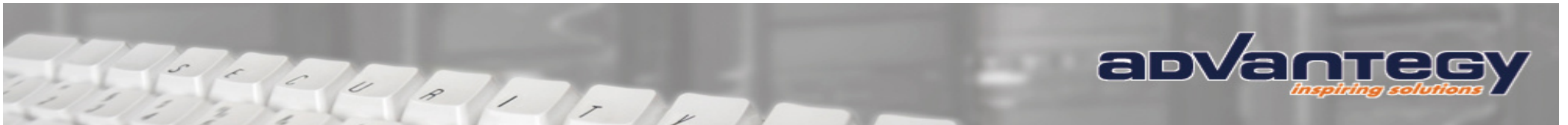


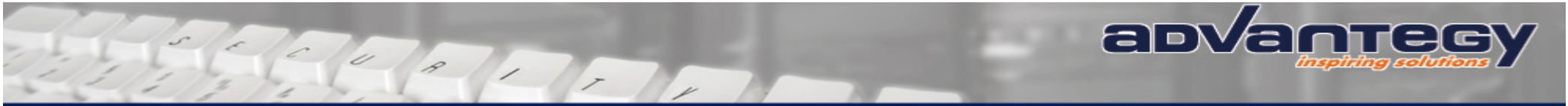


# Risikomanagement

## 5. esgeo Konferenz Sichere Geoinformation

**advantegy GmbH**  
**Uwe Rusch**  
**[uwe.rusch@advantegy.com](mailto:uwe.rusch@advantegy.com)**  
**27.01.2009**





# **Improvisation ist die Kunst, etwas Unbeabsichtigtes gut vorzubereiten!**

(Willy Millowitsch)

## Agenda

- Vorstellung advantegy GmbH
- IST-Situation und Aufgaben der Unternehmen
- Definitionen und Abgrenzungen
- Risikomanagement und Risiken
- Beispiele
  - Fragenkatalog
  - Prozessbefragung
- Kundenbeispiele

## Vorstellung der advantegy

- (IT-) Unternehmensberatung
- Gegründet 2003, Sitz in Schwerte
- Beratungsfelder
  - Digitalisierung und Optimierung von Geschäftsprozessen
  - T-O-R Analysen, Beratung, Konzepte
  - Moderierte Workshops
  - Gutachten / Studien
  - Projektmanagement
  - Management von Out-of-Line Situationen



## IST-Situation und Aufgaben der Unternehmen

- Sicherheit: nicht nur ein Frage der IT

### **Risiko-Management kann vor Kreditklemme schützen**

Der Mittelstand ist dringend gefordert, wirksame Risiko-Management-Systeme im Unternehmen einzuführen, da er sonst Gefahr laufe, Opfer der aktuellen Finanzmarktkrise zu werden.

Computerwoche online 21.10.08

### **Verfolgungswahn hilft überleben**

**19.05.2008**

Der Verfassungsschutz hat in seinem jüngsten Bericht vor Wirtschaftsspionage aus dem Ausland gewarnt. Die Angriffe erfolgten immer öfter via Internet auf die Systeme auch mittelständischer Unternehmen. Es wird Zeit, sich der Herausforderung zu stellen.

"Only the paranoid survive". Andy Grove  
(Computerwoche)

### **Hochdruckeinfluss**

#### **Die Folgen der Compliance-Debatte**

Auch Ulrich Weigel, Chief-Security-Strategist bei Attachmate, sieht eine positive Rückkopplung auf das Management: "In vielen Unternehmen wird das Thema Compliance deutlich strategischer angegangen. Da sich Compliance auf (fast) alle Bereiche eines Unternehmens bezieht, **also nicht ausschließlich auf die IT**, hat sich das Verständnis für die Probleme durchaus verbessert.

(kes online 2008)

### **Leichtsinnige Preisgabe sensibler Daten**

#### **Passwort gegen Schokoriegel**

Menschen, ob Mann oder Frau, sind verführbar. Manchmal genügt schon ein Schokoriegel als Köder und Vertreter beider Geschlechter geben Passwörter und sensible Daten preis. Das weibliche Geschlecht ist dabei deutlich anfälliger als Männer was die Weitergabe vertraulicher Informationen angeht.

