Wie viel darf IT-Sicherheit kosten?

IT-Sicherheit am Strand, 12. Juli 2007

Hannes Federrath, Thomas Nowey
Lehrstuhl Management der Informationssicherheit
Universität Regensburg

Zu hohe oder zu niedrige Ausgaben?

»…mangelnde Investition in IT-Sicherheit…«
BSI Lagebericht 2007

vs.

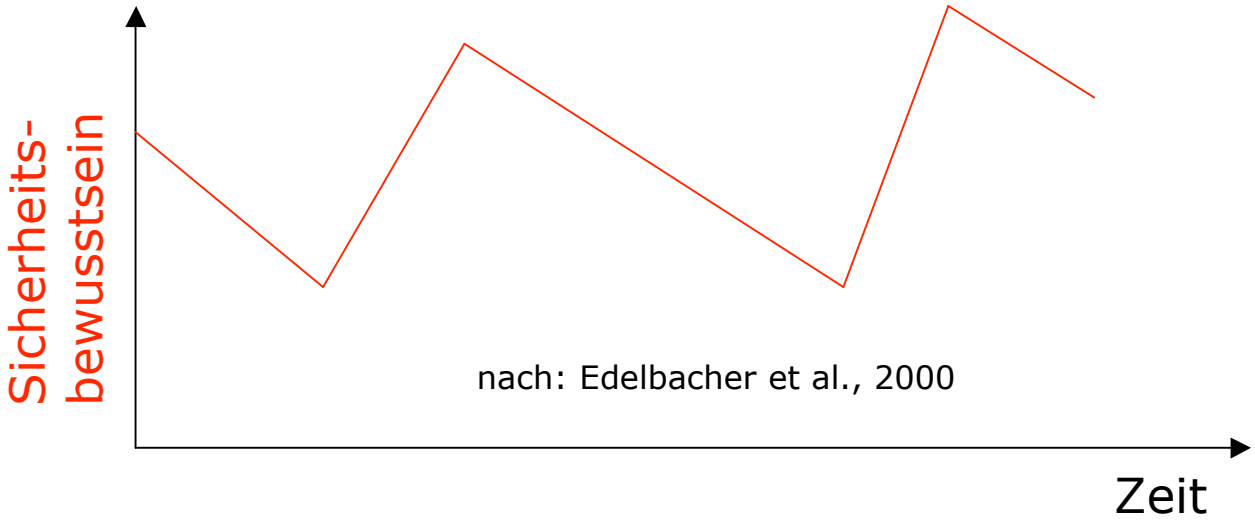
»The greatest IT risk facing most companies is more prosaic than a catastrophe. It is, simply, overspending.«
Nicolas G. Carr

- 2 Perspektiven
  - Sicherheit eines Produktes
  - Sicherheit eines Unternehmens → Fokus des Vortrags
- Ziel des Vortrags
  - Mögliche Antworten aus Wissenschaft und Praxis darstellen und kritisch hinterfragen
  - Aktuelle Forschungsansätze aufzeigen, Diskussion anregen

Erste einfache Antwort

Nichts (zusätzlich)

- Sicherheit ist eine Sekundärfunktion.
- »Kein System ist einfach nur sicher.«
- Sicherheit dient der Unterstützung und Erhaltung eines Primärziels.

