Lattwein Computersprachen

Course 2005

ADVANTEGY inspiring solutions

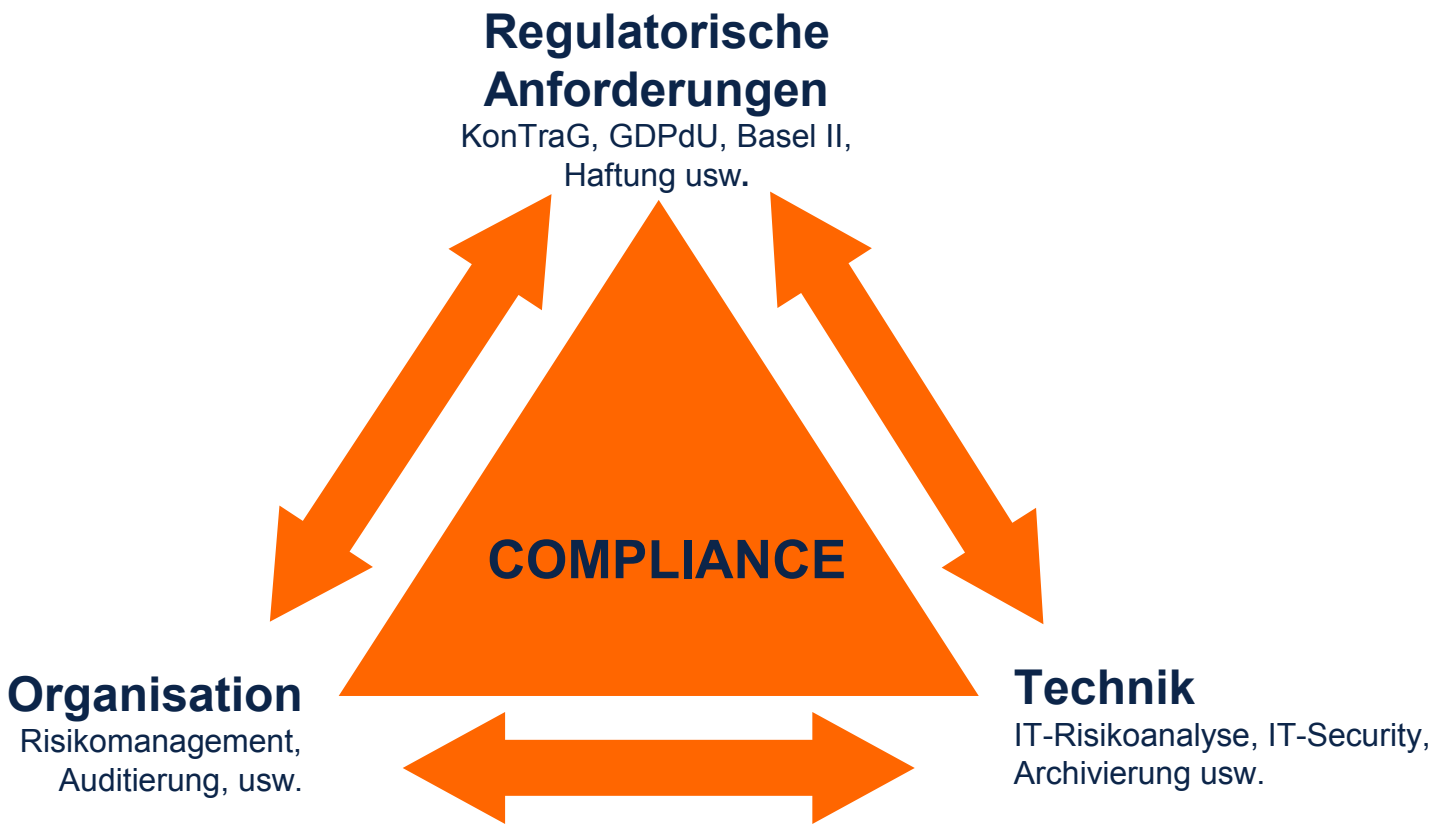
Risiken in der IT: Bringen Sie sich in Sicherheit

Die offenen und versteckten Anforderungen an die Unternehmens-IT

31.05.2005

Uwe Rusch
uwe.rusch@advantegy.com

Das Spannungsfeld



advantegy
inspiring solutions

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)

ADVANTEGY
inspiring solutions

Agenda

1 IT-Störfälle und Folgen

2 Anforderungen der Wirtschaftsprüfer / Haftungsfragen

3 Was kann man tun?

4 Was ist angemessen?

advantegy
inspiring solutions

Risiken lauern überall….