Das fand eine aktuelle Erhebung unter Büroangestellten heraus, die das Event-Portal Infosecurity Europe durchführte.

CIO online, 28.05.08



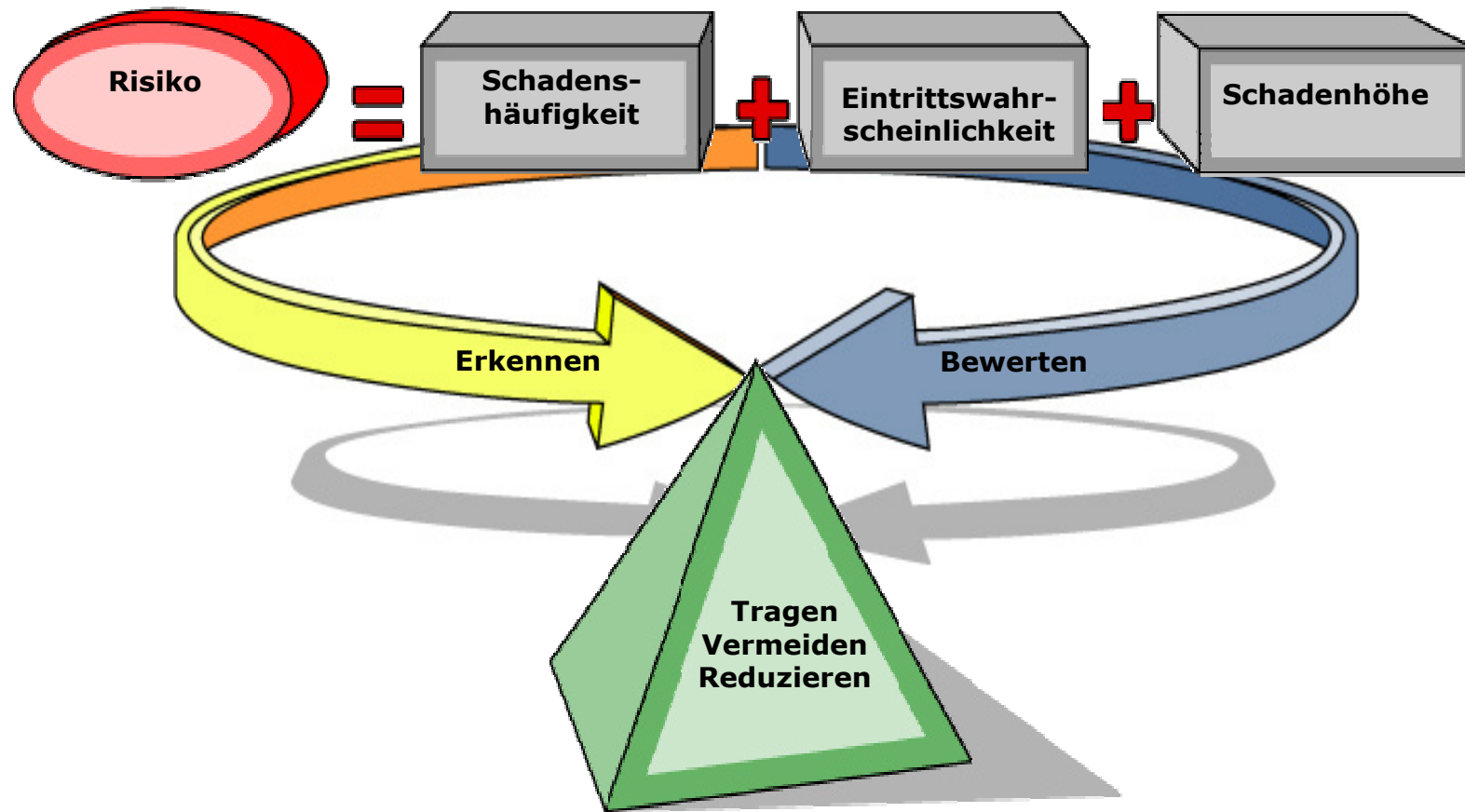
## Was ist ein Risiko?