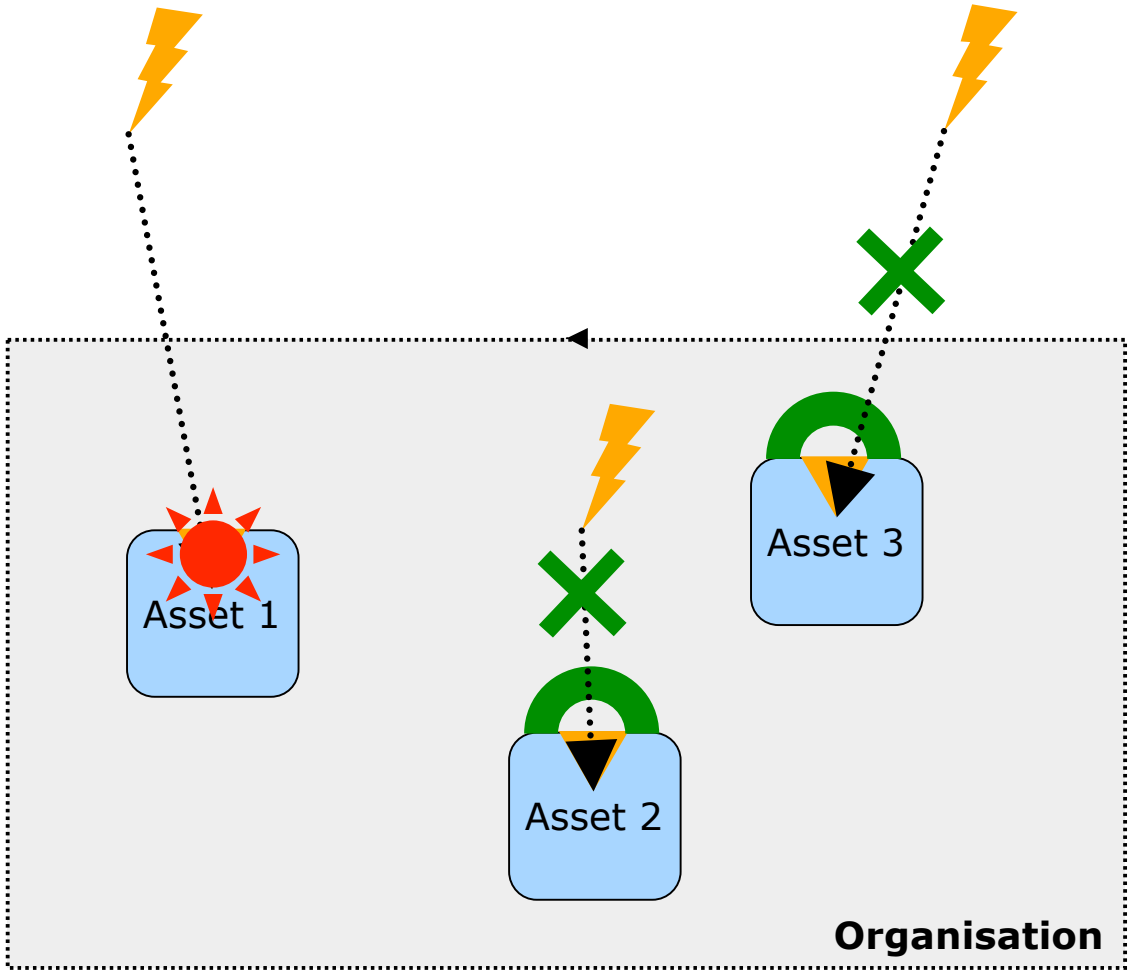


Warum braucht man IT-Sicherheit?

- IT-Sicherheitsmanagement versucht, die mit Hilfe von Informationstechnik (IT) realisierten Produktions- und Geschäftsprozesse in Unternehmen und Organisationen systematisch gegen beabsichtigte Angriffe (Security) und unbeabsichtigte Ereignisse (Safety) zu schützen.

- Motive
  - Assets/Vermögensgegenstände (materiell und immateriell) schützen
  - Schutzziele umsetzen (Vertraulichkeit, Verfügbarkeit, Integrität)
  - Externe Anforderungen erfüllen
  - Compliance erreichen
  - Individuellen Schaden/Haftung abwenden
  - Mehrwert generieren

Von der Bedrohung zum Sicherheitsvorfall



Bedrohungen, z.B.
- Viren, Würmer
- DoS
- Hacking
- Spionage
- Social Engineering

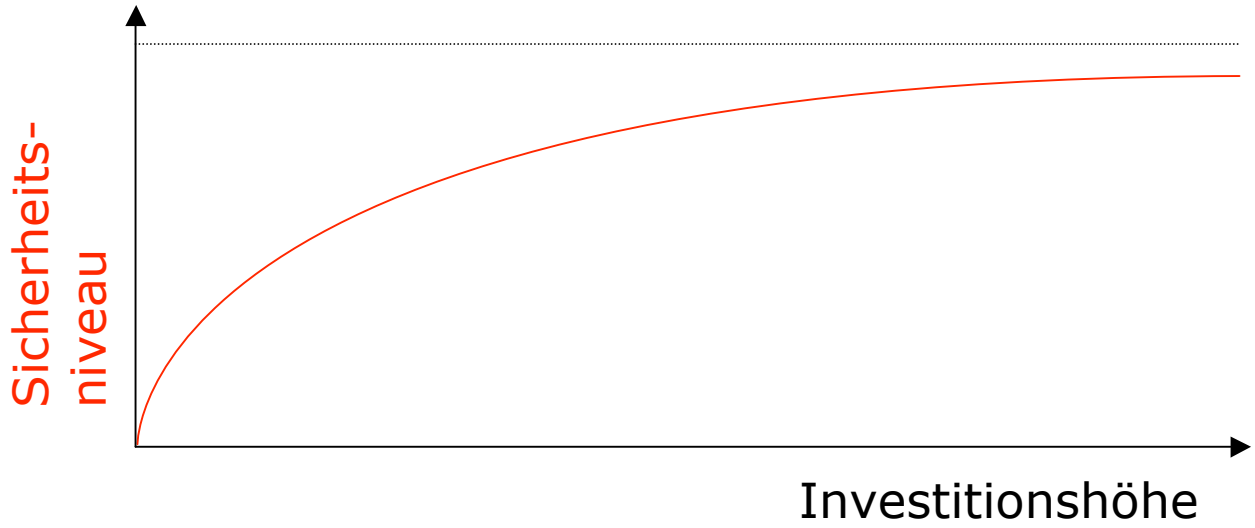
Schutzziele
- Vertraulichkeit
- Verfügbarkeit
- Integrität