Was ist ein Störfall?

Ein Brand legt Ihr Produktions-RZ lahm

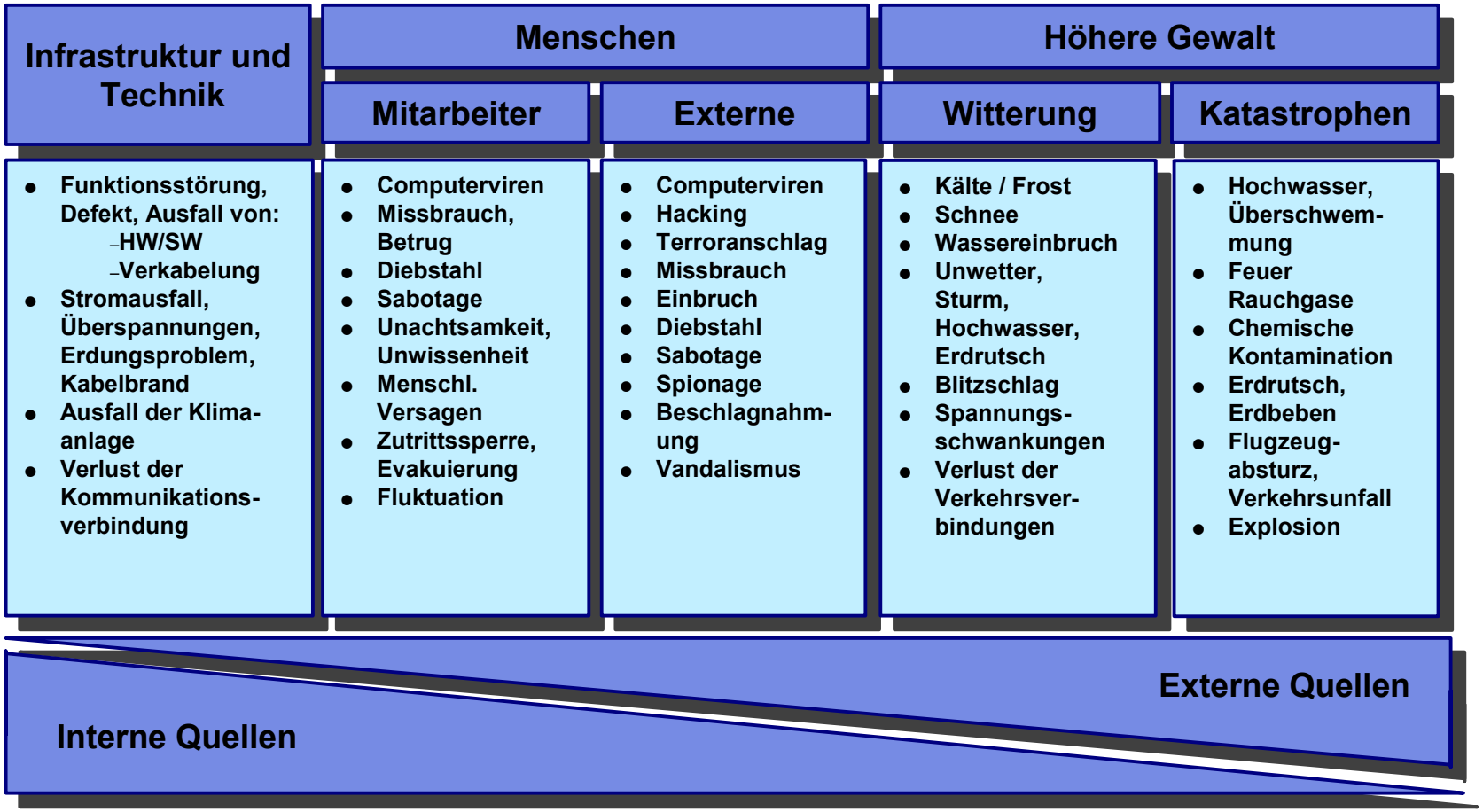
Eine wichtige Abteilung bzw. Kernanwendung ist nicht verfügbar

