ADVANTEGY
inspiring solutions

GSE GUIDE SHARE EUROPE
DEUTSCHE REGION

Risiken in der IT:
Bringen Sie sich in Sicherheit

VM / VSE / Linux für zSeries
Herbsttagung 2005
24.-26. Oktober 2005

Uwe Rusch
uwe.rusch@advantegy.com

Aktuelle Meldungen

IT-Sicherheit: Manager unterschätzen Haftungsrisiko

Heilpraktiker-Ansatz als Lösung

Der Branchenverband Bitkom hat Geschäftsführer und Vorstände davor gewarnt, das Haftungsrisiko bei mangelnden Sicherheitsvorkehrungen in einem Unternehmen zu unterschätzen. Oft werde die IT erst dann zur Chefsache, wenn ein Haftungsfall eintritt - bis dahin werde das Thema gerade in kleinen und mittleren Unternehmen gerne unter den Tisch gekehrt. (10.03.2005)

IT-Sicherheit ist noch immer keine Chefsache

Meistens bleibt es am Admin hängen

Wer ist eigentlich für die IT-Sicherheit im Unternehmen verantwortlich? Die Antwort bleibt eine neue Studie schuldig. Das ist aber kein Fauxpas, sondern zeigt, wie wenig durchdacht das Sicherheitskonzept in einer Firma oft ist und schlicht nicht klar wird, wer da eigentlich denken soll. (09.08.2005)

Quelle: www.silicon.de

Aktuelle Meldungen

IT-Sicherheit soll eine Business-Disziplin werden

Gartner will der IT die Last der alleinigen Verantwortung nehmen

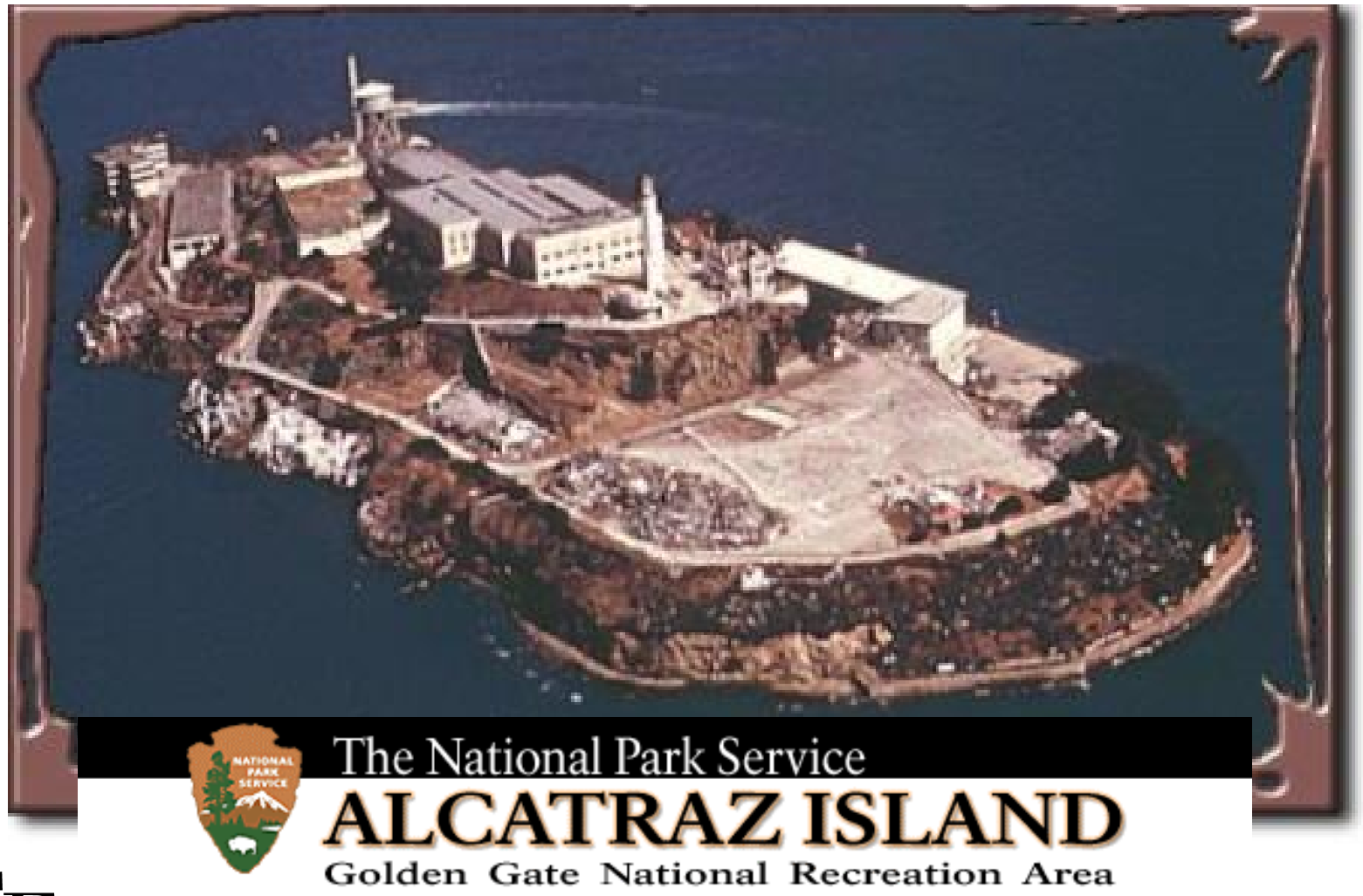
Wenn es nach dem Marktforschungsunternehmen Gartner Research geht, soll die Security in Zukunft nicht mehr allein von der IT getragen werden. Ein Chief Information Security Officer (CISO) soll vielmehr die Security-Aufgaben gleichermaßen außerhalb der IT wahrnehmen. Dies deshalb, weil diese Fragen eher in die Business-Bereiche gehören und prozess- statt technikgetrieben sind. (15.09.2005)

