aufgrund unbekannter oder nie erwarteter Risiken wie der Anschlag auf das World Trade Center</p>



Lösungsansatz

Business Continuity & Disaster Recovery soll die Sicherheit der Geschäftsprozesse unterstützen, die heutzutage typischerweise über eine Vielzahl von Systemen und Applikationen verteilt sind. Dies erschwert es, geeignete Konzepte zu entwickeln, selbst wenn man sich zunächst nur auf die geschäftskritischen Prozesse konzentriert.

Um diesem Umstand zu begegnen, sollten Notfallpläne von den Worst-Case-Szenarien ausgehen und dabei so modular aufgebaut sein, dass auf «kleinere» Notfälle durch Anwendung von Teilplänen adäquat reagiert werden kann. Eine solche Modularisierung erleichtert auch die Anwendung, wenn ein Notfall nicht einem der bei der Planung berücksichtigten Szenarien entspricht, was voraussichtlich der Regelfall sein wird.

Checkliste 1: Mögliche Ursachen für Katastrophen

Lokale Gefahren:	Logische Gefahren:	Standort-Gefahren:
■ CPU-Fehler	■ Software-Fehler	■ Telco-Ausfall
■ Disk-Fehler	■ Virus	■ XSP-Konkurs
■ Array-Fehler	■ Korrupte Daten	■ Feuer
■ HBA	■ Versehentliches Löschen	■ Sturmschäden
■ NIC	■ Gelöschte Tabelle	■ Erdbeben
■ Software		■ Hochwasser
		■ Kontamination
		■ Stromausfall
		■ Diebstahl
		■ Unfall
		■ Sabotage
		■ Terrorismus
		■ Erdloch
		■ Chemieunfall

2.2 Gründe für Business Continuity & Disaster Recovery Planning (BCP)

Wer vorbereitet ist, überlebt

Wie man aus den bisher angestellten Überlegungen erkennt, können Unterbrüche von geschäftskritischen Prozessen aus unterschiedlichsten Gründen passieren, selbst wenn die eigene Unternehmung gar nicht direkt von einem Schadensereignis betroffen ist. Dies allein ist Grund genug, Überlegungen anzustellen, wie in solchen Fällen zumindest die notfallmässige Fortführung und

Wiederaufnahme des Geschäftsbetriebs sichergestellt werden kann. Denn das erste Ziel in einer solchen Situation muss es sein, diese als Unternehmen zu überleben, und die Erfahrung zeigt, dass Unternehmen mit einem sinnvollen Notfall- und Katastrophenplan mit sehr viel höherer Wahrscheinlichkeit Ausnahmesituationen überleben und sich schneller erholen als diejenigen, die keine Vorsorge getroffen haben.

2.2.1 Rechtliche Rahmenbedingungen

Neben der Erfahrung, dass gut vorbereitete Organisationen Katastrophen (besser) überleben, stehen gesetzliche Anforderungen an die Sicherheit der Informationen. Hier wäre z.B. das Aktienrecht (Schweizerisches Aktienrecht Art. 754) zu nennen, das die Verantwortung für die Sicherheit der Unternehmensdaten eindeutig der Geschäftsleitung zuweist. Aber auch andere rechtliche Regelungen wie das Datenschutzgesetz oder das Bankengesetz schreiben die Verantwortung für die Informationssicherheit ganz klar der Geschäftsleitung zu.



Rechtliche Grundlagen:

- Aktienrecht
- Datenschutzgesetz
- Bankengesetz
- Versicherungsrecht
- Obligationenrecht

Weitere externe Regulatorien:

- Basel II
- ISO/IEC 17799/2000 (SN 17799)
- Rundschreiben der Eidg. Bankenkommission

2.2.2 Verträge und Haftung

Gerade auch im Finanzsektor werden sehr häufig in Verträgen entsprechende Ausfallsicherungsklauseln vereinbart. Damit diese nicht zu unkalkulierbaren Risiken werden, muss sichergestellt werden, dass die getroffenen Vorkehrungen im Katastrophenfall diesen vertraglichen Vereinbarungen genügen. Des Weiteren können nach einem Notfall auch noch Haftungsansprüche Dritter entstehen. Solche Haftungsansprüche sind in der Regel nicht oder nur schwer versicherbar. Die Ursache dafür ist, dass die Auswirkungen von Datenfehlern oder Verlusten nur schwer abschätzbar sind.



Falls eine Versicherung überhaupt ein Produkt anbietet, mit dem Folgeschäden von Datenfehlern oder -verlusten versichert werden können, dann bewegen sich die Prämien in der Regel in Größenordnungen, die eine solche Versicherung nicht mehr sinnvoll erscheinen lassen.

2.3 Phasen der Planung

Typischerweise verläuft die Entwicklung eines Business Continuity & Disaster Recovery-Plans in vier Phasen.



Abbildung 1: Phasen der Business-Continuity-Planung

2.3.1 Schwachstellenanalyse

Diese erste, oft auch als Health Check bezeichnete Phase soll aufzeigen, gegen welche Bedrohungen und Risiken eine Organisation unzureichend geschützt ist. Dabei stellt sich allerdings die Frage, was als Messlatte für ausreichenden Schutz herangezogen werden soll. In den letzten zwei Jahren hat sich hier die Norm ISO/IEC 17799 (SN 17799) durchgesetzt. Ausgangspunkt einer Sicherheitsprüfung ist dabei die Analyse der Auswirkungen verschiedener Bedrohungsszenarien auf die Geschäftsprozesse. Wie schon gesagt, kann ein Szenario für das eine Unternehmen schwerwiegende Folgen haben, während ein anderes überhaupt nicht oder nur marginal betroffen ist, da seine Geschäftsprozesse vom gleichen Ereignis nicht betroffen sind.



2.3.2 Risikobewertung und Risikomanagement

Nachdem festgestellt wurde, welche Risiken überhaupt relevant sind, müssen diese Risiken hinsichtlich ihrer direkten und indirekten Schadenswirkung bewertet werden. Ziel dieses Schritts ist es, festzustellen, welche Risiken mit höchster Priorität angegangen werden müssen.

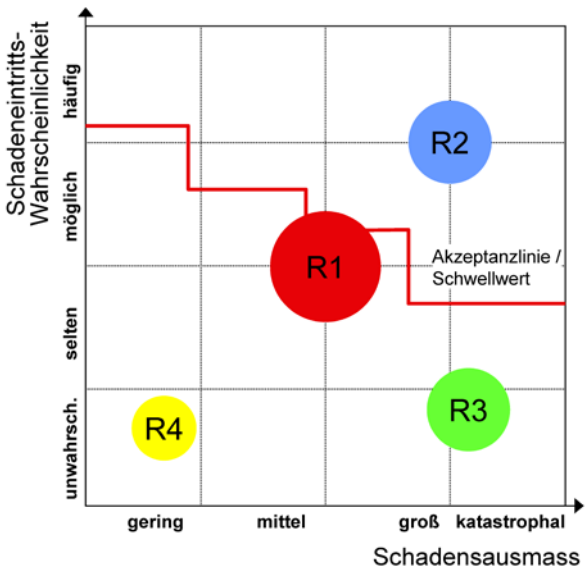


Abbildung 2: Risikokarte

Für die Darstellung hat sich die Risikokarte bewährt, da sie sehr anschaulich aufzeigt, welche Auswirkungen die verschiedenen Risiken haben und wie sich Gegenmassnahmen auswirken würden. Wichtig für die Bewertung ist die Definition der Akzeptanzlinie. Diese ist so zu wählen, dass existenzbedrohende Risiken, für die es unter den gegebenen Umständen keine Gegenmassnahmen gibt, oberhalb liegen.

Die Lage auf der x-Achse gibt das unmittelbare Schadensausmass an, mit dem gerechnet werden muss, wenn ein Schadensereignis dieser Art eintritt. Dabei sind die direkten Schadenswirkungen, z.B. Verlust von Infrastruktur, wie auch die Folgeschäden z.B. durch entgangenes Geschäft gemeint.

Die Lage auf der y-Achse gibt an, wie wahrscheinlich der Eintritt des entsprechenden Schadensereignisses ist. Dies ist ein geschätztes oder statistisches Mass. Falls z.B. von den diversen Emergency-Response-Teams Statistiken über die Wahrscheinlichkeit der betrachteten Schadensereignisse vorliegen, können diese herangezogen werden, andernfalls ist dies der eigenen Einschätzung überlassen.

Die Grösse der Kreise gibt an, wie hoch die Wiederherstellungskosten bis zur vollständigen Wiederaufnahme der Geschäftstätigkeit sind. Dabei sind die Wiederbeschaffungskosten nicht mit eingerechnet, da diese bereits in den unmittelbaren Schadenswirkungen berücksichtigt sind. Hier sind einzuschliessen

- Aufräumungsarbeiten
- Wiederherstellungsarbeiten
- Schulungsaufwand für Ersatzpersonal
- usw.

Was wäre, wenn?

Auf der Basis der Risikokarte können Überlegungen angestellt werden, welche Sicherheitsmassnahmen sinnvoll sind und wie sich dadurch die Risikobewertung verändern würde. Da jede Gegenmassnahme zunächst einmal eine Investition bedeutet und in der Regel auch in der Folge Kosten verursacht, müssen diese Kosten gegen die Schadens- und Wiederherstellungskosten gerechnet werden.

So kommt man auch in manchen Fällen zu der Einsicht, dass die Akzeptanz des Risikos günstiger sein kann als die Einführung von Gegenmassnahmen, deren Eignung man zudem nie vorher prüfen kann, da ein Notfall grundsätzlich nie so abläuft wie in einem Szenario geplant. Man erreicht somit bei guter Planung immer nur eine 80%-Lösung. Auch kann es sich bei solchen Planspielen zeigen, dass eine beabsichtigte Sicherheitsmassnahme im konkreten Umfeld überhaupt keine Risikoverringering bewirkt.

Risikomanagement

Neben dieser Risikobewertung müssen die Risiken danach beurteilt werden, wie ihnen begegnet werden soll. Die folgende Grafik zeigt die Stufen des Risikomanagements.

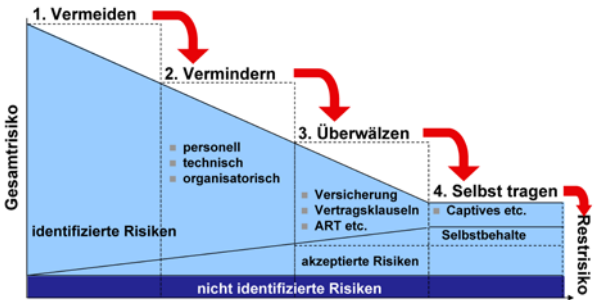


Abbildung 3: Risikomanagement-Stufen

Vermeidung



Mit höchster Priorität sollte überlegt werden, welche Risiken überhaupt vermeidbar sind. Ein Beispiel dazu wäre die Standortwahl. So sollte man für kritische Unternehmensteile einen Standort ausserhalb von hochwassergefährdeten Zonen wählen. Daneben gibt es aber auch noch vielfältige andere Kriterien. Viele Gewerbegebiete haben nur eine Zufahrt. Wenn diese wegen eines Unfalls nicht passierbar ist oder weil sie anderweitig blockiert ist, was besonders schnell auch bei Notfällen in der Nachbarschaft passieren kann, dann kann das zur Folge haben, dass Sie im Notfall Ihr Unternehmen nicht erreichen oder bei Gefahr nicht verlassen können.

Beispiele zur Vermeidung von Risiken sind:

- Vermeidung von Know-how-Verlust durch Stellvertreterregelung und Know-how-Sharing
- Verbesserung der physischen Sicherheit im Data Center
- Verbesserung der applikatorischen Sicherheit
- Klare Autorisierungsregelung

Verminderung

Der nächste Schritt ist die Verminderung von Risiken durch personelle, organisatorische und technische Massnahmen. Hierzu zählen z.B.

- klare Stellvertreterregelungen einschliesslich des dazu notwendigen Knowledge Sharing
- Prozess-Redesign
- Verantwortungsteilung

- redundante Systeme
- strikte Systemadministration (Hardening)
- regelmässige Sicherheitsprüfung durch Audit und Security Check (ethical hacking)

Überwälzung

Risiken, die auf diese Weise nicht vermieden oder reduziert werden können, können in einem weiteren Schritt überwältigt werden. Dies erfolgt in Form von Versicherungen, vertraglichen Klauseln und ähnlichen Konstrukten. Dabei ist aber gerade bei der Überwälzung durch vertragliche Regelungen in jüngster Zeit zu beobachten, dass Gerichte dazu tendieren, die Beweislast umzukehren und strenge Massstäbe zur Verhältnismässigkeit solcher Klauseln anzulegen. Eine neue Art der Überwälzung sind Konstrukte, die unter dem Namen Alternative Risk Transfer bekannt geworden sind. Dies sind Produkte, die aus einer Vermischung von Bank- und Versicherungstechniken entstehen. Details dazu findet man z.B. bei Ernst & Young².

Selbst tragen

Wie schon gesagt, lassen sich nicht alle Risiken versichern. Folglich bleibt die letzte Stufe, die darin besteht, das Risiko selbst zu tragen. Dies kann in Form eines Selbstbehalts oder über Captives und Mutuals erfolgen. Im Bereich des Selbstbehalts finden sich typischerweise auch solche Risiken, deren Wahrscheinlichkeit praktisch null ist. So ist ein Angriff auf die Sicherheit einer Internet-Banking-Anwendung, der den physischen Zugriff zu einem dedizierten Server im Sicherheitstrakt im sechsten Untergeschoss einer Haus-im-Haus-Lösung erfordert, so unwahrscheinlich, dass selbst bei hoher potenzieller Schadenswirkung keine Gegenmassnahmen ergriffen werden, es sei denn, sie wären quasi kostenlos zu bekommen.

Daneben muss man sich bewusst sein, dass es immer einen Anteil nicht identifizierter Risiken gibt. Dies kann daran liegen, dass diese Risiken erst später auftreten; dies ist z.B. typisch für neue Angriffsszenarien, die aufgrund einer neuen Programmversion auftreten, oder solche, die gar nicht in Betracht kamen. So hat in den USA auch niemand den Angriff auf das World Trade

² State of the ART Alternative Risk Transfer, Link siehe Referenzen am Ende des Booklets

Center mit vollbesetzten Linienflugzeugen als reales Risiko eingeschätzt, was, wie man heute weiss, fatale Folgen hatte.

