

COMMON Jahreskonferenz 2006

16. bis 18. November 2006 Göttingen



BCM - Anforderungen und Lösungen

Lothar Goecke





- Unternehmensstandort Hamburg
- gegründet 1.4. 2005
- langjährige Beratungserfahrungen
 - Business Continuity / IT-Recovery
 - IT-Sicherheit
 - Service Level Agreements
- bei Großunternehmen und Mittelstand
 - Banken und Versicherungen
 - Industrie und Handel
 - Logistik- und Medienunternehmen
 - Behörden
- Wir helfen unseren Kunden,
 - ihre Geschäftsfähigkeit gegen operationelle Risiken abzusichern
 - und so ihre Wettbewerbsfähigkeit zu verbessern.





Agenda

- Business Continuity Management - Krisenmanagement
- BCM – Bestandteile
- Ausfallrisiken und Wiederanlauf
- Vorgehensmethode und Lösungsmöglichkeiten
- Wiederanlaufpläne



Business Continuity Management

Krisenmanagement



Definition Störung

- Alle Ereignisse, die von Anfang an nicht als Notfall bezeichnet werden, stellen Störungen dar.
- Eine Störung ist ein Ereignis, dessen Schaden innerhalb der kritischen Wiederanlaufzeiten behoben werden kann.
- Eine Störung ist ein in der Regel beherrschbares Ereignis.
- Eine Störung lässt sich durch die Linienorganisation beheben.
- Jede Störung kann in ihrer Entwicklung oder nach Überschreiten der kritischen Wiederanlaufzeiten zu einem Notfall eskalieren.



Definition Notfall

- Ein Notfall tritt ein, wenn innerhalb einer festgelegten Zeit eine Wiederherstellung des Geschäftsbetriebs nicht möglich ist und dies von der verantwortlichen Stelle (Notfallbeauftragter und Krisenstabsleiter, ggf. Leiter der betroffenen Bereiche) festgestellt und eskaliert wird.
- Ein Notfall kann eine eskalierte Störung sein.
- Ein Notfall erfordert i.d.R. ein entsprechendes Krisenmanagement.



Definition Krise

- Eine Krise stellt ein Ereignis dar, welches jederzeit eintreten kann und für das kein Ablaufplan existiert.
- Für eine Krise existieren nur Rahmenanweisungen und -Bedingungen zur Bewältigung.
- Auch eine Krise muss durch den Krisenstab als solche festgestellt werden.
- Eine Krise erfordert immer ein entsprechendes Krisenmanagement.



Vorgehen und Ziele

Status	Kontinuität	Störung	Notfall	Krise
Vorgehen	Handlungsanweisungen zum Betrieb	Handlungsanweisungen zum Störungsmanagement	Handlungsanweisungen zur Notfallbewältigung	Krisenleitfaden
Ziel	optimaler Betrieb	Störungsbehebung	Rückkehr zum Normalbetrieb	Krisenbeherrschung



Beispiele Störung / Notfall / Katastrophe

Katastrophe

- Großflächige Verseuchung mit radioaktiven oder chemischen Substanzen,
- Epidemien.



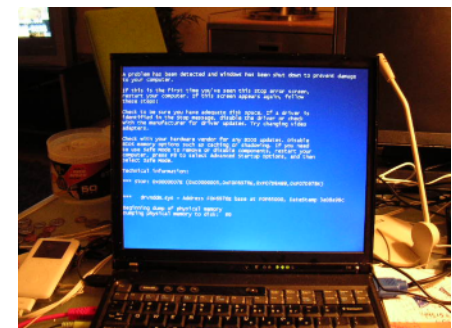
Notfall

- **Ausfall eines Gebäudes, in dem sich zentrale Funktionseinheiten befinden,**
- **der Ausfall eines Rechenzentrums.**



Störung

- Ausfall eines Servers
- Ausfall eines Arbeitsplatzes





Überstandene IT-Notfälle

- According to an article in Contingency Planning, the U.S. Labour Department reports that 43% of the companies that have experienced a disaster never reopen; 29% of the companies that do reopen will close within two years.
- NURS, Norwich Union Risk Service:
bis zu 80 % der Firmen, die keinen Plan haben, überleben die nächsten 18 Monate nach einem Notfall nicht.



Statistik

- 25 % haben keine Business Continuity Plan
- nur 50 % haben den Plan in letzten 6 Monaten gepflegt
- nur 34 % haben den Plan in den letzten 6 Monaten getestet
- **28 % haben einen Notfall erlebt**
- Schadenshöhen pro Tag:
 - < 100.000 \$ bei 50 %
 - < 500.000 \$ bei 14 %
 - > 1.000.000 \$ bei 5 %
- Imageschäden bei 28 %

AT&T 2006 Business Continuity Study
74 % hatten < 500 Mitarbeiter



Business Continuity Management

-

Bestandteile



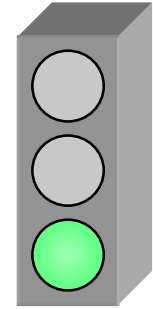
Continuity - Recovery

Continuity	Recovery
bezogen auf Verfügbarkeit und Integrität	
Erhaltung des laufenden Betriebs	Wiederherstellung des Betriebs in Stufen
alle Szenarien	Notfälle
innerhalb gängiger SLAs	Abweichungen akzeptiert
Leben	Überleben

Think big!
Act small!