## Was ist ein Risiko ?

- 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

# Risiko

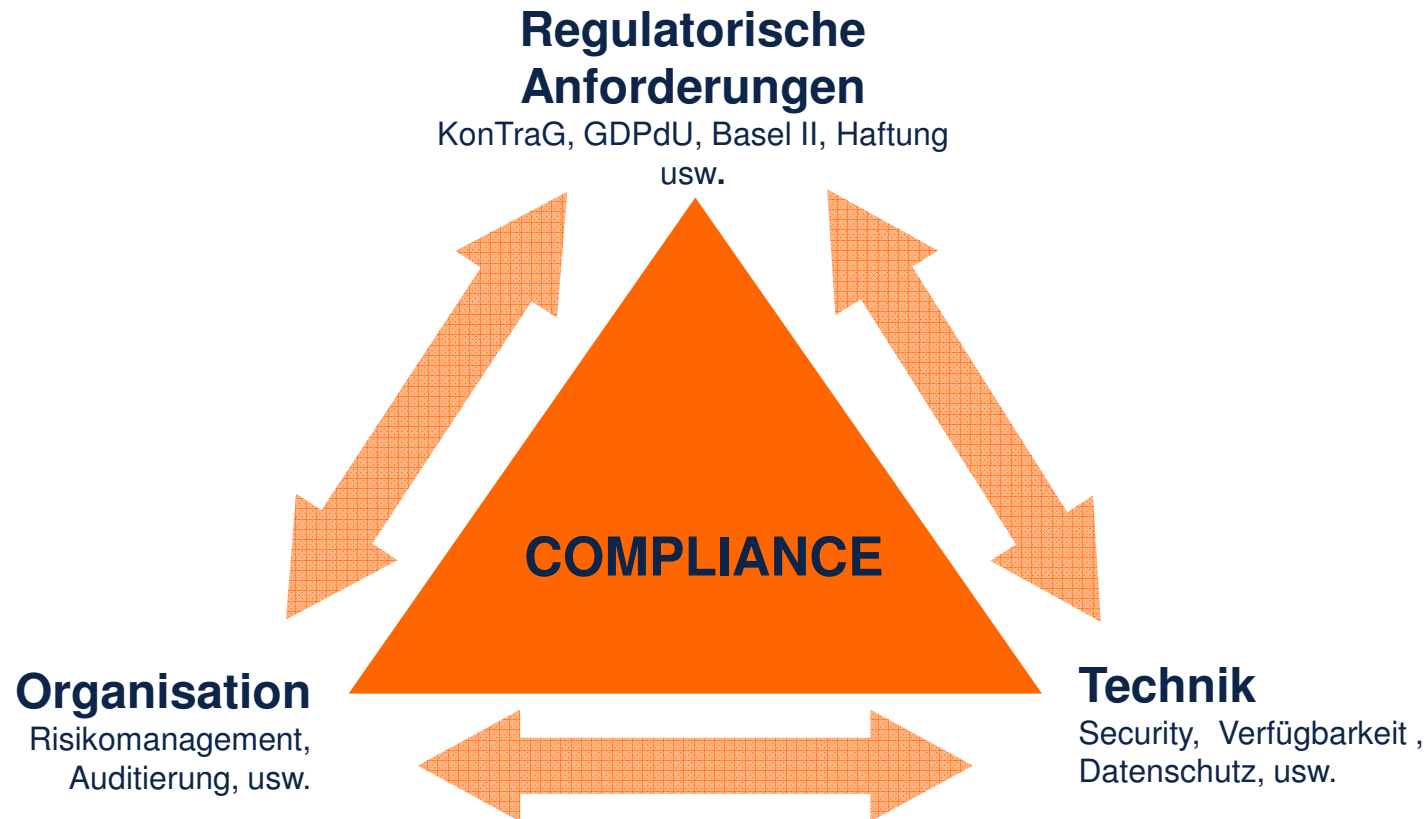