Entwickler sollen für ihre Bugs haften

64 Prozent sind sich ihrer Sache nicht sicher

Softwareentwickler sollten für die Sicherheit ihrer Codezeilen persönlich verantwortlich gemacht werden - das ist zumindest die Meinung von Howard Schmidt, der das Weiße Haus in Washington früher in Sachen Cybersecurity beraten hat. Viele Entwickler müssen nach seiner Meinung auch besser ausgebildet werden, sie hätten schlichtweg nicht die notwendigen Fähigkeiten, um Quellcode zu schreiben.(13.10.2005)

Könnte das Ihr neues Büro sein?



GSE GUIDE SHARE EUROPE

ADVANTEGY inspiring solutions

Agenda

- Was sind Störfälle
- Beispiele, wie es nicht sein sollte
- IT Sicherheit – das magische Dreieck
  - Technik
  - Organisation
  - Recht
- Möglichkeiten zur Vorsorge und Absicherung

Was ist ein Störfall?

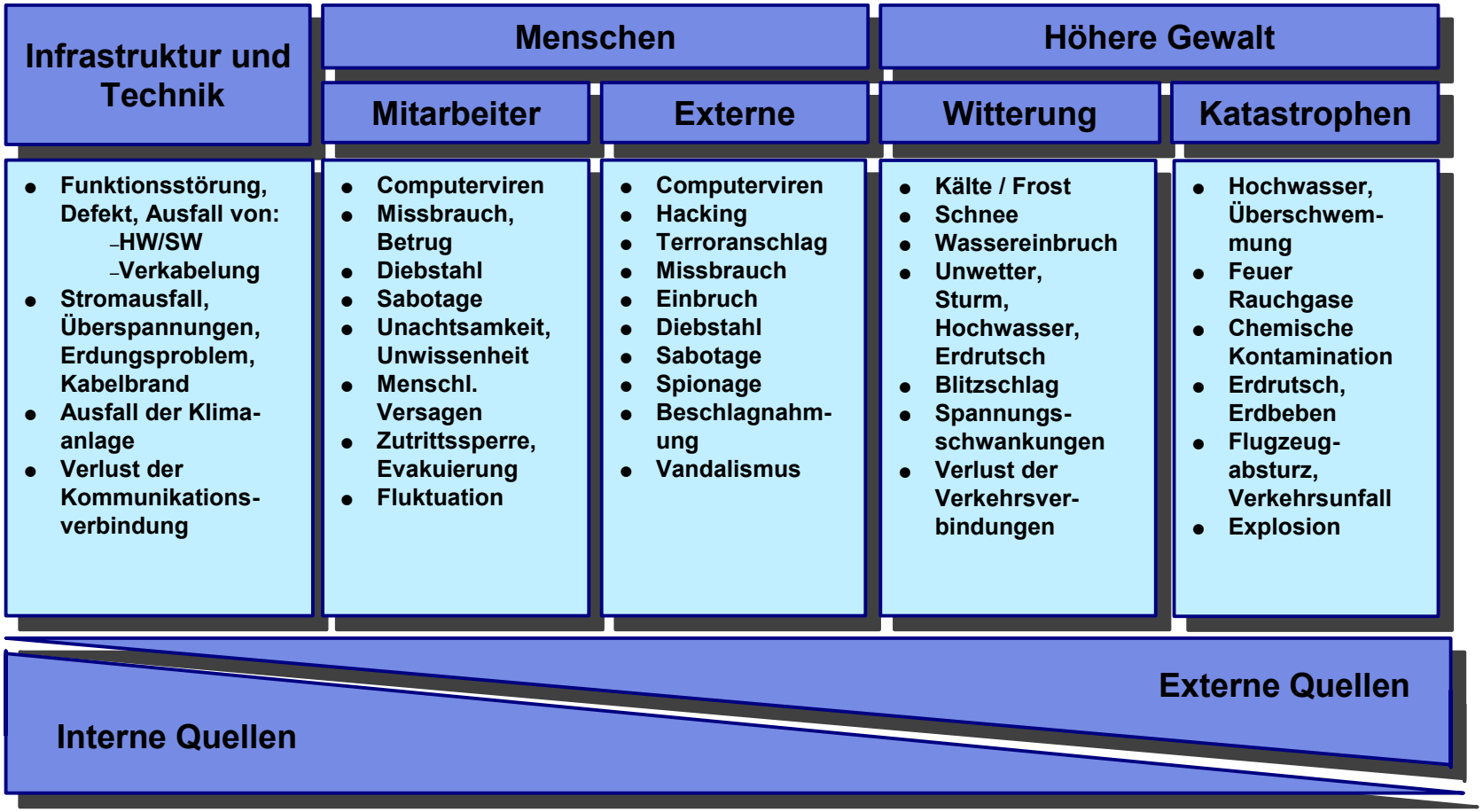
Ein Brand legt Ihr Produktions-RZ lahm

Eine wichtige Abteilung bzw. Kernanwendung ist nicht verfügbar

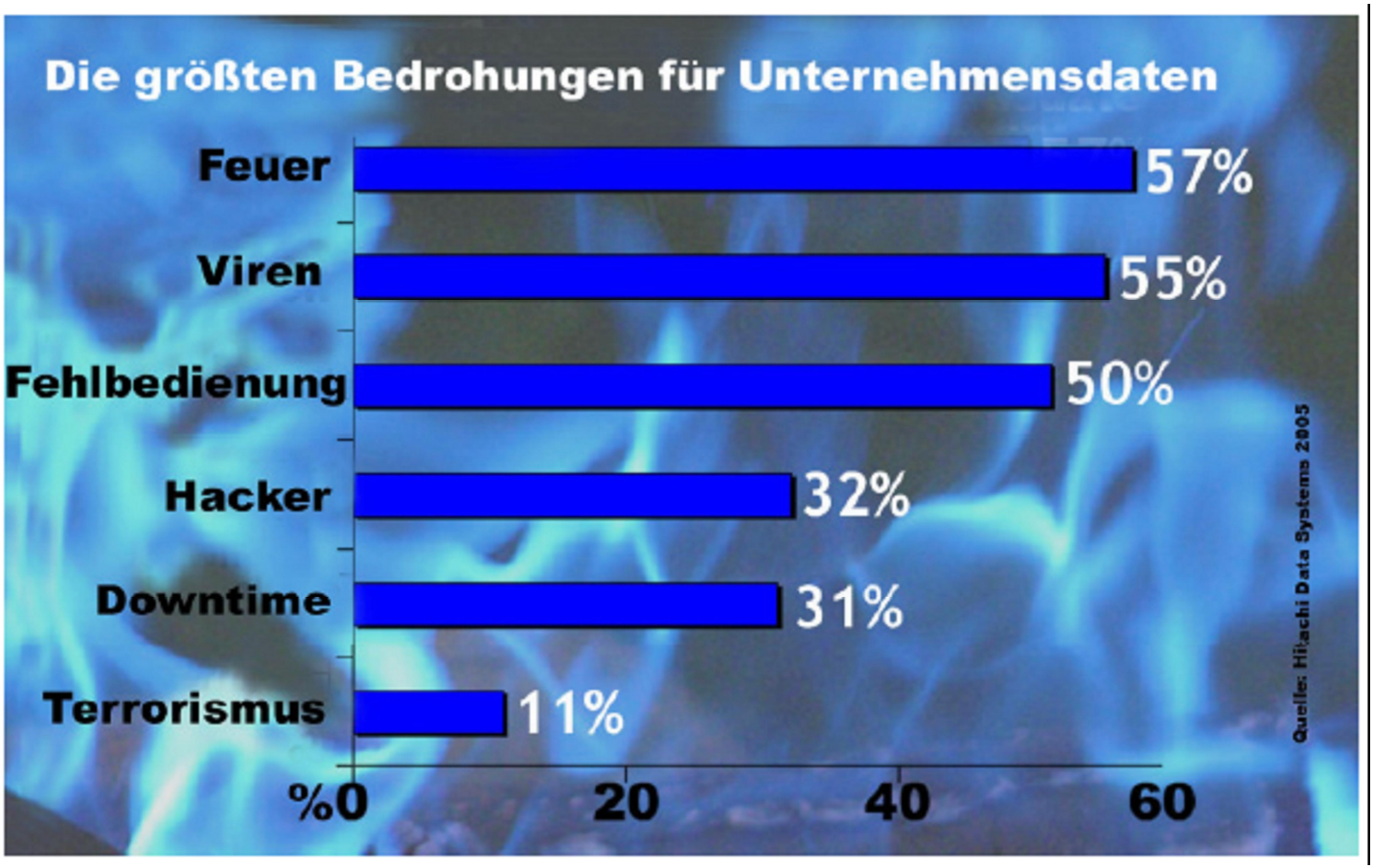
Eine Betriebsstörung eskaliert zu einer Katastrophe