Business Continuity



Business Continuity (Geschäftskontinuität)



Geschäftsfunktionen



Geschäftsprozesse

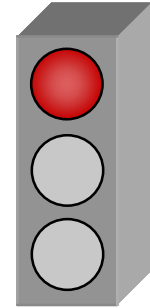
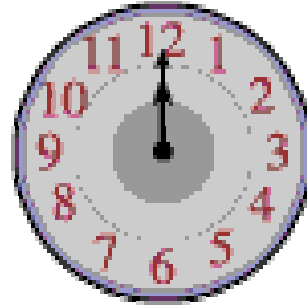


Unterstützende Infrastruktur





Business Continuity



Business Continuity (Geschäftskontinuität)

Geschäftsfunktionen



Geschäftsprozesse



Unterstützende Infrastruktur





Ausfallrisiken verringern
-
**im Notfall einen Wiederanlauf
der Prozesse sicherstellen**



Ausfallrisiken verringern

- Sichere Geschäftsprozesse gewährleisten Kontinuität im Normalbetrieb.
- Sichere Geschäftsprozesse sind
 - fehlertolerant
 - nutzen sichere IT-Infrastruktur (Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit)
- Wiederanlaflösungen gewährleisten Kontinuität nach Notfällen.
- Wiederanlaflösungen basieren auf Wiederanlaufzielen



Verfügbarkeitsziele und Wiederanlaufziele

Verfügbarkeitsziele

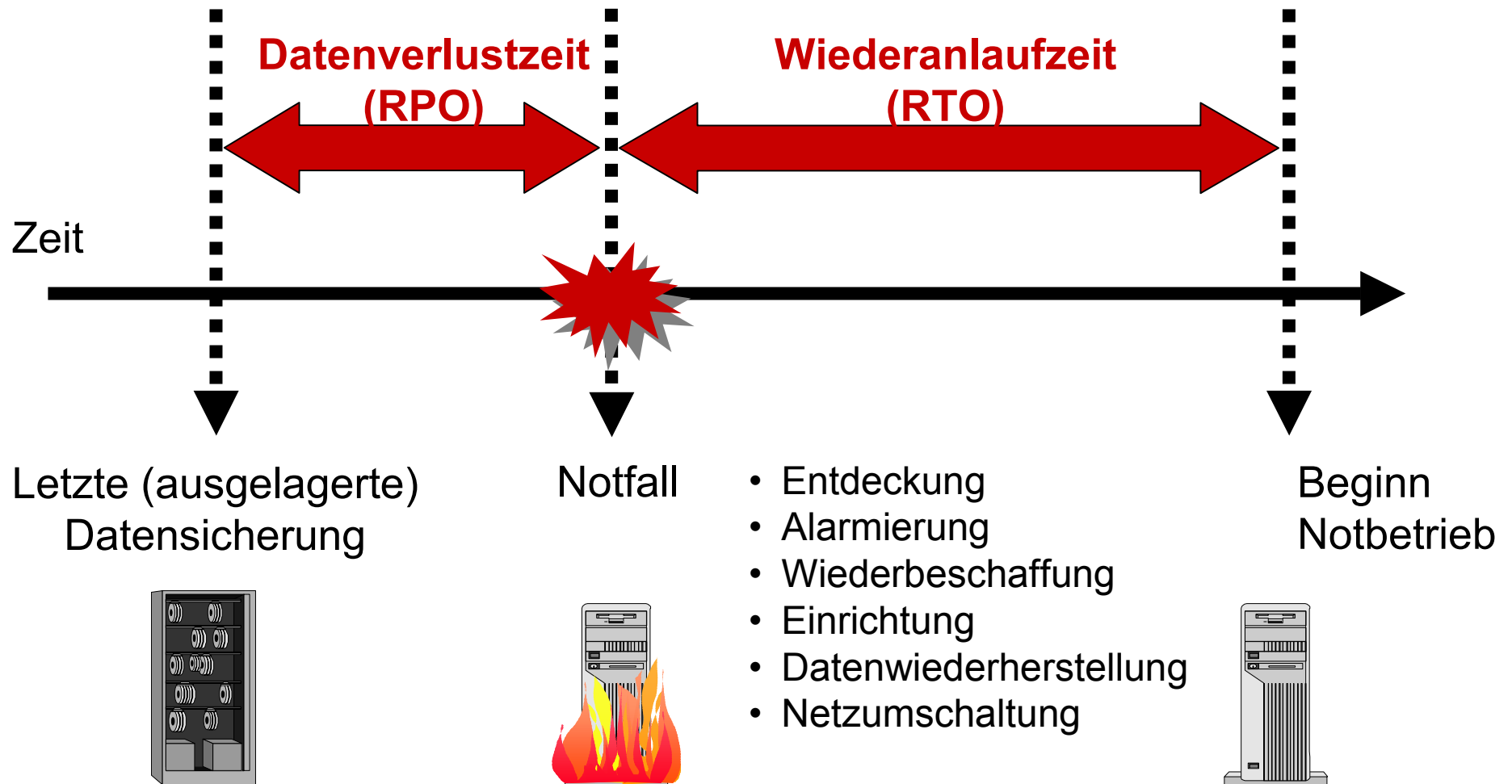
- Beschreibung des Services (Umfang, Dauer, Orte usw.)
- und dessen Einschränkungen, den die IT einer Anwendung (einer Geschäftsfunktion oder Teilen davon) unter Berücksichtigung möglicher auftretender Störungen bietet.

Wiederanlaufziele

- Wiederanlaufziele sind Teil der Verfügbarkeitsziele. Sie beschreiben die Verfügbarkeitsziele für den Geschäftsprozess nach einem Ausfall:
 - Ausfallzeit
 - Datenverlustzeit
 - Einschränkungen im Notbetrieb



