



Robustheit und Kontinuität elektronischer Geschäftsprozesse

November 2002

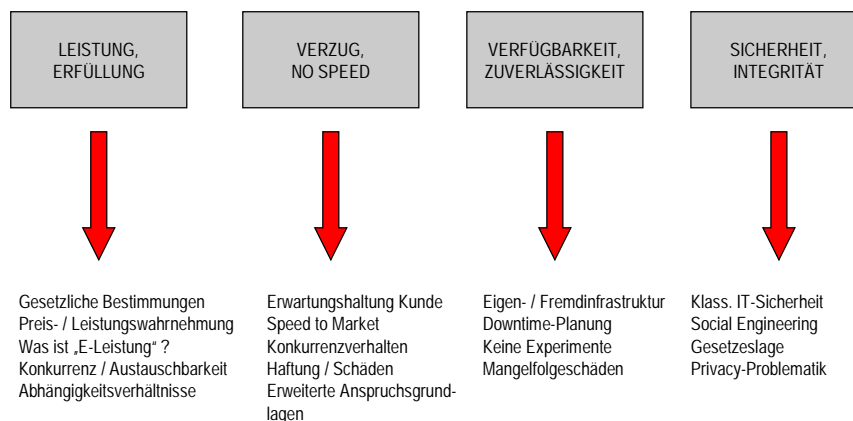
Übersicht

- Risiken und Krisenanfälligkeit elektronischer Geschäftsprozesse
- Sicherheits- und Kontinuitätsrisiken aus der Perspektive des Managements
- Einheitlicher Rahmen für „Sicherheit“, „Verfügbarkeit“ und „Kontinuität“: Standortbestimmung
- Ansatz des strategischen Kontinuitätsmanagements (SKM)
- Schlußfolgerungen und Ausblick
- Kritische Würdigung

Bedrohungslage

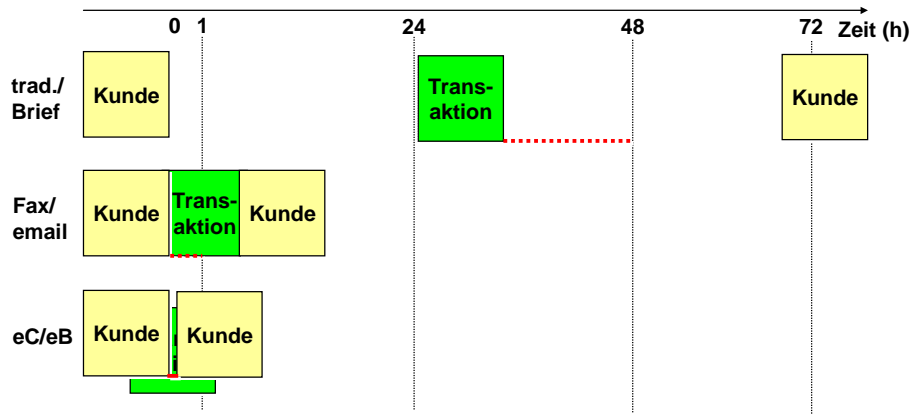
- Anzahl der Risiken für das Unternehmen vervielfacht sich
- Neuartige Bedrohungen schaffen einen veränderten Handlungsbedarf in elektronischen Geschäftsmodellen
- Optimierung der Abläufe, „Speed to Market“, „Just in Time“ führen zu einer höheren Anfälligkeit der Geschäftsprozesse
- Einzelereignisse haben weitreichende Kettenreaktionen zur Folge, die im Kontext der vernetzten Wirtschaft schwer überschaubar sind (vgl. Airlines und angeschlossene Industrien)
- Folgeschäden sind nicht transparent, aber immer häufiger bestandsgefährdend
- Beherrschbarkeit der Risiken sinkt mit zunehmendem Outsourcing

„e-Risiken“ ?