Risikobewältigung durch Wahl des Sourcing

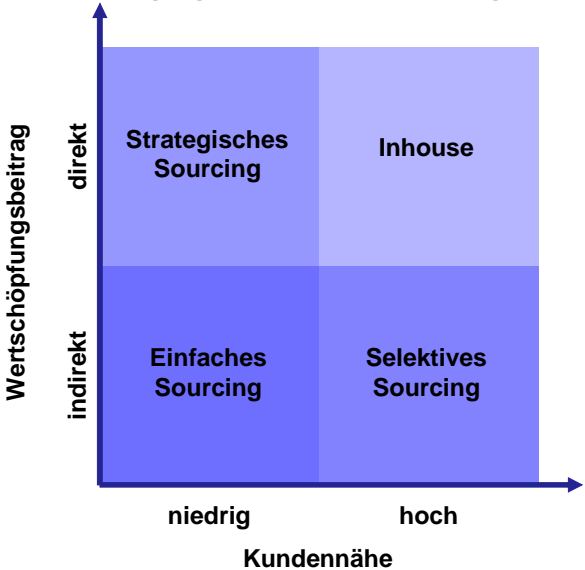


Abbildung 4: Risikobewältigung durch Wahl des Sourcing (nach Telekurs Services AG, 2003)

Neben der Überlegung, welche Risiken durch welche Massnahmen abgedeckt werden können, sollte man auch die einzelnen Anwendungen nach ihrer Bedeutung für den Wertschöpfungsbeitrag und die Kundennähe bewerten. Daraus ergibt sich der Quadrant aus Abbildung 4. Das Wesentliche an dieser Betrachtung ist die Frage, welche Lösungen sich für welches Sourcing eignen, sodass die Risiken über entsprechende Service Level Agreements auf den Sourcing-Partner überwältigt werden können. Damit lassen sich eigene Investitionen wie auch Versicherungen und Selbstbehalte reduzieren.

Variante

Inhouse	Ihre geschäftskritischen Applikationen und Ressourcen werden Sie als risikoreich und relevant bezeichnen. Dies aufgrund des direkten Wertschöpfungsbeitrages und der damit verbundenen Kundennähe. Die Risiken wollen Sie lieber selber kontrollieren.
Strategisches Sourcing	Sie wollen Ihre Geschäftsrisiken reduzieren. Sie können Applikationen ausgliedern, die einen hohen Einfluss auf Ihre IT-Umgebung haben, aber kein kritisches Geschäftsrisiko darstellen.
Selektives Sourcing	In den meisten Fällen werden Sie Interesse an der Risikovermeidung haben. Solche Prozesse oder Anwendungen weisen für Sie ein hohes Geschäftsrisiko aus, weil sie direkten Einfluss auf die Kundenbeziehung haben. Innerhalb der IT-Umgebung ist der Einfluss jedoch eher klein.
Einfaches Sourcing	Reines Bewirtschaften von Hard- und Software ist ideal für standardisierte Lösungen. Es hat keinen strategischen Einfluss und weist kein hohes Geschäftsrisiko aus.

2.3.3 Massnahmen zur Vorbereitung auf Notfälle

Fortführung der Geschäftstätigkeit im Notfall und die Wiederaufnahme nach Katastrophen bedingt eine sorgfältige Vorbereitung. Ein wichtiges Element bilden begleitende Massnahmen im laufenden Betrieb, die eine solche Fortführung oder Wiederaufnahme erst ermöglichen. Dazu zählen alle Massnahmen, die geeignet sind, eine Katastrophe zu verhindern, also den Betrieb so zu organisieren, dass Risiken ausgeschaltet werden können, und alle Massnahmen, die sicherstellen, dass im Notfall der Betrieb mit möglichst geringem Verlust wieder aufgenommen oder fortgeführt werden kann.

Disaster Recovery und Information Security

Die wichtigsten Massnahmen in diesem Sinne sind jene zur Sicherung der

- Datenintegrität
- Datenkonsistenz
- Verfügbarkeit

Speziell die Funktionen zur Sicherung der Integrität und Konsistenz spielen eine wichtige Rolle, denn damit kann in einer Notfallsituation festgestellt werden, wie alt die jüngsten korrekten Daten sind, auf die zurückgegriffen werden kann. Die Verfügbarkeit von Daten von einem Konsistenzpunkt vor der Katastrophe bedeutet

noch nicht, dass diese Daten auch korrekt sind. Die Daten können durch ein eingeschleustes Malware-Programm verfälscht worden sein, es können Integritätsfehler durch Fehlfunktionen in einer Software entstanden sein, oder es können falsche Daten wegen unzureichender Plausibilisierung der Eingaben in das System gelangt sein.

All diese Aspekte betrachtet die Business Continuity & Disaster Recovery-Planung nicht, sie sind Gegenstand des schon erwähnten Information Security Managements, in das die BC- & DR-Planung integriert sein muss.

Architektur Aspekte des Disaster Recovery

Neben diesen Vorbereitungen, welche die Datensicherheit betreffen, ist es ebenso erforderlich, die Architektur der eingesetzten Lösungen näher zu betrachten. Oftmals lassen sich durch relativ einfache Anpassungen an der Architektur die Voraussetzungen für ein erfolgreiches Business Recovery erhöhen. Berücksichtigt man z.B., dass in Banken alle Geschäftsvorgänge archiviert werden müssen, um die Anforderungen an die Revisionsfähigkeit zu erfüllen, und dass gleichzeitig viele Prozesse hochgradig asynchron ablaufen, dann kann man dies ausnutzen. Jedes Ereignis, das einen neuen Status eines Geschäftsvorgangs darstellt und deshalb vollständig und im Klartext archiviert werden muss, kann an einen anderen Standort repliziert und dort genutzt werden, um die Transaktionen auf einem zweiten System nachzuverarbeiten.



Infrastruktur Aspekte

Anders ist die Situation bei Anwendungen, die in Echtzeit oder echtzeitnah ablaufen müssen, wie z.B. ein Online-Trading-System. Für solche Anwendungen ist es sinnvoll, sie seitens der Infrastruktur, auf welcher sie laufen, von anderen, weniger kritischen Anwendungen zu separieren, sodass dafür eine Continuity & Recovery-Lösung gewählt werden kann, die kürzere Reaktionszeiten erlaubt.

Facilities Management

Das Facilities Management muss durch Bereithalten entsprechender Dienste oder durch Vorkehrungen zur Ersatzbeschaffung seinen Beitrag zum Disaster Recovery leisten. Ein wichtiger Teilbereich, an dem diese Aufgabe erläutert werden soll, ist die Verfügbarkeit von

Notfallarbeitsplätzen. Eine Variante ist, selbst für ausreichende Ausweichmöglichkeiten zu sorgen. Man kann aber durch entsprechende Verträge mit Immobilienverwaltungen, Telekommunikations- und IT-Dienstleistern dafür Sorge tragen, dass im Bedarfsfall in der vorgegebenen Zeit entsprechende Kapazitäten bereitgestellt werden können. Die gleichen Vorkehrungen muss man natürlich auch für alle anderen Bereiche treffen.

2.3.4 Notfallpläne

Um im Katastrophenfall die Durchführung der richtigen Massnahmen in der richtigen Abfolge zu gewährleisten, müssen diese Prozesse in Notfallplänen zusammengestellt werden. Dabei ist es wichtig zu beachten, dass alle Massnahmen zur Fortführung oder Wiederherstellung des Betriebs erst dann sicher greifen, wenn die Sicherheit der Mitarbeiter und ihrer Familien so weit als möglich gewährleistet ist. Es ist völlig natürlich, dass Menschen insbesondere bei regionalen oder überregionalen Katastrophen zunächst um ihre eigene Sicherheit und die der Familie besorgt sind und das ordnungsgemässe Funktionieren des Unternehmens nur zweite Priorität hat.



Gute Notfallpläne berücksichtigen solche sozialen Rahmenbedingungen und sind deshalb praktikabel. Des Weiteren müssen Notfallpläne so aufgebaut sein, dass sie auch teilweise anwendbar sind, um auf Situationen zu reagieren, die in der Konzeption nicht bedacht wurden. Die jeweils Verantwortlichen müssen mit dem Plan selbst und mit den Geschäftsfällen, die davon betroffen sind, so weit vertraut sein, dass sie in der Lage sind, auch in einer Notfallsituation notwendige, vom Plan abweichende Entscheidungen zu treffen.



Für Notfallpläne gilt zudem der allgemeine Grundsatz, dass es wichtiger ist, das Richtige zu tun, als alles richtig zu tun. Ausserdem ist natürlich das Ziel eines jeden Notfallplans, das Unternehmen auf schnellstmögliche und sinnvolle Weise wieder in den Normalbetrieb zurückzuführen, sei es durch Wiederherstellung des vorherigen Zustands (Gebäude, Data Center, ...) oder durch Aufbau entsprechenden Ersatzes.

Bei der Aufstellung von Notfallplänen sollte die folgende Prioritätenfolge beachtet werden:

- Sicherheit der Personen am Ort der Katastrophe (Mitarbeiter und Kunden)
- Sicherheit der Informationen (Kundendaten und Firmendaten)
- Sicherheit der Sachwerte

2.4 Managementverantwortung auf oberster Ebene

Ausgehend von der Definition des Begriffs «Disaster» in Kapitel 2 wird eines sehr schnell klar: Disaster oder Notfälle und deren Folgen können für ein Unternehmen existenzbedrohend sein. Da es eine der Aufgaben der Geschäftsleitung ist, die Existenz eines Unternehmens zu sichern, ergibt sich daraus zwangsläufig, dass Überlegungen hinsichtlich der Fortführung der Geschäftstätigkeit im Notfall und der Wiederherstellung der Geschäftstätigkeit nach einem Unterbruch eine Aufgabe für die Geschäftsleitung darstellen. Das ist z.B. auch ein wichtiger Grund für die Eidgenössische Bankenkommission – übrigens analog zu Bankenaufsichtsgremien in anderen Ländern –, Business Continuity & Disaster Recovery Planning einzufordern und die Bankenzulassung davon abhängig zu machen. Schliesslich ist hier nicht nur der Fortbestand einer Bank bedroht, sondern auch das Vermögen der Kunden.



BCP darf aber nicht eigenständig betrachtet werden, sondern muss als Bestandteil der Massnahmen zur Informationssicherheit verstanden werden. Da Informationen heute für jedes Unternehmen einen Geschäftswert darstellen, sollte es jedem Manager klar sein, dass Informationssicherheit und damit auch Notfallvorsorge eines der Geschäftsziele sein muss. Gleiches fordert auch die ISO/IEC 17799/2000, die heute akzeptierter Standard für Information Security Management ist und von vielen Organisationen zur Bewertung der Informationssicherheit herangezogen wird. Nachdem diese Norm unter der gleichen Nummer zur Schweizer Norm erhoben wurde, hat auch die Eidgenössische Bankenkommission angekündigt, sich künftig bei Revisionen daran zu orientieren.

Checkliste 2: Aufgaben der Geschäftsleitung

- Ordnungsgemässe Geschäftsführung
- Richtlinienverantwortung für Informationssicherheit
- Verantwortung für das Management der Informationssicherheit (direkte Unterstellung des Sicherheitsmanagements unter die Geschäftsleitung)
- Notfallvorsorge
- Regelmässige Überprüfung der Sicherheitsmassnahmen

2.4.1 ISO/IEC 17799/2000

Die ISO-Norm behandelt das Management der Informationssicherheit nach zwei einführenden Kapiteln in zehn Aspekten, auf die gewöhnlich als Section 3 bis 12 Bezug genommen wird. Diese zehn Aspekte sind

- Sicherheitsrichtlinien und -weisungen
- Sicherheitsmanagementprozess
- Katalogisierung und Klassifizierung der Unternehmenswerte (Hardware, Software, Prozesse, Unternehmensdaten)
- Personelle Sicherheit
- Physische und bauliche Sicherheit
- Sicherheit in IT-Infrastruktur und -Betrieb
- Zugangs- und Zugriffskontrolle
- Sicherheit bei Entwicklung und Wartung
- Business Continuity Planning
- Verträglichkeit mit gesetzlichen, regulatorischen und technologischen Rahmenbedingungen

Man sieht, dass BCP in diesem Standard fest in das Konzept der Informationssicherheit eingebunden ist.

2.4.2 Aufgaben der Geschäftsleitung

Aufgabe der Geschäftsleitung ist es danach, über die Sicherheitsrichtlinien die Steuerung des Sicherheitsmanagements zu übernehmen. Dabei sollte die Erstellung der Sicherheitsrichtlinien (Security Policy) an erster Stelle stehen, obwohl de facto in vielen Fällen zunächst pragmatisch Sicherheitsmassnahmen eingeführt werden und diese im Nachhinein durch Richtlinien und Weisungen den erforderlichen Unterbau erhalten.

Mit der Verabschiedung einer Sicherheitsrichtlinie verpflichtet sich die Geschäftsleitung zu Massnahmen



zur Informationssicherheit und definiert die Rahmenbedingungen, nach denen Informationssicherheit im Unternehmen erfolgen soll. Gleichzeitig wird damit der Sicherheitsmanagementprozess initiiert, was auch die Bereitstellung eines personellen und monetären Budgets beinhalten muss.

Wichtig ist dabei, dass das Management der Informationssicherheit nicht an die IT delegiert werden kann, da Informationssicherheit mehr als nur IT-Sicherheit ist.



Erfahrungen namhafter Schweizer Grossunternehmen unterschiedlicher Branchen zeigen, dass die Einrichtung eines Information Security Managements direkt unterhalb der Geschäftsleitung die effektivste Organisation darstellt.

Nun kann man sich Sicherheitsrichtlinien nicht als ein in sich geschlossenes Dokument vorstellen, das einmal geschrieben wird und dann im Archiv verstaubt. Eine solche Richtlinie besteht aus einer Vielzahl von Teildokumenten, die jeweils auf die einzelnen Aufgabengebiete zur Informationssicherheit fokussieren und die regelmässig hinsichtlich ihrer Aktualität und Deckung mit der Realität überprüft werden müssen.