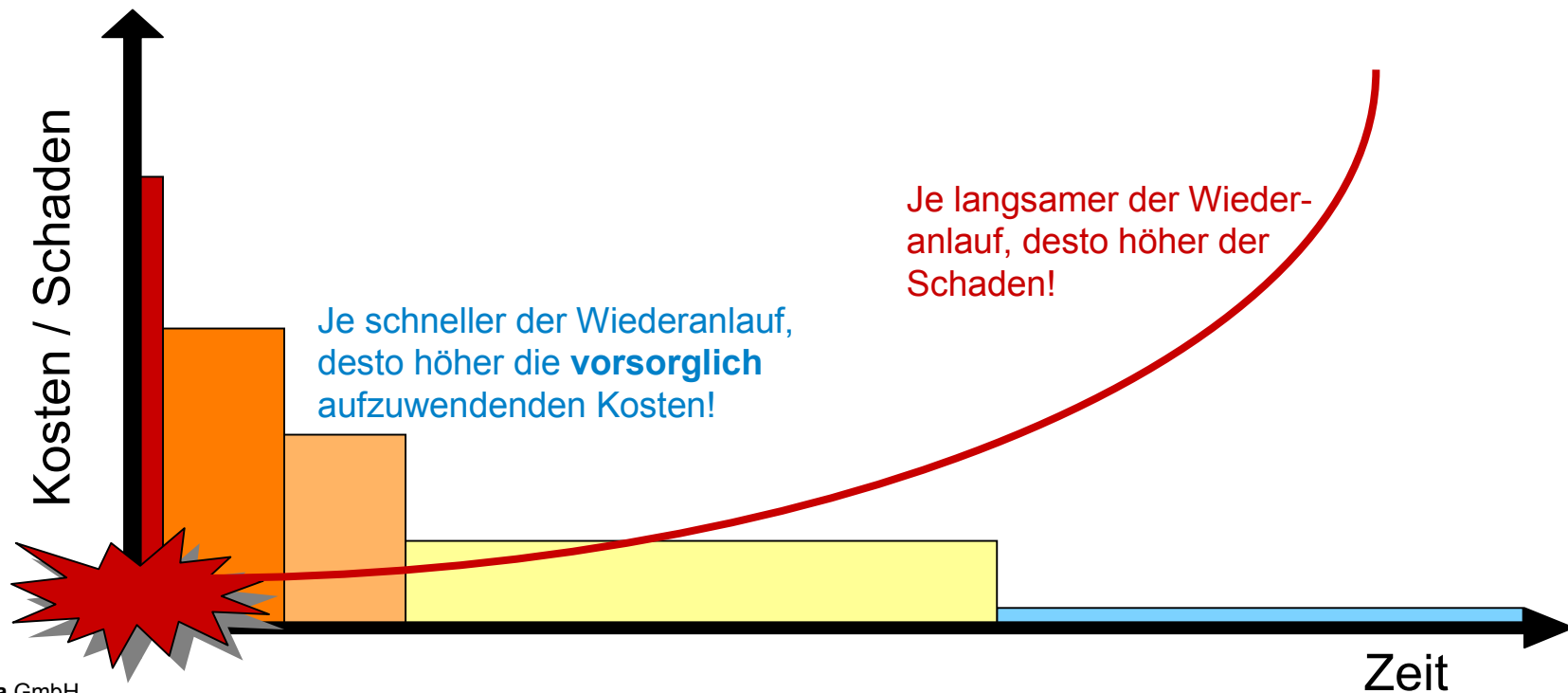
Wiederanlaufanforderungen





Wiederanlaufklassen

WAK	Bewertung	Wiederanlaufzeit	Datenverlustzeit
1	extrem zeitkritisch	0 Stunden	0 Stunden
2	sehr zeitkritisch	24 Stunden	24 Stunden
3	zeitkritisch	48 Stunden	
4	weniger zeitkritisch	7 Tage	
5	nicht zeitkritisch	keine Festlegung	





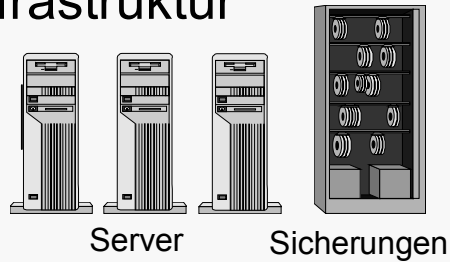
Typisches IT-Notfallszenario



RZ-Fläche und Versorgungseinrichtungen



IT-Infrastruktur



LAN / Campusnetz



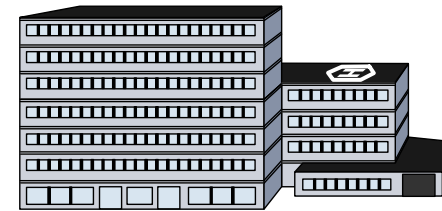
WAN



Kommunikationspartner



Produktion, Lager,
Bürogebäude



Mitarbeiter(innen)



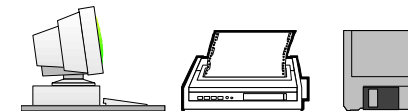
Arbeitsmittel



Arbeitsplätze
Dokumente



Kommunikation



Arbeitsplatz-IT



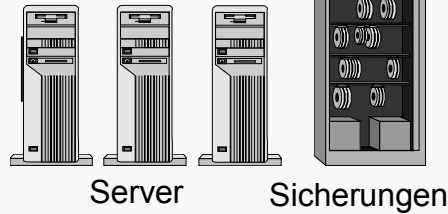
Typisches Szenario Gebäudeausfall



RZ-Fläche und Versorgungseinrichtungen



IT-Infrastruktur



LAN / Campusnetz



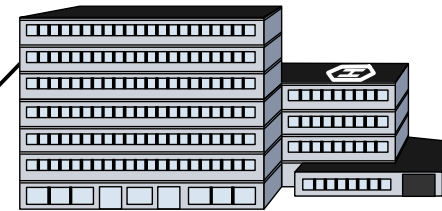
WAN



Kommunikationspartner



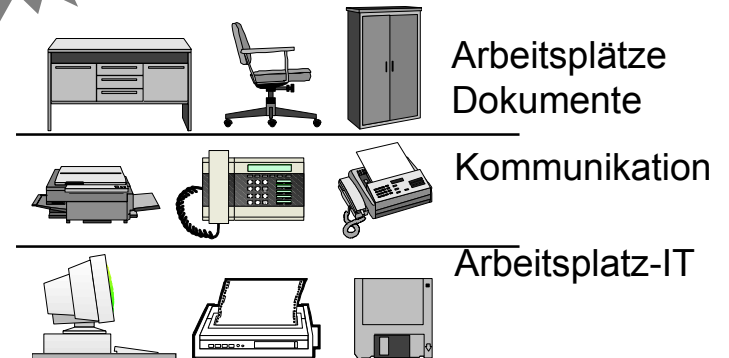
Produktion, Lager,
Bürogebäude



Mitarbeiter(innen)