Just in Time und Zeitfenster

Risiken, Krisenanfälligkeit

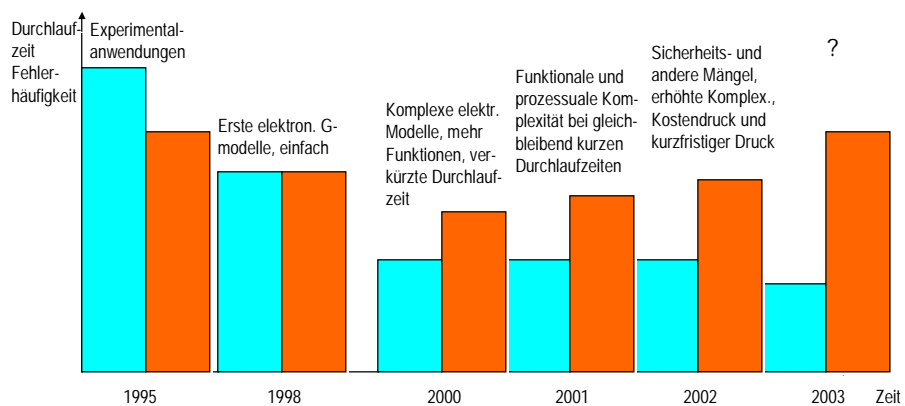


5

EUROPA TREUHAND ERNST & YOUNG

Speed to Market

Risiken, Krisenanfälligkeit

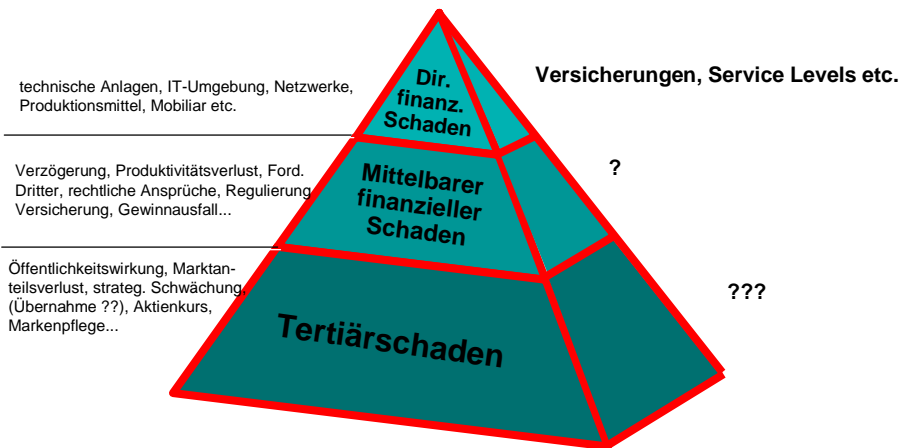


6

EUROPA TREUHAND ERNST & YOUNG

Typischer Schadensverlauf

Folgeschäden



7

EUROPA TREUHAND ERNST & YOUNG

Haftungsfragen

Folgeschäden

- Kritische Ereignisse führen immer häufiger zu Ansprüchen (Mitarbeiter, Dritte) an das Unternehmen
- Versicherungen handeln in jüngster Zeit restriktiv: nicht mehr alle Risiken sind versicherbar, Prämien sind teils prohibitiv teuer
- Haftung des Fachverantwortlichen ist beschränkt: Schaden kann durch „symbolische Pfändung“ selten abgewendet werden
- Mittelbar greift die Vorstands- / Geschäftsführerhaftung (AktG/GmbHG - kaufm. Sorgfalt, Pflicht zur Voraussicht, Pflicht zur Schadensabwendung), in Deutschland sogar mit Beweislastumkehr
- „Schuldhaftes Unterlassen geeigneter Absicherungsmaßnahmen...“ ? „...wider besseres Wissen“ (Vorsatz) ?? „... ohne sich rechtzeitig informiert zu haben“ (grobe Fahrlässigkeit) ???