# Einflussfaktoren und Risikopotenziale





# Das Spannungsfeld



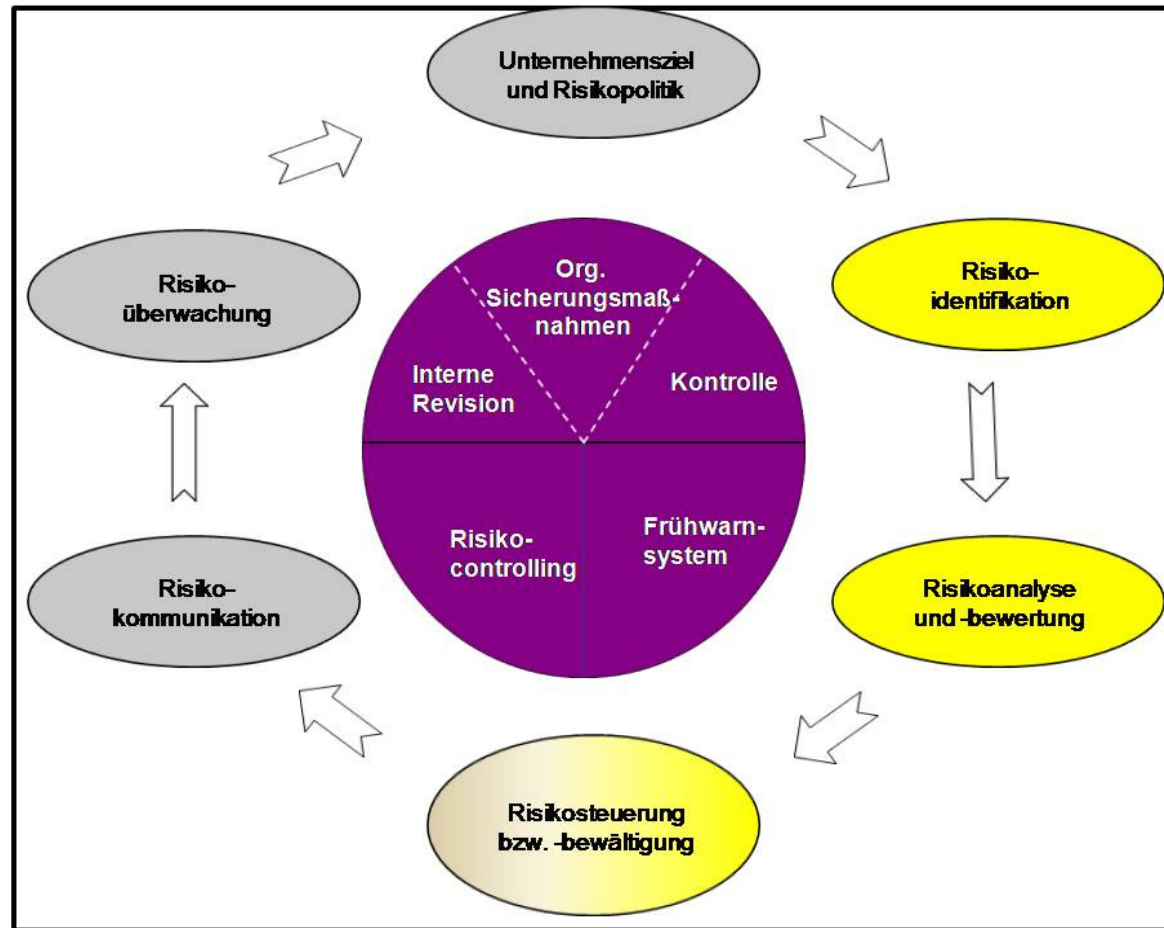
## Wer ist Verantwortlich? Geschäftsführer und Vorstände!