➔ *Ein kritischer Dienst ist nicht mehr verfügbar!*

Mögliche Bedrohungen

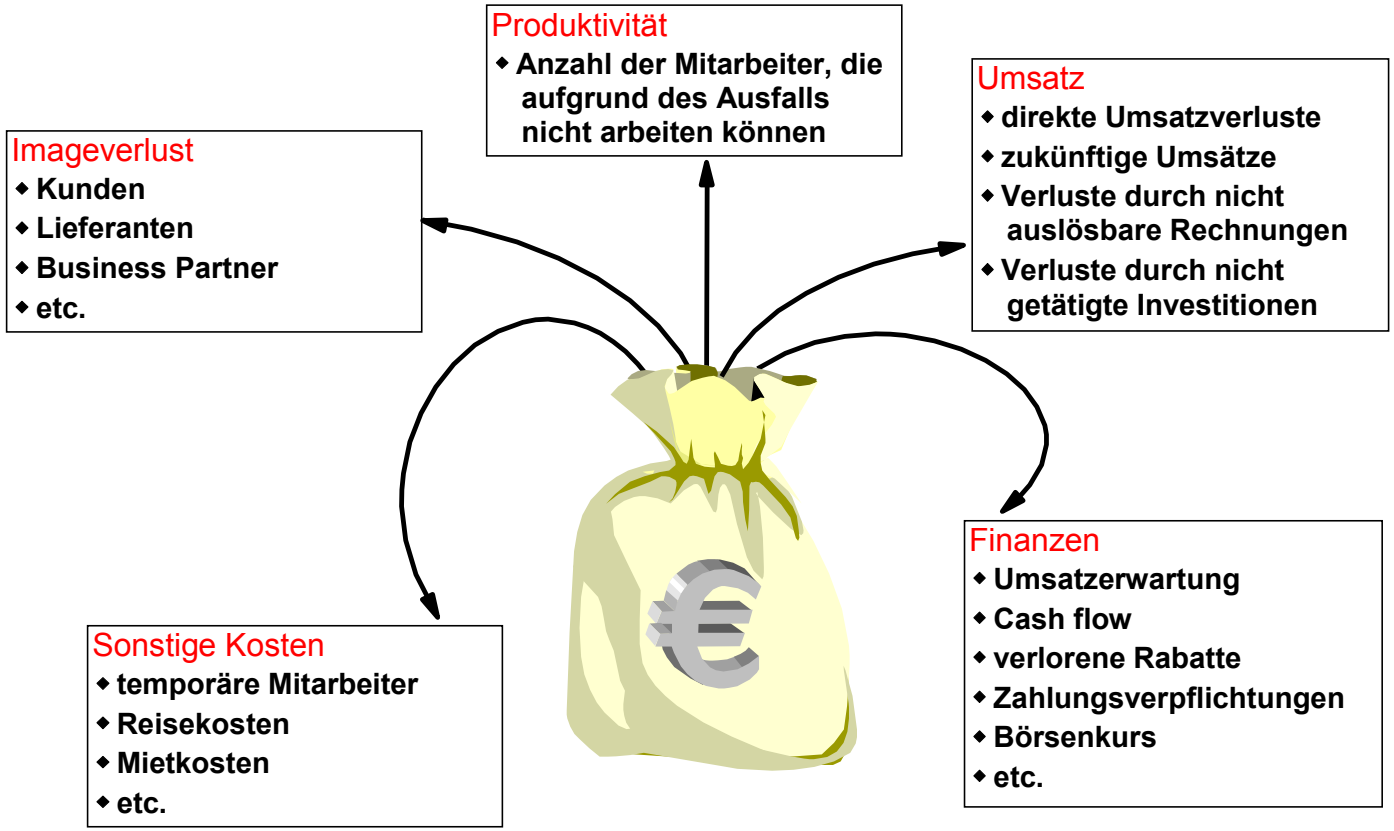


Die größten Bedrohungen für Unternehmensdaten



Auswirkungen und Folgen von Störfällen

Zusammensetzung der Kosten bei einem Ausfall



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)

