becom

Ihr Lösungs-Architekt

Angemessene Störfallvorsorge

Kundenveranstaltung VM/VSE IS-Leiter Kolloquium
25.11. - 26.11.2004 / Bad Reichenhall

Rudolf Wanner
Business Analyst

becom Informationssysteme GmbH
25. November 2004

becom

Ihr Lösungs-Architekt

Es ist besser, Deiche zu bauen, als darauf zu hoffen, dass die Flut allmählich Vernunft annimmt.

(Zitat: Hans Kasper (*1916), dt. Schriftsteller u. Hörspielautor, Quelle: www.zitate.de)

Agenda

1 IT-Störfälle und Folgen

2 Was kann man tun?

3 Was ist angemessen?

Ihr Lösungs-Architekt

Mögliche Bedrohungen

Unternehmen jeder Größenordnung sind zunehmend internen und externen, positiven und negativen Stressfaktoren und damit Geschäftsrisiken ausgesetzt, auf die sie flexibel und schnell reagieren können müssen.

Umwelt
- Naturkatastrophen
- Arbeitsbedingungen

Gesellschaft
- Terrorismus
- Cyber-Attacken
- Sabotage

Politik
- Gesetze/Regularien
- Rechtsprechung
- Deregulierung

Technologie
- Höhere Durchdringung
- Zunehmende Komplexität
- Innovationen und Trends

Wirtschaft
- Globalisierung
- Partner/Zulieferer
- Nachfrageschwankungen

Ihr Lösungs-Architekt

Mögliche Bedrohungen

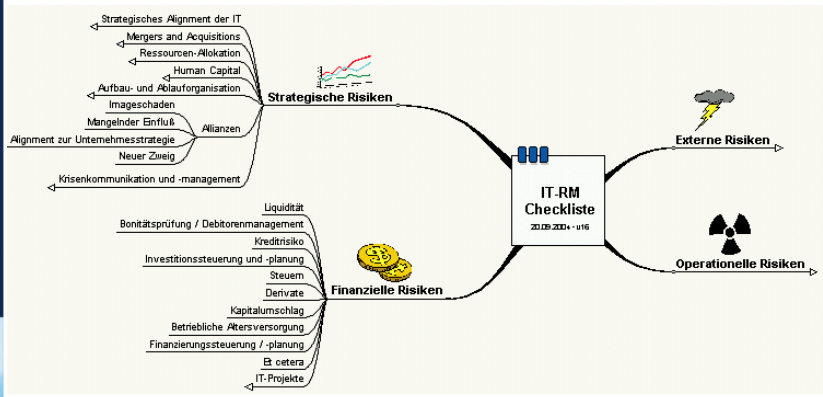
Infrastruktur und Technik	Menschen		Höhere Gewalt	
	Mitarbeiter	Externe	Witterung	Katastrophen
• Funktionsstörung, Defekt, Ausfall von: –HW/SW –Verkabelung • Stromausfall, Überspannungen, Erdungsproblem, Kabelbrand • Ausfall der Klima-anlage • Verlust der Kommunikations-verbindung	• Computerviren • Missbrauch, Betrug • Diebstahl • Sabotage • Unachtsamkeit, Unwissenheit • Menschl. Versagen • Zutrittssperre, Evakuierung • Fluktuation	• Computerviren • Hacking • Terroranschlag • Missbrauch • Einbruch • Diebstahl • Sabotage • Spionage • Beschlagnahm-ung • Vandalismus	• Kälte / Frost • Schnee • Wassereinbruch • Unwetter, Sturm, Hochwasser, Erdrutsch • Blitzschlag • Spannungs-schwankungen • Verlust der Verkehrsver-bindungen	• Hochwasser, Überschwem-mung • Feuer Rauchgase • Chemische Kontamination • Erdrutsch, Erdbeben • Flugzeug-absturz, Verkehrsunfall • Explosion

Externe Quellen

Interne Quellen

Ihr Lösungs-Architekt

Mögliche Risiken



Ihr Lösungs-Architekt

Basel II und die Auswirkungen auf die IT-Welt

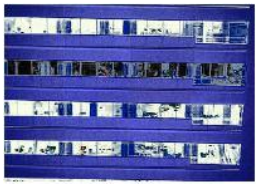
Rechte & Pflichten – Basel II

BASEL II (Auszug)