Eines dieser Teildokumente ist die Richtlinie zur Fortführung bzw. Wiederaufnahme der Geschäftstätigkeit im Notfall. In dieser Richtlinie muss die Geschäftsleitung festlegen,

- wie die Rahmenbedingungen sind, unter denen für das Unternehmen eine schwerwiegende oder existenzbedrohende Beeinträchtigung der Geschäftstätigkeit vorliegt
- wie dieser Situation begegnet werden soll
- wer für die Pflege und Aufrechterhaltung der entsprechenden Konzepte verantwortlich ist



Dazu müssen verschiedene Szenarien von Notfällen betrachtet werden, aus denen auch unter Zuhilfenahme von Zahlen aus dem Finanzdepartement Aussagen über die zu erwartenden Schadenswirkungen kalkuliert werden sollten. Diese Bewertung der Schadensrisiken ist auch für die Bewertung der Risiken in einer Risikoverteilung erforderlich.

2.4.3 Aufgaben des IT-Managements (CIO)

Die Aufgabe des IT-Managements im Rahmen des BCP ist die Umsetzung des IT-Teils eines Business Continuity & Disaster Recovery-Plans, d.h. die Planung und Durchführung aller Massnahmen zur Vorbereitung auf einen Notfall und zur Reaktion in einem Notfall, die erforderlich sind, um die Informations- und Kommunikationsdienstleistungen für das Business aufrechtzuerhalten oder wiederherzustellen.

Checkliste 3: Aufgaben des CIO

- Zugangskontrolle
- Zugriffskontrolle
- Kontrolle des Datenarchivs
- Kontrolle der Netzanbindung
- Datensicherung und Restore-Fähigkeit
- Architekturunterstützung für Informationssicherheit und Disaster Recovery (in Abstimmung mit den Fachabteilungen)
- Physische Sicherheit des Data Centers
- Backup-Lösung für lokale Daten

Disaster-Recovery-Konzept

3.1 Konzept – Zusammenspiel Mensch–Prozesse–Technologie

Jedes Disaster-Recovery-Konzept ist von den drei Komponenten

- Mensch
- Prozesse
- Technologie

abhängig. Ein erfolgreiches Business Continuity & Disaster Recovery-Konzept beruht auf dem erfolgreichen Zusammenspiel dieser Komponenten. Dazu müssen die im Folgenden aufgeführten Voraussetzungen gegeben sein.

Mensch

Um im Notfall erfolgreich einen Notfallplan ausführen zu können, ist es wichtig, dass

- die Verantwortlichkeiten klar sind
- die Verantwortlichen über das richtige Know-how verfügen
- wichtige Know-how-Träger verfügbar bzw. erreichbar sind
- klare Stellvertretungsregelungen bestehen
- bei Personalwechsel das Know-how rechtzeitig übergeben wird
- die Sicherheit der Personen gegeben ist
- die Verantwortlichen über die notwendige Entscheidungskompetenz und Entscheidungsfähigkeit verfügen

Prozesse

Ein Notfallplan muss so gestaltet sein, dass

- die erforderlichen Abläufe klar definiert sind
- die einzelnen Abläufe sinnvoll modularisiert und die Module leicht auffindbar sind
- die Zuordnung eines (Teil-)Plans zum aktuellen Notfall möglichst eindeutig ist

- die einzelnen Module und der Plan als Ganzes einen klaren Testrahmen haben
- klare Eskalationsregeln betreffend Zeitpunkt und Rahmenbedingungen gegeben sind
- die Eskalationsstellen eindeutig sind

Technologie

Der Notfallplan muss für die Informations- und Kommunikationstechnologie die erforderlichen

- Vorkehrungen
- Einrichtungen
- Ersatzbeschaffungsregelungen
- Ausweichmöglichkeiten und
- Backup-Regelungen

enthalten, die es im Notfall erlauben, den Betrieb in der vorgesehenen Zeit wieder aufnehmen zu können. Dabei müssen die technologischen Massnahmen dem betrieblichen Bedürfnis angepasst sein. Man muss dabei auch beachten, dass mit kürzer werdender Wiederherstellungszeit die Kosten steigen. Dies kann und wird oft auch bedeuten, dass für unterschiedlich kritische Anwendungen unterschiedliche technische Lösungen gewählt werden. Deshalb ist es wichtig, den Bedarf sorgfältig zu ermitteln. Dies wird in den folgenden Abschnitten aus verschiedenen Blickwinkeln beleuchtet.

Gerade weil sich vielfach das Geschäft sehr stark am Tagesrhythmus orientiert, ist nicht für jede Anwendung eine 7×24-Stunden-Verfügbarkeit erforderlich. Durch Verteilung der Anwendungen auf verschiedene Systeme je nach Bedeutung für das Business und Anforderung an die Verfügbarkeit kann so ein abgestuftes Continuity & Recovery-Konzept leichter realisiert werden.

3.2 Bedürfnisse einstufen

Wenn es darum geht, Zeiten für die Wiederaufnahme der ordentlichen Geschäftstätigkeit festzulegen, wird oft die maximale Ausfallzeit der verschiedenen Dienste definiert. Dies ist aber in der Regel unzureichend, da damit noch nicht gesagt ist, auf welchem Stand die Systeme und Daten zum Zeitpunkt der Wiederaufnahme sind. Dies lässt sich am einfachsten an einem Beispiel erläutern.



Die maximale Ausfallzeit eines Systems wird auf vier Stunden festgelegt. Dieses System fällt wegen eines Softwarefehlers aus, der die Daten korrumpiert hat. Danach gelingt es, das System in drei Stunden wieder online zu bringen. Beim Versuch nachzuvollziehen, seit wann die Daten fehlerhaft sind, kann man dies nur bis zur letzten Wochensicherung verifizieren. Somit ist der Wiederherstellungspunkt nicht der letzte Konsistenzpunkt vor dem Ausfall, sondern die Wochensicherung vom letzten Wochenende.

Für den Wiederherstellungsfall sind zwei Zeitpunkte relevant.

- Der erste Zeitpunkt ist der, von welchem die letzten konsistenten und korrekten Daten vorliegen. Dies ist der Zeitpunkt, auf den zurückgesetzt werden kann.
- Der zweite Zeitpunkt ist der, an welchem die Informations- und Kommunikationsdienstleistungen wieder verfügbar sind mit dem Stand des letzten konsistenten und korrekten Sicherungspunktes.

Die Bedingungen und Eigenschaften dieser beiden Zeitpunkte werden in der Folge näher erläutert.

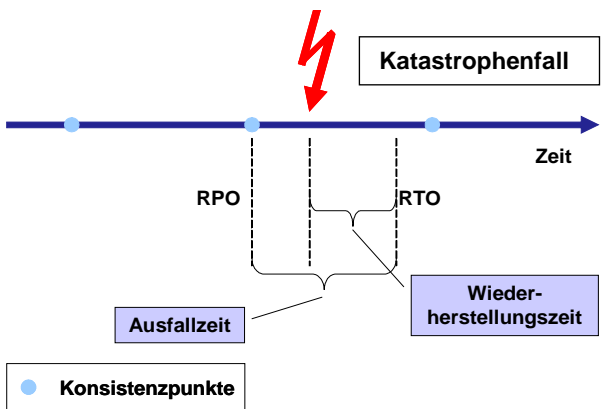


Abbildung 5: Ausfallzeiten (nach Telekurs Services AG, 2003)

3.2.1 Recovery Point Objective (RPO)

In der Einleitung des Kapitels wurde bereits festgehalten, dass es vor dem Disaster einen Zeitpunkt gibt, von dem verlässlich bekannt ist, dass die Daten korrekt und in sich konsistent waren und dass diese Daten auch

nach der Katastrophe vorhanden sind, z.B. in Form von Sicherungsbändern. Diese Daten stammen nicht unbedingt vom letzten konsistenten Sicherungspunkt, von welchem Sicherungen verfügbar sind. Dies möchte ich anhand von zwei kleinen Beispielen erläutern.

Beispiel 1:

Die Daten werden täglich gesichert einschliesslich einer doppelten Sicherung an einem anderen Standort. Dann brennt der Hauptstandort und damit verbunden das Bandarchiv vor Ort ab, das zweite Archiv ist aber vollständig mit den Daten vom Vortag. Aufgrund von Kontrollen und Plausibilitätsprüfungen kann mit ausreichender Sicherheit davon ausgegangen werden, dass die Daten auch korrekt sind. Damit wäre der verfügbare Datenstand aus Sicht des Disaster Recovery genau dieser Datenbestand.

Beispiel 2:

Im zweiten Beispiel gehen wir davon aus, dass Daten zwischen zwei Rechenzentren online repliziert werden. Der Katastrophenfall ist aber in diesem Fall ein Softwarefehler, der aufgrund einer neuen Datenkonstellation bekannt wurde. Dieser Fehler hat in der Folge zu fehlerhaften Daten geführt, die zwar in sich konsistent sind, aber eben verfälscht. Der Fehler wird erst bei der Monatsendverarbeitung erkannt, das erste Auftreten kann aber auf den 21. rückdatiert werden. In diesem Fall sind die letzten konsistenten und korrekten Daten zehn oder elf Tage alt. Vorausgesetzt man hat ein Log aller Eingangstransaktionen und aller direkten Änderungen durch Erfassung, dann kann man zwar die fehlerhaften Daten nachverarbeiten und erfassen, dies ist aber erst nach der Wiederherstellung der Betriebsbereitschaft möglich.

Für die Planung der notwendigen Business Continuity & Disaster Recovery-Massnahmen ist dieser Zeitpunkt von entscheidender Bedeutung. Denn als eigentliche Ausfallzeit kann nicht nur die Zeit vom Eintreten einer Katastrophe bis zur Wiederaufnahme des Betriebs gewertet werden, sondern auch der Datenverlust, der entsteht, weil gegebenenfalls nicht die aktuellsten Daten vor dem Ereignis zur Wiederherstellung zur Verfügung stehen. Für die verschiedenen Informationen in einem Unternehmen muss festgestellt werden, wie weit dieser Zeitpunkt in der Vergangenheit sein darf. Dies hängt natürlich im Wesentlichen auch von der Änderungsrate der jeweiligen Datenart ab.



Grundsätzlich ist es aber schwer zu beziffern, welche Schäden durch unterschiedlich «alte» Daten entstehen, selbst wenn man z.B. die Kosten auf der Basis der typischen täglichen Mengen kalkuliert, die durch eine Nacherfassung durch einen Datenerfassungsservice entstehen.

3.2.2 Recovery Time Objective (RTO)

Der zweite wesentliche Zeitpunkt ist derjenige, an dem die ausgefallenen oder behinderten Services wieder verfügbar sind. Oftmals wird dies als die maximal zulässige Ausfallzeit angegeben. Auch diese Angabe kann für unterschiedliche Datengruppen unterschiedlich sein. Wenn man auf die Definition vom Anfang zurückkommt, dann muss man diese Zeit auch danach bewerten, wie geschäftskritisch die einzelnen Datengruppen sind. Wenn man, wie in der ISO-Norm vorgesehen, die Daten klassifiziert, dann ist es sinnvoll, neben der Vertraulichkeit auch die erforderliche Verfügbarkeit festzulegen.

3.2.3 Maximale akzeptable Ausfallzeit

Unter Berücksichtigung der oben genannten Überlegungen zu RPO und RTO ist die maximale akzeptable Ausfallzeit die gesamte Zeit vom Zeitpunkt der letzten korrekten und konsistenten Daten bis zum Wiederherstellen der Betriebsbereitschaft.

Beispiel:

Die maximale akzeptable Ausfallzeit soll zwei Stunden betragen. Wenn die Wiederherstellung der Systemumgebung 30 Minuten benötigt, dann dürfen die ältesten Daten, auf die zurückgesetzt werden kann, nicht früher als eineinhalb Stunden vor dem Notfall gesichert worden sein. Daraus folgt, dass in diesem Fall eine Tagesicherung nicht ausreicht, weil bei einer Öffnungszeit von 8 bis 18 Uhr die Daten schon ab 9.30 Uhr zu alt wären.

3.3 Faktor Mensch

3.3.1 Notfallorganisation

Während im normalen Betrieb Führung durch Kommunikation die hohe Kunst des Managements sein sollte, sind in Notfallsituationen klare Führungs- und Verantwortungsstrukturen vonnöten. Diese müssen definiert und kommuniziert sein. Ein wichtiger Aspekt dabei ist

die richtige Auswahl der Verantwortlichen innerhalb einer Notfallorganisation. Diese Personen müssen

- Sozial-, Entscheidungs- und Handlungskompetenz besitzen
- gut und effektiv kommunizieren können
- komplexe Situationen und Zusammenhänge schnell und zuverlässig erkennen können
- fachliche und soziale Autorität ausstrahlen



Die Aufgabe dieser Personen ist das Krisenmanagement oder vielleicht besser das Lösungsmanagement, denn schliesslich soll nicht die Krise gemanagt, sondern eine Lösung der Krise erreicht werden.

Krisenstab

Dem engsten Kreis der Notfallorganisation, dem Krisenstab, der aus Effektivitätsgründen möglichst klein gehalten werden muss, sollten Verantwortliche aus den folgenden Bereichen angehören:

- Fachabteilungen mit geschäftskritischen Anwendungen
- Facilities Management
- IT-Betrieb
- IT-Entwicklung
- Unternehmenssicherheit



Der Krisenstab steht in einer Notfallsituation in ständiger Verbindung mit der Geschäftsleitung. Der jeweilige lokale Chief Operational Officer (COO) oder sein Stellvertreter sollte Mitglied des Krisenstabs sein. So kann sichergestellt werden, dass gegebenenfalls erforderliche Vollmachten vorhanden sind.