Arbeitsmittel





Vorgehensmethoden - Lösungsmöglichkeiten



Vorgehen Überblick

Grobkonzept Business



Grobkonzept IT-Wiederanlauf



Realisierung



Business-
Notfallhandbuch

Notfall-
handbücher

IT-
Notfallhandbuch

Testen

Übungen



Projekthinhalte


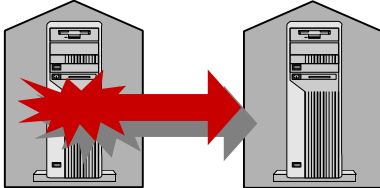
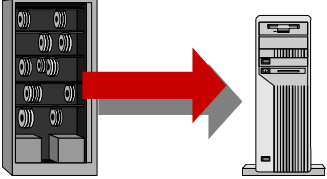
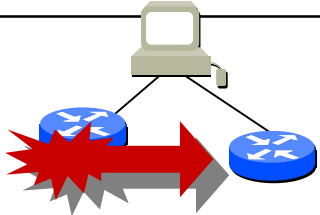
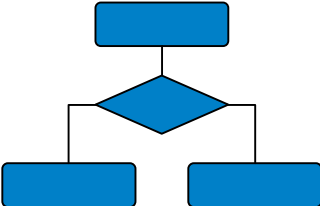
Wiederanlauffähigkeit absichern / herstellen

- Notfallszenarien festlegen
- Mögliche Schäden betrachten
- Wiederanlaufanforderungen festlegen
- vorhandene Lösungen bewerten
- Handlungsbedarf darstellen
- Restrisiken akzeptieren
- Maßnahmen planen






Komponenten der Lösung 1

Komponenten	
Notfallorganisation	<ul style="list-style-type: none">• Krisenstab• Notfallteam(s) 
Zentrale IT-Services	<ul style="list-style-type: none">• Ausweichstandorte• IT-Systeme 
Datensicherung	<ul style="list-style-type: none">• Datensicherung• Auslagerung• Datenwiederherstellung 
Datenkommunikation	<ul style="list-style-type: none">• Netzumschaltung auf Ausweichstandorte 
Notfallverfahren	<ul style="list-style-type: none">• Alarmverfahren• Ersatzverfahren• Wiederanlaufverfahren 

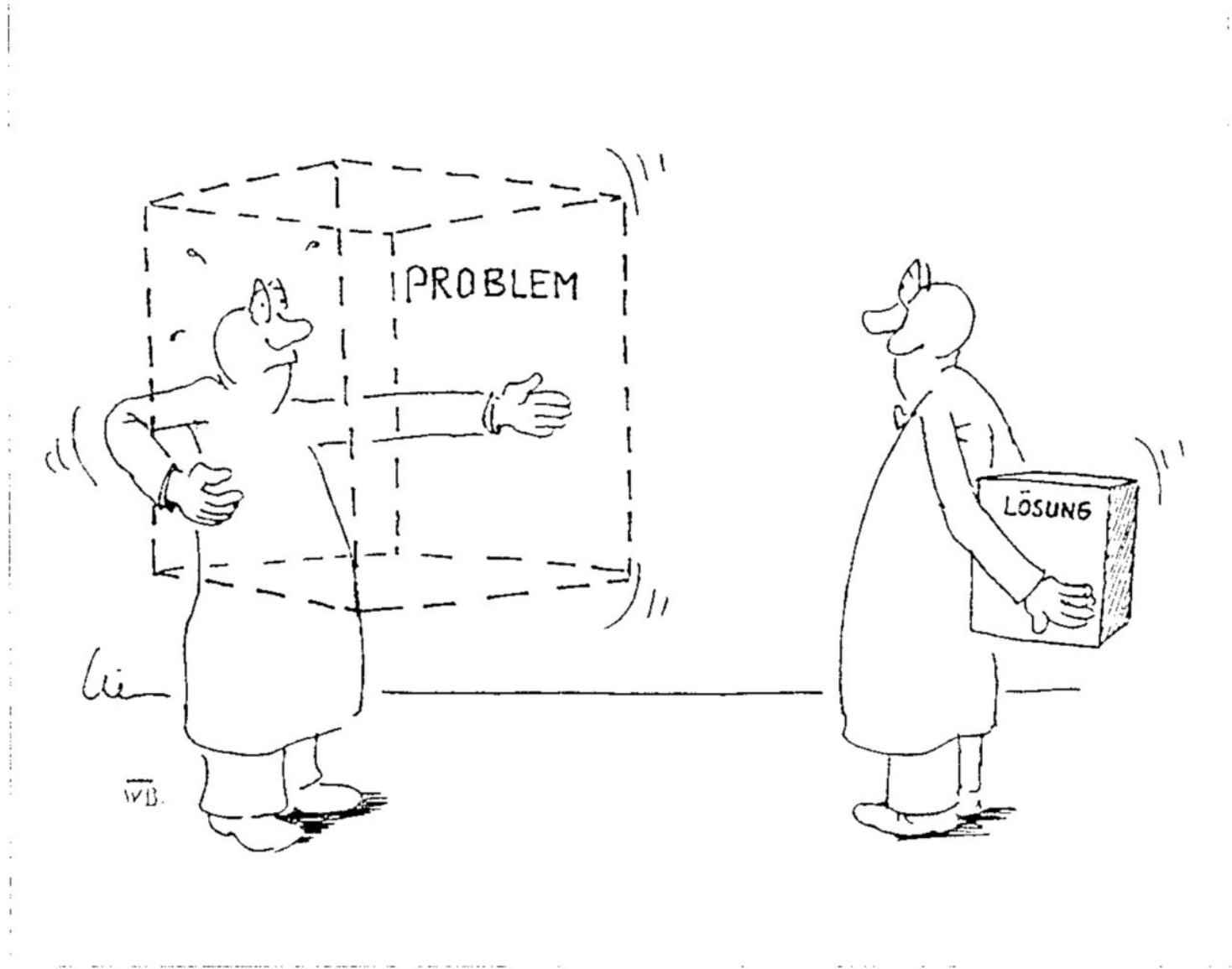


Komponenten der Lösung 2

Komponenten	
Dokumentation (Notfallplan)	<ul style="list-style-type: none">• Einleitung• Notfallorganisation• Alarmierung• Wiederanlaufverfahren• Zusatzinformationen• Address und Telefonverzeichnisse• Wiederanlaufziele und –ressourcen 
Änderungsdienst	<ul style="list-style-type: none">• Änderungen der IT• Betriebliche Änderungen
Überprüfung	<ul style="list-style-type: none">• Teststufen• Testplan• Testkalender• Testdurchführung



Lösungsmöglichkeiten





Entfernungen

- Es gibt keine gesetzlichen Vorgaben für „sichere“ Entfernungen
- SUNGARD hat bis 9/11 gesagt 500 Meter
- IBM empfiehlt 2 Meilen