- §43 GmbHG:
  - Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.
- §93 AktG
  - Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. [...]
- § 91 Abs. (2) AktG
  - Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

## Definitionen und Abgrenzungen

- Business Impact Analyse (BIA)
  - Bestandteil des BCM
  - Aufstellung
    - der Prozesse und Systeme, die für die Fortführung der Geschäftstätigkeit kritisch sind
    - der maximal vertretbaren Ausfallzeit
    - der Eintrittswahrscheinlichkeit
    - der möglichen Schadenshöhe
- Business Continuity Management (BCM)
  - Zur Sicherstellung der Fortführung der Geschäftstätigkeit
  - unter Krisenbedingungen oder unvorhersehbaren Bedingungen
  - orientiert sich an unterschiedlichen Standards (z.B. COBIT, ITIL, BSI usw.)
  - ist kein einmaliger Prozess

# BCM / Risikomanagement als permanenter Prozess



## Bewährt: Durchführung von Interviews

- „Mit denen, die's wissen, von denen, die's nicht so genau wissen“
- Übersicht über den Bereich durch den Prozess-Verantwortlichen
- Übersicht über kritische Prozesse
- Beantwortung von Fragen aus einem vorbereiteten Fragenkatalog
- Bewertung von identifizierten Risiken
  - nach Schadenshöhe
  - nach Schadenswahrscheinlichkeit
  - nach Schadenshäufigkeit

## Fragenkataloge und Beispiele

- Umfassender Fragenkatalog sollte vorhanden sein
- Auswahl für die Bereiche ist zu treffen und spezifisch anzupassen
- Risikobeurteilung (Eintrittswahrscheinlichkeit, Schadenshöhe) individualisierbar
- Handlungsbedarf und Priorität muss berücksichtigt werden

[Hier geht's zur Risiko-Checkliste](#)