Eine Betriebsstörung eskaliert zu einer Katastrophe

➔ *Ein kritischer Dienst ist nicht mehr verfügbar!*

ADVANTEGY
inspiring solutions

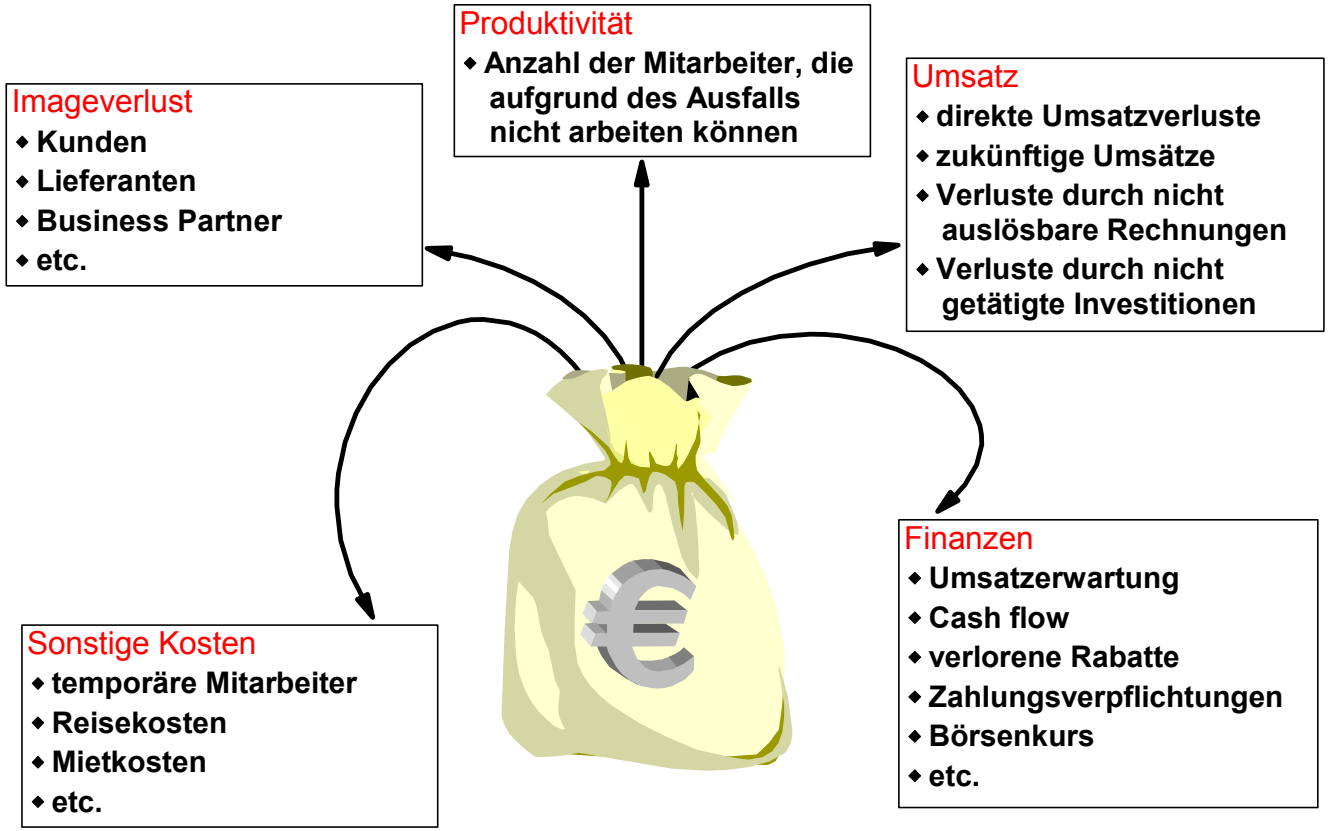
Mögliche Bedrohungen



advantegy
inspiring solutions

Auswirkungen und Folgen von Störfällen

Zusammensetzung der Kosten bei einem Ausfall



advantegy
inspiring solutions

Agenda

1 IT-Störfälle und Folgen

2 Anforderungen der Wirtschaftsprüfer / Haftungsfragen

3 Was kann man tun?

4 Was ist angemessen?

advantegy
inspiring solutions

Warum Risikomanagement ?

Warum Einrichtung eines Risikomanagements?