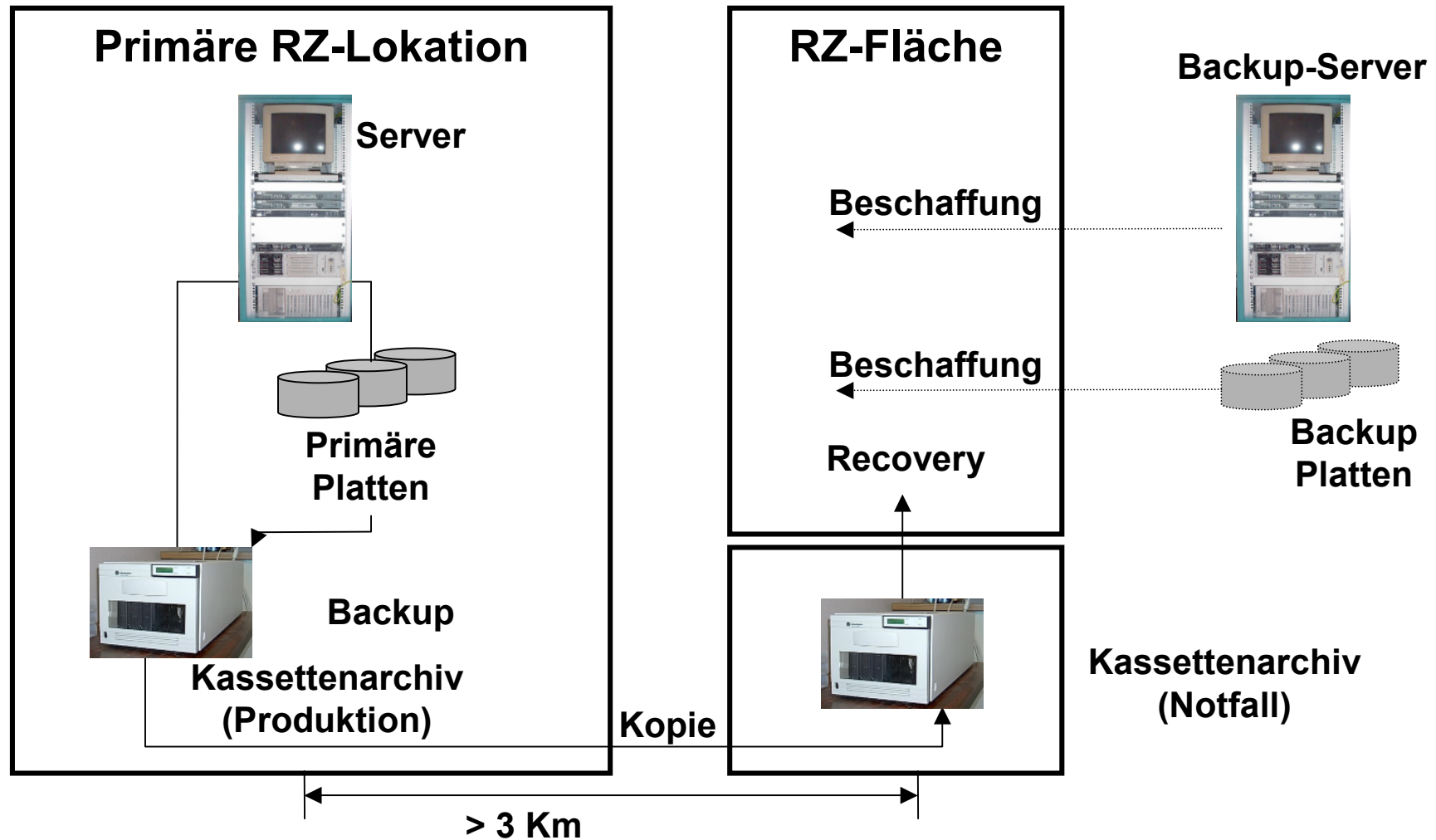


Backup-Arten

- Heißes, warmes oder kaltes Backup
- Stationäres oder mobiles Backup
- Eigene Lösung oder Dienstleister
- Beschaffung oder Vorhaltung der Betriebsmittel
- Verfügbarkeit der Daten
- Verfügbarkeit der IT-Systeme
- Netzwerk vermascht oder Netzumschaltung