8

EUROPA TREUHAND ERNST & YOUNG

Managementsicht

- Grundannahme der Unverwundbarkeit (invincibility hypothesis), oft personalisiert
- Reaktive Betrachtung, Absicherung zielt auf Einzelrisiken der Vergangenheit
- Sicherheit und Kontinuität werden bisweilen als Behinderung (Verlangsamung) des Kerngeschäfts betrachtet
- Verdrängung (denial), oft auf irrationale Argumentation gestützt
- „Bounded Rationality“ (nach Simon 1957)
- Kurzfristigkeit, Abwägung zwischen kurzfristigem Erfolgsdruck und langfristigem Risiko
- Seltener: kriminelle Energie („cutting corners“), ex post Abwehrstrategien, Projektion der Schadensursachen („blame game“)

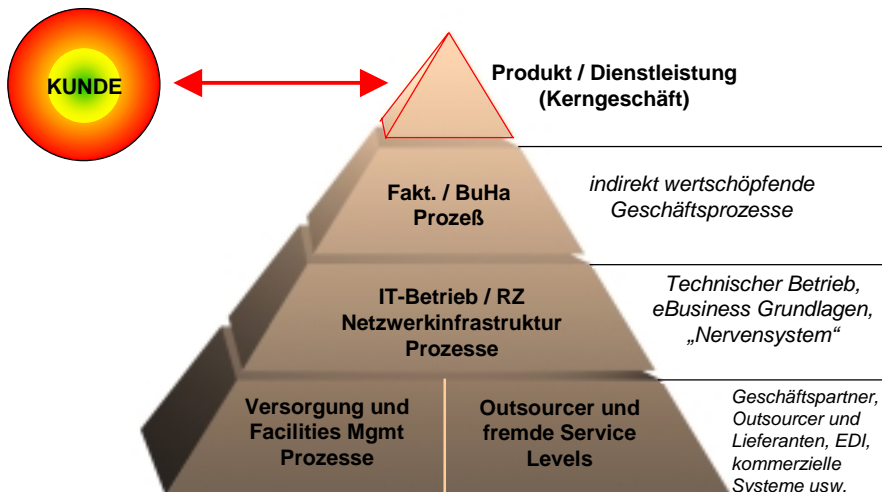
Managementsicht (2)

- Motiv 1: Zwang
 - Gesetzliche Änderungen
 - Verordnungen, Normen, Richtlinien
 - Weisungen der Aufsichtsbehörden od. d. Revision
- Motiv 2: „Me too“
 - Was machen die anderen ?
 - Gibt es „Vorlagen“ ?
 - Was kostet es, das Niveau der anderen zu erreichen ?
- Motiv 3: Anpassung
 - z. B. geplante Notierung in USA
 - Fusion, Übernahme
 - Umsetzung zentraler Konzernprojekte

Managementsicht (3)

- Desinformation
 - IT-Sicherheit = Hochverfügbarkeit
 - Notfallplanung = EDV-Thema
 - Business Continuity Planning = IT Disaster Recovery
 - Security = Risikomanagement
 - ...
- Organisatorische Fehleinschätzung
 - Krisenmanagement ist Nebenaufgabe des IT-Leiters
 - Risikomanagement in der Rechtsabteilung
 - „Minimalismus“ und fehlende Förderung durch das Management

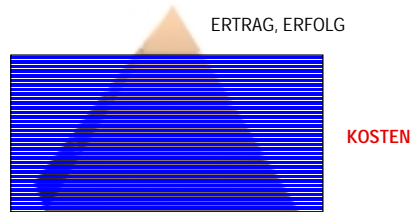
Was ist kritisch ??



Das Eisberg-Prinzip:

Einheitlicher Rahmen

Unabhängig von der Art des Geschäftsmodells...



... ist dem Kunden vieles nicht ersichtlich.

Sicherheit, Verfügbarkeit und andere Stichworte dienen in erster Linie der Lösung technischer Einzelprobleme. Kunde und Management sehen eher das Kerngeschäft und können nur schwer eine Verbindung herstellen.

13

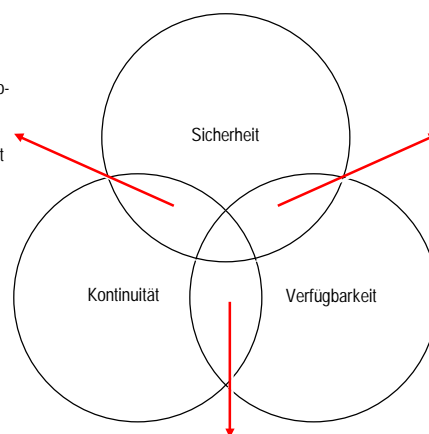
EUROPA TREUHAND  ERNST & YOUNG

Sicherheit, Verfügbarkeit, Kontinuität

Einheitlicher Rahmen

Sicherheit ist eine Risikoklasse, die es bei der Sicherstellung der organisatorischen Kontinuität zu berücksichtigen gilt.