- §91 Abs. 2 AktG: Verpflichtung des Vorstandes zur Einführung eines Überwachungssystems zur

- Erfassung, Früherkennung und Abschätzung von Risiken
- Einleitung geeigneter Vorsorge- und Sicherungsmaßnahmen
- Schaffung einer Balance zwischen Sicherheitsinteressen und Wertschöpfungsinteressen
- Begrenzung von finanziellen Verlusten und Imageschäden

Was bedeutet Risikomanagement?

Planmäßige Abwehr von Risiken im Sinne von

- Risikovermeidung, -minderung oder –begrenzung
- Risikoüberwälzung
- Risikovorsorge

ADVANTEGY
inspiring solutions

Was sind Risiken ?

- Risiko ist allgemein die Möglichkeit ungünstiger, zukünftiger Entwicklungen

- Ein Risiko beinhaltet die Möglichkeit
  - eines Eintritts eines Schadens
  - eines Nichteintritts einer positiven Entwicklung oder
  - der Abweichung vom Erwarteten

- Risiken resultieren aus dem gesamten externen und internen Unternehmensumfeld

Risikomanagement in der Praxis

Zuordnung der Risiken zum Entstehungsort in der Prozesslandkarte

Die Haftungsfragen

- Dazu ein Beispiel:
  - Unzureichende Aktualisierung des Datensicherungskonzeptes

➔ Absicherung mit Backup-Rechenzentrum für den Katastrophenfall ist zwar vorgesehen, aber

➔ es fehlt an aktualisierten Datenbanken und aktueller Software

Haftung …

… des Arbeitnehmers gegenüber seinem Arbeitgeber

- Die Prüfung durchläuft drei Schritte
  - Pflichten des Arbeitnehmers
    - Arbeitsvertrag
    - Verkehrssitte
  - Sorgfaltsmaßstab
    - Stellung des Arbeitnehmers
    - Fachkenntnis und Belastbarkeit bleiben ausser Betracht
  - Haftungsbeschränkungen
    - Fürsorgepflicht des Arbeitgebers
    - Verantwortung der Arbeitgebers
    - Weisungsrecht

advantegy
inspiring solutions

Haftung: wann und wieviel?

Vorsatz, grobe Fahrlässigkeit

Arbeitnehmer haftet grundsätzlich zu 100%

Mittlere Fahrlässigkeit

Haftung wird gequotelt

Leichte Fahrlässigkeit

Keine Haftung

Beschränkung der Haftung auf die nach Abzug des pfändungsfreien Einkommens verbleibende Summe während der nächsten fünf (BAG) oder maximal sechs Jahre (InsO)

advantegy
inspiring solutions

Beispiel Datensicherung

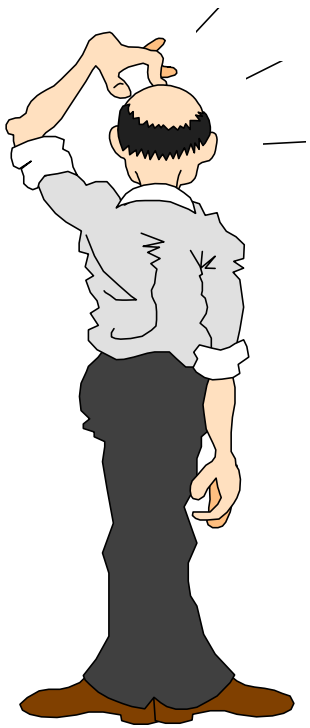
Unzureichende Aktualisierung des Datensicherungskonzeptes

- **Eine regelmäßige Aktualisierung der Datensicherung ist erforderlich**
  - **Grobe Fahrlässigkeit**
    - ✓ Grundsätzlich volle Haftung des Arbeitnehmers für alle entstandenen Schäden
    - ✓ Evtl. Haftungsbeschränkungen wegen Missverhältnis zwischen Schaden und Einkommen

advantegy
inspiring solutions

Prävention

Was hätte der angestellte IT-Manager oder der Mitarbeiter zur Vorbeugung tun können?