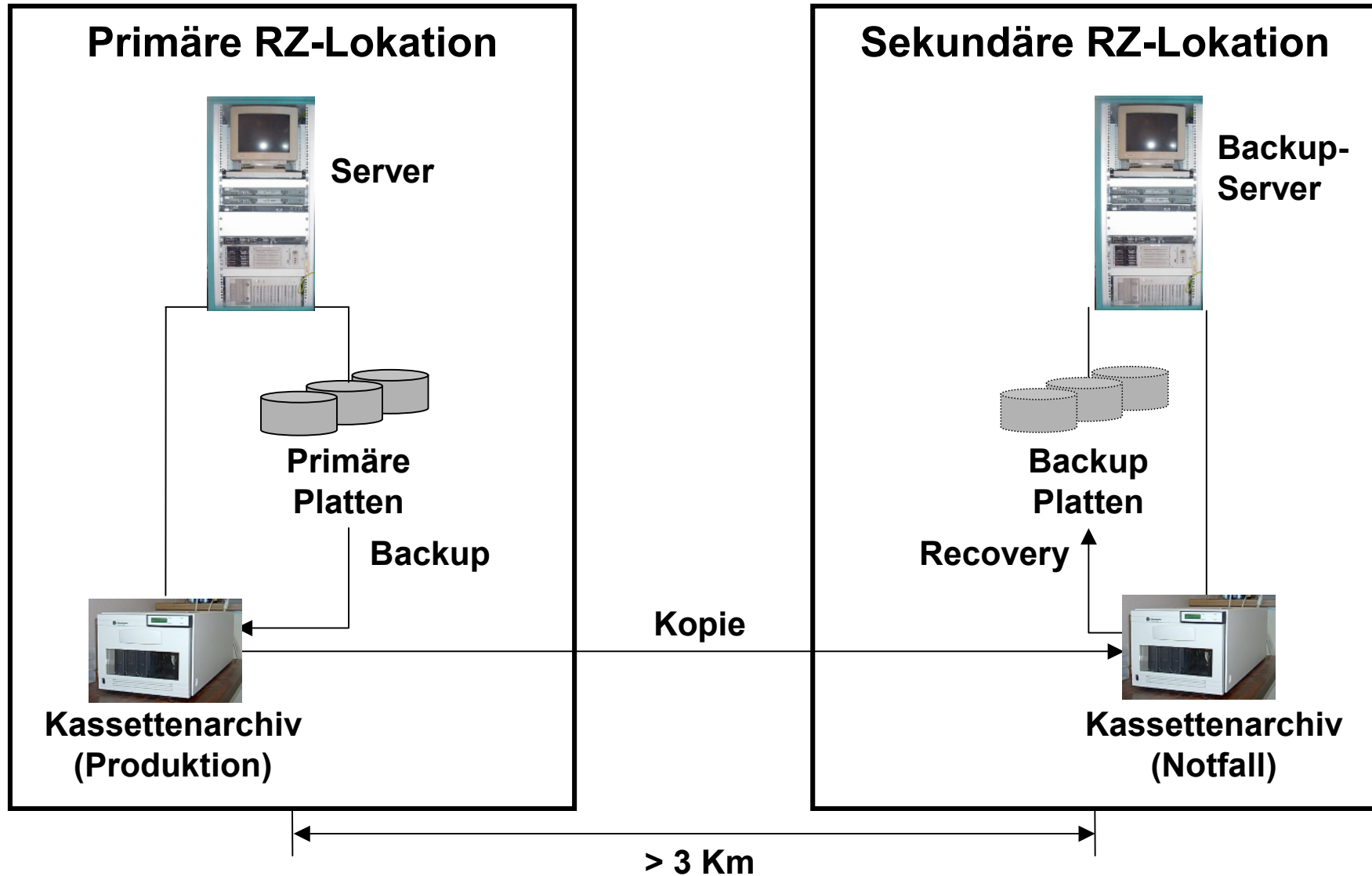


Technik - Kalter Wiederanlauf



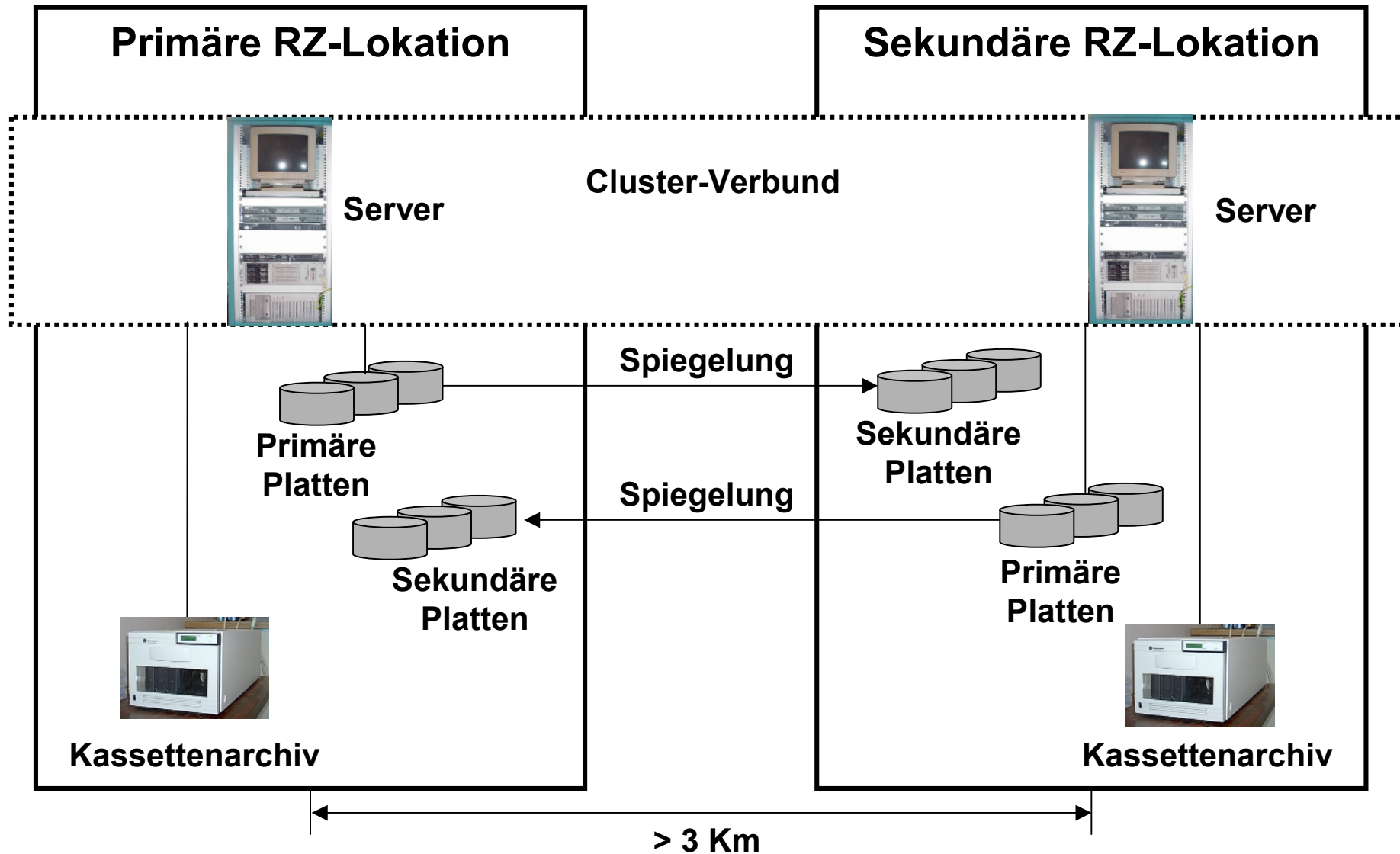


Technik - Warmer Wiederanlauf