Maßnahmen
- Präventiv
- Detektiv
- Reaktiv

Zweite einfache Antwort

So viel wie man braucht, um total sicher zu sein

- Kritik:
  - 100 %-ige Sicherheit ist nicht erreichbar



Dritte einfache Antwort

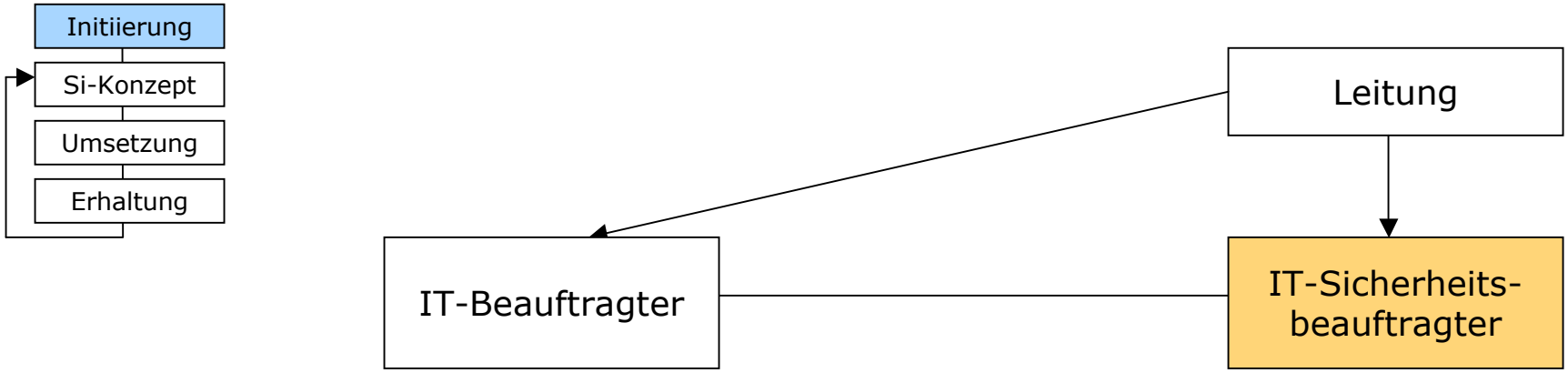
So viel wie das Budget hergibt

- Kritik
  - Budget nicht rational begründbar
- Anschlussfrage:
  - Wie groß muss das Budget gewählt werden?

Unterschiedliche Zielsetzungen

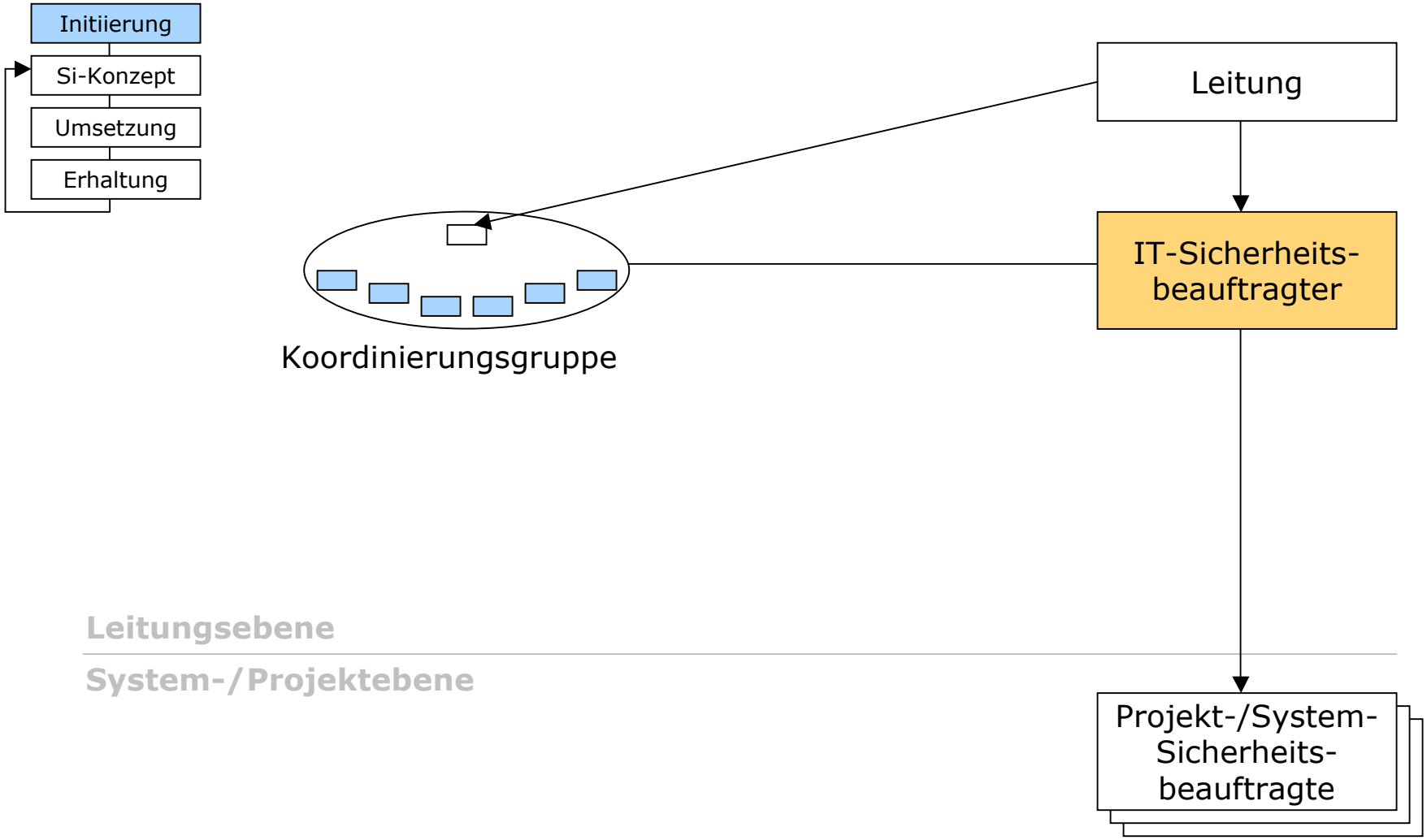
- Ziel Unternehmensleitung
  - Ausgaben gering halten
  - Kosten einsparen
  - Nur Projekte mit sichtbarem Nutzen realisieren
- Ziel Sicherheitsverantwortliche
  - Möglichst hohes Sicherheitsniveau schaffen
  - Budget erhöhen
- Was können Sie tun um Ihr Budget zu erhöhen?
  - Schüren Sie Angst!
  - Sammeln und drucken Sie Log-Files.
  - Verwenden Sie Abkürzungen und Fachbegriffe.
  - Zitieren Sie Studien von Sicherheitsfirmen und Beratungsunternehmen.