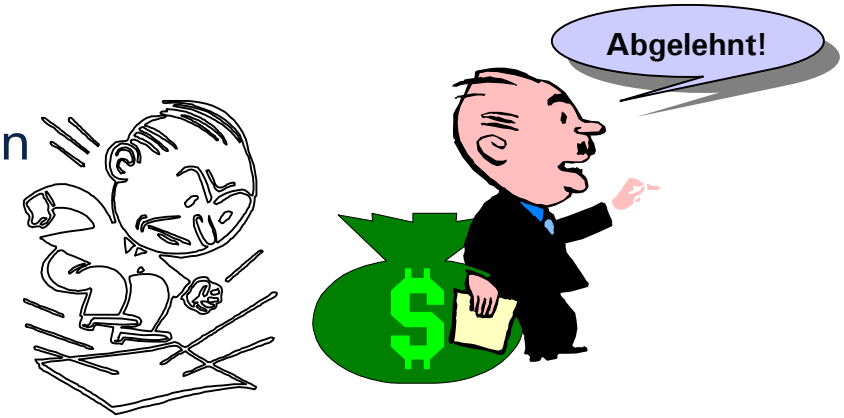
1. Memo an Geschäftsleitung, Risikopotenzial aufzeigen, Notwendigkeit der Analyse und Erhöhung der Sicherheitsstandards aufzeigen, Projektbudget beantragen
2. Analyseprojekt, am besten mit Dienstleister, aufsetzen
3. Analyseergebnis und Maßnahmenplan an Geschäftsleitung
4. Realisierung und regelmäßige Reviews

advantegy
inspiring solutions

Und wenn Prävention nicht hilft?

Und wenn die Geschäftsleitung ablehnt?

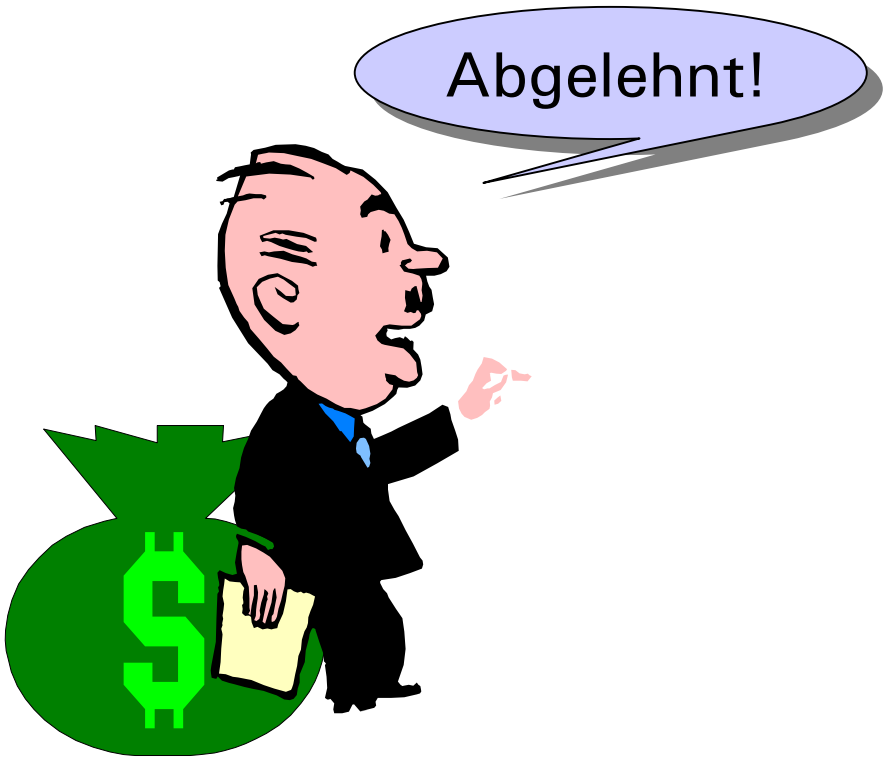
- Vorlagen an Geschäftsleitung dokumentieren
- nochmals Risiken aufzeigen
- Ablehnung schriftlich geben lassen
- weitere Verantwortung ablehnen



advantegy
inspiring solutions

Haftung der Geschäftsführer oder Vorstände

Vorstand / Geschäftsführung sorgt nicht für hinreichende Sicherheitsstandards der IT



advantegy
inspiring solutions

Haftung der Geschäftsführung und des Vorstandes

- §43 GmbHG:
  - "Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.
  - Geschäftsführer, welche ihre Obliegenheiten verletzen, haften der Gesellschaft … für den entstandenen Schaden."

- §93 AktG
  - Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. […]
  - Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet. Ist streitig, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, so trifft sie die Beweislast.