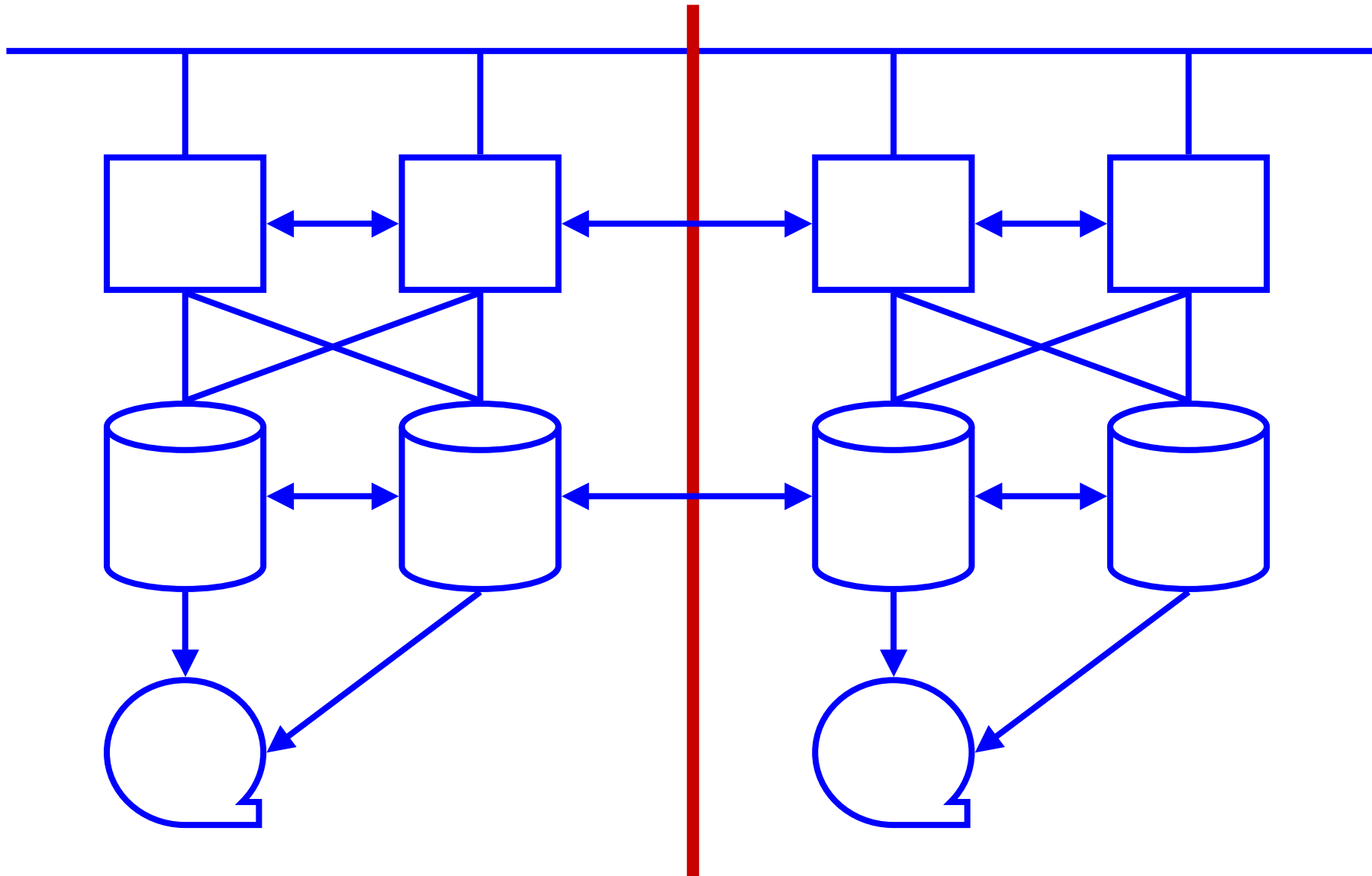


Technik - Heißer Wiederanlauf





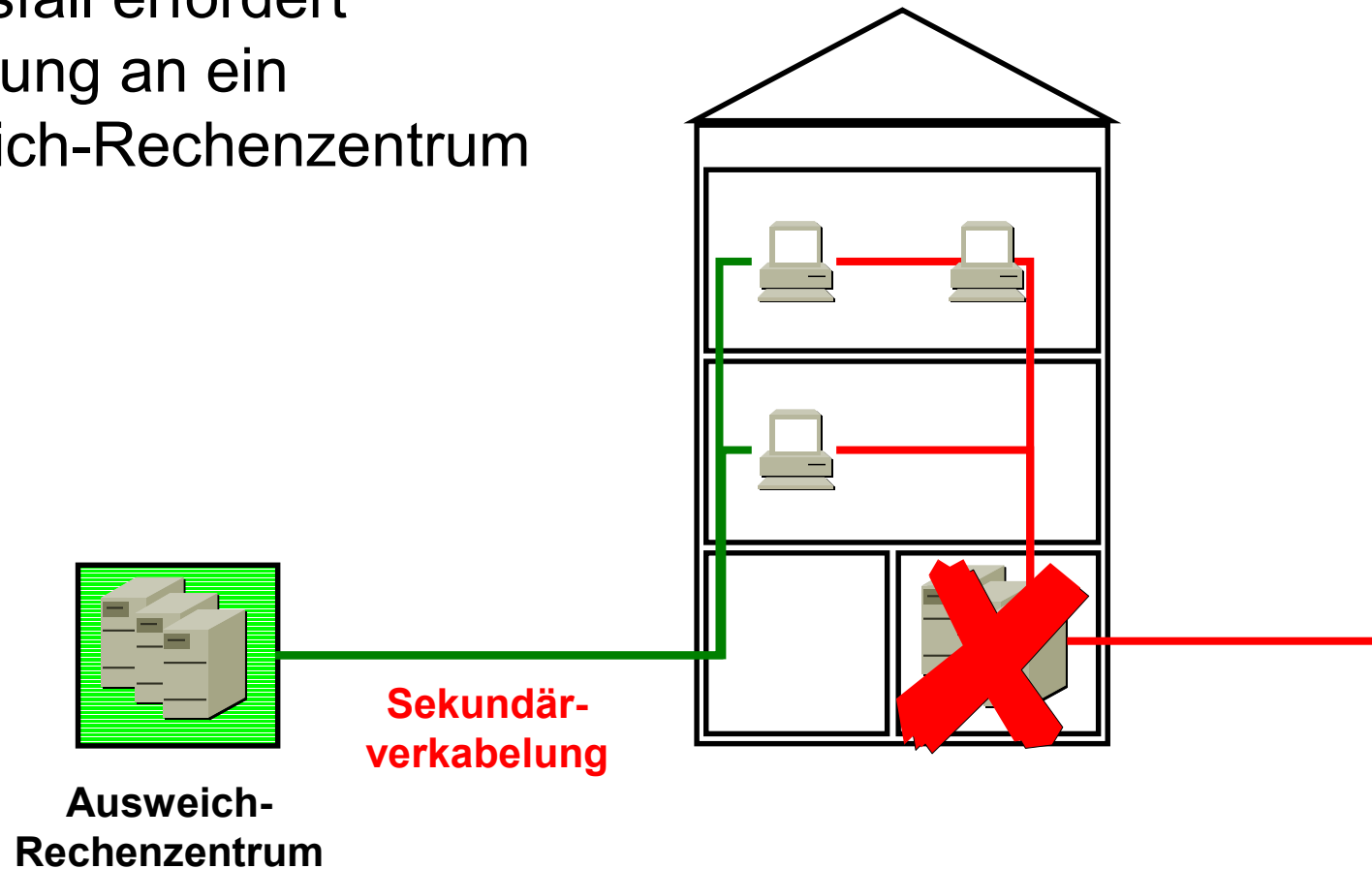
Was ist eigentlich **HOCHVERFÜGBAR** ?