Notfallteams

Daneben sollten weitere fachliche, organisatorische und technische Ansprechpartner definiert sein, die zum erweiterten Kreis gehören und den Krisenstab in seiner Arbeit unterstützen und die Umsetzung der Entscheide vorantreiben. Die folgende Grafik gibt eine Übersicht der involvierten Gruppen und der Informationsflüsse. Mit zunehmender Dauer eines Notfalls oder wenn eine längerfristige Unterbrechung absehbar wird, muss von unten nach oben kommuniziert werden.

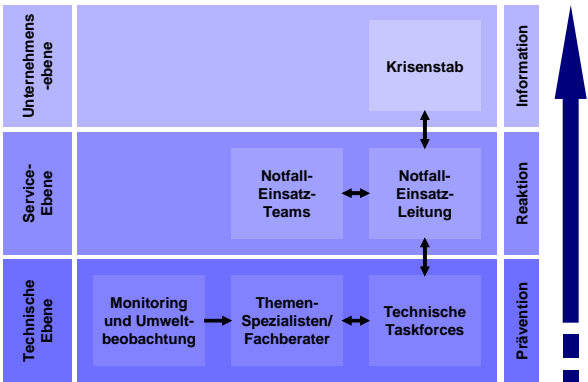


Abbildung 6: Kommunikation und Eskalation (nach Telekurs Services AG, 2003)

Abbildung 6 zeigt die erforderlichen Kommunikations- und Eskalationswege innerhalb einer Notfallorganisation. Die Kommunikation muss entlang der Pfeile erfolgen, und zwar


- delegierend von oben nach unten und von rechts nach links
- rapportierend von links nach rechts und von unten nach oben

3.3.2 Erreichbarkeit im Notfall

Eine Notfallorganisation ist nur dann effektiv, wenn sie in einer Notfallsituation auch rechtzeitig ihre Arbeit aufnehmen kann. Dazu gehört zunächst, dass das Eintreffen einer Krisensituation oder eines Notfalls auch bekannt wird. Dazu ist eine zentrale Notfallmeldestelle erforderlich, die auf allen verfügbaren Kommunikationskanälen erreichbar sein muss, damit bei Ausfall eines Kanals ein Notruf diese Meldestelle trotzdem erreichen kann.


Zentrale Telefonnummer	
	Zentrale Mobiltelefonnummer

Zentrale Pager-Nummer	
	Zentrale E-Mail-Adresse

 Die Mitglieder des Krisenstabs bzw. ihre Stellvertreter müssen im Notfall erreichbar und in der Lage sein, sich innerhalb kurzer Zeit, typischerweise nicht grösser als eine Stunde, am Firmensitz oder – falls dieser selbst von der Katastrophe betroffen ist – an einem geeigneten Ausweichstandort einzufinden. Grundsätzlich können sich die Krisenstabsmitglieder auch mit Hilfe der modernen Kommunikationstechnik koordinieren, aber die Erfahrung zeigt, dass dies nur eine Notlösung sein sollte, falls einzelne Personen den Treffpunkt nicht (rechtzeitig) erreichen können.

Alle Personen, die zum erweiterten Kreis gehören, müssen für den Krisenstab gemäss Stellvertreterregelung erreichbar sein. Sinnvoll sind hier auch Pikettregelungen mit den dazugehörigen Übergaberegungen.

3.3.3 Regelmässige Schulung und Übung von Katastrophenszenarien

 Das Verhalten in Notfällen sowie die Verhaltensregeln, die auch im Normalbetrieb erforderlich sind, um die Bereitschaft für den Notfall aufrechtzuerhalten, müssen regelmässig geschult und geübt werden. Dabei hat sich gezeigt, dass zentrale Sicherheits- und Notfallschulungen und -übungen von geringer Effektivität sind. Wichtiger als die Einübung von Verhaltensregeln im Notfall ist die Verinnerlichung der Notfallregeln und die Förderung des Sicherheitsbewusstseins. Dies ist aber über Schulungen in Form von Kursen nicht nachhaltig genug.

Um eine nachhaltige Verbesserung des Sicherheitsbewusstseins und damit auch ein sicheres Reagieren in Krisensituationen zu fördern, werden sinnvollerweise immer wieder kleine Schulungseinheiten und Massnahmen zur Förderung der Aufmerksamkeit in den Arbeitsalltag eingeflochten. Auch eine Verbindung mit Incentives hat sich als sehr erfolgreich erwiesen.

Beispiel:

Im Rahmen der regelmässigen (Nach-)Schulung wird in periodischen Abständen eine neue Ausgabe einer Broschürenreihe zu jeweils einem ausgewählten Thema aus dem Bereich Sicherheit und Notfallvorsorge verteilt. Um das Ganze aufzulockern, kann als Einstieg ein Cartoon oder eine kleine Satire gewählt werden. Als Incentive wäre eine Preisfrage zum Thema denkbar, die im Intranet beantwortet werden kann. Aus allen richtigen Antworten werden dann drei Mitarbeiterinnen und Mitarbeiter gezogen, die jeweils einen Gutschein für ein Essen zu zweit erhalten.

Für solches internes Marketing sollte man auch durchaus einmal die eigene Marketing-Abteilung bemühen. Der Vorteil dieser Art der Schulung liegt darin, dass sie nicht als lästig empfunden wird («Schon wieder so eine langweilige Sicherheitsschulung»), sondern als willkommene Unterbrechung, womit psychologisch weitaus bessere Voraussetzungen gegeben sind, dass die Informationen auch aufgenommen werden. Wenn man darüber hinaus berücksichtigt, wie viele Menschen trotz der geringen Gewinnchancen Woche für Woche Lotto spielen oder die Preisrätsel in der Fernsehzeitung lösen und einsenden, dann kann man mit einem entsprechenden Lernerfolg durch die Preisrätsel rechnen.

3.4 Faktor Prozesse

3.4.1 Drehbücher für mögliche Katastrophenszenarien

Bei der Definition der Notfallpläne gibt es zwei grundsätzlich verschiedene Vorgehensweisen.

Variante 1

Man versucht alle möglichen Szenarien zu beschreiben und Katastrophenpläne für diese verschiedenen Szenarien zu erstellen.

Variante 2

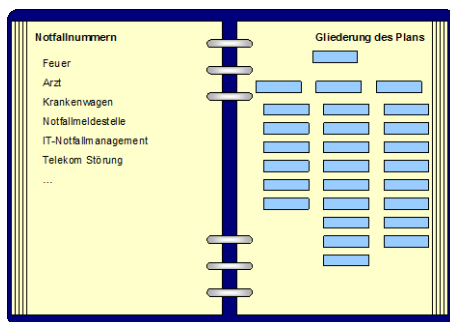
Man geht von einigen wenigen Worst-Case-Szenarien aus. Die Katastrophenpläne werden so modularisiert, dass auch eine Teilausführung möglich ist, falls ein Notfall eintritt, der einem Teil eines solchen Szenarios entspricht.

Wie aber die Betrachtungen in Abschnitt 2.3.2 gezeigt haben, ist der erste Ansatz praktisch nicht durchführbar, da nie alle möglichen Risiken und damit auch nicht alle Szenarien bekannt sein können. Zudem führt ein solches Vorgehen auch schnell zu einer unübersichtlichen Vielzahl von möglichen Notfallplänen, deren Pflege auf Dauer nicht konsistent möglich ist.

Zu empfehlen ist deshalb klar die Variante 2. Es wird ein gut modularisierter Notfallplan für den Worst Case erstellt, der in sich eigenständige Teilpläne für die einzelnen Anwendungen oder Anwendungsgebiete aufgliedert. Dabei ist die Aufteilung des Plans nach den betroffenen Geschäftsfunktionen zu wählen, da das Kriterium «geschäftskritisch» aus der eingangs zitierten Definition sich ausschliesslich aus den Bedürfnissen des Geschäfts ableiten lässt.



Der Aufbau eines Katastrophenplans ergibt sich aus der Forderung, dass er benutzbar sein muss. Es gibt durchaus Katastrophenhandbücher, die längst den Umfang eines «Handbuchs» überschritten haben. Ein gutes Katastrophenhandbuch sollte aber eher das Format dieses kleinen Wegweisers oder eines DIN-A5-Ringbuchs aufweisen.



Die nachfolgende Gliederung soll als Beispiel für den Aufbau eines Notfallhandbuchs dienen.

Übersichtsseite

Beim Aufschlagen muss als Erstes eine Übersicht mit Notfallnummern, Ansprechpartnern, Evakuierungsplan und Alarmierungsablauf dargeboten werden. Dies lässt sich übersichtlich auf einer Seite zusammenstellen.

Navigationshilfe

Als Nächstes empfiehlt sich ein Entscheidungsbaum, der den Leser durch die Module leitet und die Navigation zum richtigen Teilplan unterstützt. Gegebenenfalls kann man diesen Baum am Anfang oder Ende jedes Teilplans wiederholen, indem man den jeweiligen Teil des Baums einfärbt.

Teilpläne gemäss Entscheidungsbaum

Anschliessend an diesen Einleitungsteil müssen die einzelnen Teilpläne in logischer Abfolge erscheinen. Dabei ist es nicht notwendig, jede Prozedur, z.B. zum Start eines Anwendungskomplexes, vollständig wiederzugeben. Dies ist in den Betriebshandbüchern bereits geschehen. Das Notfallhandbuch muss den Anwender durch den übergeordneten Prozess zur Wiederherstellung der Betriebsbereitschaft führen und Querverweise auf die jeweilige Detaildokumentation sowie deren Ablageort (einschliesslich Ersatzversionen) enthalten. So kann der eigentliche Notfallplan schlank und übersichtlich gehalten werden und bietet damit am ehesten Gewähr, dass er im Falle einer Katastrophe auch wirklich richtig ausgeführt wird.

Checklisten

Es hat sich als hilfreich erwiesen, am Ende jedes Teilplans eine kurze Checkliste anzufügen, die den Anwender auf andere Teilpläne hinweist, die sich auf verwandte Aspekte beziehen. Zusammen mit der schon erwähnten Wiederholung des Entscheidungsbaums hilft diese Checkliste, die sinnvollen nächsten Schritte zu initiieren. Bezieht sich z.B. ein Teilplan auf die Wiederherstellung der Stromversorgung für einen Gebäudeteil, dann wäre ein Hinweis auf die Teilpläne für Telefonie und Netzwerk sinnvoll, denn je nach Notfall könnten diese Dienste auch betroffen sein, weil in der Regel die Trassen für Telefonie und Netzwerk in unmittelbarer Nähe der Trassen für die Stromversorgung verlaufen.

Was das Layout betrifft, so ist es hilfreich, allgemein verständliche Symbole zu verwenden, da Symbole eine schnelle Navigation unterstützen. Man sollte aber davon absehen, Symbole zu erfinden, da die damit verbundene Begrifflichkeit zunächst vermittelt werden müsste.



3.4.2 Drehbücher für Schulung und Übung

Grundsätzlich werden keine eigenen Drehbücher für die Schulung und Übung benötigt. Eine Notfallübung soll ja die Funktionsfähigkeit und Anwendbarkeit eines Notfallplans und die Vertrautheit der Mitarbeiterinnen und Mitarbeiter mit den Notfallplänen belegen.

Bezüglich der Schulung sind wesentliche Aspekte, welche die kontinuierliche Schulung betreffen, bereits im Abschnitt 3.3.3 genannt worden. Darüber hinaus werden Schulungsunterlagen für die Verantwortlichen im Notfall benötigt, die sich im Aufbau an den Notfallplänen orientieren. Ein wesentliches Element dieser Schulungsunterlagen ist es, das Verständnis für die Zusammenhänge und Hintergründe der einzelnen Massnahmen zu fördern. Nur so werden die Verantwortlichen in die Lage versetzt, im Notfall die richtigen Entscheidungen zu treffen, insbesondere dann, wenn ein unvorhergesehener und damit auch nie eingeübter Notfall vorliegt.

Es empfiehlt sich hier die Unterstützung professioneller Trainer zu nutzen, die entsprechende Erfahrung im Aufbau von Schulungsunterlagen haben. Sie können gegebenenfalls hilfreiche Tipps zu Methodik und Didaktik geben.

Daneben muss die Schulung und Übung im Information-Security-Management-Prozess verankert sein. Somit wird gewährleistet, dass

- regelmässig geschult und geübt wird
- die Schulungen regelmässig und bei Änderungen an den Systemen aktualisiert werden und
- die Qualität und der Erfolg der Schulung und Übung überwacht wird

3.4.3 Notfallprozeduren Eskalationsverfahren

Eskalationsverfahren gehören zu den Notfallplänen und Teilplänen und müssen dort als integraler Bestandteil definiert sein. Dabei muss sichergestellt werden, dass die jeweiligen Eskalationsziele bei Bedarf aktualisiert werden. Wichtig ist auch die Überlegung, wo im Notfallplan die entsprechenden Eskalationsregeln hinterlegt werden.



Nach den bisherigen Überlegungen sind Eskalationsregeln vor allem dann wichtig, wenn ein begrenzter Notfall auftritt, der zunächst lokal bearbeitet werden kann, ohne dass sofort die komplette Notfallorganisation involviert werden muss. Weitet sich der Notfall allerdings aus oder führt die direkte Bearbeitung nicht in angemessener Zeit zum Ziel, wird eine Eskalation erforderlich. Da es sich in einem solchen Fall zunächst um die Ausführung eines Teilplans handelt, ist der richtige Ort für die Hinterlegung der entsprechenden Eskalationsregel genau dieser Teilplan. Ergänzend können die Regeln auch in Kurzform in der Navigationshilfe hinterlegt werden.

Zur Vereinfachung sollten alle Meldevorgänge immer über eine zentrale Stelle erfolgen. Zudem kann dadurch ein besseres Tracking von Notfällen und Ausnahmesituationen erreicht werden.

3.5 Faktor Technologie

Wie oben bereits gesagt wurde, muss die Technologie die notwendige technische Unterstützung bieten, damit die definierten Notfallpläne umgesetzt werden können. Dies sind einerseits alle Sicherheitsmassnahmen, die der Aufrechterhaltung der Fähigkeit zur Wiederaufnahme oder Weiterführung des Betriebs dienen, wie auch alle Massnahmen, die der Vorbereitung zur Ausführung eines Katastrophenplans dienen. Letztere Massnahmen betreffen vor allem

- Bevorratung bzw. Ersatzbeschaffung von Infrastrukturkomponenten und -diensten
- Aufrechterhaltung der Betriebsbereitschaft bzw. Vorbereitung der Betriebsaufnahme dieser Ersatzinfrastruktur
- Restauration der Daten zum letzten gültigen Zeitpunkt vor dem Notfall
- gegebenenfalls Vorbereitung zur Nacherfassung und -verarbeitung verloren gegangener Geschäftsfälle

Die Umsetzung dieser Anforderungen kann je nach Bedarf auf sehr unterschiedliche Weise erfolgen.