ADVANTEGY
inspiring solutions

Haftung im Notfall

Gesetzgebung

- **BGB, allgemeine Regeln für die Haftung von Arbeitnehmern und Geschäftsführung**
- **KonTraG, AktG, GmbHG: Verpflichtung des Vorstandes**
  - **Einrichtung eines Überwachungsystems zur frühzeitigen Erkennung bestandsgefährdender Entwicklungen**
  - **Etablierung Schadensverhütungsaktivitäten, insb. Notfallplan**
- **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

advantegy
inspiring solutions

Agenda

1 IT-Störfälle und Folgen

2 Anforderungen der Wirtschaftsprüfer / Haftungsfragen

3 Was kann man tun?

4 Was ist angemessen?

advantegy
inspiring solutions

Service Continuity Management

Definition von Verfügbarkeitsanforderungen in SLAs und
Implementierung entsprechender Verfügbarkeitsmanagement
Restart/Recovery Prozesse

- Risikominimierung, Minimierung möglicher Störfälle,
- Erhöhung der Widerstandsfähigkeit der Systeme (Fehlertoleranz)
- Anpassung der möglichen Ausfallzeiten an das ‚erträgliche Maß',
- Erarbeitung Katastrophenvorsorge-Planung

Hochverfügbarkeit ist möglich, angemessene Vorsorge ist wirtschaftlich!

ADVANTEGY
inspiring solutions

Welche Bestandteile hat Vorsorge?

- Organisatorische Vorsorge
  - Prozesse
  - Dokumentation (Notfallhandbuch)
  - Schulungen und Übungen
  - Klare Verantwortlichkeiten
  - Ressourcenbereitstellung für die Planung

- Technische Vorsorge
  - Systemauslegung (Redundanzen)
    - IT-Komponenten
    - Rechenzentrum

Notfallhandbuch

Wenn Sie keinen 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 ?

advantegy
inspiring solutions

Agenda

1 IT-Störfälle und Folgen

2 Anforderungen der Wirtschaftsprüfer / Haftungsfragen

3 Was kann man tun?

4 Was ist angemessen?

advantegy
inspiring solutions

Service Continuity Management

Definition von Verfügbarkeitsanforderungen in SLAs und
Implementierung entsprechender Verfügbarkeitsmanagement
Restart/Recovery Prozesse

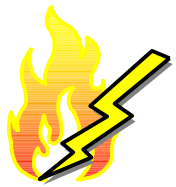
- Risikominimierung, Minimierung möglicher Störfälle,
  - *Nicht jede externe oder interne Gefährdung führt zu einer Störung des IT Betriebes*
- Erhöhung der Widerstandsfähigkeit der Systeme (Fehlertoleranz)
  - *Nicht jede Störung führt zu einem Ausfall von IT Services*
- Anpassung der möglichen Ausfallzeiten 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!

advantegy
inspiring solutions

Von der Risikoanalyse zur Strategie

Notwendige Analysen der heutigen 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?
- Wie viel Datenverlust ist tolerierbar?

advantegy
inspiring solutions

Lassen Sie sich beraten....

advantegy
inspiring solutions

Konzept einer Studie

- Der Nutzen für Sie:

  - Sicherheitslücken werden erkannt
  - Risiken können sinnvoll minimiert werden
  - Betriebsausfallkosten werden vermieden oder minimiert
  - Definiert auf Basis von wirtschaftlichen und technischen Risiko-Überlegungen die passende Strategie zur K-Fallvorsorge
  - Schafft die Basis für die nachfolgende Umsetzung
  - Reduziert Komplexität und erhöht die Planungssicherheit
  - Schafft Akzeptanz, da Geschäftsführung, Fachabteilung und IT-Abteilung einbezogen werden
  - Liefert eine Entscheidungsgrundlage für die Geschäftsleitung

Zusammenfassung

- Störfälle sind keine Zufälle, sondern vorhersehbar und zu erwarten
- Die Folgen der Störfälle können unternehmenskritisch werden
- Die Folgen können eine persönliche Haftung nach sich ziehen
- Wirtschaftsprüfer untersuchen zunehmend die IT-Systeme
- Die Anforderungen sind vielschichtig und schwer zu überschauen

➔ Sie können handeln, bevor Sie handeln müssen!

advantegy
inspiring solutions

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)

ADVANTEGY
inspiring solutions

„Lieber Staub aufwirbeln, als Staub ansetzen!“

(Hubert Burda)

advantegy
inspiring solutions