Organisationsstruktur für IT-Sicherheit: *Kleine Organisationen*



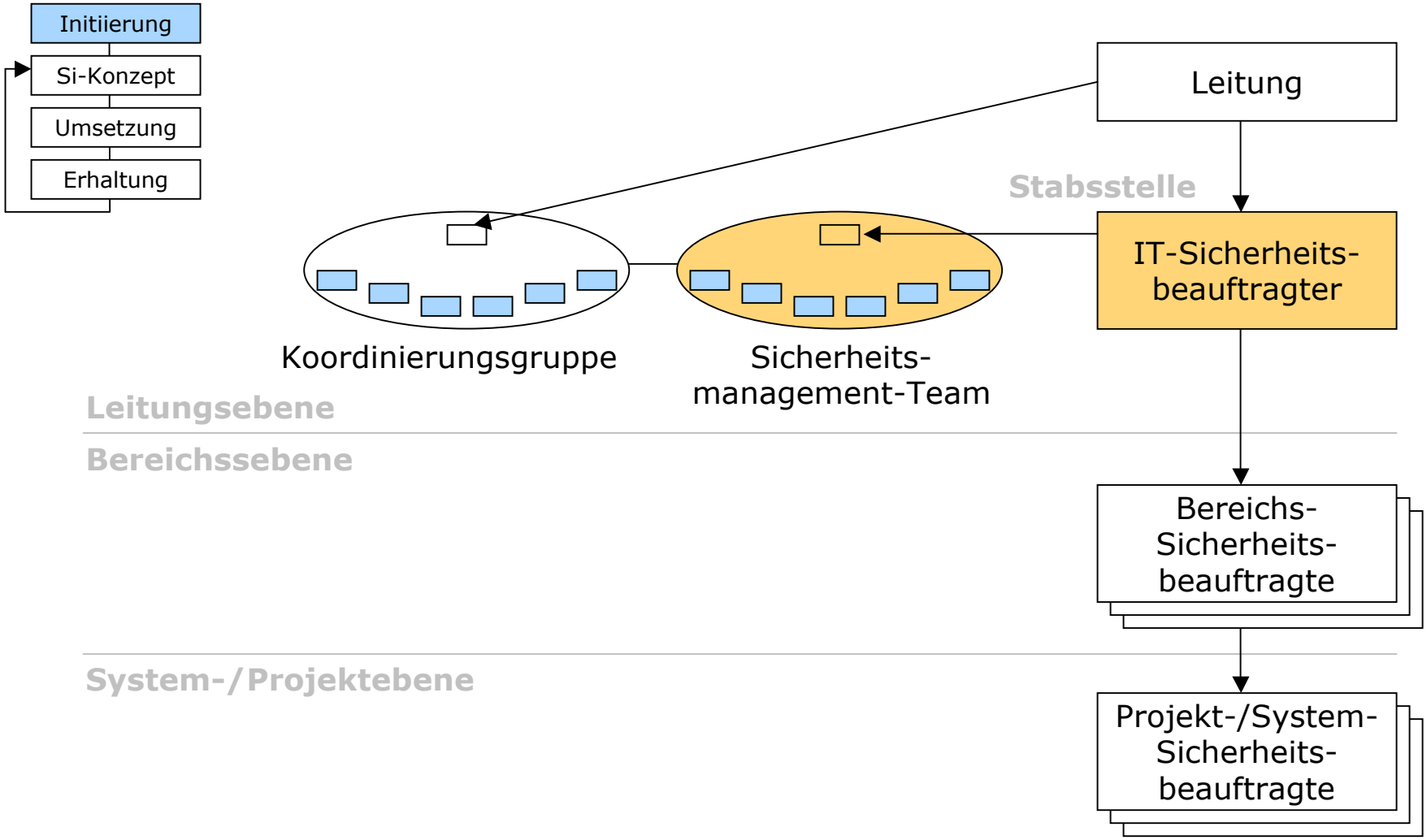
nach: GSHB, M2.193

Organisationsstruktur für IT-Sicherheit: *Mittlere Organisationen*



nach: GSHB, M2.193

Organisationsstruktur für IT-Sicherheit: *Große Organisationen*

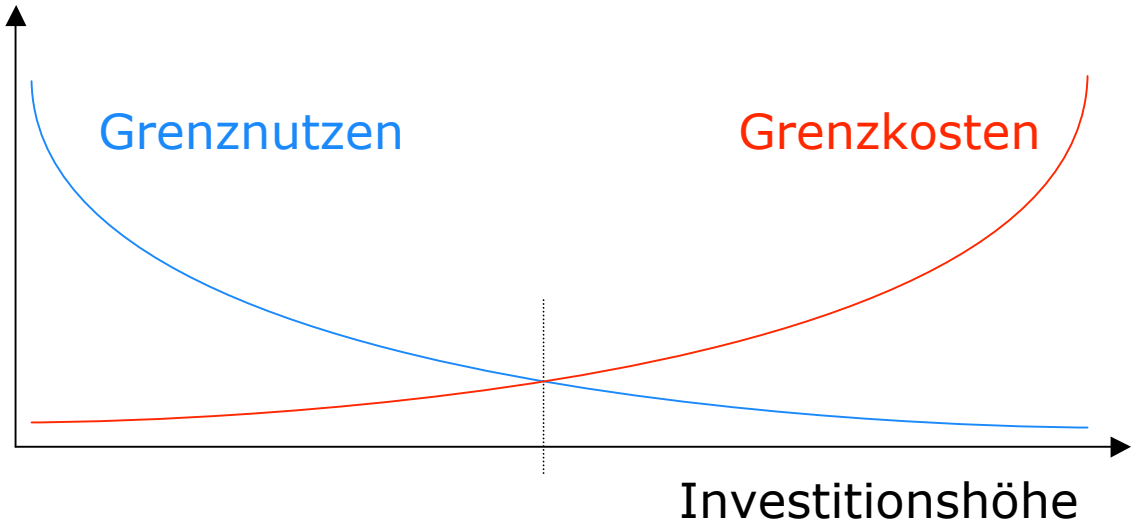


nach: GSHB, M2.193

Vierte einfache Antwort

So viel wie im Schnittpunkt von Grenzkosten und Grenznutzen an der Abszisse abzulesen ist.