Aber nicht die einzige.



Sicherheitsvorfälle können die Verfügbarkeit einiger Ressourcen gefährden.

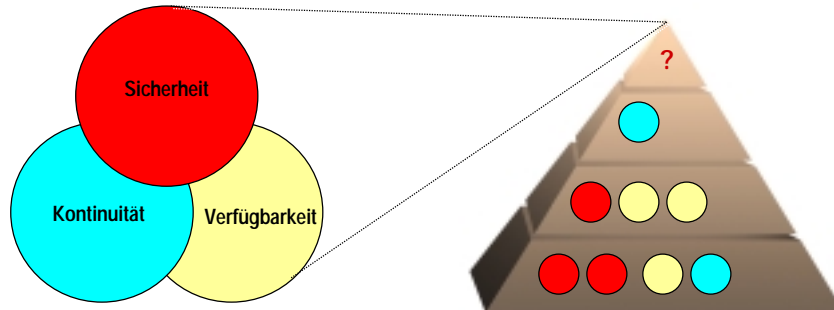
Es gibt aber auch andere Ursachen für Vorfälle.

Kontinuität setzt die Verfügbarkeit verschiedener Ressourcen voraus. Aber auch Managementtätigkeiten.

14

EUROPA TREUHAND  ERNST & YOUNG

Kostensicht vs. Erfolgssicht



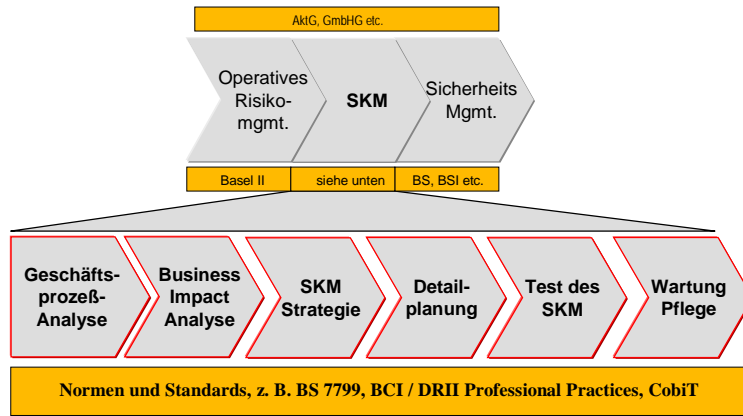
Es ist relativ leicht, einzelne Geschäftsprozesse den Kreisen zuzuordnen. Für das Kerngeschäft / die ertragswichtigen Bereiche fehlt jedoch ein Ansatz der Risikobegrenzung und der Sicherstellung der Kontinuität.

Strategisches Kontinuitätsmanagement (SKM)

- Konzentration auf das Kerngeschäft, nicht auf Technik
- Abtrennung technischer Einzeldisziplinen wie IT-Sicherheit, Hochverfügbarkeit und Neueinordnung im Hinblick auf Ertrag / Schaden
- Abkehr von der Kostensicht hin zur Betrachtung des Unternehmenserfolgs
- Grundlegende Schaffung einer Robustheit, Reduzierung der zunehmenden Anfälligkeit der Unternehmen
- Konzentration auf Fortführung der Geschäftstätigkeit im Krisenfall, Abkehr vom Konzept der vollständigen Prävention
- Einbeziehen der spezialisierteren Begriffe „IT-Sicherheit“ und „Verfügbarkeit“