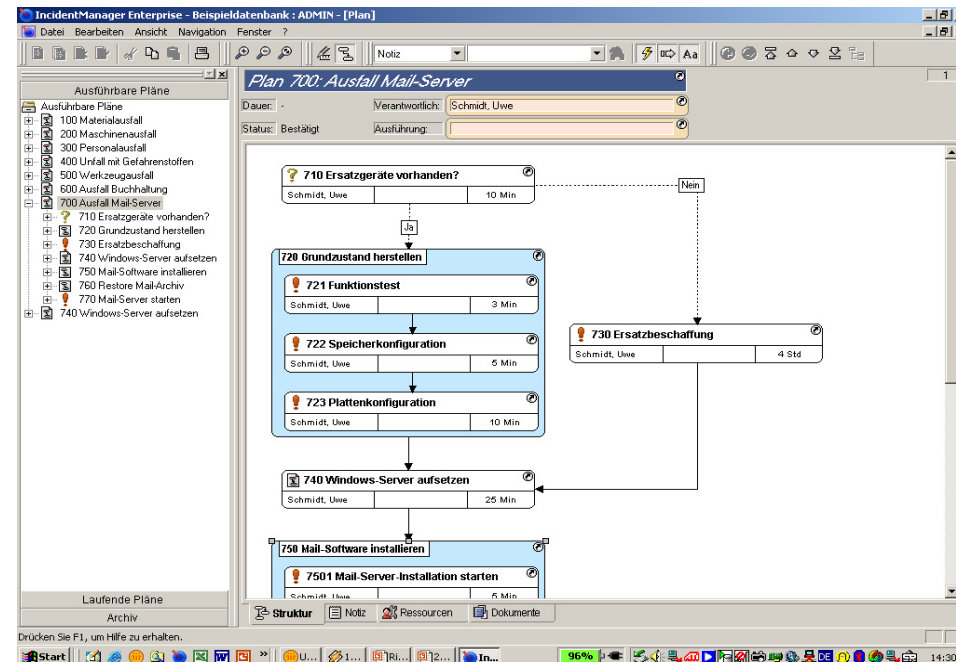
# Prozessfragebogen

Prozessdaten			
Prozessschritte Kriterien	1	2	3
kritischer Vorgang j / n	n	j	j
Ausführender / Verantwortlicher Bereich	Disposition	Disposition	Disposition
Auslöser der Tätigkeit	Lieferabruf	Lieferabruf	Versand Bestellauftrag
Aktivitäten	Lieferabruf per DFÜ (automatisch)	Generierung Bestellauftrag	manuelle Adressierung
Output / Ergebnis	Bestellung	Generierung Druckauftrag	Versand der Bestellung per DFÜ
nachfolgender Schritt	Bestellauftrag	Versand Bestellauftrag	Rückmeldung des Lieferanten
Weitere Beteiligte	keine	Lieferant	Lieferant
Hilfsmittel / IT-Systeme	Bestellsystem	Bestellsystem	Bestellsystem, eMail System
Bearbeitungsmengen pro Tag / Schicht	schneller Durchlauf / ca. 250 Bestellungen pro Tag	ca. 250 Bestellungen pro Tag	
Max tolerierbare Unterbrechung des Prozesses in Minuten (bis 60, zwischen 60 und 240, größer)	60	240	45
Alternative, wenn der Prozess unterbrochen ist	keine	Abruf per Telefon	keine
mit welchem Schaden oder Verlust ist im Falle einer Unterbrechung zu rechnen? hoch / mittel / niedrig	klein	mittel	hoch
läßt sich der Schaden abschätzen?			
wer hilft bei Problemen			
Verbesserungsvorschläge	Kontrollfunktion einrichten	Zweiten Drucker einrichten	Mail System muss die Adressen automatisch überprüfen!!!
Sonstiges / Kommentar		Vielleicht kann der Lieferant nachfassen, wenn wir nach 60 Minuten noch keine Bestellung gesendet haben?	

[Prozessfragebogen](#)

## Ein mögliches Werkzeug: Incident Manager

- Incident Manager
  - dient zur Dokumentation der Notfallpläne
  - ist ausbaubar zur Erstellung von Betriebshandbüchern und Prozessdokumentationen



IncidentManager Enterprise - Beispieldatenbank : ADMIN - [Funktionen]

Datei Bearbeiten Ansicht Navigation Fenster ?

Bezeichnung

**Daten**

- Daten
  - Allgemein
    - Personal
      - Personen
      - Funktionen
    - Firmen
    - Verzeichnisse
      - Kenntnisse
      - Dienstleistungen
      - Postleitzahlen
    - Lokationen
    - Verträge
  - Inventar
    - Objekttypen
    - Objekte
      - <ohne>
      - Hardware
      - Fahrzeug
      - Hilfsmittel
    - Verbindungen
  - Planung
    - Teams
    - Szenarien
    - Prozeduren
      - Aktivität
      - Block
      - Plan
      - Abfrage
    - Ressourcengruppen
  - Bibliothek
    - Vorlagen
    - Dokumente
    - Schlafworte
  - Berichtswesen
  - Verwaltung

Bezeichnung	Kategorie	Aufgabe	Organisation	Lokation
Abteilungsleitung Produktion		Organisation und Betriebsablauf	TAGHELL	Gebäude A
Abteilungsleitung Vertrieb		Fahrdienstleitung, Transportlogistik	TAGHELL	Gebäude B
Abteilungsleitung Verwaltung		Datenpflege	TAGHELL	Gebäude A
Berater		beratung in notfallplanungen	advantegy GmbH	Gebäude C
Geschäftsführer		Organisation, Kundenaquise	TAGHELL	Gebäude A
Lagerverwaltung		Lagerbestand, Lagerlogistik	TAGHELL	Gebäude B
Leitung Produktionsbahn 1		Überwachung Bahn 1	TAGHELL	Gebäude B
Leitung Produktionsbahn 2		Überwachung Bahn 2	TAGHELL	Gebäude B
Werkstattleitung		Werkzeugausgabe	TAGHELL	Gebäude B
*				

**Funktion: Abteilungsleitung Produktion**

Bezeichnung:

Kategorie:

Aufgabe:

Organisation: Firma:  Einheit:

Lokation:

Nummern:

Typ	Nummer
*	

Kenntnisse:

Typ	Bezeichnung
*	

## Kundenbeispiele

- Automobilzulieferer
  - Erhöhung der Prozesssicherheit (interdisziplinär)
  - Eliminierung von Schwachstellen im Prozess
  
  - Ergebnis:
    - Teamübergreifende Kommunikation und Zusammenarbeit
    - Abstellen von Prozessschwächen
    - Grundlage für eine übergreifende Notfallplanung
    - Kontinuierliche Prozessverbesserung

## Kundenbeispiele

- Mittelständisches Fertigungsunternehmen
  - BIA / Risikoanalyse und Erstellung Notfallplanung
  - Ergebnis:
    - Erkennen, Bewerten und Abstellen bzw Abwälzung der Schwachstellen
    - Erarbeitung einer Notfallstrategie
    - Umsetzung einer Notfallplanung und -dokumentation als Basis für einen umfassenden BCP
    - Umfassende Dokumentation für die WP