- Kritik
  - Viel hilft nicht unbedingt viel, es kommt auch darauf an, wie das Geld ausgegeben wird



Vierte einfache Antwort

So viel wie im Schnittpunkt von Grenzkosten und Grenznutzen an der Abszisse abzulesen ist.

- Kritik
  - Viel hilft nicht unbedingt viel, es kommt auch darauf an, wie das Geld ausgegeben wird

- Effektivität
  - = die richtigen Maßnahmen ergreifen
  - Weniger ist manchmal mehr.
- Probleme
  - Funktionen sind schwierig zu ermitteln
  - Funktionen sind nicht stetig, häufig sind Sicherheitsmaßnahmen binäre Entscheidungen

Fünfte einfache Antwort (1)

Es sollten alle Maßnahmen realisiert werden,
die einen positiven Return on Security Investment aufweisen

- ROSI
  - basiert auf dem ALE-Konzept aus den 70er Jahren
  - soll Analogie zum klassischen Return on Investment herstellen
  - verschiedene Darstellungsformen und Weiterentwicklungen

$$ALE_i = SLE_i \cdot ARO_i$$

$$ROSI_k = ALE_0 - ALE_k - Cost_k$$

$$ROSI_k = \frac{(RiskExposure_k \cdot \%RiskMitigated_k) - Cost_k}{Cost_k}$$

nach: Soo Hoo, 2000; Sonnenreich, 2006

Fünfte einfache Antwort (2)

- Kritik
  - Kosten und Nutzen schwer ermittelbar → Unterschiede zu klassischen Investitionsprojekten
  - Es geht nicht nur um operative Entscheidungen: Sicherheitsmanagement beginnt auf der strategischen Ebene
  - ROSI häufig kritisiert

- Worin liegt der Nutzen?
  - Erfüllung gesetzlicher Anforderungen, Generierung zusätzlicher Einnahmen, Effizienzgewinne, Reduktion von Risiken

- Wie setzen sich die Kosten zusammen?
  - Ausgaben für Anschaffung, Einführung, laufenden Betrieb, Kosten durch Änderung betriebl. Abläufe

➔ Risikomanagement-Ansatz auf operativer Ebene erforderlich

Sicherheitsmanagement beginnt auf der Strategieebene

	Business Engineering	Sicherheitsmanagement
Strategieebene/ Sicherheitspolitik	Festlegung der Unternehmens-aufgaben; Strategische Planung	Definition strategischer Ziele, Grundsätze und Richtlinien; Formulierung der Unterneh-mensziele aus Sicherheitssicht
Prozessebene/ Sicherheitskonzept	Gestaltung der Abläufe in Form von Prozessen	Übersetzung der Politik in Maßnahmen; Risikoanalyse
Systemebene/ Mechanismen	Unterstützung der Prozesse durch den Einsatz von Systemen; Analyse und Spezifikation der Anwendungssysteme	Detaillierung der Maßnahmen durch konkrete Mechanismen

Sicherheitsmanagement beginnt auf der Strategieebene

- Aussagen für die strategische Ebene
  - Wer nur auf vorgefertigte Lösungen setzt, verliert auf lange Sicht wertvolles Know How
  - Heterogene IT-Landschaften schützen vor Kumulrisiken
  - IT-Sicherheit ist mehr als nur Technik
  - Sicherheit sollte von Beginn an integraler Bestandteil der Prozesse werden und nicht hinterher hinzugebastelt werden
  - Die Sicherheit sollte im Einklang mit anderen Disziplinen entwickelt werden, z.B. Synergien mit dem Business Engineering nutzen