Verluste aufgrund von Beschädigungen oder des Verlustes von Sachvermögen durch Naturkatastrophen oder andere Ereignisse	Katastrophen und andere Ereignisse	Verluste durch Naturkatastrophen Personenschäden aufgrund von externen Ereignissen (Terrorismus, Vandalismus)
Verluste aufgrund von Geschäftsunterbrechungen oder Systemausfällen	Systeme	Hardware Software Telekommunikation Versorgungsausfall/-störung
Verluste aufgrund von Fehlern bei der Geschäfts-abwicklung oder im Prozessmanagement; Verluste aus Beziehungen mit Geschäftspartnern und Lieferanten/Anbietern	Erfassung, Abwicklung & Betreuung von Transaktionen	Kommunikationsstörungen Fehler bei der Dateneingabe, -pflege- oder -speicherung Überschreiten eines Termins oder Nichterfüllung einer Aufgabe Fehlerhafte Anwendung von Modellen/Systemen Buchführungsfehler / falsche Prozesszuordnung Fehler bei der Durchführung sonstiger Aufgaben Fehlerhafte Lieferung Fehlerhafte Verwaltung von Besicherungsinstrumenten Pflege der Referenzdaten
	Überwachung und Meldung	Nichteinhaltung der vorgeschriebenen Meldepflicht Ungenauer externer Bericht (Schaden eingetreten)
	Kundenaufnahme und -dokumentation	Freigabe durch Kunden/Haftungsausschluss fehlt Rechtsdokumente fehlen/unvollständig
	Kundenkontoführung	Ungenehmigter Zugriff auf Konten Fehlerhafte Kundenunterlagen (Schaden eingetreten) Fahrlässiger Verlust/Beschädigung von Kunden-Vermögenswerten
	Geschäftspartner	Fehlerhafte Erfüllung durch Geschäftspartner (Nicht-kunden) Verschiedene Unstimmigkeiten mit Geschäftspartnern (Nichtkunden)
	Lieferanten und Anbieter	Outsourcing Unstimmigkeiten mit Lieferanten

Was ist ein Störfall?

Ein Brand legt Ihr Produktions-RZ lahm



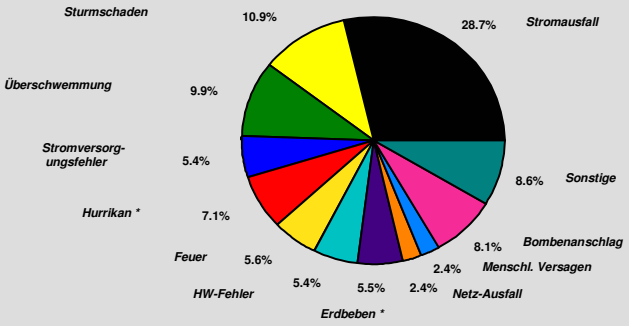
Eine wichtige Abteilung bzw. Kernanwendung ist ausgefallen

Eine Betriebsstörung eskaliert zu einer Katastrophe

=> Ein kritischer Dienst ist nicht mehr verfügbar!

Ihr Lösungs-Architekt

Ursachen für Notfälle



Quelle: Contingency Planning Research Base (USA)
Basis: 4,635 Notfälle seit 1982 (* = für Deutschland nicht/wenig wahrscheinlich)

„Einer Studie der Münchner Rückversicherung zu folge, gab es im Jahre 2000 weltweit 850 Naturkatastrophen. Das sind 100 mehr als im Jahre 1999 und über 200 mehr als der Durchschnitt der 90er Jahre“

Münchner Abendzeitung, 13. Mürz 2001

Auswirkungen von Störfällen

Produktivität
- Anzahl der Mitarbeiter, die aufgrund des Ausfalls nicht arbeiten können

Imageverlust
- Kunden
- Lieferanten
- Business Partner
- etc.