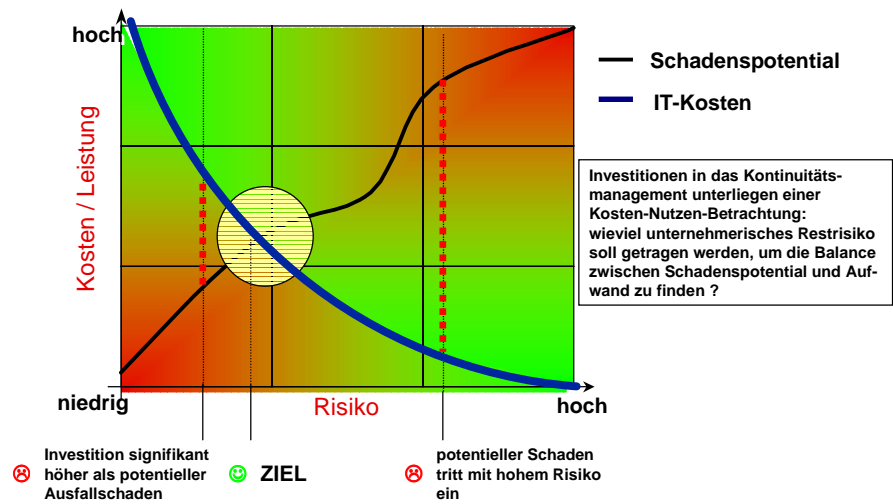
SKM-Ansatz schematisch

SKM-Ansatz



SKM-Ansatz schematisch (2)

SKM-Ansatz



SKM-Ansatz, Arbeitsgebiete (nach BCI)

- Projektmanagement
- Risikobewertung und -kontrolle
- Folgeschädenanalyse
- Strategische Optionen und Festlegungen
- Krisen- und Notfallmanagement
- Detailplanung
- Training und Bewußtseinsbildung
- Test und Wartung des Kontinuitätsprozesses
- Public Relations und Kommunikation
- Koordination mit Behörden und anderen öffentlichen Institutionen

Gesetze, Normen und Standards

- KonTraG 1998 – Frühwarn- und Früherkennungssystem
- Deutscher / österr. Corporate Governance Kodex
- Spezielle Anforderungen im Finanzsektor
- Basel II Dokumentation

- ISO 17799, BS 7799 (2002):2 (GB, international)
- NFPA 1600, HIPAA (USA)
- Fed / SEC Interagency Paper zur Kontinuität (Aug. 2002)
- FSA Working Papers zur Kontinuität (2002)

Schlußfolgerungen und Ausblick

- Herrschende Vorstellung von „IT-Sicherheitsmanagement“ besonders in elektronischen Geschäftsprozessen greift zu kurz
- Im Gegensatz zum dominanten Präventionsgedanken muß ein Kontinuitätsansatz den Eventualfall berücksichtigen (auch unerwartete Krisenereignisse sind nicht auszuschließen)
- IT-Sicherheit dient im Grunde der Robustheit des – insbesondere elektronischen – Geschäftsprozesses
- Konzentration auf das Kerngeschäft (ertragsrelevante, kritische Prozesse) und Abhängigkeiten im Prozeßmodell sind zu berücksichtigen
- SKM-Ansatz ist zwingend erforderlich, um technische Einzelprobleme mit den Erfordernissen des Kerngeschäfts in Beziehung zu setzen

Schlußfolgerungen und Ausblick

- Kulturell und historisch bedingt besteht ein Rückstand in den deutschsprachigen Ländern
- Gesetzes- und Vorschriftenlage richtet sich zunehmend am angelsächsischen (britischen) Modell aus
- Trennung zwischen IT-zentrierter Sicht und SKM-Sicht ist auch in elektronischen Geschäftsprozessen vollzogen
- Robustheit und geringere Anfälligkeit werden zu entscheidenden Erfolgsfaktoren im eBusiness
- Organisatorische Einordnung des Themas verlagert sich von IT-Leitung zur Geschäftsleitung

Kritische Würdigung

- Soziale und kulturelle Akzeptanz – Probleme in deutschsprachigen Ländern ?
- Konjunkturzyklen – SKM-Ansatz als Schönwetterveranstaltung ?
- Gesetzgebung – Perfektion als Idealvorstellung ?
- Bounded Rationality – was ist üblich, was ist notwendig ?
- Emotionsgehalt – gegen das planen, wovor man am meisten Angst hat ?
- Sonstige offene Punkte ?

Kontaktinformationen

Rolf v. Rössing CISA, CISSP, MBCI
Europa Treuhand Ernst & Young
Wagramer Straße 19
A-1220 Wien
+43-1-21170-1020
rolf.von-roessing@at.eyj.com