Die vorstehende Grafik zeigt die unterschiedlichen Ebenen, auf denen eine Wiederaufnahme bzw. Weiterführung gewährleistet werden muss. Darauf aufbauend lassen sich verschiedene technologische Komponenten definieren, die im richtigen Zusammenspiel und abgestimmt auf die Bedürfnisse die Fähigkeit zur Weiterführung oder Wiederaufnahme unterstützen.

3.5.1 Ausweichrechenzentrum

Ein Ausweichrechenzentrum stellt mit Sicherheit die komfortabelste, aber in der Regel auch kostspieligste Variante eines Notfallvorsorgekonzepts dar. Bei diesem Konzept wird an einem unabhängigen Standort mit eigener Infrastruktur und kompletter Abbildung der Anwendungsumgebung ein zweites Rechenzentrum betrieben. Damit dieses aber auch im Notfall sofort oder mit nur geringfügiger Verzögerung den Betrieb übernehmen kann, muss dafür Sorge getragen werden, dass die Daten in diesem Rechenzentrum mit jenen im Hauptrechenzentrum im Rahmen der Anforderungen an RPO und RTO synchron gehalten werden. Dies kann durch unterschiedliche Mechanismen gewährleistet werden.

Wenn das Ausweichrechenzentrum mit quasi «Zero Downtime» den Betrieb übernehmen können soll, muss de facto eine permanente, echtzeitnahe Replikation aller Daten auf Basis der Speicherobjekte erfolgen. Darunter gibt es eine Reihe von abgestuften Varianten des Datenabgleichs. Dazu zählen Datenbank-Replikation, Message Replication, File Transfer, um nur einige zu nennen. Welcher Mechanismus im Einzelfall sinnvoll ist, hängt vom Bedarf und der Architektur ab.

Mehrfachnutzung eines Ausweichrechenzentrums

Um die Kosten für ein Ausweichrechenzentrum zu rechtfertigen, wird oft angeführt, dass es als Entwicklungs- und Testrechenzentrum einsetzbar ist. Das hat aber zur Folge, dass in der Regel eine unmittelbare Übernahme des Betriebs nicht möglich ist, da Entwicklung und Test meistens nicht auf der gleichen Konfiguration erfolgen wie der Produktivbetrieb. In einem solchen Fall muss also berücksichtigt werden, dass gegebenenfalls eine Umkonfiguration der Systeme erforderlich ist. Begünstigt wird eine solche Doppelnutzung, wenn die Infrastruktur eine dynamische Partitionierung und Rekonfiguration erlaubt. Damit ist es möglich, im normalen Betrieb in einer kleinen Partition den laufenden Produktionsbetrieb zu spiegeln und diese im Notfall zu Lasten der Entwicklungsumgebung zu vergrössern.



Unternehmen mit mehreren Standorten

Eine interessante Variante ergibt sich für Unternehmen mit mehreren Standorten, die jeweils über geeignete Räumlichkeiten für die Unterbringung der erforderlichen Infrastruktur verfügen, insbesondere wenn auch noch die Tätigkeitsschwerpunkte an den verschiedenen Standorten unterschiedlich sind. In einem solchen Fall können die jeweils lokal vorwiegend benutzten Dienste lokal laufen und gleichzeitig können die Daten kreuzweise zwischen den Standorten repliziert werden.

Geografische Rahmenbedingungen

Bei der Nutzung eines Ausweichrechenzentrums sollte man generell beachten, dass der Abstand zwischen den beiden Standorten je nach regionalen Gegebenheiten zwischen 10 und 40 km betragen sollte, sodass das Ausweichrechenzentrum auch ausserhalb des mittelbaren Bereichs der Gefährdung oder Behinderung ist. Es ist auch zu überlegen, ob der Standort des Ausweichrechenzentrums zum Schutz vor Angriffen geheim gehalten werden sollte.

3.5.2 Physische Sicherheit

Um einen Katastrophenfall zu überstehen, ist die physische Sicherheit von grosser Bedeutung. Ein Rechenzentrum, aber auch dezentrale Server-Räume sollten den gängigen Sicherheitsstandards entsprechen. Dazu gehören:

- geeignete Zugangskontrollsysteme
- Feuermelde- und -löschsysteme
- Wasserschutz
- Klimatisierung
- feuersicheres Datenträgerarchiv
- Schutz gegen EMS (elektromagnetische Störungen)
- Schutz vor Störungen in der Energieversorgung (Filter, Blitzschutz, USV)
- In tektonisch aktiven Gebieten erdbebensichere Bauweise

Besonders zu beachten ist die Tatsache, dass die entsprechenden Schutzvorkehrungen auch im Katastrophenfall greifen müssen. Gegebenenfalls müssen hier Ersatzmassnahmen vorgesehen werden, z.B. Bewachung bei Ausfall der Zugangskontrollsysteme.

3.5.3 Redundante IT-Systeme

Bei redundanten IT-Systemen muss man intern redundante und redundante Arrays gleicher Systeme unterscheiden.

Intern redundante Systeme

... sind intern vollständig oder teilweise doppelt ausgelegt, beinhalten also zwei Netzteile, einen doppelten Satz Festplatten, zwei Disk-Controller, zwei Netzwerkanschlüsse und teilweise auch zwei Systemplatinen. Handelt es sich dabei um so genannte Hot-Swap-Systeme, dann lassen sich defekte Teile im laufenden Betrieb abschalten und austauschen.

Redundante Arrays gleicher Systeme

... dagegen sind speziell vernetzte Gruppen von zwei oder mehr gleichen Systemen, die alle gleich konfiguriert sind und die Leistung einem oder mehreren gemeinsamen Services zur Verfügung stellen. Auch hierbei besteht die Möglichkeit, defekte Systeme aus dem Verbund herauszunehmen und zu ersetzen, ohne dass die bereitgestellten Services komplett ausfallen. Für die Vernetzung stehen mehrere Varianten mit unterschiedlichen Schwerpunkten zur Verfügung, die hier aber nicht näher detailliert werden sollen.

Redundante Systeme dienen heute in der Regel zur Sicherstellung eines unterbrechungsfreien Betriebs oder zur Lastverteilung. Sie stellen insofern auch ein

Konzept zur Katastrophenvorsorge dar, erfüllen aber oftmals die Anforderungen an ein solches Konzept nicht, da sie in der Regel im selben Gebäude(-komplex) untergebracht sind und somit bei einer echten Katastrophe die Weiterführung oder Wiederaufnahme kaum ermöglichen können. Für kleinere Notfälle wie den Ausfall von Komponenten wird hiermit jedoch ausreichend vorgesorgt.

Anders stellt sich die Situation dar, wenn diese Systeme in getrennten Lokationen aufgestellt und durch entsprechend schnelle Verbindungen gekoppelt sind. Eine solche Anordnung kann bei lokalen und gegebenenfalls regionalen Katastrophen eine ausreichende Vorsorge darstellen, vorausgesetzt die geschäftskritischen Anwendungen laufen auch wirklich auf diesen redundanten Systemen. Man nähert sich damit aber schon dem Konzept des Ausweichrechenzentrums zumindest für Teile der eigenen Infrastruktur an.

3.5.4 Allgemeine Sicherheit

Wie schon oben mehrfach erwähnt, müssen die Systeme im laufenden Betrieb durch sinnvolle Sicherheitsmassnahmen auf organisatorischer, betrieblicher und technischer Ebene geschützt sein, um Ausfälle durch unberechtigte Eingriffe von innen und aussen, Fehlbedienungen und technische Probleme weitestgehend auszuschliessen. All diese Massnahmen müssen den geltenden Richtlinien und Standards sowie dem technologisch aktuellen Stand entsprechen.

Im Fall von Outsourcing ist auf saubere Isolierung der eigenen Systeme innerhalb der Umgebung des Outsourcing-Partners und einen sicheren Administrationszugang zu achten.

3.5.5 Service Level Management

Für alle Dienste, so auch diejenigen, die für die Bereitstellung und Aufrechterhaltung der Recovery-Fähigkeit erforderlich sind, sowie mit Dienstleistern vereinbarte Recovery-Massnahmen und -zeiten ist die klare und eindeutige vertragliche Festschreibung dieser Services erforderlich. Das gilt sowohl inhouse zwischen Fachabteilung und interner IT wie auch im Outsourcing-Bereich. Gewöhnlich erfolgt dies über Service Level Agreements (SLAs). Alle SLAs sollten im Notfallplan und den entsprechenden Teilplänen referenziert sein.



Service Level Agreement (SLA)

Das Service Level Agreement selbst definiert die Parameter und Qualitätsmerkmale eines vereinbarten Services sowie den Service-Delivery-Prozess. Gleichzeitig legt das Service Level Agreement messbare Kriterien für die Qualitätsmerkmale fest. Diese erlauben einen Nachweis über die erbrachte Leistung im Vergleich zu vordefinierten Standards. Im Bereich der technischen Unterstützung dient das Service Level Agreement als Basis für die Identifikation der betroffenen Systemkomponenten, und es legt deren Unterhalt fest. Im Hinblick auf Business Continuity & Disaster Recovery ist darauf zu achten, dass auch die Service-Rahmenbedingungen für mögliche Notfälle klar vereinbart werden.

Checkliste 4: Parameter und Qualitätsmerkmale eines SLA

- Kontaktschnittstellen (Service Delivery, Helpdesk, 3rd Level Support usw.)
- Serviceverfügbarkeit, beschrieben mit Service-Örtlichkeiten, maximaler jährlicher Ausfallzeit usw.
- Lieferzeit und Lieferprozess bei Erstinstallation und Änderungen inkl. Test und Abnahme
- Fehlerbehebung mit Support- und Reaktionszeiten (Office Hours, 24/7 usw.)
- Kompensation im Falle einer Nichterfüllung der Lieferzeiten und Verfügbarkeiten des SLA
- Eskalationsprozess im Fehlerfall

3.5.6 Notfall-Arbeitsplätze (intern/extern)

Neben den IT- und Kommunikationssystemen können natürlich auch die Office-Umgebungen eines Unternehmens von einem Notfall betroffen sein. Das kann ein Wassereinbruch in einem Gebäudeteil wegen eines fehlerhaften Dachs sein, ein Stromausfall in einer Abteilung oder auch der Totalverlust eines Bürogebäudes. In all den Fällen müssen gegebenenfalls kurzfristig Ersatzarbeitsplätze geschaffen werden. Dabei geht es nicht nur darum, den erforderlichen Raum bereitzustellen. Auch die Büro-Infrastruktur muss vorhanden sein, d.h. Büromöbel, Workstations, Telefone und die erforderlichen Leitungen. Wenn möglich sollten die Telefone an den Ersatzarbeitsplätzen so geschaltet werden, dass die Mitarbeiterinnen und Mitarbeiter für externe Anrufe unter den gewohnten Rufnummern erreichbar sind.

Begrenzte Ausfälle innerhalb des Standorts

Für Teilausfälle in einem Gebäude mag es noch möglich sein, kurzfristig Ersatzarbeitsplätze in anderen

Gebäudeteilen bereitzustellen. So können gegebenenfalls kurzfristig Schulungsräume, Besprechungszimmer und auch freie Plätze in anderen Büros belegt werden. Da innerhalb desselben Gebäudes in der Regel die erforderlichen Verkabelungen vorhanden sind und allenfalls ausgefallene Workstations relativ schnell wieder beschafft werden können, lassen sich solche begrenzte Notfälle oftmals ohne grösseren Unterbruch für die Betroffenen überwinden.

Komplettausfall eines Standorts

Schwieriger wird es, wenn Gebäude vollständig ausfallen. In solchen Fällen bleibt oft nur die Möglichkeit, externe Ersatzarbeitsplätze zu schaffen. Dazu sollten mit Liegenschaftsverwaltungen, die geeignete Liegenschaften haben, entsprechende Verträge abgeschlossen werden. Gleichzeitig muss dann aber auch mit dem eigenen Netzbetreiber und Telekommunikationsdienstleister eine Vereinbarung zur Umschaltung der Verbindungen an einen zugewiesenen Ersatzstandort vereinbart werden. Besonders schwierig gestaltet sich eine solche Umsiedlung jedoch, wenn bei einer regionalen Katastrophe, z.B. bei Hochwasser, gleichzeitig eine Vielzahl von Unternehmen Ersatzarbeitsplätze sucht. In solchen Fällen stossen oft auch die besten Katastrophenpläne an ihre Grenzen. Solche Probleme können nur durch eine geeignete Standortwahl vermieden werden.

Lokale Daten

Ein wichtiger Aspekt bei der Vorbereitung von Notfällen in der Office-Umgebung ist die Datensicherheit lokaler Daten. Zwar gilt in den meisten Unternehmen die Regel, dass Daten nicht lokal gespeichert werden sollen, aber das lässt sich zumindest bei Notebook-Benutzern, die auch unterwegs ihre Daten brauchen und Daten erzeugen, nie vermeiden. Umso wichtiger ist es, einen möglichst automatischen Backup-Service der Workstation- und Notebook-Daten auf die zentralen Server einzurichten. Hierfür stehen diverse Tools zur Verfügung, die einen differenziellen Abgleich der Daten ermöglichen.