Umsatz
- direkte Umsatzverluste
- zukünftige Umsätze
- Verluste durch nicht auslösbare Rechnungen
- Verluste durch nicht getätigte Investitionen

Finanzen
- Umsatzerwartung
- Cash flow
- verlorene Rabatte
- Zahlungsverpflichtungen
- Börsenkurs
- etc.

Sonstige Kosten
- temporäre Mitarbeiter
- Reisekosten
- Mietkosten
- etc.

Zusammensetzung der Kosten bei einem Ausfall

Haftung im Notfall

Gesetzgebung

- BGB, allgemeine Regeln für die Haftung von Arbeitnehmern und Geschäftsführung
- KonTraG, Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
  - Inkrafttreten 1.5.1998: Verpflichtung des Vorstandes
    - Einrichtung eines Überwachungssystems zur frühzeitigen Erkennung bestandsgefährdender Entwicklungen
    - Etablierung Schadensverhütungsaktivitäten, insb. Notfallplan
- Bundesaufsichtsamt für Kreditwesen (EDV-Systemwiederanlauf innerhalb 48h)
- Bundesdatenschutzgesetz

Betriebliche Schutzbedürfnisse

- Datensicherheit
- Revisionsfähigkeit

Konsequenzen

- Eine nicht etablierte K-Vorsorgelösung wird dem RZ-Leiter und dem zuständigen Geschäftsführer im K-Fall als ***grobe Fahrlässigkeit*** ausgelegt
- Uneingeschränkte Haftung für den Geschäftsführer und volle Haftung, mit eventueller Haftungs-privilegierung, für den Arbeitnehmer

Quelle: Dr. Joachim Schrey, EDV-Rechtsexperte

Agenda

1 IT-Störfälle und Folgen

2 Was kann man tun?

3 Was ist angemessen?

IT - Service Continuity Management

- Definition von Verfügbarkeitsanforderungen in SLAs und Implementierung entsprechender Verfügbarkeitsmanagement Restart/Recovery Prozesse
- Risikominimierung, Minimierung möglicher Störfälle,
  - Nicht jede externe oder interne Gefährdung führt zu einer Störung des IT Betriebes
- Erhöhung der Widerstandsfähigkeit der Systeme (Fehlertoleranz)
  - Nicht jede Störung führt zu einem Ausfall von IT Services
- Anpassung der möglichen Ausfallzeiten an das 'erträgliche Maß'
  - Nicht jeder Ausfall wird zu einem Notfall
- Erarbeitung Katastrophenvorsorge-Planung
  - Nicht jeder IT-Notfall wird zur Katastrophe für das Unternehmen

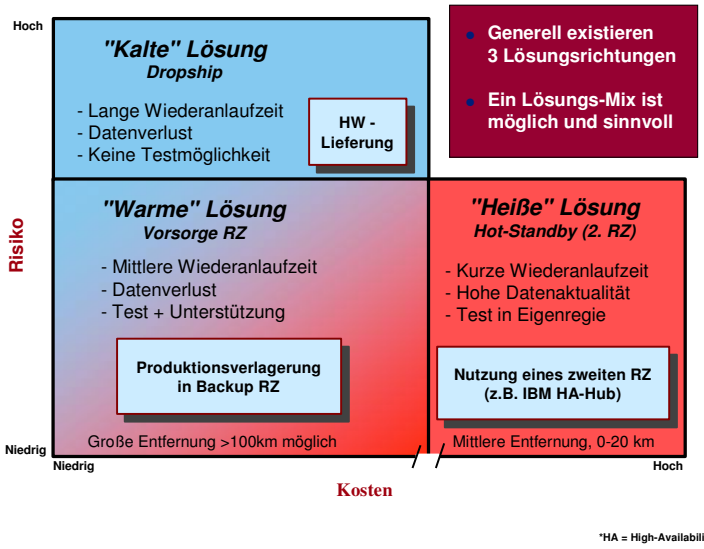
Hochverfügbarkeit ist möglich, Angemessene Vorsorge ist wirtschaftlich!

Die Services sollen nach **Plan in der benötigten Zeit** wieder verfügbar sein!