Operative Ebene – Betrachtung im Risikomanagement Kreislauf

Checklisten
Workshops
Experten
Histor. Daten

Identifikation

Basisansatz
Kategorien
Quantitative
Verfahren

Bewertung

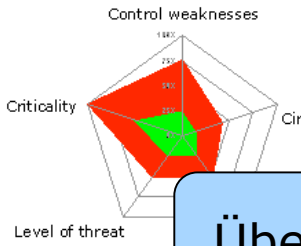
Best Practice
Scoring
Quant.
Verfahren

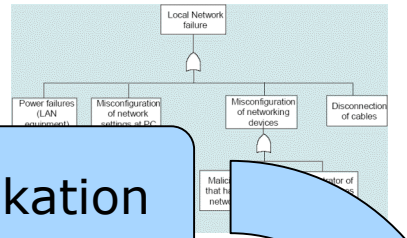
Steuerung

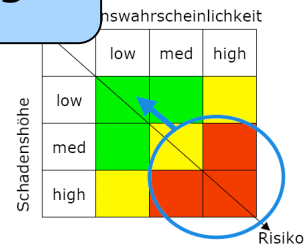
Checklisten
Scorecards
Kennzahlen

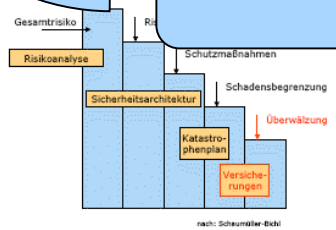
Überwachung

Risiko =
Eintrittswahrscheinlichkeit
X
Schadenshöhe



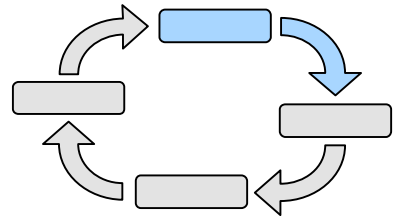




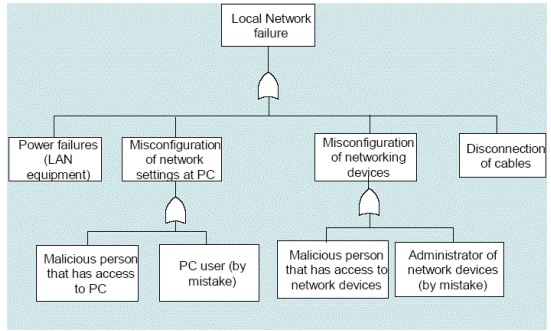


Identifikation von Bedrohungen

- Frage
  - »Welche Bedrohungen gibt es?«



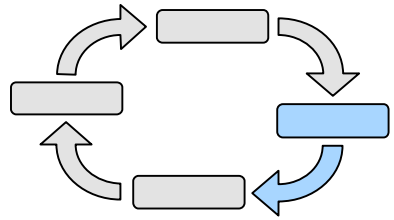
- Methoden & Werkzeuge
  - OCTAVE-Methodik, CORAS-Framework
  - Checklisten
  - Workshops
  - Fehlerbäume, Attack-Trees
  - Szenarioanalysen



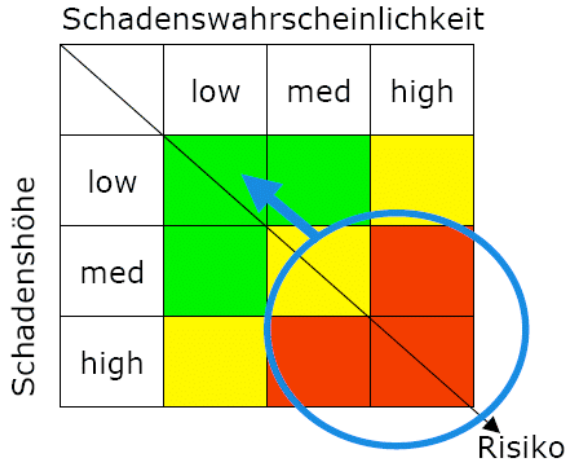
- Herausforderungen
  - Vollständige Erfassung aller Bedrohungen

Bewertung von Risiken

- Frage
  - »Wie groß sind Eintrittswahrscheinlichkeit und Schadenshöhe eines potentiellen Schadensereignisses?«



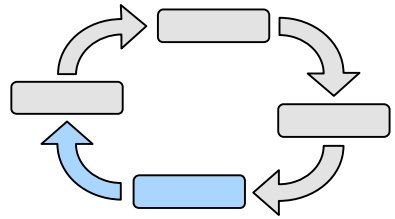
- Methoden & Werkzeuge
  - Qualitative Bewertung
  - Quantitative Bewertung
  - Spieltheorie
  - Maximalwirkungsanalyse



- Herausforderungen
  - Abhängigkeit von den zu Grunde liegenden Assets
  - Strategische Angreifer
  - Korrelationen zwischen Bedrohungen
  - Quantifizierbarkeit

Steuerung der Risiken

- Frage
  - »Welche Risiken sollen wie behandelt werden?«



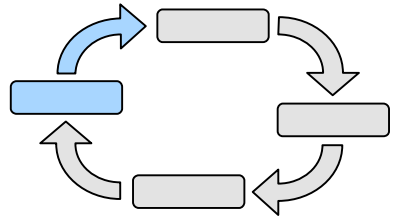
- Methoden
  - Best Practice Ansätze / Grundschutz
  - Hilfsmittel aus der Investitionsrechnung und Entscheidungstheorie, z.B. NPV, IRR, AHP

- Herausforderungen
  - Qualität der Entscheidung hängt von zu Grunde liegenden Daten ab (baut auf dem Bewertungsschritt auf)

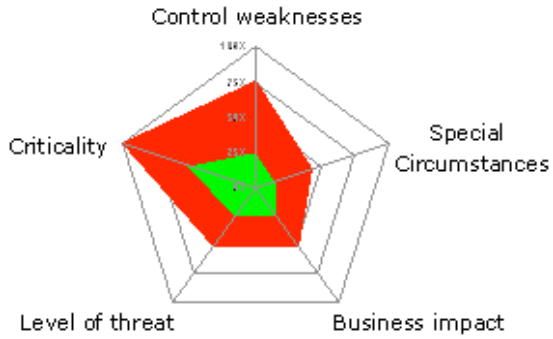
$$NPV_0 = -I_0 + \sum_{t=1}^{T} \frac{\Delta E(L_t) + \Delta OCC_t - C_t}{(1 + i_{calc})^t}$$

nach: Faisst et al., 2007

Überwachung der Risiken und Maßnahmen



- Frage
  - »Waren die Maßnahmen effektiv und effizient? Wie sicher ist die Organisation?«
- Methoden
  - Kennzahlen Systeme (z.B. TÜV Secure IT)
  - Security Scorecard oder Integration in Balanced Scorecard
- Herausforderungen
  - Die „richtigen" Kennzahlen verwenden
  - Kennzahlen „richtig" ermitteln/messen
  - Kennzahlen aktuell halten