Checkliste 5: Vorbereitung auf den Katastrophenfall

- Verträge mit Immobilienverwaltungen
- Bereitstellung der Kommunikationsinfrastruktur
- Workstations und Office-Infrastruktur (Drucker, Kopierer, Telefone, ...)
- Office-Applikationen
- Dezentrale Server mit den entsprechenden Applikationen
- Netzanbindung an das Rechenzentrum
- Evtl. Unterbringung und Versorgung der Mitarbeiter
- Transport zum Ausweicharbeitsort
- Evtl. Schaltung von Info-Ansagen
- Falls nötig Publikation des Ausweichstandorts
- Mitteilung an Lieferanten, Zustelldienste und Kunden

3.5.7 Daten-Kommunikation

Für die Disaster-Recovery-Datenkommunikation zwischen Rechenzentrum und Ausweichrechenzentrum gibt es grundsätzlich zwei Möglichkeiten:

MAKE	<ul style="list-style-type: none">■ Eigenes Verlegen, Einkaufen oder Mieten von Leitungskapazitäten■ Verwendung eigener aktiver Infrastruktur (Switch, Router)■ Aufbau einer Organisation mit Engineering und Operation zum Betrieb der Netzwerkverbindungen
BUY	<ul style="list-style-type: none">■ Einkaufen eines bedürfnisgerechten WAN-Services■ Betrieb durch den Service-Provider■ SLA für garantierte Verfügbarkeit, Fehlerbehebung usw. der Netzwerkverbindungen

Die Entscheidung zwischen MAKE und BUY wird bestimmt von der bestehenden Organisation, sicherheitstechnischen Überlegungen oder Kostengründen.

Für die Wahl der richtigen Netzwerkverbindung, namentlich die Wahl des Protokolls, der Bandbreite, der Verfügbarkeiten und der Sicherheit, gilt Folgendes:

IP (Public Internet)	<ul style="list-style-type: none">■ bei kleinem Volumen zur günstigen Datenreplikation geeignet■ Best Effort Bandwidth – Beeinflussung der Bandbreite beinahe unmöglich■ Sicherheit ist durch geeignete Verfahren, z.B. IP Sec VPN, sicherzustellen■ Netzleistung ist stark abhängig von der Gesamtlast
ATM, FR	<ul style="list-style-type: none">■ optimal für die asynchrone Replikation und Remote Backup über Nacht■ Backup-Verbindung für DWDM-Lösungen■ für kleine bis mittlere Datenmengen (≤ 700 MB/h)
SDH	<ul style="list-style-type: none">■ optimal für die asynchrone Replikation■ auch für Distanzen ab 100 km zwischen den Rechenzentren geeignet■ für mittlere bis grössere Datenmengen■ Bandbreite bis einige 100 Mbps
DWDM	<ul style="list-style-type: none">■ Flexibilität – Übertragung jedes gewünschten Protokolls■ bit- und protokolltransparenter Transport■ skalierbar, z.B. bis zu 64 Verbindungen à 10 Gbps (Wellenlängen) über eine Glasfaser■ optimal für die synchrone Replikation■ geeignet für die Vernetzung grosser Rechenzentren

Beim heutigen Stand ist für die meisten Anwender der Eigenbetrieb nicht sinnvoll. Wer nicht bereits über eigene ausreichend leistungsfähige Netze verfügt, sollte die erforderliche Netzwerkleistung einkaufen. Nationale Service-Provider offerieren die ganze Protokoll-Palette und bieten z.B. Einstiegsmöglichkeiten mit SDH mit späterer Migration auf einen DWDM-Service. Der WAN-Service entwickelt sich mit den Kundenbedürfnissen.

Professionelle Telekommunikationsanbieter bieten für ihre Datenservices ein umfangreiches Service Level Agreement an. Die Parameter werden den jeweiligen Kundenbedürfnissen angepasst.

WAN-Service-Trends für Disaster Recovery

Die aktuelle Entwicklung der Storage-Protokolle, Fibre Channel und ESCON, geht klar in Richtung IP. Eine Konvergenz mit dem LAN-Standard Ethernet ist zu erwarten. Betrachtet man den Schichtenaufbau der Netzwerkplattform, dann zeichnet sich für die kommenden Jahre folgender Aufbau (OSI Layer 1 bis 3) ab:

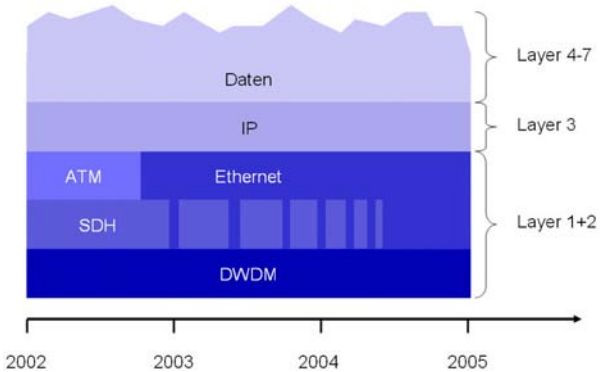


Abbildung 7: Schichtenaufbau der Netzwerkplattform (nach sunrise Business Solutions, 2003)

Heutige Multiservice-Netzwerke bieten ausreichend Flexibilität, um sich ändernden Anforderungen Rechnung zu tragen. Die Migration auf leistungsfähigere Services im Bedarfsfall wird wirkungsvoll unterstützt, sodass wachsende Datenmengen jeweils zu einem guten Preis-Leistungs-Verhältnis transportiert werden können.

Remote Access/Administrationszugang

Für den Unterhalt und das Monitoring der Infrastruktur kann ein Zugang von Remote-Usern über eine Remote-Access-Server-Plattform (RAS) sinnvoll sein. Der RAS optimiert vor allem den Aufwand bei kleineren Störungen, da sie von Engineering-Mitarbeitern ferngesteuert z.B. von zu Hause aus beseitigt werden können. Sind wichtige Prozesse zu überwachen oder ist eine Überwachung mit grosser Unabhängigkeit zu implementieren, ist RAS ein gutes Hilfsmittel. Natürlich müssen sowohl das RZ wie das Ausweichrechenzentrum angeschlossen sein. Der Remote-Access-Service kann durch den Rechenzentrum-Betreiber selbst aufgesetzt oder beim Service-Provider eingekauft werden.

Da der Remote-Zugang für die Administration der Systeme genutzt wird und damit einen sehr tiefen Eingriff

in die Infrastruktur erlaubt, sind die Zugriffsregeln hierfür sehr genau zu definieren. Zudem sollte ein Remote-Zugang immer nur mit starker Authentisierung erlaubt werden. Eine schwache Authentisierung nur mit Benutzername und Passwort ist hier völlig unzulänglich.

3.5.8 Voice-Kommunikation

Die Gewährleistung von ununterbrochenen Rechenzentrumsservices, insbesondere im Fall von Fehlfunktionen und Ausfällen, beruht massgeblich auf einer einwandfreien Sprachkommunikation. Für die telefonische Erreichbarkeit ist es sinnvoll, zwei Service-Provider zu nutzen. Mit Vorteil wählt ein Rechenzentrumsbetreiber auch zwei getrennte Netze, das Festnetz und das Mobilfunknetz.

Zwei Festnetze zu benutzen, birgt die Gefahr der gemeinsamen Nutzung der «letzten Meile» der Swisscom und bringt daher ein Klumpenrisiko. Ein Alternativanbieter mit eigener letzter Meile z.B. über Glasfaseranschluss wäre eine Option.

Neben der Unabhängigkeit bis zur letzten Meile bietet die Mobiltelefonie gegenüber zwei Festnetzen noch eine erhöhte Flexibilität. SMS könnte als Zusatzfunktion genutzt werden, z.B. für Fehleralarmierungen. Beim Mobilnetz ist die Servicequalität nicht nur in den Büros zu testen, sondern auch in den Infrastrukturräumen im Gebäudezentrum oder Untergeschoss mit tendenziell erhöhter Abschirmung der Funkstrahlung.

Die Nutzung von Mobiltelefonen birgt jedoch insbesondere in Rechenzentrumsräumen ein erhöhtes Gefahrenpotenzial im Hinblick auf Betriebsspionage, da nicht nachvollziehbar ist, wer mit wem zu welchem Zweck telefoniert hat. Bei grundsätzlich möglicher Mobiltelefonie kann ja nicht gewährleistet werden, dass nur Firmen-Handys benutzt werden. Aus diesem Grund ist Mobiltelefonie in vielen Rechenzentren grundsätzlich untersagt und wenn möglich auch technisch unterbunden.

Eine interessante Alternative bietet Voice over IP (VoIP), zumal neuere Entwicklungen auch den direkten Anruf erlauben. Dabei wird die Sprachübertragung über das bestehende Datennetz ermöglicht.

4 Disaster Recovery Services

Je nach tolerierbarer Ausfallzeit gibt es unterschiedliche Services für den Katastrophenfall, die gewöhnlich als Cold, Warm und Hot Standby bezeichnet werden. Die wesentlichen Charakteristika sind in der folgenden Tabelle zusammengestellt.

4.1 Cold Service – Datensicherung an Zweitstandort

Cold	<ul style="list-style-type: none">■ Datensicherung ausserhalb des Hauptstandorts■ Bereitstellung von Ersatzsystemen im Notfall, z.B. über Serviceverträge mit dem Hardware-Lieferanten■ Wiederherstellungszeit je nach Servicevertrag für die Hardware und Zeitbedarf für Inbetriebnahme und Restore■ Aktuellste Daten typischerweise vom Vortag■ Ausfallzeit typisch < 2–5 Tage
-------------	---

4.2 Warm Service – Betriebsbereite Stand-by-IT-Systeme an Zweitstandort

Warm	<ul style="list-style-type: none">■ Bereitstellung von betriebsbereiten Systemen an einem Ausweichstandort■ Datensicherung am Ausweichstandort■ Regelmässiges Laden der Backups auf die vorhandenen Systeme■ Wartung der Systeme am Ausweichstandort synchron mit den Produktivsystemen (Konfigurationen, Patch-Level, ...)■ Manuelle Inbetriebnahme und Umschaltung■ Wiederherstellungszeit bestimmt durch Zeitbedarf für Hochfahren der Systeme und Restore■ Aktuellste Daten typischerweise vom Vortag■ Notfallarbeitsplätze■ Ausfallzeit typisch < 24 Stunden
-------------	--

4.3 Hot Service – Paralleler Betrieb der IT-Systeme an zwei Standorten

Hot	<ul style="list-style-type: none">■ Bereitstellung von laufenden Systemen an einem Zweitstandort■ Online-Replikation der Daten und Konfigurationen auf die Systeme■ Umschaltung «on the fly» bei Ausfall des Hauptstandorts■ Wiederherstellungszeit im Minutenbereich im Wesentlichen bestimmt durch Konfiguration der Netzanbindung (Adress-Umsetzung und ggf. Restart)■ Aktuellste Daten abhängig von Latenzzeit der Replikation, typisch 1–20 Transaktionen■ Notfallarbeitsplätze■ Ausfallzeit wenige Sekunden bis einige Minuten, typisch < 5 Minuten
------------	--

5 Tools und Instrumente

5.1 Werkzeuge für Disaster Backup

Es gibt derzeit eine Vielzahl von Werkzeugen zur Replikation von Unternehmensdaten zwischen verschiedenen Standorten, die als Basis für den Aufbau einer Disaster-Backup-Lösung dienen können. Welche Tools im Einzelfall zum Einsatz kommen, hängt sehr stark von den Anforderungen, den eingesetzten Plattformen und dem gewünschten Service Level ab. Aus diesem Grunde soll hier nur auf die grundsätzlichen Charakteristika solcher Tools eingegangen werden.

Werkzeug	Charakteristika
Datenbank-Replikation	<ul style="list-style-type: none">■ Replikation der Transaktionsdaten auf der Basis des Datenbank-Transaktionslogs■ Latency typisch 1–20 Transaktionen■ Sehr stabile und ausgereifte Technik praktisch für alle RDBMS verfügbar■ Nicht in der Datenbank vorhandene Daten werden nicht repliziert, bei Bedarf muss dafür eine Zusatzlösung eingesetzt werden■ Konfiguration und Fine-Tuning einer Replikation ist recht aufwendig
Replikation von Speicherobjekten	<ul style="list-style-type: none">■ Alle Speicherobjekte, Datenbanken, Dateien, Bibliotheken, Konfigurationen, ... werden auf binärer Ebene repliziert ungeachtet des Inhalts■ Für eine sinnvolle Konfiguration ist die Zentralisierung des Speichers über SAN sinnvoll■ Zur Kontrolle des Datenvolumens ist eine gute Differenzenbildung erforderlich■ Grundsätzlich einfache Konfiguration und damit auch einfache Anpassung bei Änderungen in der Konfiguration■ Bei entsprechender Konfiguration werden neu entstehende Speicherobjekte automatisch in die Replikation einbezogen

Nachrichten-orientierte Replikation	<ul style="list-style-type: none">■ In message-orientierten Architekturen mit durchgängiger Integrationsschicht können alle Geschäftsvorfälle auch in Form der sie repräsentierenden Nachrichten repliziert werden■ Die Replikation auf Nachrichtebasis ist in der Regel sehr schlank■ Im Bankenbereich kann diese Art der Replikation z.B. genutzt werden, wenn auch die interne Interapplikationskommunikation auf Basis von SWIFT erfolgt■ Alle replizierten Nachrichten werden im Backup-System genauso verarbeitet wie im Produktivsystem. Damit wird sichergestellt, dass sich beide Systeme identisch verhalten■ Bei der nachrichten-basierten Replikation handelt es sich nicht um ein Produkt, sondern um eine grundlegende Funktionalität message-orientierter Middleware■ Nachrichten-basierte Replikation setzt eine middleware-basierte Applikationsarchitektur voraus
Remote Backup	<ul style="list-style-type: none">■ Beim Backup des Produktivsystems werden alle Daten dupliziert und an das lokale Backup-System und via Netzwerk an ein entferntes in einem Zweitstandort übertragen■ Aufgrund der grossen Datenmengen entstehen im Remote-System Verzögerungen, da in der Regel die Backup-Geschwindigkeit die Netzleistung um einiges übersteigt■ Für ein effektives Netz-Backup werden am entfernten Standort in der Regel schnelle Plattenpuffer benötigt, auf denen die Backup-Daten zwischengespeichert werden■ Neben kommerziellen Lösungen gibt es in diesem Bereich auch sehr zuverlässige und erprobte Open-Source-Lösungen wie z.B. AMANDA

5.2 Evaluationskriterien

Welche Disaster-Recovery-Lösung für die eigene Situation sinnvoll ist oder ob gegebenenfalls ein Mix gefahren werden muss, hängt von den Bedürfnissen des Business ab. Je kürzer die tolerablen Ausfallzeiten sind, um so «wärmer» muss der Service werden. Dies kann für unterschiedliche Anwendungen durchaus unterschiedlich sein, sodass in einem Fall Hot-Standby-Betrieb anzuraten ist, während eine andere Applikation mit einem Cold-Service ausreichend abgedeckt wäre.