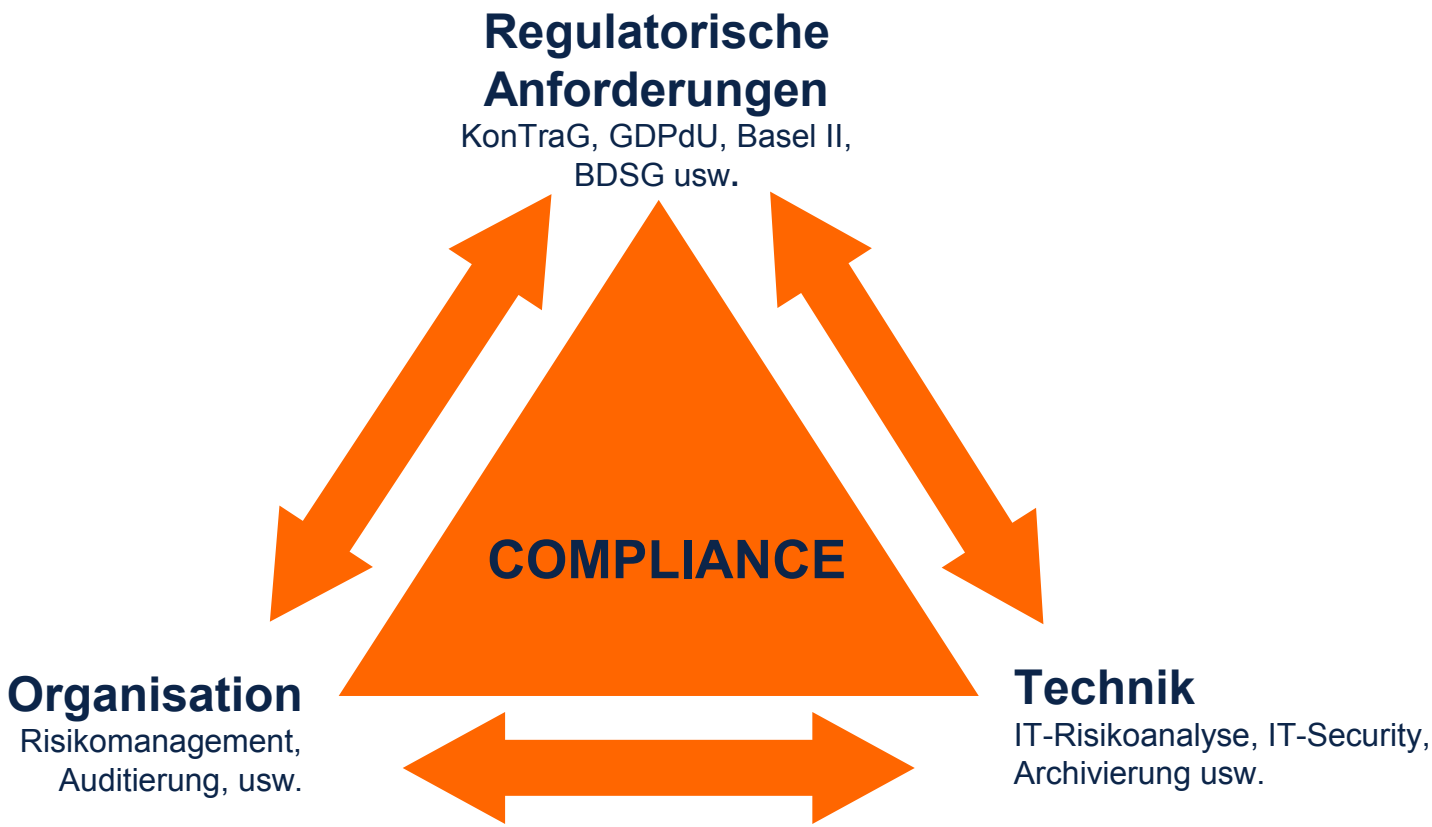
Agenda

- Was sind Störfälle
- **Beispiele, wie es nicht sein sollte**
- IT Sicherheit – das magische Dreieck
  - Technik
  - Organisation
  - Recht
- Möglichkeiten zur Vorsorge und Absicherung