Bestandteile der Vorsorge

- **Organisatorische Vorsorge**
  - Prozesse
  - Dokumentation (Notfallhandbuch)
  - Schulungen und Übungen
  - Klare Verantwortlichkeiten
  - Ressourcenbereitstellung für die Planung
- **Technische Vorsorge**
  - Systemauslegung (Redundanzen)
    - IT-Komponenten
    - Rechenzentrum

Technische Vorsorge

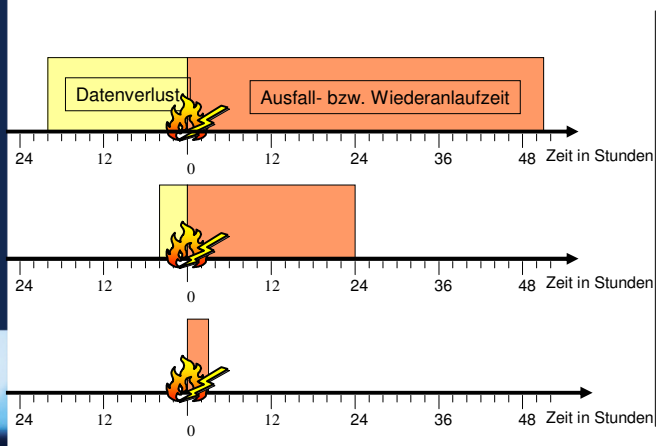


*HA = High-Availability

Technische Vorsorge

	„Kalte“ Lösungen	„Warme“ Lösungen	„Heiße“ Lösungen
Lösungsrichtung	Drop Ship	Vorsorge RZ	Hot-Standby
ealisierbare Wiederanlaufzeit	>48 h	24h – 48h	<4h
Datenaktualität	Vortag	Vortag bzw. n Stunden	aktuell
Restrisiko	hoch, da ungetestet und Wiederanlaufzeit ungewiß	niedrig trotz shared Ressources, da Backup mehrfach in Europa vorhanden	niedrig, abhängig von Abstand der 2 RZs
Voraussetzungen	Infrastruktur ist im Notfall verfügbar	Netzwerkanbindung zum VRZ	2. RZ, Backuphardware, Spiegelung
Wiederanlaufverfahren	Restore von Kassette	Restore von Kassette	automatisches oder manuelles Umschalten
Investitionskosten	gering	gering - mittel	mittel - hoch
laufende Kosten	sehr gering	gering - mittel	mittel - hoch
Anwendungen	unkritische Anwendungen	kritische Anwendungen mit mittlerer Wiederanlaufzeit	sehr kritische Anwendungen mit schneller Wiederanlaufzeit

Wideranlaufzeit vs. Datenverlust



Mögliche Lösung

Dropship,
Restore von Kassette

Vorsorge RZ +
Restore von Kassette,
Datenaktualisierung
(Forward Recovery)

Plattenspiegelung,
Hot-Standby,
High Availability (HA)

*bei den angegebenen Zeiten handelt es sich um Beispiele

Notfallhandbuch

- **Wenn Sie <u>keinen</u> Notfallplan haben, vergeht kostbare Zeit !!!!**

Was kostet das ?

Wen erreichen Sie wo?

Wer sitzt im Krisenstab ?

Was genau ist zu tun?

Welche Sofortmaßnahmen sind zu erledigen ?

Welche Anbieter gibt es?

Wo ist der Vertreter des Spezialisten ?

Welches Notverfahren / welche Ausweichlösung Könnte installiert werden ?

Agenda

1 IT-Störfälle und Folgen

2 Was kann man tun?

3 Was ist angemessen?

Ihr Lösungs-Architekt

Schlüsselfragen für die Notfallvorsorge

- Wie ist der K-Fall für das Unternehmen definiert?
- Was sind die kritischen und unkritischen Geschäftsprozesse bzw. Anwendungen?
- Was sind die Auswirkungen auf die Geschäftsprozesse (Schadenspotential)?
- Wie schnell muss die Produktion wieder laufen?
- Wie aktuell müssen die Daten sein?
- Wie sind die Datensicherungs- und Archivierungsverfahren zu erweitern?
- Welche zusätzlichen kritischen Ressourcen sind zu betrachten und zu schützen?
- Was kann zur Vermeidung des K-Falles und Risikominderung getan werden?
- Wie sind die bereits getroffenen Maßnahmen zur K-Vorsorge zu beurteilen?
- Wieviel muss bzw. sollte in eine K-Vorsorgelösung investiert werden?