Hot	Warm	Cold
Zentrale Geschäfts-lösungen <ul style="list-style-type: none"> • Bankenlösung • Versicherungs-leistungssystem • etc. 	Office Umgebung <ul style="list-style-type: none"> • Textverarbeitung • Kalkulation • Andere Desktop-Anwendungen 	Back Office Applikationen <ul style="list-style-type: none"> • Financial Reporting • Personal
Auftragsbearbeitung		
Online Systeme		
<ul style="list-style-type: none"> • Web-Server • Applikations-server • Online DB-Anwendungen 		

Abbildung 8: Typische Anforderungen an Recovery Services

Cold

Für Cold-Standby basierend auf Remote-Backup-Lösungen ist wichtig, dass die eingesetzten Backup-Systeme (Tape-Library, Backup-Roboter, ...) unbe-wacht betrieben werden können. Sie sollten zudem über ausreichenden internen Pufferspeicher verfügen, um in der Lage zu sein, so viele Daten zunächst zu sammeln, bis ein Band ohne Unterbruch geschrieben werden kann. Softwareseitig ist eine einfache Remote-Administration von entscheidender Bedeutung, damit auch ein Zurückspielen von Daten grundsätzlich ohne Eingriff möglich ist. Was diese Fähigkeiten angeht, so sind die im Markt gängigen Lösungen wie auch die Open-Source-Lösungen weitestgehend gleichwertig. Je nach vorhandenen Arbeitsumgebungen und verfügbarem IT-Personal kann noch entscheidend sein, auf welchen Plattformen der Administration-Client verfügbar ist und wie bedienerfreundlich er ist. Neben dem regel-mässigen Backup sollte auch ein regelmässiger Restore-Test durchgeführt werden, um sicherzustellen, dass im Notfall ein Restore auch möglich ist.

Warm

Für Warm-Standby gilt hinsichtlich des Remote-Backup grundsätzlich dasselbe wie für Cold-Standby. Ansonsten sollten die Systeme remote administrierbar sein.

Hot

Im Fall des Hot-Standby muss zuerst die geeignete Replikationslösung ausgewählt werden. Diese ist zunächst einmal von der eingesetzten Plattform abhängig, da nicht alle Hersteller alle Plattformen gleichermassen unterstützen. Dies spielt keine grosse Rolle im Unix-Bereich. Kommen aber andere Plattformen vor allem aus dem Mainframe-Bereich zum Einsatz, dann sollte man sich doch auch bei den Spezialanbietern für diese Plattformen umschauchen, da diese oftmals optimierte Lösungen anbieten, welche die Systemfunktionalitäten der jeweiligen Plattform optimal ausnützen.

Die Hauptschwierigkeit bei Hot-Standby-Lösungen liegt in der Regel in der Installation und Optimierung. Hier ist wichtig, dass der Lieferant oder Integrationspartner ausreichende Unterstützung anbietet. Zudem muss eine solche Lösung in das Standard-Monitoring einbindbar sein, sodass es gemeinsam mit den Produktivsystemen überwacht werden kann.

Je weniger die Replikationslösung von den eingesetzten Produkten und Applikationen abhängig ist, umso flexibler ist man in der Gestaltung der Geschäftslösungen insbesondere auch für die Zukunft.

5.3 Checklisten

Zur Ermittlung des Bedarfs an Business Continuity & Disaster Recovery-Vorkehrungen existiert eine Vielzahl von Checklisten. Die generelle Empfehlung hierzu lautet:

«Orientieren Sie sich an der ISO 17799 und nutzen Sie hinsichtlich der Informationssicherheit allgemein und des Business Continuity Planning im Besonderen darauf aufbauende Checklisten.»

Wenn man unter dem Stichwort ISO 17799 im Internet sucht, findet man eine Reihe von Anbietern von Sicherheitschecks nach ISO 17799 sowie einige Tools.

Falls Sie sich für ein Tool zur Bedarfsermittlung interessieren, sollten Sie die folgenden Kriterien anlegen:

- Das Tool sollte von Praktikern erstellt sein.
- Die einzelnen Fragebogen-Komplexe müssen adaptierbar sein; z.B. müssen Fragen nach IBM-Mainframe-Systemen in einer reinen Midrange- oder Server-basierten Infrastruktur ausblendbar sein, da sonst keine sinnvollen Ergebnisse zu erwarten sind.
- Aufgrund der Antworten sollten Massnahmenvorschläge erstellt werden, die als Ausgangsbasis für die Vorsorgeplanung dienen.
- Zum Tool sollten möglichst umfangreiche Fragebogen-Module bereits vorhanden sein.
- Eigene Fragebogen-Module sollten unabhängig oder aufbauend auf vorhandenen erstellbar sein.
- Vollständigkeit in der Abdeckung der Problematik sollte bei der Auswahl wichtiger sein als ein «fancy» GUI.



Wenn Sie tiefer auf die Ebene der einzelnen Systeme vordringen wollen, empfiehlt sich das IT-Grundschutztool des Bundesamtes für Sicherheit in der Informationstechnik (BSI), das auch als 30-Tage-Testversion zum Download unter <http://www.bsi.bund.de> bereitsteht. Dort gibt es auch einen Themenschwerpunkt «Kritische Infrastrukturen» mit einer Vielzahl von Links zum Thema.

6 Kosten: Wie rechnet sich Business Continuity?

6.1 Modellrechnungen

Immer wieder taucht in der Diskussion um Informationssicherheit und Business Continuity Planning die Frage nach der Rentabilität oder dem Return on Investment auf. Nun kann man mit viel Statistik und noch mehr Annahmen solche Zahlen rechnen, aber ich glaube, man sollte einen anderen Ansatzpunkt wählen. Wer ein Haus baut, muss es versichern, obwohl natürlich jeder hofft, dass es nie zu einem Versicherungsfall kommt. Genauso trifft man in der Regel auch einige Vorkehrungen, die dafür sorgen sollen, dass das Haus erhalten bleibt und es nie zu einer Katastrophe kommt. In diesem Bereich kommt kaum jemand auf die Idee, eine Kosten-Nutzen-Rechnung anzustellen, weil jeder weiss, dass er im Katastrophenfall obdachlos ist.

Andererseits entwickeln die meisten Menschen ein recht gutes Gefühl dafür, was an Vorkehrungen sinnvoll ist und was nicht. Das wiederum hängt mit einer sehr pragmatischen Risikoeinschätzung zusammen. Einen ähnlichen Pragmatismus sollte man bei der Risikoeinschätzung in einer Unternehmung einsetzen. Wenn man dann zu dem Schluss kommt, ein Totalausfall der Informations- und Kommunikationssysteme sei nicht auszuschliessen und ein damit verbundener Verlust würde die Existenz des Unternehmens gefährden, dann muss eine Ausweichmöglichkeit geschaffen werden. Ob diese nun im Cold-, Warm- oder Hot-Modus betrieben wird, hängt von der tolerierbaren Ausfallzeit und dem zu erwartenden Schaden ab.



Letztendlich ist aber jedes Disaster-Recovery-Konzept eine Versicherung für den Fall, der hoffentlich nie eintritt. Für die meisten Unternehmen dürfte aber der Ernstfall so teuer werden, dass ein gutes Disaster-Recovery-Konzept in jedem Fall günstiger ist!

Eine Abschätzung der Kosten für die verschiedenen Servicevarianten zeigt die folgende Tabelle:

Cold	<ul style="list-style-type: none"> ■ Initialleistung: typischerweise CHF 50 000 – 150 000 ■ Wiederkehrende Betriebsleistungen: typischerweise CHF 100 000 – 200 000 pro Jahr ■ Kommunikationskosten WAN-Service: typischerweise CHF 25 000 – 75 000 pro Jahr
Warm	<ul style="list-style-type: none"> ■ Initialleistung: typischerweise CHF 150 000 – 250 000 ■ Wiederkehrende Betriebsleistungen: typischerweise CHF 300 000 – 400 000 pro Jahr ■ Kommunikationskosten WAN-Service: typischerweise CHF 75 000 – 200 000 pro Jahr
Hot	<ul style="list-style-type: none"> ■ Initialleistung: typischerweise CHF 250 000 – 350 000 ■ Wiederkehrende Betriebsleistungen: typischerweise CHF 400 000 – 1 000 000 pro Jahr ■ Kommunikationskosten WAN-Service: typischerweise CHF 100 000 – 400 000 pro Jahr

Die Preisgestaltung der drei Varianten wird massgeblich durch die jeweiligen Kundenanforderungen beeinflusst.

Cold	<ul style="list-style-type: none"> ■ Datenmenge (GB) ■ Backup-Prozedur ■ Datenwachstum pro Jahr ■ maximale Aufbewahrungszeit (Tape)
Warm	<ul style="list-style-type: none"> ■ Datenmenge (GB) ■ Backup-Prozedur ■ Datenwachstum pro Jahr ■ maximale Aufbewahrungszeit (Tape) ■ Anzahl Server ■ Detailspezifikation der Server ■ Datenbank-Spezifikation

Hot	<ul style="list-style-type: none">■ Datenmenge (GB)■ Backup-Prozedur■ Datenwachstum pro Jahr■ Maximale Aufbewahrungszeit der Backups■ Anzahl Server■ Detailspezifikation der Server■ Datenbank-Spezifikation■ Zugriffsgeschwindigkeit der Disks
------------	--

Auch die Kommunikationskosten werden stark durch die jeweiligen Kundenanforderungen beeinflusst. Nachfolgende Punkte fallen ins Gewicht:

- AW- und AWRZ-Standorte; Distanz zum jeweils nächstgelegenen Point of Presence (POP) des Service-Providers und die Distanz zwischen Standorten
- WAN-Technologie und -Protokoll sowie die benötigte Bandbreite
- erwartete WAN-Verfügbarkeit und weitere SLA-Parameter

6.2 Vergleich Insourcing mit Outsourcing von Disaster-Recovery-Lösungen

Grundsätzlich lassen sich Disaster-Recovery-Lösungen gut outsourcen. Dies ist dann sinnvoll, wenn

- kein eigener Ausweichstandort vorhanden ist
- der normale Betrieb auch bereits outsourct ist
- grundsätzlich über Outsourcing nachgedacht wird

Dagegen ist Outsourcing dann nicht unbedingt sinnvoll, wenn man, wie schon erwähnt, selbst über mehrere geeignete Standorte verfügt und ohnehin einen eigenen Betrieb hat.

Vorteilhaft ist das Outsourcing selbst bei eigenem Betrieb der Disaster-Recovery-Lösung für die Data-Center-Funktion für Notfallarbeitsplätze. Da Arbeitsplatzkosten relativ hoch sind, kann man die eigene Bevorratung von zusätzlichen Arbeitsplatzkapazitäten für kleinere Notfälle gering halten. Der Outsourcing-Partner, der Arbeitsplatzkapazität bereitstellt, kann mit relativ kleiner Kapazität, die flexibel genutzt werden kann, ausreichende Leistung für mehrere Unternehmen bereitstellen, da



selbst unter Berücksichtigung regionaler Katastrophen nicht die volle Kapazität für alle Kunden vorgehalten werden muss. Dadurch sind die Kosten mit hoher Wahrscheinlichkeit geringer als bei eigener Bevorratung.

Zusätzliche Sicherheitskriterien im Outsourcing

Bei Outsourcing-Lösungen sind aber in der Regel zusätzliche Sicherheitskriterien zu beachten. Für Banken gelten in diesem Umfeld vor allem die Regelungen des Rundschreibens EBK-RS 99/2 der Eidgenössischen Bankenkommission³. Daneben muss aber auch darauf geachtet werden, dass der Outsourcing-Anbieter eine geeignete Sicherheitsinfrastruktur hat, welche die eigene Backup-Installation nicht nur wirkungsvoll nach aussen, sondern auch gegenüber den Installationen anderer Kunden abschirmt.

6.3 Kosten-Nutzen-Analyse

Die Kosten-Nutzen-Analyse einer BC & DR-Lösung ergibt sich im Wesentlichen aus der Risikobewertung. Dies ist in Kapitel 2.3.2 beschrieben.

6.4 Investitionsrechnung gegenüber Versicherungskosten

Ein Vergleich von Investitionskosten mit Versicherungskosten ist direkt nicht möglich, da über eigene Vorkehrungen zum grossen Teil Risiken abgedeckt werden, die nicht versicherbar sind oder für die unbezahlbare Prämien entstünden. Hinsichtlich der Versicherung haben Risikoanalyse und anschliessende Entwicklung eines BCP noch einen weiteren Vorteil. Nach einer Risikoanalyse lassen sich die Prämien für die versicherten Risiken oftmals mit der Versicherung neu verhandeln. Der Grund ist, dass aufgrund der gewonnenen Informationen eine bessere Abgrenzung der versicherten Risiken möglich ist oder einzelne Risiken aus der Versicherung herausgenommen werden können, weil sie entweder nicht relevant sind (Ergebnis der Risikoanalyse) oder durch die BCP-Massnahmen verringert wurden.



³ EBK-RS 99/2: Auslagerung von Geschäftsbereichen (Outsourcing)

7 Trends und Ausblick

Je stärker Unternehmen von der Funktionalität und Verfügbarkeit ihrer Informations- und Kommunikationstechnik abhängig sind, umso wichtiger werden Vorkehrungen, diese Verfügbarkeit aufrechtzuerhalten. Dabei sollten die BC & DR-Massnahmen in ein gesamtheitliches Konzept zur Informationssicherheit eingebunden werden. Daneben steigen auch die externen Anforderungen an ein gutes Risikomanagement, z.B. durch die Auflagen aus Basel II.