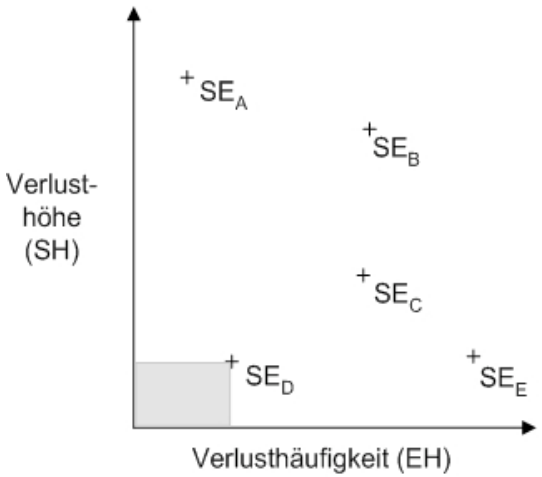


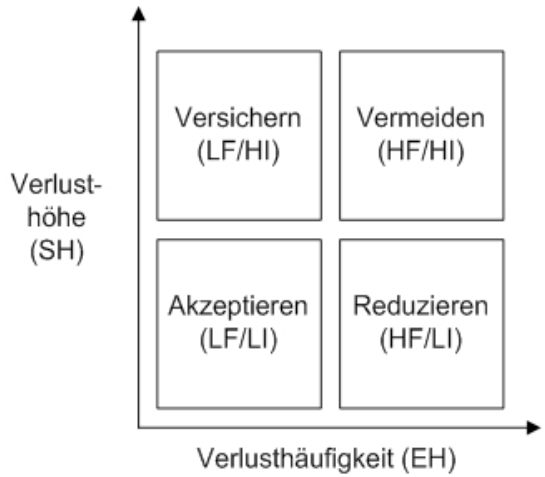
nach: Loomans, 2002

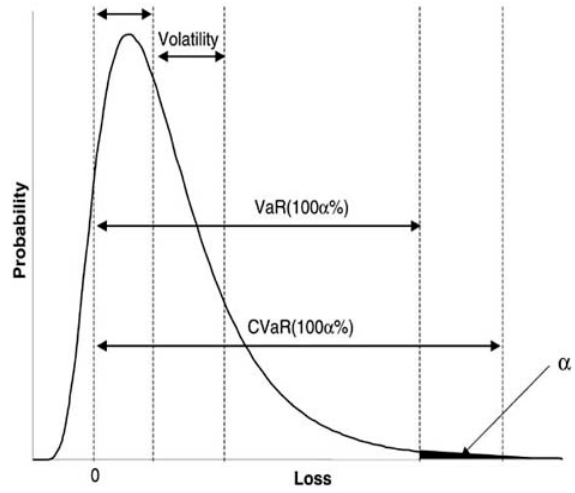
Quantitative Daten werden als Basis benötigt

- Daten zur Charakterisierung von Risiken
  - Eintrittswahrscheinlichkeit
  - Schadenshöhe
  - Verteilungsfunktion

- Anforderungen an Datenquellen
  - Hohe Datenqualität und Aktualität
  - Vollständigkeit und Organisationsbezogenheit
  - Einfachheit