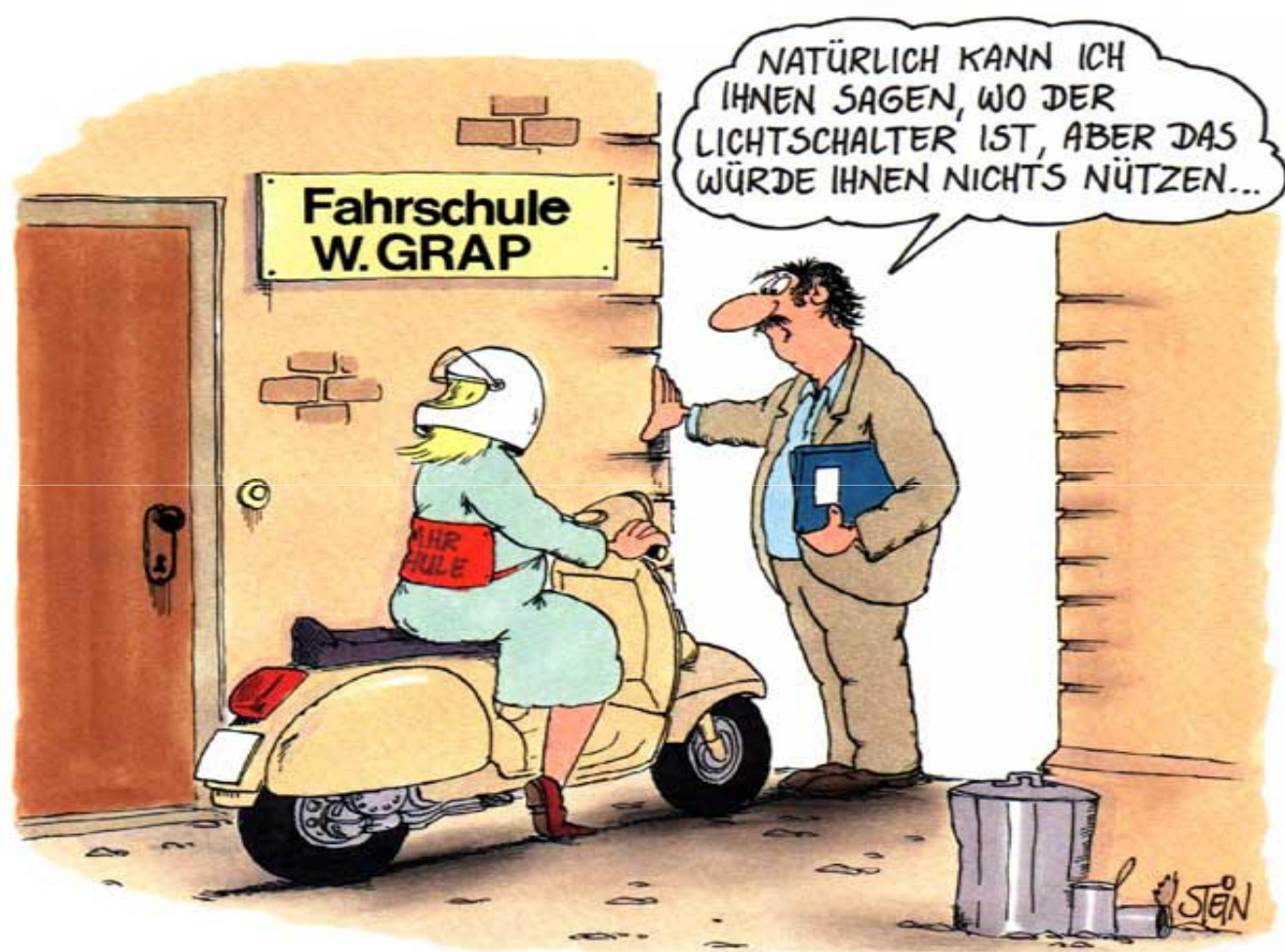
## Kundenbeispiele

- Großhandel / Automobil
  - Erarbeitung und Umsetzung einer Hochverfügbarkeitsstrategie
  - Ergebnis:
    - Erkennen und Bewerten der Risiken
    - Erkennen und Bewerten von Lösungsszenarien
    - Entscheidungshilfe für den Vorstand
    - Reduzierung der Versicherungsaufwände
    - Umsetzung einer Notfallplanung und in der Folge eines BCP
    - signifikante Reduzierung der Aufwände bei Betriebsprüfungen aufgrund der vorliegenden und aktuellen Dokumentation