Ihr Lösungs-Architekt

Von der Risikoanalyse zur Strategie

Notwendige Analysen der IST Situation:

- Konkretes Risiko
  - Welche Bedrohungen existieren?
  - Wie kann man sich schützen?
- Schadenspotential
  - Welche finanzielle Schäden drohen bei Ausfall?
  - Welche unwägbare Schäden?
- Status der Vorsorge
  - Ist ein Wiederanlauf möglich?
  - Wie lange würden die Systeme ausfallen?

Ziel ist die Formulierung einer Unternehmensstrategie bzgl. der Notfallvorsorge:

- Welche IT-Prozesse und Ressourcen sind kritisch?
- Wie schnell muß ein Wiederanlauf möglich sein?
- Wieviel Datenverlust ist tolerierbar?

IT-Risikomanagement – Risikoanalyse

- **Identifikation des IT-Service Portfolio**
  - **Welche IT-Services gibt es?**
    - Service Level Management (Profit Center)
    - Allgemeine Services ohne Agreement
    - Nicht wahrgenommene Services
  - **Welche Qualitätsmaßstäbe gelten für IT-Services?**
    - Verfügbarkeit am Benutzerarbeitsplatz
    - SLA´s
    - „IT muss immer laufen“

IT-Risikomanagement – Risikoanalyse

- **Identifikation der IT-Service Infrastruktur**
  - **Welche Systeme bilden welchen IT-Service**?
    - IT-Systeme (Router, Switche, Appliances, Mainframe, Server,...)
    - Abhängigkeiten
    - Umgebung (Strom, Klima, RZ, Verkabelung)
    - Dienstleistungen (externer Dienstleister)
  - **Wie verfügbar sind die Einzelsysteme?**
    - Widerstandsfähigkeit (äußere Bedrohung)
    - Fehlertoleranz (technische Fehler)
    - Redundanzen, Auslegung
    - Wartungsverträge

IT-Risikomanagement – Risikoanalyse

- **Identifikation der IT-Serviceverfügbarkeit**
  - **Wie verfügbar ist der IT-Service?**
    - Können SLA´s eingehalten werden?
    - Room for improvement?

IT-Risikomanagement – Risikoanalyse

- **Identifikation der Desaster-Recovery-Verfahren**
  - **Welche Desaster-Recovery-Verfahren greifen für welchen IT-Service?**
    - Backup Rechenzentren, Hot-Standby, Cold-Standby
    - Datensicherungsverfahren (Backup/Restore)
    - Notfallabkommen, Wartungsverträge mit Herstellern
  - **Wie sind diese Desaster-Recovery-Verfahren dokumentiert?**
    - Lagerort bzw. Speicherort der Dokumentation
    - Form der Dokumentation
  - **Sind diese (Desaster-)Recovery-Verfahren erprobt und geübt?**
    - Wie oft wurden/werden diese geübt?

IT-Risikomanagement – Risikoanalyse

- **Identifikation der reellen Bedrohungen**
  - Hochwasser ist überall eine Gefahr, aber nur unter bestimmten Rahmenbedingungen eine reelle Bedrohung
    - Exponierte Lage nahe einem Fluss, Meer oder Gewässer
  - Ziel dieser Phase ist die Erkennung der Gefahren, die in der konkreten Kundensituation eine Bedrohung für die IT-Service Erbringung darstellen
  - Basis
    - Erfahrungswerte
    - Allgemeine Trends und Entwicklungen (Terror)
    - Technische Gegebenheiten