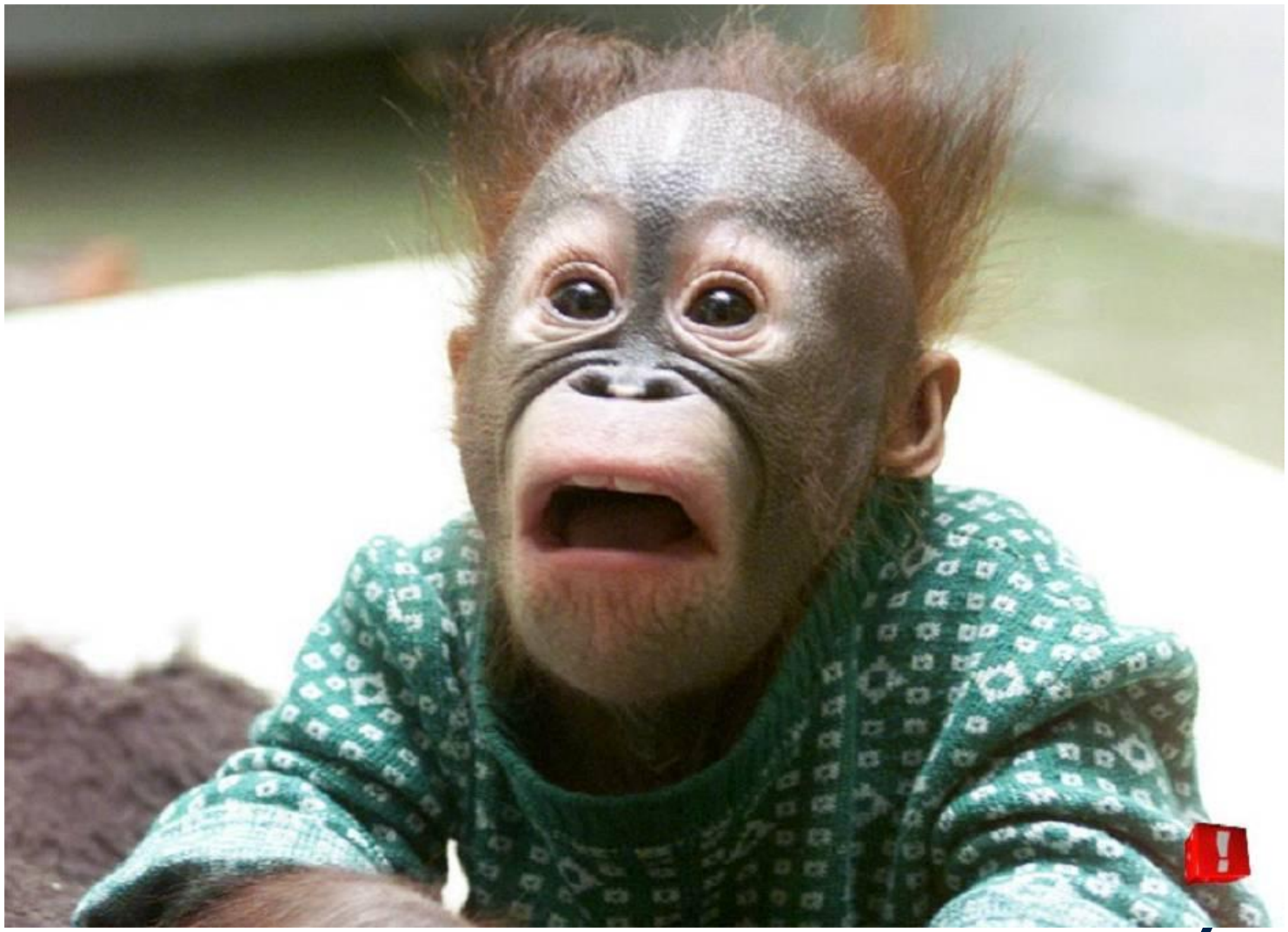
Agenda

- Was sind Störfälle
- Beispiele, wie es nicht sein sollte
- **IT Sicherheit – das magische Dreieck**
  - **Technik**
  - **Organisation**
  - **Recht**
- Möglichkeiten zur Vorsorge und Absicherung

Das Spannungsfeld IT Sicherheit



Alles im Griff?



Fragen auch Sie sich manchmal: wo fange ich an ?

Sicherheit durch Standards

Ganzheitliches Vorgehensmodell

- TORA: Technik, Organisation, Recht und Awareness

Vorgehensmodelle in Anlehnung an Standards

- BSI-Grundschutzhandbuch
- IT Infrastructure Library (ITIL)
- Sarbanes-Oxley-Act (SOX)