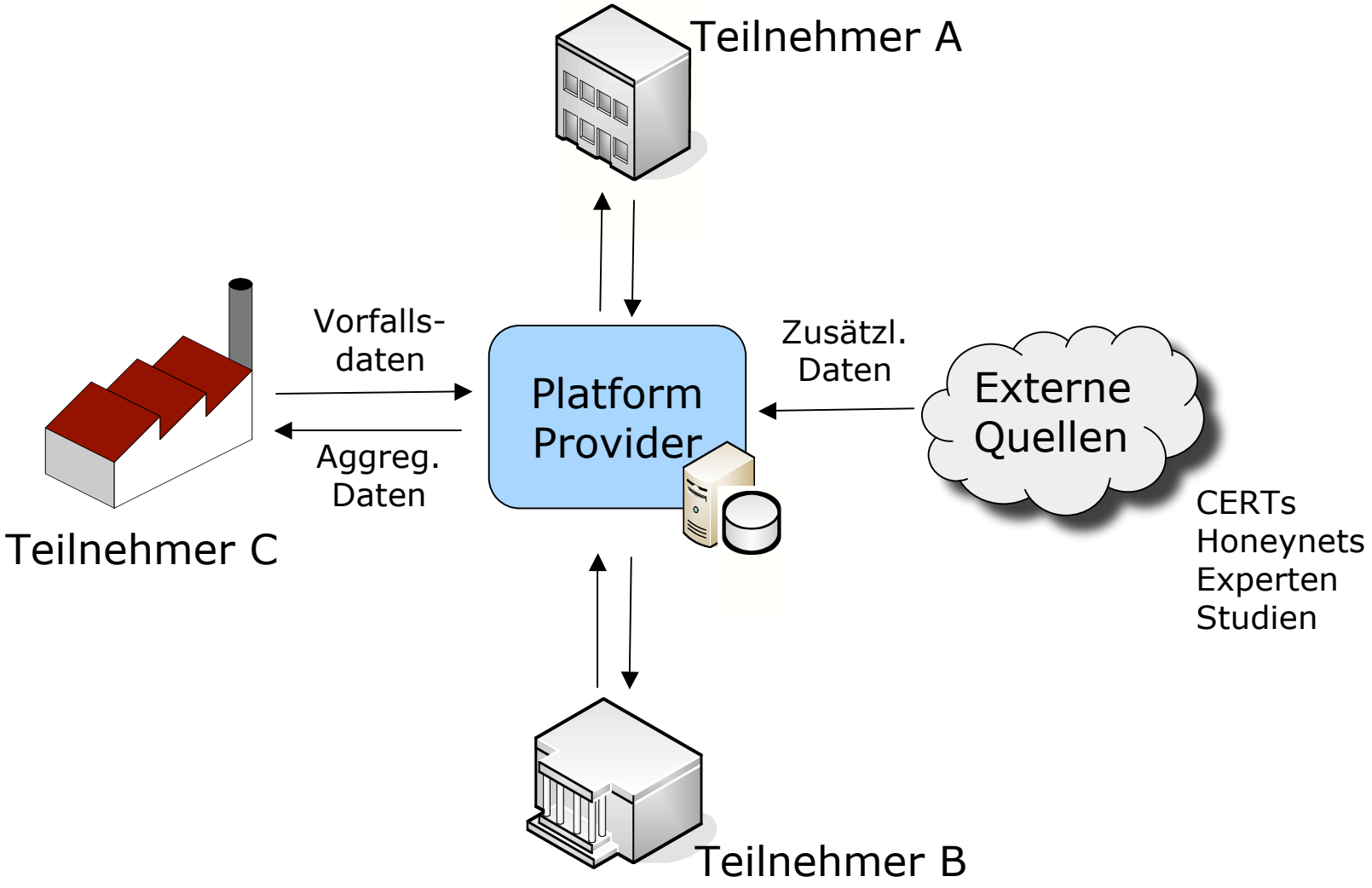
Mögliche Quellen für quantitative Daten

Quelle	Beispiel	Bewertung
Expertenurteile	Interviews mit internen oder externen Experten CSI/FBI Survey	Häufig verwendet, aber nicht messbar Subjektiv, unvollständig
Simulationen	Historische oder Monte Carlo Simulationen	Noch kaum verbreitet Gut, wenn Ausgangs-daten vorhanden
Marktmechanismen	Kapitalmarktanalysen Bug Challenges Derivative Produkte	Nicht für alle Bereiche anwendbar Noch nicht verfügbar
Historische Daten	CERTs/CSIRTs Interne Vorfallsbearbeitungs-systeme	In anderen Bereichen weit verbreitet Prognosequalität? Kaum verfügbar

Idee: Sammlung und Austausch historischer Daten

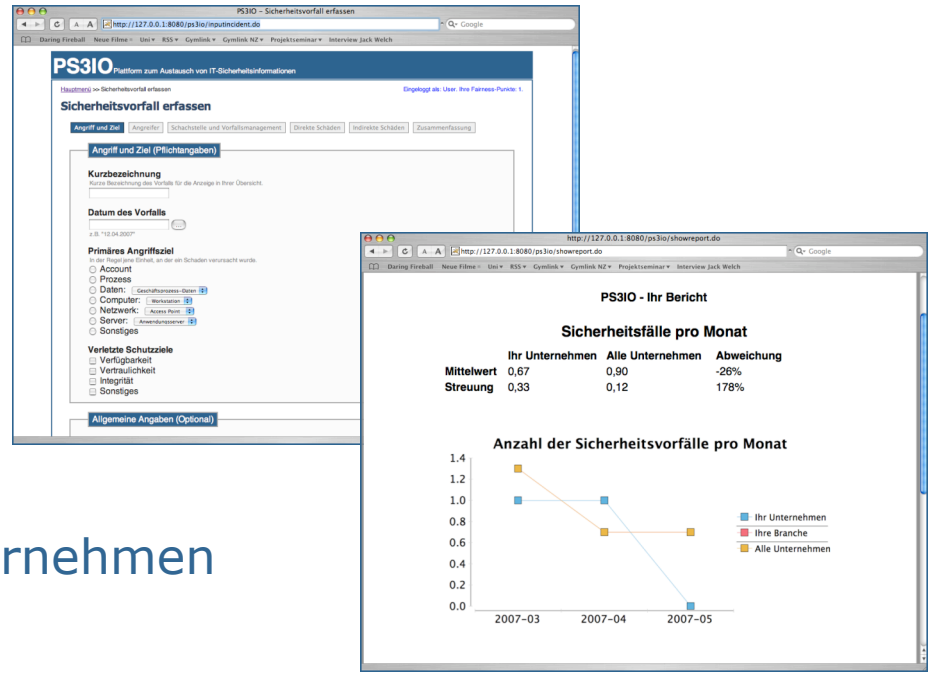
- Idee
  - Entwurf eines Systems zur Sammlung von quantitativen historischen Daten über Sicherheitsvorfälle in Organisationen.
- Ziel
  - Aufbau einer Datenbasis die Informationen über Schadenshöhe, Eintrittswahrscheinlichkeit und Wahrscheinlichkeitsverteilungen von Sicherheitsvorfällen in verschiedenen Organisationen gibt.
- Verschiedene Möglichkeiten zur Verwendung der generierten Daten
  - Risikobewertung, Evaluation von Investitionsentscheidungen
  - Benchmarking zwischen Organisationen
  - Untersuchung Korrelationen zwischen Schadensereignissen
  - Wissenstransfer von Organisation zu Organisation

Basisarchitektur



Implementierung/Umsetzung

- Prototyp als J2EE Webanwendung
  - Erfassung von Vorfällen
  - Erste Auswertungsmöglichkeiten
  - Benutzerverwaltung



- Nächste Schritte
  - Datenanalyse
  - Externe Daten
  - Fairness-Mechanismen
  - Testphase

- Wir suchen interessierte Unternehmen
  - Evaluation des Prototypen
  - Teilnahme am Testbetrieb

http://www-sec.uni-regensburg.de/research/#secmgmt

Fazit

- Die Frage wie viel IT-Sicherheit kosten darf ist nicht mit Pauschalantworten zu lösen
- Praxis und Forschung stellen zahlreiche Methoden bereit, die bei sinnvoller Kombination bei der Lösung der Frage helfen können
- Weniger ist manchmal mehr
- Sicherheit ist mehr als nur Technik
- Sicherheit beginnt auf der Ebene der Strategie
- Für die Risikoanalyse werden quantitative Daten benötigt
- Informationsaustausch kann allen helfen

Kontakt

- Lehrstuhl Management der Informationssicherheit
  Universität Regensburg
  - Prof. Dr. Hannes Federrath
    Tel. 0941 943-2870
    hannes.federrath@wiwi.uni-regensburg.de
  - Dipl.-Wirtsch.-Inf. Thomas Nowey
    Tel. 0941 943-2865
    thomas.nowey@wiwi.uni-regensburg.de

http://www-sec.uni-regensburg.de