Anbindung an ein Ausweich-Rechenzentrum

RZ-Ausfall erfordert
Anbindung an ein
Ausweich-Rechenzentrum





Wiederaanlaufpläne



Notfallhandbücher

- Handbuchstrukturen
- Alarmierung
- Schnittstelle zum Krisenmanagement
- Notfallorganisation
- Besetzung der Notfallteams
- Aktivitätenpläne
- Wiederanlaufziele
- Ressourcen
- Kontakte



Mustergliederung BC-Plan

1	Einleitung	5	Zusatzinformationen
1.1	Vorwort zum BC-Plan	5.1	Anfahrtspläne
1.2	Änderungsnachweis	5.2
1.3	Abkürzungsverzeichnis		
1.4	Pflege- und Änderungsdienst	6	Adress- und Telefon-Verzeichnisse
1.5	Mitgeltende Dokumente	6.1	Mitarbeiterliste
		6.2	Standorte
2	Notfallorganisation	6.3	Dienstleister
2.1	Notfallteams		
		7	Wiederanlaufziele und Ressourcen
3	Alarmierung / Eskalationsverfahren	7.1	Allgemeine Beschreibung der Wiederanlaufstrategie
		7.2	Wiederanlaufklassen
4.	Wiederanlauf der Geschäftsfunktionen (je Notfallteam ein Kapitel)	7.3	Mindestressourcen
4.1	Ausweichstandorte		
4.2	Erste Aktivitäten am Ausweicarbeitsplatz		
4.3	Notbetrieb		
4.3.1	Ersatzverfahren		
4.3.2	Abweichungen gegenüber dem Normalbetrieb		
4.3.3	Zusätzliche Tätigkeiten im Notbetrieb		
4.4	Für den Notbetrieb benötigte Dokumente und Formulare		

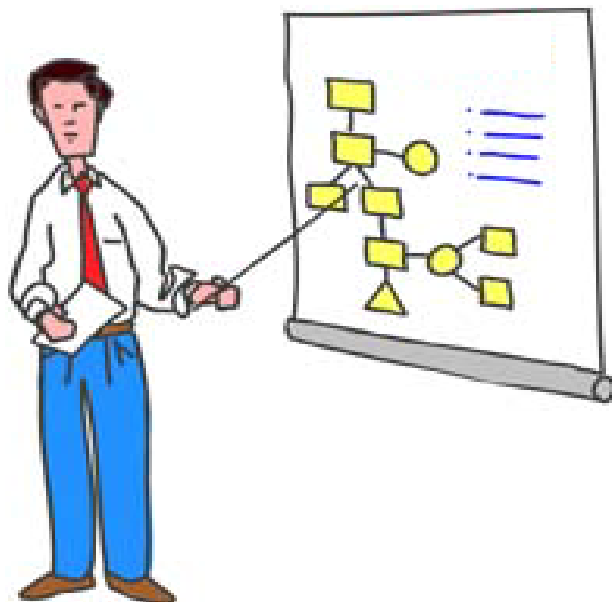


Mustergliederung Infrastruktur-Plan

- | | | | |
|-----|--|-----|---|
| 1 | Einleitung | 5 | Zusatzinformationen |
| 1.1 | Vorwort zum IT-Plan | 6 | Adress- und Telefon-Verzeichnisse |
| 1.2 | Änderungsnachweis | 6.1 | Mitarbeiterliste |
| 1.3 | Abkürzungsverzeichnis | 6.2 | Standorte |
| 1.4 | Pflege- und Änderungsdienst | 6.3 | Dienstleister |
| 1.5 | Mitgeltende Dokumente | | |
| 2 | Notfallorganisation | 7 | Wiederanlaufziele und Ressourcen |
| 2.1 | Notfallteams | 7.1 | Allgemeine Beschreibung der Wiederanlaufstrategie |
| 3 | Alarmierung / Eskalationsverfahren | 7.2 | Wiederanlaufklassen |
| | | 7.3 | Konfigurationen |
| 4. | Wiederanlauf der Infrastruktur
(je Notfallteam ein Kapitel) | | |
| 4.1 | Ausweichstandorte | | |
| 4.2 | Rekonstruktion Hardware | | |
| 4.3 | Rekonstruktion Betriebssystem | | |
| 4.4 | Datenrücksicherung | | |
| 4.4 | Anwendungsfreigabe | | |



Vielen Dank für Ihre Aufmerksamkeit!



Dipl.-Math.

Lothar Goecke

Geschäftsführer

consequa GmbH
Süderstraße 73
20097 Hamburg
www.consequa.de

Tel.: 040 / 78 89 70 62
Fax: 040 / 78 89 70 66
Mob: 0171 / 863 50 17
lothar.goecke@consequa.de