- Control Objectives for Information and Realated Technology (COBIT)
- ...

Risiken lauern überall….

Agenda

- Was sind Störfälle
- Beispiele, wie es nicht sein sollte
- IT Sicherheit – das magische Dreieck
  - Technik
  - Organisation
  - Recht
- **Möglichkeiten zur Vorsorge und Absicherung**

Welche Bestandteile hat Vorsorge?

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

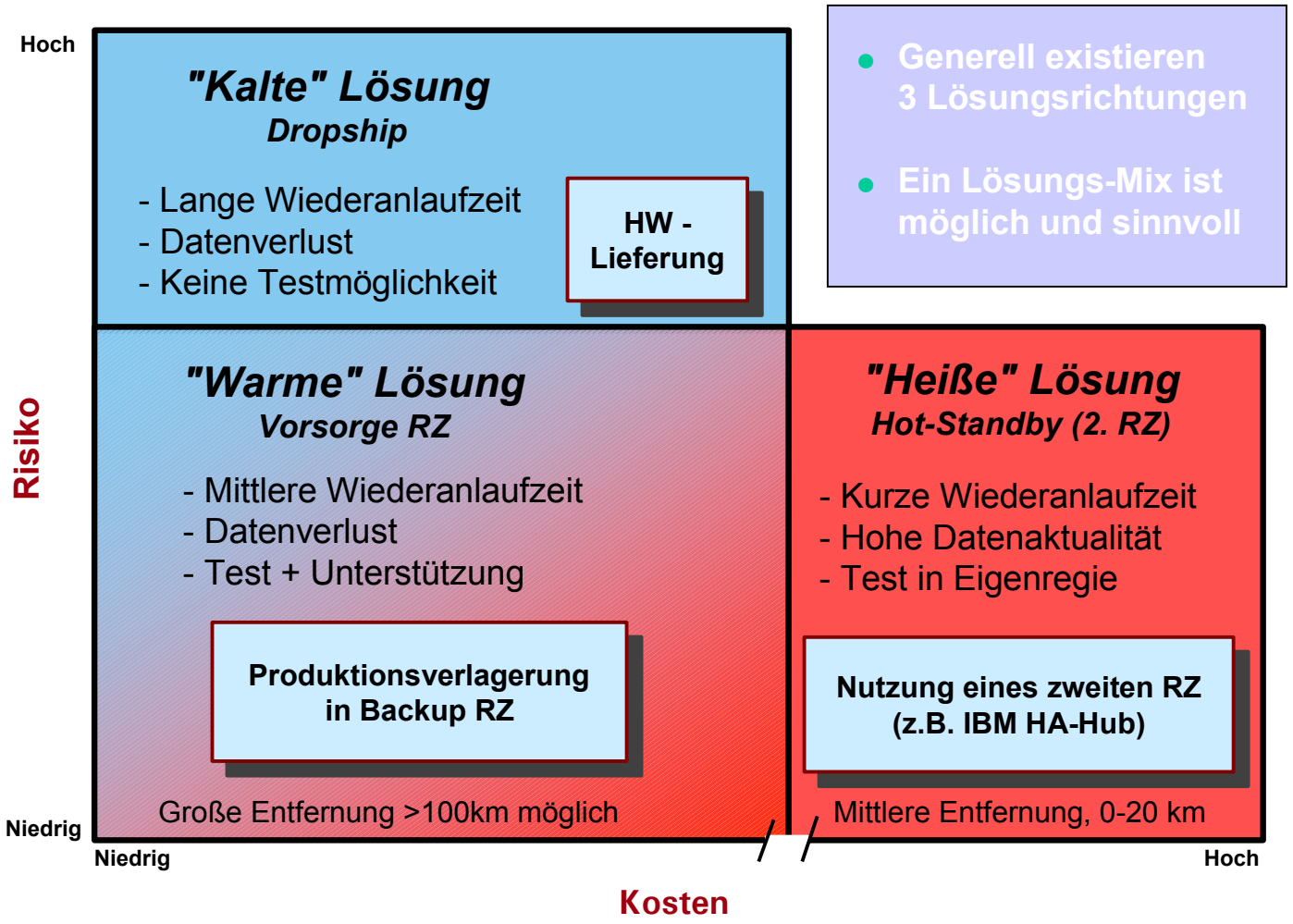
- Organisatorische Vorsorge
  - Prozesse
  - Dokumentation (Notfallhandbuch)
  - Schulungen und Übungen
  - Klare Verantwortlichkeiten
  - Ressourcenbereitstellung für die Planung