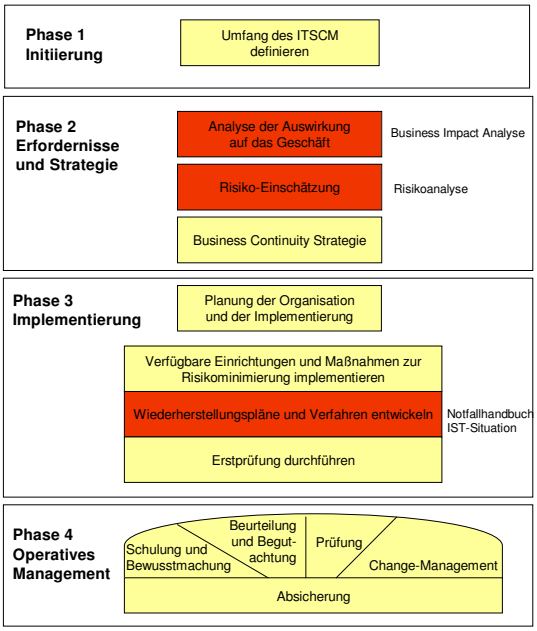
IT-Risikomanagement – Risikoanalyse

- **Bewertung der Eintrittswahrscheinlichkeiten**
  - Ermittlung der Eintrittswahrscheinlichkeiten für die jeweiligen Bedrohungen
    - z.B. einmal alle zehn Jahre gibt es ein Hochwasser in der Region X
  - Alternativ kann ein Kategoriensystem etabliert werden
    - Hoch, mittel oder niedrig

Eine Studie zur Risikoanalyse bringt:

- **Nutzen**
  - Sicherheitslücken erkennen
  - Risiken minimieren
  - Betriebsausfallkosten vermeiden
  - Entscheidungsgrundlage für die Geschäftsleitung
  - Definiert auf Basis von wirtschaftlichen und technischen Risiko-Überlegungen die passende Strategie zur K-Fallvorsorge
- **Leistungen**
  - Liefert das maßgeschneiderte und praktikable K-Fallvorsorgekonzept
  - Schafft Akzeptanz da Geschäftsführung, Fachabteilung und IT-Abteilung einbezogen werden
  - Schafft die Basis für die nachfolgende Umsetzung
  - Reduziert Komplexität und erhöht die Planungssicherheit

Handlungsrahmen ITSCM



IT-Risikomanagement – Risikoanalyse

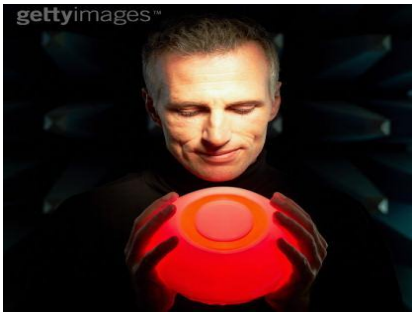
Identifikation der Gefahren mit Hilfe von Standards und Normen

- **COBIT** – Control Objectives for Information and Related Technology
- **DIN ISO 15408** – Evaluationskriterien für IT-Sicherheit
- **ISO / IEC 17799** – Code of Practice for Information Security Management
- **ISO / IEC TR 13335** – Guidelines for the Management of IT Security
- **IT–Grundschutzhandbuch**
- **ITIL** – IT Infrastructure Library
- **VDI 5002** – Informationssicherheit in der Bürokommunikation

IT-Risikomanagement

Engagement und Zusammenarbeit der becom Group mit:

- IBM
- TNCC (Trustet Network Competence Circle) für aktive und passive IT-Sicherheit
- Forschungsgruppe für Informationsmanagement & Unternehmensführung
  European Research Center for Information Systems University of Münster
  Leonardo Campus 3
- LGAD - Landesverband Groß- und Außenhandel, Vertrieb und Dienstleistungen Bayern e.V.
- Interne Projekte Sirius 2 und Risikoatlas
- Wirtschaftsprüfer (OTRG Oberbayerische Treuhand- und Revisionsgesellschaft)
- EDV Rechtsexperten (Wilfried Reiners - PRW Rechtanwälte u.a.)



Der Mensch hat dreierlei Wege, klug zu handeln:

- **erstens durch Nachdenken, das ist der edelste**
- **zweitens durch Nachahmen, das ist der leichteste**
- **und drittens durch Erfahrung, das ist der bitterste!**

(Konfuzius)

- **Nix tun kann ein jeder** **(Rudolf Wanner 2004)**