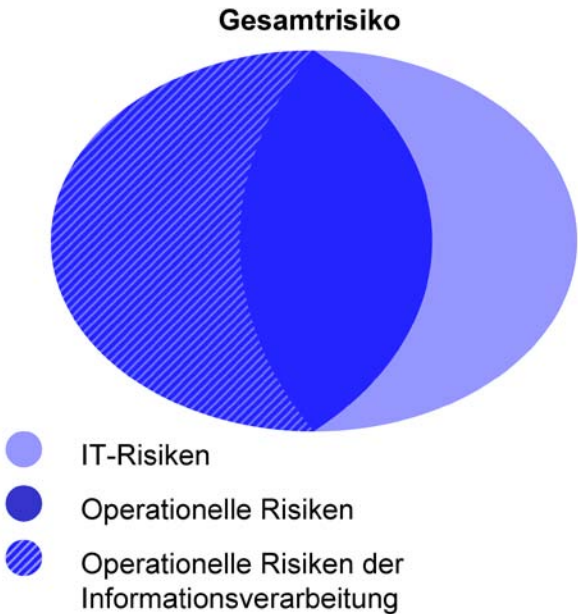


Abbildung 9: Aufteilung des Gesamtrisikos

Kernthema von Basel II sind die operationellen Risiken, die zu einem wesentlichen Teil heute durch die Risiken in der Informationsverarbeitung bestimmt sind. Dies ist – wie schon mehrfach erwähnt – darauf zurückzuführen, dass heute nahezu alle Unternehmen stark vom Funktionieren ihrer Informationsverarbeitungsdienste abhängig sind. Business Continuity & Disaster Recovery-Massnahmen tragen massgeblich zur Senkung dieser Risiken bei und dienen damit auch direkt dem Ziel, die Auflagen aus Basel II zu erfüllen.



Um diesen Anforderungen gerecht zu werden, ist es sinnvoll, rechtzeitig die eigenen Geschäftsprozesse zu dokumentieren und die Prozessrisiken zu bewerten. Damit ist man in der Lage, einerseits entsprechende Massnahmen zur Risikosenkung und zum Risikomanagement einzuleiten und hat andererseits ausreichende Informationen zur eigenen Vorbereitung z.B. auf ein Basel-II-Rating. Zudem ist davon auszugehen, dass mit einem etablierten Risikomanagement und einer guten Vorbereitung auf Notfälle ein solches Rating positiver ausfällt.

Was die technischen Lösungen betrifft, sollte man aktuelle Technologien einsetzen. Dazu gehört die Trennung von Verarbeitungsleistung (CPU) und Speicherung durch Auslagerung der Daten vom Server ins Netz (SAN). Moderne Replikationslösungen erleichtern dann den Aufbau entsprechender Standby-Lösungen.

Der Trend bei Arbeitsplatzumgebungen geht derzeit in zwei Richtungen: einerseits möglichst einfach zu verwaltende feste Arbeitsplätze und andererseits stärkere Verbreitung von Notebooks. Um erfolgreiches Disaster Recovery bis zur Office- und Workstation-Umgebung zu ermöglichen, sollte man bei festen Arbeitsplätzen verstärkt Thin Clients einsetzen, um eine unkontrollierte dezentrale Speicherung evtl. wichtiger Informationen zu vermeiden, und Notebooks mit automatischer Replikation der lokalen Daten bei vorhandener Netzwerk-Connection versehen.

8 Referenzen

8.1 Bücher

Toigo, Jon W., Disaster Recovery Planning, New York 1996, John Wiley & Sons, Inc., ISBN 0-471-12175-4

British Standards Institution (BSI), Information Security Management Part 1: Code of practice for information security management (ISO 17799)

Massiglia, Paul & Marcus, Evan (Hrsg.), The resilient Enterprise, Mountain View CA 2002, VERITAS Software Corporation (Erscheinungsdatum 04/2003)

Wieczorek, Martin, Naujoks, Uwe, Bartlett, Bob (Hrsg.), Business Continuity, Notfallplanung für Geschäftsprozesse, Berlin 2003, Springer Verlag, ISBN 3-540-44285-5

Elliott, Dominic, Business Continuity Management: A Crisis Management Approach, Routledge 2002, ISBN 0415204917

Ghosh, Anup K., Security & Privacy for E-Business, New York 2001, John Wiley & Sons, Inc., ISBN 0-471-38421-6

Wood, Charles Cresson, Information Security Policies made easy, Sausalito CA 1999, Baseline Software Inc., ISBN 1-881585-06-9

Tipton, Harold F., Krause, Micki (Hrsg.), Information Security Management, Boca Raton FL 1999, Auerbach Publications, ISBN 1-8493-9829-0

Thodén, Nora, Managing the Vulnerability of Banks to Information Technology Related Criminal Type Risks, Dissertation der Universität St.Gallen (HSG) Nr. 2206, Bamberg 1999, Difo-Druck OHG

8.2 Links

Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutzhandbuch (www.bsi.bund.de)

Eidg. Bankenkommission, Rundschreiben zur Auslagerung von Geschäftsbereichen (Outsourcing) vom 26. August 1999 mit Änderungen vom 22. August 2002, EBK-RS 99/2 (www.ebk.ch/d/publik/rundsch/index.html)

Ernst & Young, State of the ART Alternative Risk Transfer ([www.ey.com/global/content.nsf/International/Issues & Perspectives-State of the ART Alternative Risk Transfer That Is](http://www.ey.com/global/content.nsf/International/Issues%20%26%20Perspectives-State%20of%20the%20ART%20Alternative%20Risk%20Transfer%20That%20Is))

InfoSurance, Stiftung für die Sicherheit der Informationsinfrastruktur in der Schweiz (www.infosurance.ch)

CRN – Comprehensive Risk Analysis and Management Network (www.isn.ethz.ch/crn)

Computerwoche Archiv und Computerwoche online (www.computerwoche.de)

9 Glossar

ART	Alternative Risk Transfer
ATM	ATM bedeutet Asynchronous Transfer Mode. Universelles Übermittlungsprinzip für breitbandige Anwendungen im Bereich von 2 Mbit/s bis zu 622 Mbit/s. Basistechnologie für das Breitband-ISDN. Die ATM-Technologie basiert auf der speichervermittelten, asynchronen Übertragung von Daten in Form adressierter Zellen fester Länge. Die ATM-Pakete nutzen – im Gegensatz zur im Internet verwendeten TCP/IP-Technologie – auf ihrem Weg vom Sender zum Empfänger alle den gleichen Weg
BC	Business Continuity
BCP	Business Continuity Planning
CEO	Chief Executive Officer; Leiter der Geschäftsleitung
CIO	Chief Information Officer; Leiter der IT-Services eines Unternehmens
CPU	Central Processing Unit; Prozessor eines IT-Systems; CPU-Leistung ist die Verarbeitungsleistung im Unterschied zur Speicherkapazität
CSO	Chief Security Officer; Sicherheitsverantwortlicher eines Unternehmens
Disaster	Ein Disaster ist die Unterbrechung von geschäftskritischen IT-Dienstleistungen für eine unakzeptable Dauer
DR	Disaster Recovery; teilweise auch als Business Recovery bezeichnet
DWDM	Abkürzung für Dense Wavelength Division Multiplexing. DWDM erlaubt es, verschiedene Wellenlängenbereiche des Laserlichts als einzelne Kanäle innerhalb einer Glasfaserleitung zu nutzen. Standardmässig werden heute bis 64 separate Kanäle benutzt, auf denen jeweils bis zu 40 Gbps mit den unterschiedlichsten Datenformaten transportiert werden können
EBK	Eidgenössische Bankenkommission, Aufsichtsbehörde des Bundes für das Bankenwesen
ERT	Emergency Response Teams; auch Computer Emergency Response Teams CERT

Ethernet	Verbreitetste Netztechnologie nach IEEE 802.3 mit dem Netzwerkzugangsverfahren CSMA/CD <GlossarC.htm>. Schicht 2 (Data-Link-Layer) im OSI-Sieben-Schichten-Referenzmodell. Skalierung in 10 Mbit/s, Fast-Ethernet mit 100 Mbit/s und Gigabit-Ethernet mit 1000 Mbit/s
GB	Gigabyte
Hacking	Der Versuch, auf elektronischem Weg unberechtigten Zugriff auf die Informationssysteme eines Dritten zu erhalten
ICT	Information and Communication Technology, siehe IuK
IEC	Die 1906 gegründete International Electrotechnical Commission (IEC) mit Sitz in Genf (Schweiz) ist eine weltweite Organisation, die internationale Standards für elektrische, elektronische und verwandte Technologien erarbeitet und veröffentlicht
IMS	Information Security Management; das übergeordnete Management der Informationssicherheit
IP	Internet Protocol. Die Daten werden in kleine Pakete unterteilt, die einzeln versendet werden. Übergeordnete Transportprotokolle (meistens TCP) sorgen dafür, dass fehlerhafte, verlorene oder nicht reihenfolgetreue Pakete erneut übertragen bzw. in die richtige Reihenfolge gebracht werden
ISO	Die 1946 gegründete International Organization for Standardization (ISO) ist ein weltweiter Zusammenschluss von nationalen Standardisierungsgremien
IuK	Informations- und Kommunikationstechnologie
LAN	Local Area Network; Unternehmensnetzwerk innerhalb einer Lokalität
Log	Lückenlose Aufzeichnung von Transaktionen oder Ereignissen in Form von Log-Dateien, Datenbank-Logs, ...
Malware	Software, die unberechtigterweise in fremde Systeme eingeschleust wird, um dort Schäden zu verursachen, Daten auszuspähen oder Rechenleistung zu missbrauchen; Oberbegriff für Viren, Würmer, Trojaner, ...; siehe auch ↗ Spyware
NAS	Network Attached Storage; Verbindung der Speichersysteme mit dem Netzwerk statt mit den Servern; ermöglicht gleichzeitigen Zugriff auf gleiche Speichersysteme von verschiedenen Servern aus

Risikokarte	Grafische Darstellung von Schadensausmass und Schadenswahrscheinlichkeit
RPO	Recovery Point Objective; in der Vorgeschichte eines Notfalls derjenige Zeitpunkt, auf den mit konsistenten und korrekten Daten zurückgesetzt werden kann
RTO	Recovery Time Objective; der Zeitpunkt, zu dem ein ausgefallenes IT-System mit dem Datenbestand des RPO wieder betriebsbereit ist
SAN	Storage Area Network; Speichersysteme zur Speicherung der Daten getrennt von den Servern, die als eigenständige Systeme im Netzwerk integriert sind
SDH	Synchronous Digital Hierarchy; ein 1988 vom CCITT als weltweiter Standard definiertes Übertragungssystem. SDH beschreibt Übertragungsrahmen auf OSI-Ebene 1 und kann zum Beispiel von ATM als physikalisches Transportmedium genutzt werden. Derzeit sind Schnittstellen für STM-1 bis 155 Mbps und STM-64 bis 10 Gbps definiert
Security Policy	Sicherheitsrichtlinien und -weisungen; Sammlung von aufeinander aufbauenden Richtlinien und Weisungen zum sicheren Umgang mit Informationen im Unternehmen
SLA	Service Level Agreement; detaillierter Vertrag über vereinbarte Dienstleistungen
Social Engineering	Versuch, unberechtigterweise an Zugriffsmöglichkeiten oder Informationen zu gelangen durch Ausspähung des sozialen Umfelds von Mitarbeitern
Sourcing	Quelle des Leistungsbezugs. Welche Leistungen sollten von wem erbracht werden. Alternativen sind: Strategisches Sourcing, einfaches Sourcing und Selektives Sourcing
Spyware	Software, die zum Zweck der Ausspähung von Informationen unberechtigterweise in fremde Systeme eingeschleust wird; häufig in Form von Trojanern anzutreffen
VoIP	Voice over IP; Verfahren zur digitalisierten Übertragung von Sprache über das Internet-Protokoll
VPN	Virtual Private Network; virtuelles, durch Verschlüsselungstechnologie geschütztes, logisch abgeschlossenes Netz auf öffentlichen Trägernetzen
WAN	Wide Area Network; Netzwerk, das sich über öffentlichen Grund erstreckt

10 Autor und BPX



Ulrich Moser

Diplom-Mathematiker

Senior Solution Architect bei der SYSTOR AG, Zürich

Lehrbeauftragter für Informationssicherheit an der
FH Konstanz, Fachbereich Informatik, und
Dozent an der Fachhochschule Beider Basel im
Nachdiplomkurs E-Procurement

ulrich.moser@kujm.de

BPX steht für Best Practice Xperts

Ziel von BPX ist es, schwierige Themen praxisgerecht für das Management aufzubereiten: kurz und prägnant. Auf 80 Seiten finden Manager relevante Entscheidungsgrundlagen, Beispiele, Checklisten sowie Tipps.

www.bpx.ch

Was passiert, wenn in Ihrem Unternehmen die IT ausfällt? Werden Sie Daten verlieren? Sind Sie ausreichend auf diese Situation vorbereitet? Wie lange darf es dauern, bis nach einer Katastrophe alle Prozesse wieder laufen? Und was kostet das?

Worst-Case-Szenario in jedem Unternehmen ist der IT-Crash! Keine Mails, keine elektronischen Verkäufe, Bestellungen oder Transaktionen.

Der Ernstfall kann Unternehmen stark zurückwerfen oder ihnen gar das Genick brechen. Wie hoch ist der Schaden bei einem Teil- oder Totalausfall der Informationstechnologie? Wie lange überlebt Ihr Geschäft ohne eine intakte IT-Umgebung? Wie verhindern Sie den Ernstfall? Welche Prioritäten setzen Sie für die Wiederherstellung? Wie ist ein Wiederanlauf organisiert?

In diesem Booklet finden Sie Antworten auf Fragen, die sich Manager heute stellen müssen. Komplexe Inhalte werden einfach dargestellt und auf den Punkt gebracht.

Checklisten und Praxistipps machen aus diesem Booklet eine wertvolle Informationsquelle und ein übersichtliches Nachschlagewerk.

Rheinfelden/Schweiz
BPX-Edition, 2003/2004

30 CHF, 20 €

ISBN 3-905413-23-X

Editionspartner

 **Telekurs Services**

AC 