Welche Bestandteile hat Vorsorge?

- Rechtliche Vorsorge
  - Berücksichtigung von Gesetzen
    - BDSG
    - GDPdU etc

    durch
  - Regulierungen
    - private Mail
    - Internetzugriff
    - ....
  - Schulungen / Einweisungen

Technische Vorsorge



Technische Vorsorge

	„Kalte“ Lösungen	„Warme“ Lösungen	„Heiße“ Lösungen
Lösungsrichtung	Drop Ship	Vorsorge RZ	Hot-Standby
realisierbare 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

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?

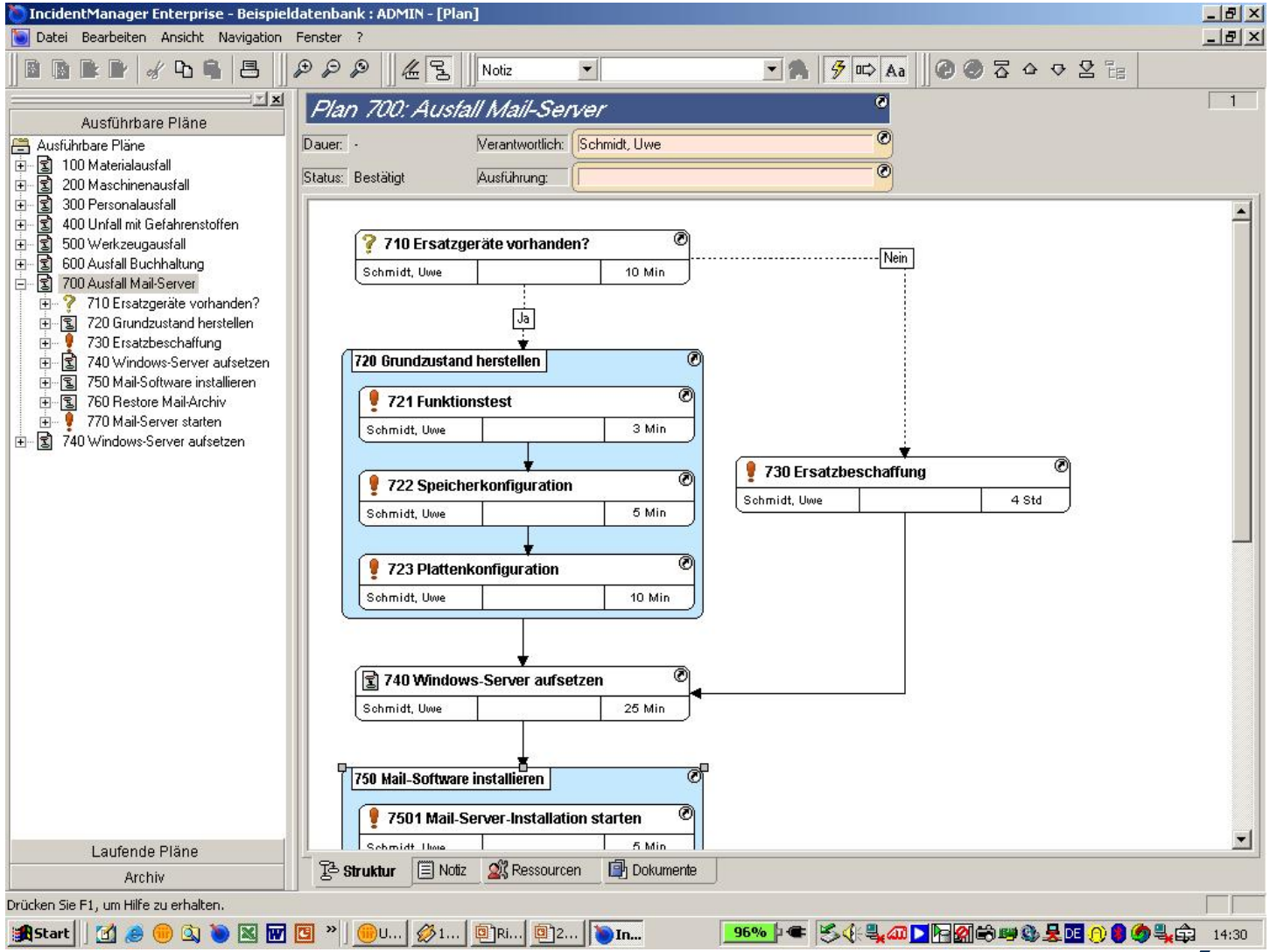
Welche Sofortmaßnahmen sind zu erledigen ?