## Zusammenfassung

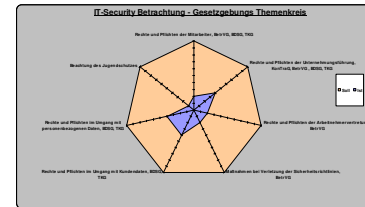
- Risikomanagement ist „Chef“-Sache
- Risikomanagement ist kein Produkt, sondern ihre individuelle Lösung
- Flexibilität ist gefragt, kein starres: „Das haben wir schon immer so gemacht!“
- Top – Down Ansatz – vom Groben ins Feine
- Strukturieren und priorisieren Sie!

Zu guter Letzt: Hören Sie auch mal auf Andere!



# Die Vorgehensweise – eine Empfehlung

- strukturierte Aufnahme der Ist-Situation und individuellen Anforderungen (individualisierte Fragebögen, Spidercharts etc)
- Bewertung der Ist-Situation, Identifizieren von möglichen Schwachstellen und Empfehlungen für eine rasche und pragmatische Beseitigung
- Vorbereitung und Durchführung eines methodisch geführten und interdisziplinären Workshops unter dem Aspekt T-O-R
- Entwicklung des zukünftigen „IT-Bebauungsplanes“, orientiert an Standards und Normen



IT Infrastruktur		
Frage	Status / geplant	
Sind Ihre zentralen IT – Systeme, redundiert ausgelegt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein <input type="checkbox"/> teilweise <input type="checkbox"/> nicht bekannt	Bemerkungen
Deuchten Sie hierbei auch Gebäude, Räumlichkeiten, Verkabelung, Stromversorgung, aktive & passive Netzwerkinfrastrukturen, dh. z.B. auch Themen wie Brand, Blitz, Wasser, phys. Zugang in Ihre Untervergütungen?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein <input type="checkbox"/> teilweise <input type="checkbox"/> nicht bekannt	Bemerkungen
Werden Backup- & Restoreverfahren	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Geplant zum

## 23.1 Überblick Firewall

nr.	Ursachefakt.	Kommentar	wert
1.1	Firewall-Konzept	Die Firewall zum öffentlichen Internet und zu anderen DMZ-ADA-ADA-ADA in dieser Umgebung ist eingehenden und ausgehenden Traffic zwischen dem Internet und der LAN-Örtlichkeit, ohne DMZ ist nicht implementiert + Einführung einer DMZ zwischen dem Internet und dem LAN	!!
1.2	Firewall-Regelwerk		
1.2.1	Firewall-Policy	Das Regelwerk regelt die äußere Port der eingehenden und an internen Port der ausgehenden Traffic. Das Regelwerk ist auf ausgehenden Basis prinzipiell nicht verstanden ist und Ports sind Dienste nur bei Bedarf frei geschaltet werden. Das ist positiv zu bewerten.	+
1.2.2	Regelwerk: icmp	Das Regelwerk regelt die äußere Port der eingehenden und an internen Port der ausgehenden Traffic. Das Regelwerk ist auf ausgehenden Basis prinzipiell nicht verstanden ist und Ports sind Dienste nur bei Bedarf frei geschaltet werden. Das ist positiv zu bewerten.	+
1.2.3	Regelwerk: ssl	Das Regelwerk regelt die äußere Port der eingehenden und an internen Port der ausgehenden Traffic. Das Regelwerk ist auf ausgehenden Basis prinzipiell nicht verstanden ist und Ports sind Dienste nur bei Bedarf frei geschaltet werden. Das ist positiv zu bewerten.	!!