Welche Anbieter gibt es?

Wo ist der Vertreter des Spezialisten ?

Welches Notverfahren / welche Ausweichlösung könnte installiert werden ?

Beispiel eines Tools zur Notfallplanung



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.

Welche Gesetze und Vorschriften können zutreffen?
(ein kleiner Auszug…)

HGB

GoBS

Post- und Fermeldegesetz

SOX

GDPdU

SigG

BDSG

AO

UrhG

StGB

IAS / IFRS

Ein Beispiel: AZ 1Ws 152/04 (vom 10.01.2005):
Das Tatbestandsmerkmal des „Unterdrückens“ im Sinne des §206 StGB wird durch das Ausfiltern von Emails erfüllt!

(§206 StGB: Verletzung des Post- und Fernmeldegeheimnisse – Unterdrücken einer dem Unternehmen zur Übermittlung anvertrauten Sendung)

Rechtliche Vorsorge

- Berücksichtigung von GDPdU Vorschriften (ILM)
- Datenschutz
- Vereinbarungen mit Mitarbeitern zur privaten Nutzung von Mail's und Internet
- Backup und angemessene K-Fall-Vorsorge
- Anlehnung an Standards (BSI, Cobit….)
- Prozessdokumentation
- Im Zweifel Beratung durch einen Fachanwalt
- ….

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!

Empfehlung für die Vorgehensweise (Risikoanalyse)

- Identifikation
  - Workshop mit der gesamten IT
    - Definition der IT-Services und IT-Prozesse
    - Definition der Anforderungen an die IT-Services
    - Identifikation der IT-Service Infrastruktur
  - Analyse der Verfügbarkeiten
  - Identifikation der Gefährdungslage anhand einer standardisierten Checkliste
  - Identifikation der reellen Bedrohungslage
- Bewertung der Eintrittswahrscheinlichkeiten
  - Anhand einer mehrstufigen Skala
  - Bewertung der Schadenspotenziale Erstellung eines Risikoinventars
  - Darstellung als Risikoportfolio

Nutzen einer Analyse

- Der Nutzen für Sie:

  - Sicherheitslücken werden erkannt
  - Risiken können sinnvoll minimiert werden
  - Betriebsausfallkosten werden vermieden oder minimiert
  - Berücksichtigung von wirtschaftlichen und technischen Risiko-Überlegungen
  - Reduziert Komplexität und erhöht die Planungssicherheit
  - Schafft Akzeptanz, da Geschäftsführung, Fachabteilung und IT-Abteilung einbezogen werden
  - Liefert eine Entscheidungsgrundlage für die Geschäftsleitung

  ➔ ***die Basis für Ihre IT-Sicherheit***

Wer hilft Ihnen dabei?

Am besten ein erfahrener Berater!

Zusammenfassung

- Störfälle sind keine Zufälle, sondern vorhersehbar und zu erwarten
- Die Folgen der Störfälle können unternehmenskritisch werden
- Mangelnde Vorsorge kann eine persönliche Haftung nach sich ziehen
- Externe (WP's, Gesetzgeber, Kapitalgeber, Versicherer) auditieren zunehmend die IT-Systeme
- Die Anforderungen sind komplex, aber beherrschbar

➔ Sie können handeln, bevor Sie handeln müssen!

Und zu guter letzt:

Ein weiser Spruch aus Ägypten:

Vertraue auf Allah, ...

...aber binde Dein Kamel an!

Viel Erfolg bei der Erreichung Ihrer IT Sicherheit!